kaspersky

# Kaspersky SD-WAN

© 2026 AO Kaspersky Lab

# Contenido


Ayuda de Kaspersky SD-WAN

Acerca de Kaspersky SD-WAN

- Kit de distribución
- Requisitos de hardware y software
- Garantizar la seguridad

Novedades

Arquitectura de la solución

Implementar Kaspersky SD-WAN

- Redundancia de los componentes de la solución
- Configurar el equilibrio de carga entre las instancias del orquestador
- Acerca del archivo de instalación
- Acerca de los modos de acción atendido, desatendido y parcialmente atendido
- Preparar el dispositivo administrador
- Administrar contraseñas
  - Generar contraseñas manualmente
  - Cambiar contraseñas
- Preparar el archivo de configuración
- Reemplazar los gráficos de la interfaz web del orquestador
- Reemplazar un nodo de controlador fallido
- Actualizar Kaspersky SD-WAN
- Eliminar Kaspersky SD-WAN

Iniciar y cerrar sesión en la interfaz web del orquestador

Licencias de Kaspersky SD-WAN

- Acerca del Contrato de licencia de usuario final
- Acerca del suministro de datos

Interfaz de usuario de la solución

- Configurar y restablecer la página predeterminada
- Alternar entre los modos claro y oscuro de la interfaz web del orquestador
- Cambiar el idioma de la interfaz web del orquestador
- Administrar tablas de componentes de la solución

Navegación a la API de orquestador

Administrar la infraestructura de Kaspersky SD-WAN

- Administrar dominios
  - Crear un dominio
  - Editar un dominio
  - Eliminar un dominio
- Administrar centros de datos
  - Agregar un centro de datos
  - Editar un centro de datos
  - Migrar un centro de datos a un dominio diferente
  - Eliminar un centro de datos

- Administrar subredes de administración
  - Crear una subred de administración
  - Edición de una subred de administración
  - Eliminar una subred de administración
- Administrar controladores
  - Editar un controlador
  - Reaprovisionar un controlador
  - Restaurar la configuración del controlador
  - Habilitar o deshabilitar el modo de mantenimiento en un controlador
  - Eliminar un controlador
  - Administración de las propiedades del controlador
    - Descripción de las propiedades editables del controlador
    - Editar una propiedad del controlador
    - Eliminar valores planificados de las propiedades del controlador
    - Restablecer las propiedades del controlador a los valores predeterminados
  - Ver información acerca de los nodos del controlador
- Administrar un VIM
  - Configurar un VIM implementado en un centro de datos
  - Configurar un VIM implementado en un dispositivo uCPE
  - Editar un VIM implementado en un centro de datos
  - Ver los recursos informáticos que utiliza un VIM
  - Eliminar un VIM

Administrar usuarios y sus permisos de acceso

- Administrar permisos de acceso
  - Crear permisos de acceso
  - Editar permisos de acceso
  - Clonar permisos de acceso
  - Eliminación de un permiso de acceso
- Administrar conexiones de LDAP
  - Crear una conexión de LDAP
  - Editar una conexión de LDAP
  - Cambiar la contraseña de una conexión LDAP
  - Eliminar una conexión de LDAP
- Administrar usuarios
  - Crear un usuario
  - Activar o bloquear un usuario
  - Editar un usuario
  - Cambiar la contraseña de un usuario local
  - Autenticación de dos factores repetida de un usuario
  - Eliminar un usuario
- Administrar grupos de usuarios de LDAP
  - Crear un grupo de usuarios LDAP
  - Editar un grupo de usuarios de LDAP
  - Eliminar un grupo de usuarios de LDAP
- Habilitar o deshabilitar la autenticación de dos factores para todos los usuarios
- Administrar solicitudes de confirmación
- Administrar las sesiones de usuario

Tenencia múltiple
Escenario: implementación de una instancia SD-WAN para un inquilino
Administrar inquilinos
Crear un inquilino
Agregar un usuario a un inquilino
Asignar un grupo de usuarios LDAP a un inquilino
Asignar recursos informáticos a un inquilino
Asignación de componentes de servicio de red a un inquilino
Asignar un VIM a un inquilino
Iniciar sesión en el portal de autoservicio de inquilinos
Editar un inquilino
Eliminar un inquilino
Administrar plantillas de instancia SD-WAN
Crear una plantilla de instancia SD-WAN
Configurar la plantilla de instancia SD-WAN predeterminada
Seleccionar el número de nodos de controlador para una instancia de SD-WAN
Agregar un inquilino a una plantilla de instancia SD-WAN
Eliminar un inquilino de una plantilla de instancia SD-WAN
Eliminar una plantilla de instancia SD-WAN
Administrar instancias SD-WAN
Configurar nodos de controlador de una instancia SD-WAN
Ver el uso de una instancia SD-WAN
Ver la topología de una instancia SD-WAN
Agregar un inquilino a una instancia de SD-WAN
Eliminar un inquilino de una instancia SD-WAN
Eliminar una instancia de SD-WAN
Administrar agrupaciones de instancias SD-WAN
Crear un grupo de instancias SD-WAN
Agregar una instancia SD-WAN a una agrupación de instancias SD WAN
Eliminar una instancia SD-WAN de una agrupación de instancias SD-WAN
Eliminar una agrupación de instancias SD-WAN
Administrar dispositivos CPE
Acerca de la interacción del dispositivo CPE y el orquestador
Acerca de la interacción del dispositivo CPE y el controlador
Credenciales predeterminadas de dispositivos CPE de KESR
Comprobación de integridad
Registrar dispositivos CPE
Escenario: registro automático de un dispositivo CPE con la tecnología de aprovisionamiento sin intervención.
Escenario: implementación de un dispositivo vCPE en la plataforma de virtualización de VMware y registro del mismo con la tecnología de aprovisionamiento Zero Touch
Escenario: volver a registrar un dispositivo CPE
Reanudar el registro del dispositivo CPE en caso de error
Administrar plantillas de CPE
Crear una plantilla de CPE
Importar una plantilla de CPE
Clonación de una plantilla de CPE

- Exportar la configuración de conexión del orquestador y del controlador y las interfaces SD-WAN desde una plantilla de CPE
- Exportar interfaces de red desde una plantilla de CPE
- Ver el uso de una plantilla de CPE
- Eliminar una plantilla de CPE

Administrar dispositivos CPE

- Agregar dispositivos CPE
- Importación masiva de dispositivos CPE desde un archivo CSV
- Generar una URL con la configuración básica del dispositivo CPE
- Registro manual de un dispositivo CPE
- Anular el registro de un dispositivo CPE
- Especificar la dirección de un dispositivo CPE
- Habilitar y deshabilitar un dispositivo CPE
- Reiniciar un dispositivo CPE
- Apagar un dispositivo CPE
- Conectarse a la consola del dispositivo CPE
- Visualizar la contraseña de un dispositivo CPE
- Exportar la configuración de conexión del orquestador y del controlador y las interfaces SD-WAN desde un dispositivo CPE
- Exportar interfaces de red desde un dispositivo CPE
- Cambiar el DPID de un dispositivo CPE
- Editar la configuración del dispositivo CPE
- Eliminar dispositivos CPE

Autenticación de dos factores de un dispositivo CPE

Administrar certificados

- Cargar un certificado mediante la interfaz web del orquestador
- Instalar certificados manualmente en dispositivos CPE
- Escenario: instalación de certificados en un dispositivo CPE con la versión de firmware 23.07
- Exportar un certificado
- Eliminar certificados

Administrar directorios de APN

- Crear un directorio de APN

Ver y restablecer sesiones en dispositivos CPE

Eliminar y deshabilitar automáticamente los dispositivos CPE

Agrupar dispositivos CPE mediante etiquetas

- Asignar una etiqueta a dispositivos CPE
- Eliminar una etiqueta de dispositivos CPE

Configurar registros en dispositivos CPE

Administrar módems

Actualizar el firmware

- Actualizar manualmente el firmware en un dispositivo CPE
- Cargar el firmware a la interfaz web del orquestador
- Programar actualizaciones de firmware en dispositivos CPE seleccionados
- Programar actualizaciones de firmware en dispositivos CPE con etiquetas específicas
- Restaurar el firmware de un dispositivo CPE KESR-M1
- Restaurar el firmware de un dispositivo CPE KESR-M2-5

- Correspondencia de modelos de dispositivos CPE con versiones de firmware
- Eliminar firmware

Configuración adicional de dispositivos CPE mediante scripts

- Agregar un script a dispositivos CPE
- Ejecutar un script en dispositivos CPE manualmente
- Programar scripts en dispositivos CPE
- Editar un script en dispositivos CPE
- Eliminar un script en dispositivos CPE

Administrar la configuración de DNS en dispositivos CPE

- Habilitar DNS en interfaces de red
- Administrar el reenvío de DNS condicional
  - Crear reglas de reenvío condicional
  - Editar reglas de reenvío condicional
  - Eliminar reglas de reenvío condicional

Configurar la conexión de un dispositivo CPE al orquestador y al controlador

Administrar la configuración de conexión del dispositivo CPE mediante la consola del sistema

Administrar interfaces de red

- Crear interfaces de red
  - Crear una interfaz de red con asignación automática de una dirección IP mediante DHCP
  - Crear una interfaz de red con una dirección IPv4 estática
  - Crear una interfaz de red con una dirección IPv6 estática
  - Crear una interfaz de red para conectarse a una red LTE
  - Crear una interfaz de red para conectarse a un servidor PPPoE
  - Crear una interfaz de red sin dirección IP
- Editar una interfaz de red
- Deshabilitar o habilitar una interfaz de red
- Cancelar la aplicación de la configuración de la interfaz de red a un dispositivo CPE
- Eliminación de una interfaz de red
- Protección contra la suplantación de IP mediante uRPF

Administrar interfaces de SD-WAN

- Acerca del envío de información sobre interfaces SD-WAN del tipo WAN al controlador
- Fragmentación de paquetes
- Colas de tráfico en interfaces de SD-WAN
- Crear una interfaz SD-WAN del tipo WAN
- Editar una interfaz SD-WAN
- Deshabilitar o habilitar una interfaz SD-WAN
- Eliminación de una interfaz SD-WAN de tipo WAN

Administrar interfaces de servicio

- Crear una interfaz de servicio
- Crear una interfaz de ACL
- Ver el uso de una interfaz de servicio y una interfaz de ACL
- Eliminar una interfaz de servicio o una interfaz de ACL

Administrar grupos de puertos OpenFlow

- Crear un grupo de puertos OpenFlow
- Editar un grupo de puertos OpenFlow
- Eliminar un grupo de puertos OpenFlow

Configurar una UNI para la conexión de dispositivos CPE a los servicios de red
- Administrar plantillas de UNI
  - Crear una plantilla de UNI
  - Eliminar una plantilla de UNI
- Administrar las UNI
  - Crear una UNI
  - Ver el uso de la UNI
  - Editar una UNI
  - Eliminar una UNI

Agregar una ruta estática
- Tabla de correspondencia de distancias administrativas y protocolos de enrutamiento

Filtrar rutas y paquetes de tráfico
- Administrar listas de control de acceso (ACL)
  - Creación de una lista de control de acceso
  - Editar una lista de control de acceso
  - Eliminación de una lista de control de acceso
- Administrar listas de prefijos
  - Crear una lista de prefijos
  - Editar una lista de prefijos
  - Eliminar una lista de prefijos
- Administrar listas de comunidades
  - Crear una lista de comunidades
  - Editar una lista de comunidades
  - Eliminar una lista de comunidades
- Administrar mapas de ruta
  - Creación de un mapa de ruta
  - Editar un mapa de ruta
  - Eliminar un mapa de ruta

Enrutamiento basado en directivas (PBR)
- Administrar reglas de enrutamiento IP
  - Crear una regla de IP
  - Editar una regla de IP
  - Eliminar una regla de IP

Intercambio de rutas a través de BGP
- Configuración básica de BGP
- Administrar pares de BGP
  - Crear un par de BGP
  - Editar un par BGP
  - Eliminar un par BGP
- Administrar grupos de pares de BGP
  - Crear un grupo de pares de BGP
  - Editar un grupo de pares de BGP
  - Eliminar un grupo de pares de BGP
- Configurar fugas de rutas entre VRF

Intercambio de rutas a través de OSPF
Configuración básica de OSPF
Administrar áreas de OSPF
Crear un área de OSPF
Editar un área de OSPF
Eliminar un área de OSPF
Administrar interfaces de OSPF
Crear una interfaz de OSPF
Editar una interfaz OSPF
Eliminar una interfaz de OSPF
Utilizar BFD para detectar fallas de enrutamiento
Habilitar o deshabilitar el protocolo BFD
Crear un par de BFD
Editar un par de BFD
Eliminación de un par BFD
Garantizar una alta disponibilidad con VRRP
Habilitar o deshabilitar el protocolo VRRP
Administrar instancias de VRRP
Crear una instancia de VRRP
Editar una instancia de VRRP
Eliminar una instancia de VRRP
Administrar grupos de instancias de VRRP
Crear un grupo de instancias de VRRP
Editar un grupo de instancias de VRRP
Eliminar un grupo de instancias de VRRP
Transmisión de tráfico multidifusión mediante protocolos PIM e IGMP
Configuración básica de PIM
Administrar interfaces de multidifusión
Crear una interfaz de multidifusión
Editar una interfaz de multidifusión
Eliminar una interfaz de multidifusión
Administrar tablas de enrutamiento y reenvío virtuales (VRF)
Especificar la configuración del kernel relacionada con las tablas de enrutamiento virtual
Crear una tabla de enrutamiento y reenvío virtuales
Modificar la tabla de enrutamiento y reenvío virtuales
Eliminar una tabla de enrutamiento y reenvío virtuales
Supervisar la información de paquetes de tráfico mediante el protocolo NetFlow
Administrar plantillas de NetFlow
Crear una plantilla de NetFlow
Seleccionar una plantilla de NetFlow asignada
Importar una plantilla de NetFlow
Clonar una plantilla de NetFlow
Verificar el uso de una plantilla de NetFlow
Eliminar una plantilla de NetFlow
Configuración básica de NetFlow
Cambiar la plantilla de NetFlow de un dispositivo CPE

- Diagnosticar un dispositivo CPE
  - Solicitar información de diagnóstico
  - Utilizar el modo de depuración para protocolos de enrutamiento dinámico en dispositivos CPE
  - Especificar servidores NTP en dispositivos CPE
  - Habilitar el modo interactivo
  - Ejecutar la utilidad ping
  - Ejecutar la utilidad traceroute
  - Ejecutar la utilidad tcpdump
  - Ejecutar la utilidad iperf
  - Ejecutar la utilidad sweep
  - Ejecutar la utilidad de volcado OpenFlow
  - Restablecer las sesiones de BGP/OSPF
  - Administrar informes
    - Descargar un informe
    - Eliminar un informe
- Ejecución de tareas en dispositivos CPE
  - Crear una tarea
  - Ejecutar una tarea manualmente
  - Eliminar una tarea
- Comprobaciones en dispositivos CPE
  - Comprobación de integridad
    - Ejecutar una comprobación de integridad manual
    - Configuración de la comprobación de integridad programada
  - Autocomprobación del firewall
    - Ejecución manual de una comprobación automática del firewall
    - Configuración de la comprobación automática programada del firewall
  - Bloquear tráfico si falla la comprobación de la integridad o la comprobación automática

Auditoría de eventos de seguridad
- Configurar el registro de eventos de seguridad para la auditoría
- Lista de eventos de seguridad que se pueden registrar en el orquestador y los dispositivos CPE

Rangos de subredes y direcciones IP para dispositivos CPE
- Administrar rangos de direcciones IP
  - Crear un rango de direcciones IP
  - Editar un rango de direcciones IP
  - Ver el uso de un rango de direcciones IP
  - Eliminar rangos de direcciones IP
- Administrar rangos de subredes
  - Crear un rango de subredes
  - Editar un rango de subredes
  - Ver el uso de un rango de subredes
  - Eliminar rangos de subredes

Administrar el firewall
- Administrar zonas de firewall
  - Crear una zona de firewall
  - Clonar una zona común de firewall
  - Ver el uso de una zona común de firewall

- Editar una zona de firewall
- Eliminar una zona de firewall
- Administrar plantillas de firewall
  - Crear una plantilla de firewall
  - Seleccionar una plantilla de firewall asignada
  - Importar una plantilla de firewall
  - Clonar una plantilla de firewall
  - Ver el uso de una plantilla de firewall
  - Eliminar una plantilla de firewall
- Configuración básica del firewall
- Configurar el marcado de DPI
- Administrar reglas de firewall
  - Crear una regla de firewall
  - Configurar el orden de las reglas del firewall
  - Habilitar o deshabilitar una regla de firewall
  - Editar una regla de firewall
  - Eliminar una regla de firewall
- Administrar reglas de firewall avanzadas
  - Criterios de coincidencia adicionales para reglas avanzadas
    - Paquete fragmentado
    - Coincidencia por marca
    - TOS
    - Coincidencia por cadena
    - Coincidencia por reciente
    - Marcas TCP no válidas
    - Tasa límite
    - Código móvil
    - Emparejamiento por comandos del protocolo de la capa de aplicación
  - Crear una regla avanzada
  - Habilitar y deshabilitar reglas avanzadas
  - Editar una regla avanzada
  - Eliminar una regla avanzada
  - Escenario: ocultar un dispositivo CPE en la ruta de tráfico mediante reglas de firewall
- Administrar conjuntos de IP
  - Crear un conjunto de IP
  - Deshabilitar o habilitar un conjunto de IP
  - Editar un conjunto de IP
  - Eliminar un conjunto de direcciones IP
- Administrar reglas DNAT
  - Crear una regla DNAT
  - Configurar el orden de las reglas DNAT
  - Deshabilitar o habilitar una regla DNAT
  - Editar una regla DNAT
  - Eliminar una regla DNAT
- Administrar reglas de SNAT
  - Crear una regla SNAT
  - Configurar el orden de las reglas SNAT

Deshabilitar o habilitar una regla SNAT
Editar una regla SNAT
Eliminar una regla SNAT
Administrar un reenvío
Crear un reenvío
Eliminar un reenvío
Cambiar la plantilla de firewall de un dispositivo CPE
Integración con herramientas de seguridad de la información externas
Administrar servicios de red y virtualización de funciones de la red
Administrar plantillas de servicios de red
Crear una plantilla de servicio de red
Editar una plantilla de servicio de red
Eliminar una plantilla de servicio de red
Administrar servicios de red
Crear un servicio de red
Editar un servicio de red
Implementar servicio de red
Comprobar la integridad de un servicio de red
Volver a implementar un servicio de red
Deshabilitar o habilitar la reparación automática para un servicio de red
Ver el registro de servicios de red
Eliminar un servicio de red
Escenario: implementación de una función de la red virtual
Escenario: implementación de una función de la red física
Administrar paquetes VNF y PNF
Configurar el descriptor VNF
Configurar descriptor PNF
Protección de paquetes VNF y PNF contra la sustitución y la modificación
Cargar un paquete VNF o PNF a la interfaz web del orquestador
Especificar una breve descripción de un servicio de red compartido
Administrar funciones de red virtual
Seleccionar el tipo de función de la red virtual
Configurar puntos de conexión externos de una función de la red virtual
Configuración básica de una función de red virtual
Alojar la función de la red virtual en un centro de datos y en un dispositivo uCPE
Detener o iniciar una función de la red virtual o una VDU que forma parte de ella
Pausar o reanudar una función de la red virtual o una VDU que forma parte de ella
Suspender o anular la suspensión de una función de la red virtual o una VDU que forma parte de ella
Reinicio suave de una función de la red virtual o una VDU que forma parte de ella
Reinicio forzado de una función de la red virtual o una VDU que forma parte de ella
Volver a implementar una función de la red virtual o una VDU que forma parte de ella
Reparar automáticamente una función de la red virtual o una VDU que forma parte de ella
Administrar instantáneas de la VDU
Crear una instantánea de la VDU
Restaurar la configuración de la VDU mediante una instantánea
Editar una instantánea de la VDU
Eliminar una instantánea de la VDU

- Administrar funciones de la red física
  - Seleccionar el tipo de función de una red física
  - Configuración básica de una función de la red física
- Configuración de un servicio P2P
- Configurar un servicio P2M
- Configurar un servicio M2M
- Configurar una red compartida (OS 2 SHARED)
- Configuración de un enrutador virtual (OS vRouter)
- Configuración de una VLAN
- Configurar una VXLAN
- Configurar una red plana
- Configurar una UNI

Supervisar los componentes de una solución
- Especificar el servidor Zabbix
- Especificar el servidor proxy Zabbix
- Configurar la supervisión de dispositivos CPE
- Visualizar los resultados del control
- Visualización de problemas
- Ver el estado de la solución y sus componentes
- Ver registros
- Ver y eliminar solicitudes de servicio
- Enviar notificaciones del dispositivo CPE a los usuarios
  - Especificar el servidor SMTP
  - Configurar notificaciones
- Seleccionar la verbosidad del registro del contenedor Docker
- Supervisar dispositivos CPE, VNF y PNF mediante el SNMP
  - Configurar la conexión del administrador de SNMP a los agentes de SNMP
  - Crear una captura
  - Editar una captura
  - Eliminar una captura
- Supervisión de vínculos

Crear una red de SD-WAN entre dispositivos CPE
- Acerca de la topología de centro y radios
- Acerca de las topologías de malla completa y malla parcial
- Asignar una función a un dispositivo CPE
- Asignar una etiqueta de topología a un dispositivo CPE
- Configurar rutas
- Administrar vínculos
  - Ver estadísticas para un vínculo
  - Actualizar automáticamente el costo del vínculo en función de la velocidad de datos máxima de la interfaz
  - Especificar el costo de un vínculo
  - Habilitar la amortiguación
  - Habilitar la corrección de errores de reenvío
  - Determinar el valor de MTU
  - Cifrado de tráfico
    - Habilitación del cifrado de tráfico en un dispositivo CPE
    - Habilitar el cifrado de tráfico en un vínculo

- Administración de errores de conectividad (CFM)
  - Habilitar CFM en un dispositivo CPE
  - Habilitar CFM en un vínculo
- Administrar segmentos
  - Crear una ruta Manual-TE
  - Edición de una ruta Manual-TE
  - Eliminación de una ruta Manual-TE

Calidad de servicio (QoS)
- Mecanismos de la calidad del servicio
- Marcado y remarcado del tráfico
- Administrar clases de tráfico
- Administrar clasificadores de tráfico
  - Crear un clasificador de tráfico
  - Edición de un clasificador de tráfico
  - Eliminar un clasificador de tráfico
- Administrar las reglas de calidad del servicio
  - Crear una regla de calidad de servicio
  - Editar una regla de calidad de servicio
  - Eliminar una regla de calidad del servicio
- Administrar restricciones de Manual-TE
  - Crear una restricción de Manual-TE
  - Editar una restricción de Manual-TE
  - Eliminar una restricción de Manual-TE
- Administrar restricciones de umbral
  - Crear una restricción de umbral
  - Editar una restricción de umbral
  - Eliminar una restricción de umbral
- Administrar reglas de clasificación de tráfico
  - Crear una regla de clasificación de tráfico
  - Editar una regla de clasificación de tráfico
  - Eliminar una regla de clasificación de tráfico
- Administrar filtros de tráfico
  - Crear un filtro de tráfico
  - Editar un filtro de tráfico
  - Eliminar un filtro de tráfico

Transmisión de tráfico entre dispositivos CPE y dispositivos cliente mediante servicios de transporte
- Duplicación de paquetes de tráfico
- Escenario: dirigir el tráfico de la aplicación a un servicio de transporte
- Escenario: establecer la conexión L2 entre dispositivos CPE
- Escenario: administración del tráfico de aplicaciones de acuerdo con un SLA
- Administrar servicios de transporte punto a punto (P2P)
  - Crear un servicio P2P
  - Ver estadísticas de un servicio P2P
  - Ver y configurar la visualización de la topología de un servicio P2P
  - Editar un servicio P2P
  - Reiniciar un servicio P2P
  - Eliminar un servicio P2P

Administrar servicios de transporte punto a multipunto (P2M)
- Crear un servicio P2M
- Ver estadísticas de un servicio P2M
- Ver la tabla MAC de un servicio P2M
- Visualización y configuración de la visualización de una topología de servicio P2M
- Editar un servicio P2M
- Reiniciar un servicio P2M
- Eliminar un servicio P2M

Administrar servicios de transporte multipunto a multipunto (M2M)
- Crear un servicio M2M
- Ver las estadísticas de un servicio M2M
- Ver la tabla MAC de un servicio M2M
- Ver y configurar la visualización de una topología de servicio M2M
- Editar un servicio M2M
- Reiniciar un servicio M2M
- Eliminación de un servicio M2M

Administrar servicios de transporte de multidifusión IP
- Creación de un servicio de multidifusión IP
- Ver las estadísticas de un servicio de multidifusión IP
- Editar un servicio de multidifusión IP
- Eliminar un servicio de multidifusión IP

Administrar servicios de transporte VPN L3
- Crear un servicio VPN L3
- Administrar la tabla ARP de un servicio de VPN L3
  - Crear un registro estático en la tabla ARP de un servicio VPN L3
  - Editar un registro estático en la tabla ARP de un servicio VPN L3
  - Eliminar un registro estático en la tabla ARP de un servicio VPN L3
- Ver la tabla de enrutamiento y reenvío de un servicio de VPN L3
- Editar un servicio de VPN L3
- Reiniciar un servicio de VPN L3
- Eliminación de un servicio de VPN L3

Administrar servicios de transporte en una plantilla de instancia SD-WAN
- Crear un servicio P2M o un servicio M2M en una plantilla de instancia SD-WAN
- Crear un servicio VPN L3 en una plantilla de instancia SD-WAN
- Editar un servicio de transporte en una plantilla de instancia SD-WAN
- Eliminar un servicio de transporte en una plantilla de instancia SD-WAN

Administrar servicios de transporte en una plantilla de CPE
- Agregar un servicio de transporte a una plantilla de CPE
- Editar un servicio de transporte en una plantilla de CPE
- Eliminar un servicio de transporte de una plantilla de CPE

Duplicación y reenvío de tráfico entre dispositivos CPE
- Administrar destinos de tráfico
  - Crear un destino de tráfico
  - Eliminar un destino de tráfico
- Administrar servicios de TAP
  - Crear un servicio de TAP
  - Ver estadísticas de un servicio de TAP

Editar un servicio de TAP
Eliminar un servicio de TAP
Integración con la Kaspersky Unified Monitoring and Analysis Platform
Instalación de KUMA
Escenario: configuración de KUMA
Configuración de almacenamiento en KUMA
Creación y configuración de un normalizador en KUMA para mensajes de syslog
Configuración del correlacionador y reglas de correlación en KUMA
Tabla de referencia para crear reglas de correlación KUMA
Configuración de un recopilador para eventos syslog en KUMA
Configuración del servicio de correo en KUMA
Configuración de reglas de notificación en KUMA
Ejemplos de configuración para la búsqueda por eventos clave en KUMA
Integración con Kaspersky CyberSecurity for Networks
Ponerse en contacto con el Servicio de soporte técnico
Cómo obtener Servicio de soporte técnico
Soporte técnico a través de Kaspersky CompanyAccount
Fuentes de información acerca de la solución
Apéndices
Glosario
Administrador de funciones de la red virtual (VNFM)
Administrador de infraestructura virtual (VIM)
Controlador
CPE universal (uCPE)
Equipo local del cliente (CPE)
Estrategia de transporte
Función de red física (PNF)
Función de red virtual (VNF)
Inquilino
Instancia SD-WAN
Open vSwitch (OVS)
Orquestador
Paquete PNF
Paquete VNF
Plano de control
Plano de datos
Puerta de enlace SD-WAN
Red de área amplia definida por software (SD-WAN)
Redes definidas por software (SDN)
Seguridad de puerto
Sistema operativo del conmutador (SWOS)
Unidad de implementación virtual (VDU)
Información sobre código de terceros
Avisos de marcas registradas

# Ayuda de Kaspersky SD-WAN

## Funciones nuevas

Novedades en cada versión de Kaspersky SD-WAN

## Requisitos de hardware y software

Revisión de los requisitos de hardware y software

## Primeros pasos

- Implementar Kaspersky SD-WAN
- Administrar la infraestructura corporativa
- Administrar usuarios y sus permisos de acceso
- Tenencia múltiple

## Supervisión y generación de informes

- Configurar registros en dispositivos CPE
- Supervisar la información de paquetes de tráfico mediante el protocolo NetFlow
- Diagnosticar los dispositivos CPE
- Supervisar los componentes de una solución

## Actualización

Actualizar Kaspersky SD-WAN desde un versión anterior

## Características adicionales

- Administrar el firewall
- Calidad de servicio (QoS)
- Duplicación de tráfico

## Apéndices

Obtenga información sobre Kaspersky SD-WAN en guías adicionales

# Acerca de Kaspersky SD-WAN

Kaspersky SD-WAN se utiliza para crear redes de área amplia definidas por software (WAN definida por software; SD-WAN). En las redes SD-WAN, las rutas con la latencia más baja y el mayor ancho de banda se determinan automáticamente. El tráfico se enruta mediante la tecnología SDN (Redes definidas por software).

La *tecnología SDN* separa el plano de control del plano de datos y permite administrar la infraestructura de red mediante un orquestador (a través de la interfaz web o la API). Separar el plano de control del plano de datos permite *virtualizar las funciones de la red* (Virtualización de funciones de la red; NFV), por lo cual las funciones de la red como firewalls, enrutadores y equilibradores de carga se implementan en equipos estándar. La virtualización de funciones de la red en la solución cumple con la especificación NFV MANO (Administración y orquestación de la virtualización de funciones de la red) del Instituto Europeo de Normas de Telecomunicaciones (ETSI).

La creación de una red SD-WAN no depende de las tecnologías de transporte. También puede enviar tráfico a través de varios vínculos según los requisitos de la aplicación con respecto al ancho de banda y la calidad del servicio. Se admiten los siguientes tipos de redes subyacentes:

- Redes de transporte MPLS
- Vínculos de banda ancha para la conexión a Internet
- Líneas de comunicación arrendadas
- Conexiones inalámbricas que incluyen 3G, 4G y LTE
- Vínculos satelitales

La solución está destinada a proveedores de servicios y organizaciones que tienen una gran red de sucursales. Reemplaza los enrutadores estándar en las redes distribuidas con dispositivos del equipo local del cliente (en adelante, dispositivos CPE, CPE).

Kaspersky SD-WAN le permite hacer lo siguiente:

- Administración inteligente del tráfico
- Configuración automática del dispositivo CPE
- Administración centralizada de los componentes de la solución mediante la interfaz web
- Supervisión de la red
- Respuesta automática a los cambios en las directivas de calidad de servicio para cumplir con los requisitos de las aplicaciones

En la siguiente figura se muestra un diagrama de una red SD-WAN creada con la solución Kaspersky SD-WAN.

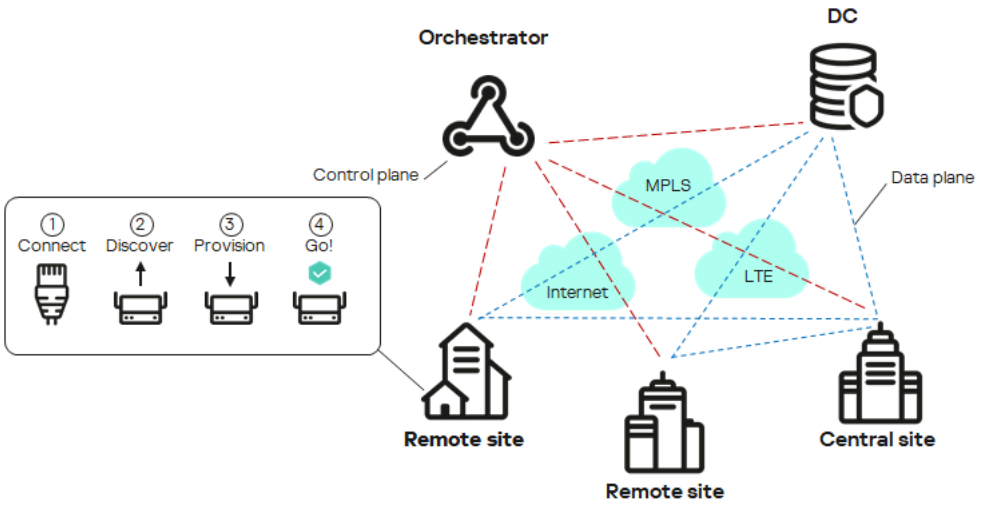



Diagrama de una red SD-WAN

# Kit de distribución

Para obtener más información sobre la compra de la solución, visite el sitio web de Kaspersky (https://www.kaspersky.com) o comuníquese con empresas asociadas.

El kit de distribución incluye los siguientes componentes:

- knaas-installer_<información de la versión> en formato TAR.GZ (en adelante también denominado archivo de instalación) para la implementación de la solución.
- Contenedores Docker para implementar componentes de Kaspersky SD-WAN:
  - knaas-ctl
  - knaas-orc
  - knaas-www
  - knass-vnfm
  - knaas-vnfm-proxy
  - mockpnf

  Debe descargar los siguientes contenedores del repositorio común de Docker:
  - mariaDB
  - mongo
  - redis
  - syslog-ng

- zabbix-proxy-mysql
- zabbix-server-mysql
- zabbix-web-nginx-mysql

- Firmware del dispositivo CPE.
- Un archivo con el texto del Contrato de licencia de usuario final, que estipula los términos y condiciones que debe aceptar para utilizar la solución.
- Archivos de ayuda en línea de Kaspersky SD-WAN que le permiten leer la documentación sin una conexión a Internet.

El contenido del kit de distribución puede variar en función de la región en la que se distribuye la solución.

# Requisitos de hardware y software

Kaspersky SD-WAN presenta los siguientes requisitos de hardware y software:

Los requisitos de hardware dependen de la cantidad de dispositivos CPE que se administran (consulte los escenarios de implementación recomendados a continuación). Si necesita calcular los requisitos de hardware para un esquema de implementación específico con mayor precisión, le recomendamos comunicarse con el Servicio de soporte técnico de Kaspersky.

## 1. Recursos informáticos recomendados para los componentes de la solución, versión 2.4 o posterior

Las siguientes son especificaciones admitidas para instancias del Orquestador de Kaspersky SD-WAN (ORC), el Controlador de Kaspersky SD-WAN (CTL), el componente de supervisión (MON) y la utilidad del Kit de herramientas de implementación de Kaspersky (KDT). Estos son válidos siempre que se utilicen componentes y versiones de software idénticos.

### 1.1. Orquestador de SD-WAN

Tabla 1. Definiciones de tipos de instancias de ORC

| Tipo de instancia | Cantidad de dispositivos CPE | Especificaciones (aproximadas) | | | | |
|---|---|---|---|---|---|---|
| | | CPU* | RAM | Tamaño de almacenamiento** | IOPS de almacenamiento** | Adaptador de red |
| ORC pequeño | 1000 | 16 núcleos | 32 GB | 256 GB | 3,000 | 2 x 1 Gbps |
| ORC mediano | 5,000 | 24 núcleos | 64 GB | 512 GB | 5,000 | 2 x 1 Gbps |
| ORC grande | 10,000 | 16 núcleos | 128 GB | 1 TB | 10,000 | 2 x 10 Gbps |

* CPU sin Hyper-Threading. Recomendaciones:

- Xeon Silver 4314 para instancias de ORC pequeño
- Xeon Gold 5318Y, Xeon Gold 5418Y o superior para instancias de ORC mediano
- Xeon Gold 6414U, Xeon Gold 6438Y+ o superior para instancias de ORC grande

** SSD

## 1.2. Controlador de SD-WAN

Tabla 2. Definiciones de tipos de instancias de CTL

| Tipo de instancia | Cantidad de dispositivos CPE | Especificaciones (aproximadas) | | | | |
|---|---|---|---|---|---|---|
| | | CPU* | RAM | Tamaño de almacenamiento** | IOPS de almacenamiento** | Adaptador de red |
| CTL pequeño | 250 | 16 núcleos | 32 GB | 64 GB | 3,000 | 2 x 1 Gbps |
| CTL mediano | 500 | 24 núcleos | 48 GB | 128 GB | 5,000 | 2 x 1 Gbps |
| CTL grande | 1000 | 32 núcleos | 64 GB | 256 GB | 10,000 | 2 x 10 Gbps |

* CPU sin Hyper-Threading. Recomendaciones:

- Xeon Silver 4314 para instancias de CTL pequeño
- Xeon Gold 5318Y, Xeon Gold 5418Y o superior para instancias de CTL mediano
- Xeon Gold 6414U, Xeon Gold 6438Y+ o superior para instancias de CTL grande

** SSD

## 1.3. Componente de supervisión de SD-WAN

Tabla 3. Definiciones de tipos de instancias de MON

| Tipo de instancia | Cantidad de dispositivos CPE | Especificaciones (aproximadas) | | | | |
|---|---|---|---|---|---|---|
| | | CPU* | RAM | Tamaño de almacenamiento** | IOPS de almacenamiento** | Adaptador de red |
| MON pequeño | 1,000 | 8 núcleos | 16 GB | 1 TB | 3,000 | 2 x 1 Gbps |
| MON mediano | 5,000 | 24 núcleos | 64 GB | 5 TB | 5,000 | 2 x 1 Gbps |
| MON grande | 10,000 | 16 núcleos | 96 GB | 10 TB | 10,000 | 2 x 10 Gbps |

* CPU sin Hyper-Threading. Recomendaciones:

- Xeon Silver 4309Y para instancias de MON pequeño
- Xeon Gold 5318Y, Xeon Gold 5418Y o superior para instancias de MON mediano
- Xeon Gold 6414U, Xeon Gold 6438Y+ o superior para instancias de MON grande

** SSD, RAID 10

## 1.4. SD-WAN todo-en-uno

Una instancia SD-WAN todo-en-uno (AIO) incluye los siguientes componentes de administración: el Orquestador de Kaspersky SD-WAN (ORC), el Controlador de Kaspersky SD-WAN (CTL) y el componente de supervisión de Kaspersky SD-WAN (MON). Se admiten las siguientes especificaciones de instancia:

Tabla 4. Definiciones de tipos de instancias de AIO

| Tipo de instancia | Cantidad de dispositivos CPE | Especificaciones (aproximadas) | | | | |
|---|---|---|---|---|---|---|
| | | CPU* | RAM | Tamaño de almacenamiento** | IOPS de almacenamiento** | Adaptador de red |
| AIO pequeño | 50 | 16 núcleos | 32 GB | 256 GB | 3,000 | 1 Gbps |
| AIO mediano | 100 | 24 núcleos | 48 GB | 512 GB | 5,000 | 2 x 1 Gbps |
| AIO grande | 250 | 32 núcleos | 64 GB | 1024 GB | 10,000 | 2 x 10 Gbps |

## 1.5. Host para la implementación de SD-WAN

Para implementar y actualizar los componentes de administración de la solución en escenarios de alta disponibilidad e implementación distribuida, necesita un host dedicado con el Kit de herramientas de implementación de Kaspersky (KDT).

Tabla 5. Definiciones de tipos de instancias de KDT

| Escenario de implementación | Especificaciones (aproximadas) | | | | |
|---|---|---|---|---|---|
| | CPU* | RAM | Tamaño de almacenamiento** | IOPS de almacenamiento** | Adaptador de red |
| Alta disponibilidad e implementación distribuida | 8 núcleos | 16 GB | 512 GB | 5,000 | 1 Gbps |

* CPU sin Hyper-Threading. Recomendaciones:

- Xeon Silver 4309Y para instancias de KDT

** SSD

# 2. Escenarios de implementación del sistema de administración

## 2.1. Implementación independiente

El escenario de implementación independiente del sistema de administración de Kaspersky SD-WAN está diseñado solo para fines de demostración y no se recomienda para un entorno de producción.

## 2.2. Implementación de alta disponibilidad

La implementación del sistema de administración de Kaspersky SD-WAN en un escenario de alta disponibilidad (HA) requiere tres instancias AIO (HA3). Los requisitos de hardware de las instancias se especifican en la Tabla 4. En la siguiente tabla se enumeran las recomendaciones de tamaño para la implementación de HA3.

Tabla 6. Requisitos de las instancias para la implementación de HA3

| Cantidad de dispositivos CPE | Instancia HA3 |
|---|---|
| 50 | 3 x AIO pequeño |

| | |
|---|---|
| 100 | 3 x AIO mediano |
| 250 | 3 x AIO grande |

## 2.3. Implementación distribuida

La implementación del sistema de administración de Kaspersky SD-WAN en un escenario de implementación distribuida requiere tres instancias de ORC exclusivas, tres instancias de CTL exclusivas, tres instancias de MON exclusivas y un host de KDT.

Tabla 7. Requisitos de las instancias para la implementación

| Cantidad de dispositivos CPE | ORC | CTL | MON | KDT |
|---|---|---|---|---|
| 250 | 3 x ORC pequeño | 3 x CTL pequeño | 3 x MON pequeño | 1 x KDT |
| 500 | 3 x ORC pequeño | 3 x CTL mediano | 3 x MON pequeño | 1 x KDT |
| 1,000 | 3 x ORC pequeño | 3 x CTL grande | 3 x MON pequeño | 1 x KDT |
| 2,500 | 3 x ORC pequeño | 15 x CTL mediano | 3 x MON pequeño | 1 x KDT |
| 5,000 | 3 x ORC mediano | 30 x CTL mediano | 3 x MON mediano | 1 x KDT |
| 7,500 | 3 x ORC mediano | 45 x CTL mediano | 3 x MON mediano | 1 x KDT |
| 10,000 | 3 x ORC grande | 60 x CTL mediano | 3 x MON grande | 1 x KDT |
| 20,000 | 6 x ORC grande | 120 x CTL mediano | 6 x MON grande | 1 x KDT |
| 25,000 | 9 x ORC grande | 150 x CTL mediano | 9 x MON grande | 1 x KDT |

## 3. Requisitos de soluciones de terceros

Las siguientes soluciones de terceros son necesarias para implementar Kaspersky SD- WAN:

- La plataforma de Docker versión 1.5 o posterior para implementar contenedores de Docker de componentes de la solución. Para obtener más información, consulte la documentación oficial de la plataforma de Docker.
- Las versiones 5.0.26 o 6.0.0 del sistema de supervisión Zabbix. Para obtener más información, consulte la documentación oficial de la solución Zabbix.
- El servicio OpenStreetMap para ver la topología del servicio de transporte superpuesta en un mapa. Si la infraestructura de su organización no proporciona una conexión a Internet, puede usar mapas sin conexión. Los mapas sin conexión ocupan espacio adicional en el disco:
  - El mapa sin conexión (central-fed-district-latest.osm.pbf) ocupa aproximadamente 100 GB.
  - Los datos de geocodificación ocupan aproximadamente 10 GB.

  Para obtener información detallada, consulte la documentación oficial del servicio OpenStreetMap.

## Requisitos del sistema operativo

Se admiten los siguientes sistemas operativos de 64 bits:

- Ubuntu 22.04.5 LTS.
- Astra Linux 1.8.5 (nivel de seguridad: "Orel").
- RED OS 7.3 "MUROM".

## Requisitos para los vínculos entre los nodos de los componentes de la solución

Cuando implementa Kaspersky SD-WAN, puede implementar varios nodos de componentes de la solución. Los siguientes requisitos se aplican a los vínculos entre los nodos de los componentes de la solución:

- Requisitos para los vínculos entre los nodos del controlador:
  - Ancho de banda: 1 Gbps
  - RTT (tiempo de ida y vuelta): 200 ms o menos
  - Pérdida de paquetes: 0 %
- Requisitos para los vínculos entre los nodos de la base de datos MongoDB:
  - Ancho de banda: 1 Gbps
  - RTT: 50 ms o menos
  - Pérdida de paquetes: 0 %
- Requisitos para los vínculos entre los nodos de la base de datos Redis:
  - Ancho de banda: 1 Mbps
  - RTT: 50 ms o menos
  - Pérdida de paquetes: 0 %

## Requisitos del navegador

Se admiten los siguientes navegadores para administrar la interfaz web del orquestador:

- Google Chrome 100 o posterior
- Mozilla Firefox 100 o posterior
- Microsoft Edge 100 o posterior
- Opera 90 o posterior
- Safari 15 o posterior

## Requisitos del dispositivo CPE

Se admiten los siguientes modelos de dispositivos CPE:

- KESR-M1-R-5G-2L-W
- KESR-M2-K-5G-1L-W
- KESR-M2-K-5G-1S
- KESR-M3-K-4G-4S
- KESR-M4-K-2X-1CPU
- KESR-M4-K-8G-4X-1CPU
- KESR-M5-K-8G-4X-2CPU
- KESR-M5-K-8X-2CPU

Los dispositivos CPE del modelo KESR están basados en arquitecturas de procesador x86 (Intel 80x86) y MIPS (microprocesador sin etapas de interconexión entrelazadas).

Los dispositivos CPE KESR M3–M5 tienen adaptadores de red Intel que son compatibles con los transceptores SFP Intel. Para obtener más información sobre los transceptores SFP compatibles, puede utilizar la Herramienta de compatibilidad de productos Intel

https://compatibleproducts.intel.com/ProductDetails?activeModule=Intel%C2%AE%20Ethernet#
(en el territorio de la Federación de Rusia, se puede acceder al vínculo solo a través de una VPN). Cuando usa la Herramienta de compatibilidad de productos de Intel, debe seleccionar una de las siguientes categorías de productos:

- **Serie 500** para ver los transceptores SFP que son compatibles con los dispositivos CPE KESR M3.
- **Serie 700** para ver los transceptores SFP que son compatibles con los dispositivos CPE KESR M4–M5.

Los expertos de Kaspersky llevaron a cabo pruebas para confirmar la funcionalidad de los dispositivos CPE al proporcionar el servicio VPN L3 (consulte la tabla a continuación). No se utilizó DPI (Inspección profunda de paquetes) en los dispositivos evaluados y se deshabilitó el cifrado de tráfico.

| Hardware | Tamaño del paquete (bytes) | Ancho de banda (Mbps) |
|---|---|---|
| KESR-M1 | IMIX (417) | 30 |
| | Grande (1300) | 115 |
| KESR-M2 | IMIX (417) | 165 |
| | Grande (1300) | 241 |
| KESR-M3 | IMIX (417) | 805 |
| | Grande (1300) | 1150 |
| KESR-M4 | IMIX (417) | 1430 |
| | Grande (1300) | 2870 |

Para obtener información detallada sobre las características de los dispositivos CPE, consulte la página oficial de la solución.

Puede implementar dispositivos uCPE en servidores con arquitecturas de procesador x86 (Intel 80x86) o ARM64.

### Requisitos del dispositivo vCPE

El kit de distribución incluye el siguiente firmware para implementar dispositivos vCPE:

- vKESR-M1
- vKESR-M2
- vKESR-M3
- vKESR-M4

Los siguientes entornos de virtualización son compatibles con los dispositivos vCPE:

- VMware 7.0 o posterior
- KVM con kernel versión 5.15 o posterior

> Solo se admite el entorno de virtualización KVM original sin herramientas de orquestación adicionales.

En la siguiente tabla, se enumeran los requisitos de recursos virtuales para implementar dispositivos vCPE.

| Firmware | CPU | RAM, GB | Disco, GB |
|---|---|---|---|
| vKESR-M1 | 2 | 0.5 | 1 |
| vKESR-M2 | 4 | 8 | 1 |
| vKESR-M3 | 12 | 16 | 1 |
| vKESR-M4 | 24 | 32 | 1 |

Cuando actualiza Kaspersky SD-WAN de la versión 2.2 a 2.3, debe asegurarse de que los dispositivos vCPE implementados anteriormente cumplan con los requisitos de la nueva versión, después de lo cual puede actualizar sus dispositivos vCPE mediante el firmware vKESR-M1-5.

# Garantizar la seguridad

La seguridad en Kaspersky SD-WAN está garantizada en el plano de datos, el plano de control y el plano de orquestación. El nivel de seguridad de la solución en su conjunto está determinado por el nivel de seguridad de cada uno de estos planos, así como por la seguridad de su interacción. Se llevan a cabo los siguientes procesos en cada plano:

- Autenticación y autorización de usuarios
- Uso de protocolos de administración seguros
- Cifrado del tráfico de control
- Conexión segura de dispositivos CPE

## Protocolos de administración seguros

Recomendamos usar HTTPS para comunicarse con la red SD-WAN a través de la interfaz web o API del orquestador. Puede cargar sus propios certificados en la interfaz web o utilizar certificados autofirmados generados automáticamente. La solución utiliza varios protocolos para transmitir el tráfico de control a los componentes (consulte la tabla a continuación).

| Componentes que interactúan | Protocolo | Medidas de seguridad adicionales |
|---|---|---|
| Orquestador y controlador | gRPC | Se utiliza TLS para la autenticación y el cifrado del tráfico entre el cliente y el servidor. |
| Orquestador y dispositivo CPE | HTTPS | Se utilizan la verificación del certificado y un token para la autenticación y el cifrado del tráfico entre el orquestador y el dispositivo CPE. |
| Controlador y dispositivo CPE | OpenFlow 1.3.4 | Se utiliza TLS para la autenticación y el cifrado de tráfico entre el controlador y el dispositivo CPE. |

## Conexión segura de dispositivos CPE

La solución utiliza los siguientes mecanismos para la conexión segura de dispositivos CPE:

- Descubrimiento de dispositivos CPE por los DPID (identificadores de rutas de datos).
- Registro diferido. Puede seleccionar el estado del dispositivo CPE después de registrarse correctamente: **Habilitado** o **Deshabilitado**. Un dispositivo CPE deshabilitado debe habilitarse después de asegurarse de que esté instalado en la ubicación.
- Autenticación de dos factores.

## Utilizar funciones de la red virtual

Puede proporcionar una capa adicional de seguridad con funciones de red virtual implementadas en el centro de datos o en uCPE. Por ejemplo, el tráfico se puede transmitir desde un dispositivo CPE a una función de la red virtual que actúa como un servidor proxy o firewall. Las funciones de la red virtual pueden realizar las siguientes funciones de protección de SD-WAN:

- Firewall de próxima generación (NGFW)
- Protección contra ataques DDoS (Denegación de servicio distribuida)
- Sistema de detección de intrusiones (IDS) y Sistema de prevención de intrusiones (IPS)
- Antivirus
- Antispam
- Sistema de filtrado de contenido y filtrado de URL
- Sistema de DLP (Prevención de pérdida de datos) para evitar filtraciones de información confidencial
- Proxy web seguro

# Novedades

Kaspersky SD-WAN tiene la siguiente funcionalidad nueva y mejorada:

- La solución se preparó para el inicio del procedimiento de certificación estatal (solo se aplica en la Federación de Rusia)

  La certificación de la solución Kaspersky SD-WAN confirmará el cumplimiento de los estrictos estándares de seguridad impuestos por el estado y la capacidad de resistir ciberamenazas graves mientras se proporciona el más alto nivel de protección para los sistemas de información del estado (SIG), los datos personales (ISPDN) y los sistemas de control industrial. Al elegir esta solución, nuestros clientes no solo cumplen con sus obligaciones legales formales, sino que también obtienen una ventaja estratégica mediante el desarrollo de su infraestructura de TI sobre una solución que tiene un nivel de seguridad confirmado de manera independiente.

- Protección de ataques de inundación de SYN

  Introducción de la protección contra ataques de desbordamiento de recursos del servidor a través de la inundación de TCP SYN. Dicho ataque tiene como objetivo hacer que el dispositivo CPE no esté disponible para el tráfico legítimo. La solución ahora incluye un mecanismo interno que ayudará a prevenir ataques de este tipo.

- Nuevo menú lateral

  El menú lateral rediseñado es un 26 % más amplio, lo que facilita la administración de la solución.

- Visualización de tablas de sesiones en el orquestador

  Anteriormente, tenía que iniciar sesión manualmente en cada dispositivo CPE para ver las tablas de sesiones; ahora puede ver los parámetros directamente en el orquestador. Esta nueva función facilita la resolución de problemas.

- Compatibilidad con la comunidad BGP

  Kaspersky SD-WAN ahora es compatible con la comunidad BGP, que permite una administración flexible de las directivas de enrutamiento sin aumentar la complejidad de la topología: la información acerca de las rutas se lleva a cabo mediante etiquetas de la comunidad, que los CPE utilizan para aplicar mecanismos de equilibrio.

- Registro mejorado

  Cada evento de seguridad ahora tiene criterios mediante los cuales puede saber si se trata de una infracción de seguridad. Ahora también puede hacer que las notificaciones acerca de infracciones de seguridad que se produzcan en los CPE y el orquestador se envíen a un recopilador de Kaspersky Unified Monitoring and Analysis Platform (KUMA). Anteriormente, los datos se podían enviar a KUMA como una transmisión, lo que le permitía clasificar manualmente lo que era o no una infracción. Esta nueva característica mejora el control y la seguridad y facilita la supervisión de la red.

- Cifrado de Syslog

  Ahora puede cifrar la comunicación de syslog (el cifrado de túnel cuando se envía a través de Internet no desaparece), lo que protege los registros cuando se transmiten a una solución de Kaspersky SIEM.

- QoS para el tráfico de tránsito

  Según la topología de la red, algunos CPE pueden retransmitir el tráfico de tránsito. Para una transmisión de tráfico y una red más eficientes, ahora puede priorizar dicho tráfico de tránsito. Antes, solo se podía priorizar el tráfico principal.

- Filtrado de paquetes fragmentados

  Un nuevo mecanismo de procesamiento de tráfico de red analiza los paquetes IP y permite o bloquea los paquetes fragmentados. Esta nueva característica mejora la seguridad de la red al tiempo que aumenta el rendimiento.

## Limitaciones conocidas

Kaspersky SD-WAN tiene las siguientes limitaciones:

- Limitaciones al integrar la solución con Kaspersky KSC/OSMP:
  - Solo disponible para nuevas instalaciones
  - No se admite la consola SSH
  - No se admite la consola VNC
- Las reglas de firewall no tienen en cuenta las tablas de enrutamiento y reenvío virtuales creadas por el usuario de la cuenta (no puede especificar reglas que coincidan con una tabla de enrutamiento y reenvío virtuales; en su lugar, debe usar otros atributos, por ejemplo, interfaces, direcciones IP).
- Cuando se modifican rutas estáticas, el daemon FRR puede reiniciarse.
- Alternar los modos de módem entre LTE y 3G (UMTS, CDMA, TD-SCDMA) puede causar una brecha en los cuadros de diagnóstico, ya que, para LTE, los parámetros RSSI, RSRQ, RSRP, SNR están disponibles, y para 3G, solo RSSI y ECIO.
- En el modo que no es VNFM, no están disponibles SSH, VNC y la consola web.

# Arquitectura de la solución

Kaspersky SD-WAN incluye los siguientes componentes principales:

- Orquestador

  Controla la infraestructura de la solución, funciona como un orquestador de NFV (NFVO) y administra los servicios de red y los administradores de VNF (VNFM) distribuidos. Puede administrar el orquestador a través de la interfaz web o la API REST cuando se utilizan sistemas externos ascendentes.

- Controlador

  Administra de forma centralizada la red superpuesta:

  - Crea la topología de la red.
  - Crea servicios de transporte.
  - Administra dispositivos CPE mediante el protocolo OpenFlow.
  - Equilibra el tráfico entre vínculos.
  - Supervisa los vínculos y cambia automáticamente el tráfico a un vínculo de respaldo si el vínculo principal falla.

  Para implementar el controlador, debe implementar la función de la red física del controlador, que se encuentra en el archivo de instalación. El orquestador es el encargado de administrar el controlador.

- Dispositivos CPE

  Se instalan en ubicaciones remotas para retransmitir el tráfico y formar una estructura SDN en forma de red superpuesta. Puede asignar la función de puerta de enlace SD-WAN o la función de dispositivo CPE estándar o el dispositivo CPE. Las puertas de enlace SD-WAN establecen vínculos con todos los dispositivos CPE estándar y otras puertas de enlace SD-WAN. Los dispositivos CPE estándar establecen vínculos solo con puertas de enlace SD-WAN. De manera predeterminada, todos los dispositivos CPE tienen la función de dispositivo CPE estándar.

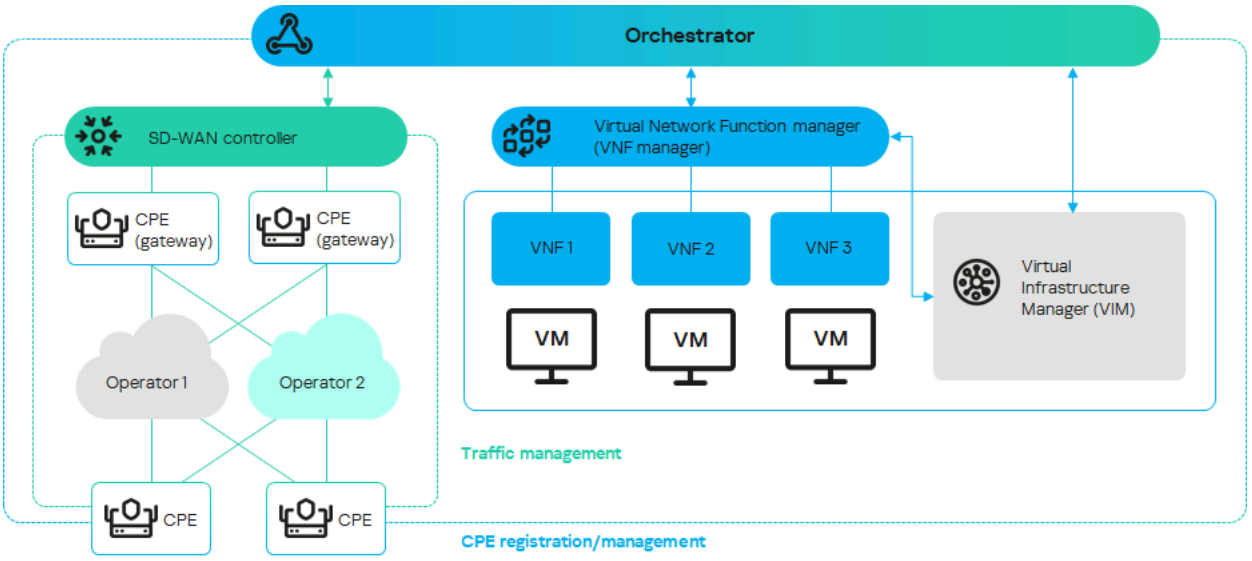
  Si desea que se establezca un vínculo entre dos dispositivos CPE estándar, debe asignarles la misma etiqueta de topología. Puede convertir un dispositivo CPE estándar en un dispositivo de tránsito para permitir que otros dispositivos CPE establezcan vínculos a través de él.

- VNFM (Administrador de funciones de la red virtual)

  Administra el ciclo de vida de las funciones de la red virtual mediante SSH, manuales de Ansible, scripts y atributos de inicio en la nube.

Si se utilizan funciones de la red virtual, la arquitectura de la solución incluye un Administrador de infraestructura virtual (VIM) que administra los recursos informáticos, de red y de almacenamiento dentro de la infraestructura de NFV. Un VIM conecta las funciones de la red virtual mediante vínculos, subredes y puertos virtuales. La plataforma en la nube de OpenStack se utiliza como VIM.

Kaspersky SD-WAN tiene una arquitectura de microservicio distribuida basada en contenedores Docker (consulte la figura a continuación). Un controlador puede incluir uno, tres o cinco nodos. Para la tolerancia a errores, puede implementar nodos de controlador en máquinas virtuales o servidores físicos independientes. Puede especificar máquinas virtuales o servidores físicos para la implementación de nodos del controlador al implementar la solución, en la sección `ctl` del archivo de configuración.




Arquitectura de Kaspersky SD-WAN

# Implementar Kaspersky SD-WAN

Puede implementar Kaspersky SD-WAN mediante el archivo de instalación knaas-installer_<información de la versión> que forma parte del kit de distribución. Antes de seguir este procedimiento, debe preparar un escenario de implementación de la solución. Si tiene algún problema para preparar un escenario de implementación, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.

Un escenario de implementación de la solución consta de los siguientes pasos:

1. **Preparar el dispositivo administrador**

   Prepare el dispositivo administrador para la implementación de la solución. Puede usar una máquina virtual local o remota, o una computadora personal como dispositivo administrador. Cuando implementa un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo-en-uno, debe usar una máquina virtual como dispositivo administrador.

2. **Garantizar la conectividad de la red entre el dispositivo administrador y los componentes de la solución**

   Garantice la conectividad de la red entre el dispositivo administrador y las máquinas virtuales o los servidores físicos en los que desea implementar los componentes de Kaspersky SD-WAN. Si tiene pensado implementar varios nodos de componentes de la solución, asegúrese de que los vínculos entre las máquinas virtuales o los servidores físicos cumplan con los requisitos de hardware y software.

   > Las máquinas virtuales o los servidores físicos deben implementarse en un segmento de red de confianza para no poner en riesgo el tráfico transmitido.

3. **Generar contraseñas manualmente**

   Si es necesario, genere contraseñas manualmente para garantizar la seguridad de los componentes de Kaspersky SD-WAN y sus certificados SSL.

4. **Preparar el archivo de configuración**

   Prepare el archivo de configuración de acuerdo con el escenario de implementación elegido. Puede usar archivos de configuración de ejemplo para escenarios de implementación típicos en los directorios Inventory/external/pnf e inventory/external/vnf del archivo de instalación.

5. **Reemplazar los gráficos de la interfaz web del orquestador**

   Si es necesario, reemplace los gráficos de la interfaz web del orquestador. Por ejemplo, puede reemplazar la imagen que se muestra en segundo plano cuando se produce un error durante el registro en la interfaz web del orquestador.

6. **Implementar Kaspersky SD-WAN**

   Haga lo siguiente en el dispositivo administrador:

   1. Acepte el Contrato de licencia de usuario final; para ello, ejecute el siguiente comando:

      ```
      export KNAAS_EULA_AGREED="true"
      ```

   2. Vaya al directorio con el archivo de instalación extraído.

3. Si desea implementar Kaspersky SD-WAN en modo atendido, realice una de las siguientes acciones:

   - Si generó las contraseñas manualmente, ejecute el comando:

     ```
     ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
     "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
     ```

     Cuando ejecute el comando, ingrese la contraseña de la cuenta raíz y la contraseña maestra generada.

   - Si no generó las contraseñas manualmente, ejecute el comando:

     ```
     ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
     "@inventory/external/images.yml" -K knaas/knaas-install.yml
     ```

4. Si desea implementar Kaspersky SD-WAN en modo desatendido, realice una de las siguientes acciones:

   Recomendamos usar este modo solo en un entorno de confianza, ya que de lo contrario los piratas informáticos pueden interceptar sus contraseñas.

   - Si generó las contraseñas manualmente, ejecute el comando:

     ```
     ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
     vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

   - Si no generó las contraseñas manualmente, ejecute el comando:

     ```
     ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword"
     knaas/knaas-install.yml
     ```

Los componentes de Kaspersky SD-WAN se implementan en las máquinas virtuales o los servidores físicos que especificó en el archivo de configuración. Se muestra un mensaje de implementación exitosa en la consola del dispositivo administrador.

Si ocurre un problema de conectividad de la red con una de las máquinas virtuales o los servidores físicos durante la implementación de los componentes de la solución, se muestra un mensaje de error en la consola del dispositivo administrador y la solución no se implementa. En ese caso, debe restaurar la conectividad de la red, limpiar las máquinas virtuales o los servidores físicos y luego volver a ejecutar el comando de implementación.

# Redundancia de los componentes de la solución

## Acerca de los esquemas de redundancia para los componentes de la solución

Kaspersky SD-WAN admite dos escenarios de implementación para los componentes de la solución:

- En el escenario de implementación *N + 1*, usted implementa dos nodos del componente de la solución. Si un nodo falla, el segundo nodo proporciona la funcionalidad del componente de la solución.
- En el escenario de implementación *2N + 1*, usted implementa varios nodos del componente de la solución. Un nodo es el nodo principal y el resto son nodos secundarios. Si el nodo principal falla, un nodo secundario elegido al azar ocupa su lugar. Este esquema de redundancia permite que los componentes de la solución permanezcan operativos incluso cuando ocurren varios errores seguidos.

La siguiente tabla enumera los componentes de la solución y los escenarios de implementación que les son aplicables.

| Componente de la solución | Esquema de redundancia |
|---|---|
| Base de datos del sistema de supervisión Zabbix | 2N + 1 |
| Servidor Zabbix | N + 1 |
| Parte frontend del sistema de supervisión Zabbix | N + 1 |
| Servidor proxy Zabbix | N + 1 |
| Base de datos MongoDB | 2N + 1 |
| Base de datos Redis:<br>• Servidor de réplica Redis<br>• Sistema Redis Sentinel | 2N + 1 |
| Controlador | 2N + 1 |
| Parte frontend de la solución | N + 1 |
| Orquestador | N + 1 |
| Administrador de funciones de red virtual | N + 1 |
| Proxy de Administrador de funciones de red virtual | N + 1 |

Puede especificar el número de nodos que desea implementar para cada componente de la solución en el archivo de configuración.

Cuando establece la configuración de implementación para la base de datos MongoDB o el nodo controlador de acuerdo con el escenario de implementación 2N+1, el último nodo que especifique se convierte en el nodo árbitro. El *nodo árbitro* está vinculado a otros nodos y se utiliza para elegir el nodo principal. Un nodo que perdió contacto con el nodo árbitro entra en modo de espera. Uno de los nodos que mantuvo contacto con el nodo árbitro permanece o se convierte en el nodo principal. Un nodo árbitro no puede convertirse en un nodo principal y no almacena datos.

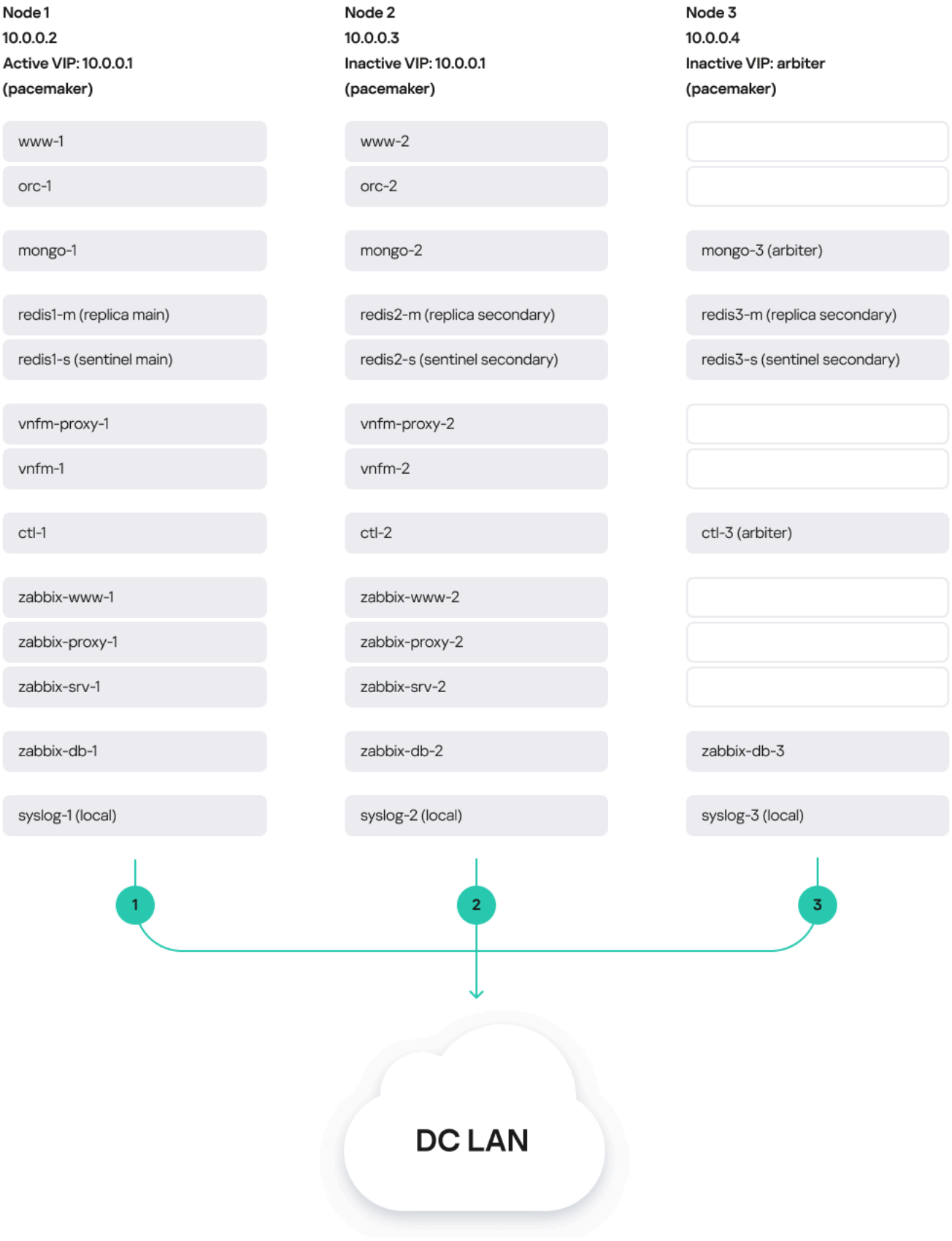
## Escenarios de fallo de los nodos de componentes de la solución

La siguiente figura muestra un diagrama de Kaspersky SD-WAN implementado en tres máquinas virtuales en un centro de datos. El diagrama utiliza los siguientes símbolos:

- "www" es la parte frontend de la solución
- "orc" es el orquestador
- "mongo" es la base de datos de MongoDB
- "redis-m" es un servidor de réplica de Redis
- "redis-s" es un sistema Redis Sentinel
- "vnfm-proxy" es un proxy de administrador de funciones de red virtual
- "vnfm" es un Administrador de funciones de red virtual
- "ctl" es el controlador y su base de datos
- "zabbix-www'" es la parte frontend del sistema de supervisión de Zabbix

- "zabbix-proxy" es el servidor proxy Zabbix
- "zabbix-srv" es el servidor Zabbix
- "zabbix-db" es la base de datos del sistema de supervisión Zabbix
- "syslog" es el servidor syslog

Los usuarios y los dispositivos CPE obtienen acceso a la interfaz web del orquestador y a la interfaz web del sistema de supervisión Zabbix usando una dirección IP virtual. La dirección IP virtual se asigna a la máquina virtual 1.




Solución implementada en tres máquinas virtuales

En este escenario de implementación, son posibles los siguientes modos de fallo:

- **Fallo de la máquina virtual 1 o su vínculo**.

  Si la máquina virtual 1 o su vínculo fallan, la solución permanece operativa. Los siguientes cambios ocurren en el estado de los nodos de los componentes de la solución:

  - La dirección IP virtual se asigna a la máquina virtual 2.
  - El nodo www-1 de la parte frontend no está disponible; www-2 está disponible. La interfaz web del orquestador se muestra en el navegador.
  - El nodo del orquestador orc-1 no está disponible; orc-2 está disponible. La parte backend de la solución es funcional, los usuarios pueden iniciar sesión en la interfaz web del orquestador y administrarla.
  - El nodo mongo-1 de la base de datos MongoDB no está disponible; mongo-2 y mongo-3 están disponibles; mongo-2 se convierte en el nodo principal porque mongo-3 es el nodo árbitro y no puede convertirse en el nodo principal. El orquestador continúa usando la base de datos MongoDB.
  - Estado de la base de datos Redis:
    - El nodo redis1-m del servidor de réplica de Redis no está disponible; redis2-my redis3-m están disponibles.
    - El nodo redis1-s del sistema Redis Sentinel no está disponible; redis2-s y redis3-s están disponibles; redis2-s se convierte en el nodo principal y asigna aleatoriamente el nodo redis2-mo el nodo redis3-m del servidor de réplica de Redis como nodo principal.

    El orquestador continúa usando la base de datos Redis.
  - Estados del Administrador de funciones de red virtual:
    - El nodo vnfm-proxy-1 del proxy del administrador de funciones de red virtual no está disponible; vnfm-proxy-2 está disponible.
    - El nodo Administrador de funciones de red virtual vnfm-1 no está disponible; vnfm-2 está disponible.

    Las consolas SSH de los componentes de la solución están operativas.
  - El nodo ctl-1 del controlador no está disponible; ctl-2 y ctl-3 están disponibles; ctl-2 se convierte en el nodo principal porque ctl-3 es el nodo árbitro y no puede convertirse en el nodo principal. Se mantiene la conexión física entre los dispositivos CPE.
  - Estado del sistema de supervisión Zabbix:
    - El nodo zabbix-www-1 de la parte frontend de la solución no está disponible; zabbix-www-2 está disponible.
    - El nodo zabbix-proxy-1 del servidor proxy Zabbix no está disponible; zabbix-proxy-2 está disponible.
    - El nodo zabbix-srv-1 del servidor Zabbix no está disponible; zabbix-srv-2 está disponible.
    - El nodo zabbix-db-1 de la base de datos del sistema de supervisión Zabbix no está disponible; zabbix-db-2 está disponible.

    El sistema de supervisión Zabbix está operativo.

- **Fallo de la máquina virtual 2 o 3, o su vínculo**.

  Si la máquina virtual 2 o 3 o su vínculo fallan, los nodos de los componentes de la solución que se implementan en la máquina virtual 1 permanecen principales y la solución permanece operativa.

- **Fallo simultáneo de las máquinas virtuales 1 y 3 o 2 y 3 o sus vínculos**.

  Si las máquinas virtuales 1 y 3 o las máquinas virtuales 2 y 3, o sus vínculos fallan simultáneamente, la solución deja de funcionar. Los siguientes cambios ocurren en el estado de los nodos de los componentes de la solución:

  - La interfaz web del orquestador no se muestra en el navegador. Los usuarios no pueden iniciar sesión en la interfaz web del orquestador y administrarla.
  - El sistema de supervisión Zabbix deja de funcionar.
  - Se mantiene la conexión de red entre los dispositivos CPE y los dispositivos de red conectados a ellos; el tráfico continúa transmitiéndose.
  - Se mantiene la conexión de red dentro de los servicios P2P y servicios TAP.
  - La conexión de red dentro de los servicios P2M y servicios M2M se mantiene durante las sesiones establecidas. Para las sesiones nuevas, la conexión de la red se mantiene si, al crear el servicio P2P o el servicio M2M, en la lista desplegable **Modo de aprendizaje de MAC**, seleccionó **Aprender e inundar**.
  - Los dispositivos CPE utilizan un mecanismo de compensación de reordenamiento para reducir la cantidad de paquetes duplicados en los dispositivos de red conectados a los dispositivos CPE.
  - La carga en los dispositivos CPE y la red SD-WAN aumenta proporcionalmente a la cantidad de dispositivos y vínculos CPE.

  Si se restauran los vínculos, la solución también se restaura y se reanuda el funcionamiento normal.

  Si las máquinas virtuales 1 y 3 o las máquinas virtuales 2 y 3 fallan simultáneamente, la configuración de los componentes de la solución se pierde. Para restaurar la configuración de los componentes de la solución, puede comunicarse con Kaspersky Professional Services.

- **Fallo simultáneo de las máquinas virtuales 1 y 2**

  Si las máquinas virtuales 1 y 2 fallan simultáneamente, la configuración de los componentes de la solución se pierde irreversiblemente porque la máquina virtual 3 tiene un árbitro que no almacena datos. Para evitar esta situación, recomendamos implementar bases de datos y controladores en máquinas virtuales o servidores físicos separados y realizar copias de seguridad periódicas.

# Configurar el equilibrio de carga entre las instancias del orquestador

Para mejorar el rendimiento en entornos de producción con muchos dispositivos CPE, cuando implementa la solución, puede crear varias instancias de contenedor del orquestador para distribuir la carga entre ellas. Cada instancia del contenedor del orquestador puede servir hasta 5000 dispositivos CPE.

Las instancias del contenedor se combinan en *grupos de equilibrio*. Un grupo de equilibrio incluye un contenedor `www` y de uno a cinco contenedores de orquestador. El número de grupos de equilibrio depende del esquema de implementación: 1 para un esquema todo-en-uno, 2 para un esquema de alta disponibilidad. Los nombres del contenedor siguen el patrón `orc-nm`, donde `n` representa el número del grupo de equilibrio y `m` representa el número ordinal de la instancia del contenedor dentro del grupo, si el grupo incluye más de una instancia. Ejemplos: `orc-12` (contenedor del primer grupo de equilibrio, segunda instancia); `orc-2` (la única instancia de contenedor del segundo grupo de equilibrio).

Cuando implementa Kaspersky SD-WAN, los grupos de equilibrio se pueden implementar de dos maneras:

- Implementar el contenedor `www` y los contenedores del orquestador del grupo de equilibrio en el mismo nodo.

  Si desea seleccionar esta opción para implementar un grupo de equilibrio, cuando edite el archivo de configuración, en la variable `number_of_containers`, debe especificar el número de contenedores que se deben implementar para el grupo de equilibrio en el nodo correspondiente (de 1 a 5).

- El contenedor `www` y cada uno de los contenedores del orquestador del grupo de equilibrio se implementan en un nodo independiente.

  Esta opción se puede usar para escalar de forma horizontal y hacer un uso más eficiente de los recursos. Si desea seleccionar esta opción para implementar un grupo de equilibrio, cuando edite el archivo de configuración, en la variable `ansible_host` en las secciones `orc_1` y `orc_2`, debe enumerar los nodos relevantes de la sección `nodes` en los que desea implementar las instancias de los contenedores del orquestador. Solo se puede implementar una instancia de contenedor del orquestador en cada nodo especificado.

  Si se especifica más de un nodo en la variable `ansible_host`, se ignora la configuración `de number_of_containers`.

# Acerca del archivo de instalación

El archivo de instalación knaas-installer_ <información de versión> tiene el formato TAR y se utiliza para la implementación de la solución. Puede descargar el archivo de instalación desde el directorio raíz del kit de distribución. El archivo de instalación tiene la siguiente estructura:

No recomendamos editar los archivos del sistema porque esto puede causar errores en la implementación de la solución.

- El archivo ansible.cfg es un archivo del sistema con la configuración de Ansible.
- CHANGELOG.md es el registro de cambios de archivo en formato YAML.
- /docs contiene la documentación del archivo de instalación.
- /images contiene imágenes de los componentes de la solución.

- /inventory:
  - /external:
    - /pnf contiene archivos de configuración de ejemplo para escenarios típicos de implementación de la solución con el controlador como una función de la red física.
    - /vnf contiene archivos de configuración de ejemplo para escenarios típicos de implementación de la solución con el controlador como una función de la red virtual.
- /generic contiene archivos comunes del sistema.
- /knaas contiene archivos del sistema con manuales para implementar la solución.
- /oem contiene gráficos predeterminados de la interfaz web del orquestador.
- /pnfs contiene funciones de la red física para la implementación de uno, tres o cinco nodos de controlador.
- README.md contiene instrucciones para implementar la solución mediante el archivo de instalación.
- requirements.txt es un archivo del sistema con requisitos de Python.

# Acerca de los modos de acción atendido, desatendido y parcialmente atendido

Si realiza acciones en el dispositivo administrador cuando implementa Kaspersky SD-WAN, es posible que deba ingresar la contraseña raíz así como la contraseña principal. La forma en que se ingresan las contraseñas depende del modo en que esté realizando la acción. Se admiten los siguientes modos de acción:

- En el modo atendido, un empleado debe participar en la acción. Para realizar una acción, debe ingresar manualmente la contraseña raíz y la contraseña principal. Este es el modo más seguro que evita guardar contraseñas en el dispositivo administrador.
- En el modo desatendido, la acción se realiza sin involucrar a un empleado. Para realizar una acción, la contraseña raíz y la contraseña principal se ingresan automáticamente. En este modo, puede ejecutar pruebas automatizadas.

  Recomendamos usar este modo solo en un entorno de confianza, ya que de lo contrario los piratas informáticos pueden interceptar sus contraseñas.

- En el modo parcialmente atendido, la acción se realiza con la participación parcial de un empleado. Cuando realiza una acción, debe ingresar la contraseña raíz, pero la contraseña principal se ingresa automáticamente.

# Preparar el dispositivo administrador

Puede usar una máquina virtual local o remota, o una computadora personal como dispositivo administrador. Cuando implementa un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo-en-uno, debe usar una máquina virtual como dispositivo administrador.

Si tiene algún problema mientras prepara el dispositivo administrador, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.

*Para preparar el dispositivo administrador, siga estos pasos:*

1. Asegúrese de que el dispositivo administrador cumpla con los requisitos de hardware y software.
2. Asegúrese de que se use la misma cuenta raíz en el dispositivo administrador y en las máquinas virtuales o los servidores físicos en los que desea implementar los componentes de Kaspersky SD-WAN. Después de implementar la solución, puede usar una cuenta raíz diferente en las máquinas virtuales o en los servidores físicos.
3. Descargue el archivo de instalación knaas-installer_<información de la versión> del directorio raíz del kit de distribución y extraiga el archivo de instalación en el dispositivo administrador.
4. Vaya al directorio que tiene el archivo de instalación extraído y prepare el dispositivo administrador:
   a. Asegúrese de que la herramienta de administración de paquetes pip esté instalada; para ello, ejecute el comando:
      ```
      python3 -m pip -V
      ```
   b. Si la herramienta de administración de paquetes pip no está presente, realice una de las siguientes acciones:
      - Si el dispositivo administrador ejecuta Ubuntu:
        ```
        apt-get install python3-pip
        ```
      - Si el dispositivo administrador ejecuta RED OS 8:
        ```
        yum install python3-pip
        ```
   c. Instale la herramienta Ansible y sus dependencias:
      ```
      python 3 -m pip install -U --user -r requirements.txt
      ```
   d. Actualice la variable PATH:
      1. `echo 'export PATH=$PATH:$HOME/.local/bin' >> ~/.bashrc`
      2. `source ~/.bashrc`
   e. Verifique que la herramienta Ansible esté lista para usar:
      ```
      ansible --version
      ```
   f. Instale los paquetes del sistema operativo para la implementación de Kaspersky SD-WAN en el dispositivo administrador:

```
ansible-playbook -K knaas/utilities/toolserver_prepare/bootstrap.yml
```

Ingrese la contraseña raíz cuando ejecute el comando.

Solo necesita completar este paso cuando implementa la solución por primera vez.

5. Asegúrese de que el dispositivo administrador esté listo para usar:

   a. Reinicie el dispositivo administrador.

   b. Vaya al archivo de instalación extraído e inicie la verificación automática del dispositivo administrador:

   ```
   ansible-playbook knaas/utilities/pre-flight.yml
   ```

6. Si desea implementar Kaspersky SD-WAN en múltiples máquinas virtuales o servidores físicos:

   a. Asegúrese de que las claves SSH se hayan generado en el dispositivo administrador. Si las claves SSH no existen, genérelas.

   b. Coloque las claves SSH en las máquinas virtuales o los servidores físicos:

   ```
   ssh-copy-id user@<dirección IP de la máquina virtual o del servidor físico>
   ```

Si está implementando un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo-en-uno, omita este paso.

El dispositivo administrador está preparado para la implementación de Kaspersky SD-WAN.

# Administrar contraseñas

Las contraseñas ayudan a garantizar la seguridad de los componentes de Kaspersky SD-WAN implementados. Puede generar las contraseñas manualmente. Si no genera manualmente las contraseñas, se generan de forma automática cuando implementa la solución.

Las contraseñas están contenidas en los siguientes archivos:

- keystore.yml contiene las contraseñas de los componentes de Kaspersky SD-WAN y sus certificados SSL.
- vault_password.txt contiene la contraseña principal.

Recomendamos almacenar los archivos de contraseñas en un directorio protegido, ya que se pueden usar para obtener acceso a la solución implementada.

Después de la implementación, las contraseñas generadas se colocan automáticamente en los contenedores Docker de los componentes de Kaspersky SD-WAN. Los componentes de la solución intercambian contraseñas cuando interactúan entre sí.

# Generar contraseñas manualmente

*Para generar manualmente las contraseñas, siga estos pasos:*

1. Cree el directorio /passwords en el dispositivo administrador. Especifique la ruta al directorio creado en la sección `external` del archivo de configuración mediante la configuración `vault_password_dirname`.
2. Cree un archivo keystore.yml y, en ese archivo, especifique las contraseñas con la siguiente configuración:
   - `ZABBIX_DB_SECRET` es la contraseña raíz de la base de datos del sistema de supervisión Zabbix.
   - `MONGO_ADMIN_SECRET` es la contraseña de administrador de la base de datos MongoDB.
   - `MONGO_USER_SECRET` es la contraseña de usuario de la base de datos MongoDB. El orquestador utiliza esta contraseña.
   - `CTL_CERT_SECRET` es la contraseña del certificado SSL del controlador.
   - `ORC_CERT_SECRET` es la contraseña del certificado SSL del orquestador.
   - `ORC_ENC_SECRET` es la contraseña para cifrar datos confidenciales en la base de datos MongoDB. Longitud mínima: 32 caracteres.
   - `VNFM_CERT_SECRET` es la contraseña del certificado SSL de VNFM.

   Para todas las contraseñas, excepto `ORC_ENC_SECRET`, recomendamos especificar al menos 16 caracteres.
3. Cree el archivo vault_password.txt y, en ese archivo, especifique la contraseña principal.
4. Cifre el archivo keystore.yml:
   - Si desea cifrar el archivo keystore.yml en modo atendido:

     ```
     ansible-vault encrypt --ask-vault-pass keystore.yml
     ```
   - Si desea cifrar el archivo keystore.yml en modo desatendido:

     ```
     ansible-vault encrypt --vault-password-file vault_password.txt keystore.yml
     ```

Las contraseñas se generan y cifran.

# Cambiar contraseñas

*Para cambiar las contraseñas, siga estos pasos:*

1. Descifre el archivo keystore.yml:
   - Si desea descifrar el archivo keystore.yml en modo atendido:

     ```
     ansible-vault decrypt --vault-password-file vault_password.txt keystore.yml
     ```

- Si desea descifrar el archivo keystore.yml en modo desatendido:

  ```
  ansible-vault encrypt --ask-vault-pass keystore.yml
  ```

2. Cambie las siguientes contraseñas en el archivo keystore.yml:

   - `ZABBIX_DB_SECRET` es la contraseña raíz de la base de datos del sistema de supervisión Zabbix.
   - `MONGO_ADMIN_SECRET` es la contraseña de administrador de la base de datos MongoDB.
   - `MONGO_USER_SECRET` es la contraseña de usuario de la base de datos MongoDB. El orquestador utiliza esta contraseña.
   - `CTL_CERT_SECRET` es la contraseña del certificado SSL del controlador.
   - `ORC_CERT_SECRET` es la contraseña del certificado SSL del orquestador.
   - `ORC_ENC_SECRET` es la contraseña para cifrar datos confidenciales en la base de datos MongoDB. Longitud mínima: 32 caracteres.
   - `VNFM_CERT_SECRET` es la contraseña del certificado SSL de VNFM.

   Para todas las contraseñas, excepto `ORC_ENC_SECRET`, recomendamos especificar al menos 16 caracteres.

3. Cifre el archivo keystore.yml:

   - Si desea cifrar el archivo keystore.yml en modo atendido:

     ```
     ansible-vault encrypt --ask-vault-pass keystore.yml
     ```

   - Si desea cifrar el archivo keystore.yml en modo desatendido:

     ```
     ansible-vault encrypt --vault-password-file vault_password.txt keystore.yml
     ```

   Las contraseñas se cambian y se cifran.

# Preparar el archivo de configuración

Especifique la configuración de implementación de Kaspersky SD-WAN en el archivo de configuración YAML del dispositivo administrador. La ruta al archivo de configuración debe especificarse cuando implementa la solución. Puede usar archivos de configuración de ejemplo para escenarios de implementación típicos en los directorios Inventory/external/pnf e inventory/external/vnf del archivo de instalación.

El archivo de configuración consta de dos secciones principales:

- En la sección `nodes` se especifican las máquinas virtuales o los servidores físicos para implementar los componentes de Kaspersky SD-WAN. Cuando implementa la solución en máquinas virtuales o servidores físicos, las reglas de iptables para la interacción entre los componentes de la solución se generan automáticamente.

- En la sección `external` se especifica la configuración de la implementación de Kaspersky SD-WAN.

No recomendamos cambiar la configuración predeterminada.

La sección `nodes` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `node_ < número de máquina virtual o servidor físico >` | | | Configuración de implementación de la máquina virtual o del servidor físico. |
| | `ip` | | Dirección IP de la máquina virtual o del servidor físico. Ingrese un valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126` |
| | `vip` | | Dirección IP virtual de la máquina virtual o del servidor físico. Ingrese un valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126`<br>Esta configuración debe especificarse para todas las máquinas virtuales o servidores físicos en los que tiene pensado usar direcciones IP virtuales. |
| | `knaas_aio_int` | | Configuración para conectar los contenedores Docker de los componentes de Kaspersky SD-WAN a la red virtual local de la máquina virtual o del servidor físico. |
| | | `base` | Los primeros tres octetos de la dirección IP de la red virtual local. Valor predeterminado: `10.11.11`. Ingrese un valor en el formato `XXX.XXX.XXX`, por ejemplo:<br>`192.168.110`<br>Puede cambiar los primeros tres octetos de la dirección IP predeterminada si se superponen con su espacio de direcciones. |
| | | `mode` | Modo de funcionamiento de la red virtual local. Valores posibles:<br>• `bridge` significa que se crea un puente de Linux en la máquina virtual o el servidor físico. Los contenedores de Docker se conectan al puente de Linux a través de una conexión de red L3 mediante NAT e iptables.<br>• `vlan` significa que los contenedores Docker se conectan a la interfaz de la máquina virtual o el servidor físico a través de una red L2 utilizando el controlador macvlan. Recomendamos elegir esta opción solo cuando se usa una red L2 de confianza, ya que en este caso no se usa ningún firewall en la máquina virtual o el servidor físico. |
| | | `iface` | Nombre de la interfaz de la máquina virtual o del servidor físico para conectar los contenedores Docker a través de la red L2, por ejemplo:<br>`enp6s0`<br>Este parámetro debe especificarse si, para `mode`, eligió `vlan`. |
| | | `vlan` | Etiqueta VLAN de la red L2. Ingrese un valor en el rango de 1 a 4095. Si no desea usar una etiqueta VLAN, ingrese `0`.<br>Este parámetro debe especificarse si, para `mode`, eligió `vlan`. |
| | `knaas_os_man` | | Configuración conectar los contenedores Docker de componentes de los de Kaspersky SD-WAN a la red virtual de administración o al servidor físico de la máquina virtual. |
| | | `base` | Los primeros tres octetos de la dirección IP de la red virtual de administración. Valor predeterminado: `10.11.11`. Ingrese un valor en el formato `XXX.XXX.XXX`, por ejemplo:<br>`192.168.110`<br>Puede cambiar los primeros tres octetos de la dirección IP predeterminada si se superponen con su espacio de direcciones. |
| | | `mode` | Modo de funcionamiento de la red virtual de administración. Valores posibles:<br>• `bridge` significa que se crea un puente de Linux en la máquina virtual o el servidor físico. Los contenedores de Docker se conectan al puente de Linux a través de una conexión de red L3 mediante NAT e iptables.<br>• `vlan` significa que los contenedores Docker se conectan a la interfaz de la máquina virtual o el servidor físico a través de una red L2 utilizando el controlador macvlan. Recomendamos elegir esta opción solo cuando se usa una red L2 de confianza, ya que en este caso no se usa ningún firewall en la máquina virtual o el servidor físico. |
| | | `iface` | Nombre de la interfaz de la máquina virtual o del servidor físico para conectar los contenedores Docker a través de la red L2, por ejemplo:<br>`enp6s0`<br>Este parámetro debe especificarse si, para `mode`, eligió `vlan`. |
| | | `vlan` | Etiqueta VLAN de la red L2. Ingrese un valor en el rango de 1 a 4095. Si no desea usar una etiqueta VLAN, ingrese `0`.<br>Este parámetro debe especificarse si, para `mode`, eligió `vlan`. |

La sección `external` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `vault_passwords_dirname` | | | Ruta al directorio /passwords en el dispositivo administrador con contraseñas generadas manualmente. Si no genera las contraseñas manualmente, se generan de forma automática durante la implementación de la solución y se colocan en el directorio /passwords del archivo de instalación extraído en el dispositivo administrador. |
| `ansible_user` | | | Nombre de la cuenta de usuario en el dispositivo administrador y en las máquinas virtuales o servidores físicos para ejecutar los manuales durante la implementación de la solución. |
| `ssl` | | | Configuración de los certificados SSL de los componentes de Kaspersky SD-WAN. |
| | `san_list` | | Información que se agrega a los certificados SSL. |
| | | `ip` | Direcciones IP que se agregan a los certificados SSL. Especifique una lista de valores en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`ip`<br>`- 192.168.2.0`<br>`- 192.168.2.1` |
| | | `dns` | Nombres de dominio que se agregan a los certificados SSL. Especifique una lista de valores, por ejemplo:<br>`dns:`<br>`- sdwan.kaspersky.com`<br>`- kaspersky.sdwan.com` |
| | `path_local` | | Ruta al directorio del dispositivo administrador que contiene los certificados SSL generados manualmente. Si no genera certificados SSL manualmente, se generan de forma automática durante la implementación de la solución y se colocan en el directorio /ssl del archivo de instalación extraído en el dispositivo administrador. |
| | `path_remote` | | Ruta al directorio en las máquinas virtuales o servidores físicos que contiene certificados SSL generados manualmente. Si no genera certificados SSL manualmente, se generan de forma automática durante la implementación de la solución y se colocan en el directorio /ssl en máquinas virtuales o los servidores físicos. |
| `syslog` | | | Configuración del servidor syslog. |
| | `docker_memory_limit` | | Cantidad de RAM en megabytes para contenedores Docker del servidor syslog. |
| | `max_log_size` | | Cantidad de RAM en gigabytes para los registros del servidor syslog. |
| | `state` | | Implementación de un servidor syslog en máquinas virtuales o servidores físicos. Valores posibles:<br>• `enabled`<br>• `disabled` |
| `zabbix` | | | Configuración del sistema de supervisión Zabbix. Para obtener más información, consulte la documentación oficial de la solución Zabbix. |

| | |
|---|---|
| `syslog_server_address` | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| `secure_syslog` | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| `syslog_server_ca_cert_file_path` | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| `syslog_format` | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| `db_docker_memory_limit` | Cantidad de RAM en megabytes para contenedores Docker de la base de datos del sistema de supervisión Zabbix. |
| `srv_docker_memory_limit` | Cantidad de RAM en megabytes para contenedores Docker del servidor Zabbix. |
| `www_docker_memory_limit` | Cantidad de RAM en megabytes para contenedores Docker de la interfaz del sistema de supervisión Zabbix. |
| `proxy_docker_memory_limit` | Cantidad de RAM en megabytes para contenedores Docker del servidor proxy Zabbix. |
| `cachesize` | Cantidad de RAM en gigabytes para la caché del sistema de supervisión Zabbix. Ingrese un valor en el formato `< gigabytes >`, por ejemplo:<br>`8G` |
| `zabbix_<1-3>` | Configuración de implementación de los nodos del sistema de supervisión Zabbix. Puede implementar un nodo del sistema de supervisión Zabbix sin alta disponibilidad o tres nodos con alta disponibilidad. |

| | | | |
|---|---|---|---|
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el sistema de supervisión Zabbix. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| | | `db` | Configuración de implementación de la base de datos del sistema de supervisión Zabbix. |
| | | `inventory_hostname` | Nombre de host de la base de datos del sistema de supervisión Zabbix. Valor predeterminado: `zabbix-db-<1-3>`. |
| | | `state` | Implementación de la base de datos del sistema de supervisión Zabbix en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `srv` | Configuración de implementación del servidor Zabbix. Cuando implementa tres nodos del sistema de supervisión Zabbix, solo necesita especificar esta configuración para dos de los nodos. |
| | | `inventory_hostname` | Nombre de host del servidor Zabbix. Valor predeterminado: `zabbix-srv-<1-3>`. |
| | | `state` | Implementación del servidor Zabbix en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `www` | Configuración de implementación de la interfaz del sistema de supervisión Zabbix. Cuando implementa tres nodos del sistema de supervisión Zabbix, solo necesita especificar esta configuración para dos de los nodos. |
| | | `inventory_hostname` | Nombre de host de la interfaz del sistema de supervisión Zabbix. Valor predeterminado: `zabbix-www-<1-3>`. |
| | | `state` | Implementación de la interfaz del sistema de supervisión Zabbix en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `proxy` | Configuración de implementación del servidor proxy Zabbix. Cuando implementa tres nodos del sistema de supervisión Zabbix, solo necesita especificar esta configuración para dos de los nodos. |
| | | `inventory_hostname` | Nombre de host del servidor proxy Zabbix. Valor predeterminado: `zabbix-proxy-<1-3>`. |
| | | `state` | Implementación del servidor proxy Zabbix en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| `mongo` | | | Configuración de la base de datos MongoDB. Para obtener más información, consulte la documentación oficial de la base de datos MongoDB. |

| | | | |
|---|---|---|---|
| | `syslog_server_address` | | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `<protocolo>://<dirección del host>:<número de puerto>`. Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| | `secure_syslog` | | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| | `syslog_server_ca_cert_file_path` | | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| | `syslog_format` | | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| | `docker_memory_limit` | | Cantidad de RAM en megabytes para contenedores Docker de la base de datos MongoDB. |
| | `mongo_<1-3>` | | Configuración de implementación de los nodos de la base de datos MongoDB. Puede implementar un nodo de base de datos MongoDB sin alta disponibilidad o tres nodos con alta disponibilidad. Si implementa tres nodos de base de datos MongoDB, el último nodo se convierte en el nodo árbitro. |
| | | `inventory_hostname` | Nombre de host de la base de datos MongoDB. Valor predeterminado: `mongo-<1-3>` |
| | | `state` | Implementación de la base de datos MongoDB en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar la base de datos MongoDB. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| `redis` | | | Configuración de la base de datos de Redis. Para obtener más información, consulte la documentación oficial de la base de datos de Redis. |

| | | |
|---|---|---|
| | `syslog_server_address` | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| | `secure_syslog` | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| | `syslog_server_ca_cert_file_path` | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| | `syslog_format` | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| | `docker_memory_limit` | Cantidad de RAM en megabytes para contenedores Docker de la base de datos de Redis. |
| | `redis_<1-3>m` | Configuración de implementación para los nodos del servidor de réplica de Redis. Puede implementar un nodo del servidor de réplica de Redis sin alta disponibilidad o tres nodos con alta disponibilidad. |
| | `inventory_hostname` | Nombre de host del servidor de réplica de Redis. Valor predeterminado: `redis- <1-3>m`. |
| | `state` | Implementación del servidor de réplica de Redis en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el servidor de réplica de Redis. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| | `redis_<1-3>s` | Configuración de implementación de los nodos del sistema Redis Sentinel. Si implementará tres nodos del servidor de réplica de Redis con alta disponibilidad, también debe implementar tres nodos del sistema Redis Sentinel. |

| | | | |
|---|---|---|---|
| | | `inventory_hostname` | Nombre de host del sistema Redis Sentinel. Valor predeterminado: `redis-<1-3>s`. |
| | | `state` | Implementar el sistema Redis Sentinel en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el sistema Redis Sentinel. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| `ctl` | | | Configuración de implementación del controlador. Para implementar una instancia SD-WAN para un inquilino, debe implementar el controlador como una función de la red física.<br>Junto con cada nodo del controlador, el componente MOCKPNF se implementa automáticamente en la máquina virtual o el servidor físico para garantizar la seguridad de la configuración del contenedor Docker del nodo del controlador. |

| | | | |
|---|---|---|---|
| `tenants` | | | Configuración de inquilinos para los que está implementando instancias SD-WAN. |
| `- name` | | | Nombre del inquilino. |
| | `state` | | Creación de un inquilino e implementación del controlador en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | `ctl_base` | | Los primeros tres octetos de la dirección IP de la red virtual del controlador. Ingrese un valor en el formato `XXX.XXX.XXX`, por ejemplo:<br>`192.168.110`<br>Cuando implementa un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo en uno, el valor de esta configuración puede ser el mismo que el valor de la configuración `base` en la sección `nodes`. |
| | `mock_base` | | Los primeros tres octetos de la dirección IP de la red virtual de administración del controlador. Ingrese un valor en el formato `XXX.XXX.XXX`, por ejemplo:<br>`192.168.110` |
| | `hosts` | | Configuración de implementación del controlador. Puede implementar un nodo de controlador sin alta disponibilidad o, de forma alternativa, tres o cinco nodos con alta disponibilidad. Si implementa tres o cinco nodos de controlador, el último nodo se convierte en el nodo árbitro. |
| | `- inventory_hostname` | | Nombre de host del nodo del controlador. Valor predeterminado: `ctl-<1-5>`. |
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el nodo del controlador. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| | `docker_memory_limit` | | Cantidad de RAM en megabytes para los contenedores Docker del controlador. |
| | `JAVA_OPTS` | | Configuración de RAM de la máquina virtual Java. |
| | | `Xms` | La cantidad mínima de memoria dinámica que la máquina virtual Java puede asignar al controlador. Ingrese un valor en uno de los siguientes formatos:<br>• `<cantidad de RAM>m` es la cantidad de RAM en megabytes, por ejemplo: `512m`<br>• `<cantidad de RAM>g` es la cantidad de RAM en gigabytes, por ejemplo: `2g`<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de `Xmx`. |
| | | `Xmx` | La cantidad máxima de memoria dinámica que la máquina virtual Java puede asignar al controlador. Ingrese un valor en uno de los siguientes formatos:<br>• `<cantidad de RAM>m` es la cantidad de RAM en megabytes, por ejemplo: `512m`<br>• `<cantidad de RAM>g` es la cantidad de RAM en gigabytes, por ejemplo: `4g`<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de `docker_memory_limit`. |
| | | `MaxDirectMemorySize` | La cantidad máxima de memoria directa que la máquina virtual Java puede asignar al controlador. Ingrese un valor en uno de los siguientes formatos:<br>• `<cantidad de RAM>m` es la cantidad de RAM en megabytes, por ejemplo: `512m`<br>• `<cantidad de RAM>g` es la cantidad de RAM en gigabytes, por ejemplo: `4g`<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de `docker_memory_limit`. |

| | | |
|---|---|---|
| | `syslog_server_address` | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| | `secure_syslog` | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| | `syslog_server_ca_cert_file_path` | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| | `syslog_format` | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| `www` | | Configuración de la interfaz de la solución. |

| | | |
|---|---|---|
| | `syslog_server_address` | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| | `secure_syslog` | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| | `syslog_server_ca_cert_file_path` | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| | `syslog_format` | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| | `docker_memory_limit` | Cantidad de RAM en megabytes para los contenedores Docker de la interfaz de la solución. |
| | `oem` | Configuración de visualización de los gráficos de la interfaz web del orquestador. Esta sección le permite cambiar los gráficos de la interfaz web del orquestador. |

| | | | |
|---|---|---|---|
| | | `state` | Reemplazo de los gráficos predeterminados de la interfaz web del orquestador Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `path_local` | Ruta al directorio en el dispositivo administrador con los gráficos de la interfaz web del orquestador. Puede encontrar los gráficos predeterminados de la interfaz web del orquestador en el directorio /oem del archivo de instalación extraído en el dispositivo de administrador. |
| | | `path_remote` | Ruta al directorio en máquinas virtuales o servidores físicos con los gráficos de la interfaz web del orquestador. |
| | | `title` | El título que se muestra en segundo plano cuando inicia sesión en la interfaz web del orquestador. Valor predeterminado: `Kaspersky SD-WAN`. Longitud recomendada: no más de 128 caracteres. |
| | | `support` | La dirección web que se muestra en la parte inferior de la interfaz web del orquestador. Valor predeterminado: `support.kaspersky.com`. Longitud recomendada: no más de 128 caracteres. |
| | | `assets` | Los gráficos predeterminados para la interfaz web del orquestador se reemplazan por los que colocó en este directorio en el dispositivo administrador. Valores posibles:<br>• `enabled`<br>• `disabled`<br>En el parámetro `path_local`, especifique el directorio del dispositivo administrador que contiene los gráficos de la interfaz web del orquestador. |
| | `www_<1-2>` | | Configuración de implementación de los nodos de la interfaz de la solución. Puede implementar un nodo de la parte frontend de la solución sin alta disponibilidad o dos nodos con alta disponibilidad.<br>Debe implementar los nodos frontend de la solución y los nodos del orquestador en las mismas máquinas virtuales o servidores físicos. Por ejemplo, debe implementar el primer nodo de la interfaz de la solución en la misma máquina virtual o servidor físico que el primer nodo del orquestador. Puede especificar la configuración del orquestador en la sección `orc`. |
| | | `inventory_hostname` | Nombre de host de la interfaz de la solución. Valor predeterminado: `www-<1-2>`. |
| | | `state` | Implementación de la interfaz de la solución en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `ansible_host` | Dirección IP de la máquina virtual o del servidor físico de la sección `nodes` para implementar la interfaz de la solución. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| `orc` | | | Configuración del orquestador. |

| | | |
|---|---|---|
| syslog_server_address | | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato < protocolo >://< dirección del host >:< número de puerto >. Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>udp://192.168.2.15:1514<br>tcp+tls://my-syslog-server:1514<br>Si la variable secure_syslog se establece en true, debe especificar tcp+tls como prefijo de protocolo, por ejemplo:<br>tcp+tls://192.168.2.15:1514<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección syslog. |
| secure_syslog | | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• true<br>• false<br>Valor predeterminado: false.<br>Si se establece en false, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en true, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable syslog_server_ca_cert_file_path. |
| syslog_server_ca_cert_file_path | | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si secure_syslog se establece en true. |
| syslog_format | | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>rfc3164 para formato compatible con RFC 3164.<br>rfc5424 para formato compatible con RFC 5424.<br>rfc5424micro para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique rfc3164. |
| docker_memory_limit | | Cantidad de RAM en megabytes para contenedores Docker del orquestador. |
| JAVA_OPTS | | Configuración de RAM de la máquina virtual Java. |
| | Xms | La cantidad mínima de memoria dinámica que la máquina virtual de Java puede asignar al orquestador. Ingrese un valor en uno de los siguientes formatos:<br>• < cantidad de RAM >m es la cantidad de RAM en megabytes, por ejemplo: 512m<br>• < cantidad de RAM >g es la cantidad de RAM en gigabytes, por ejemplo: 4g<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de Xmx. |
| | Xmx | La cantidad máxima de memoria dinámica que la máquina virtual Java puede asignar al orquestador. Ingrese un valor en uno de los siguientes formatos:<br>• < cantidad de RAM >m es la cantidad de RAM en megabytes, por ejemplo: 512m<br>• < cantidad de RAM >g es la cantidad de RAM en gigabytes, por ejemplo: 4g<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de docker_memory_limit. |
| number_of_containers | | El número de instancias de contenedor del orquestador para el equilibrio de carga. Rango de valores: 1 a 5. Si no se especifica esta configuración, se utiliza 1 de manera predeterminada.<br>Esta configuración se ignora si se especifica una matriz de más de un elemento en el parámetro ansible_host para las secciones orc_1 y orc_2. |

| | | | |
|---|---|---|---|
| | orc_<1-2> | | Configuración de implementación de los nodos del orquestador. Puede implementar un nodo del orquestador sin alta disponibilidad o dos nodos con alta disponibilidad.<br>Debe implementar los nodos del orquestador y los nodos de la interfaz de la solución en las mismas máquinas virtuales o servidores físicos. Por ejemplo, debe implementar el primer nodo del orquestador en la misma máquina virtual o servidor físico que el primer nodo de la interfaz de la solución. Puede especificar la configuración de la interfaz de la solución en la sección `www`. |
| | | inventory_hostname | Nombre de host del orquestador. Valor predeterminado: `orc-<1-2>`. |
| | | state | Implementación del orquestador en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | ansible_host | Dirección IP de los nodos (máquinas virtuales o servidores físicos) de la sección `nodes` para implementar el orquestador. Puede especificar una única dirección IP como una cadena o una lista de direcciones IP como una matriz de cadenas. El valor de la dirección IP se puede especificar como una cadena en el formato `XXX.XXX.XXX.XXX` o como una variable de Ansible.<br>Ejemplos:<br>• Cadena en el formato `XXX.XXX.XXX.XXX`: `192.168.110.126`<br>• Variable de Ansible: `{{ nodes.node_1.ip }}`<br>• Matriz de variables de Ansible: `{{ [nodes.node_1.ip, nodes.node_2.ip, nodes.node_3.ip, nodes.node_4.ip, nodes.node_5.ip] }}`<br>Si se especifica una matriz, se ignora la configuración `number_of_containers`, y el equilibrio de carga entre las instancias del orquestador se logra moviendo los contenedores del orquestador a los nodos separados especificados en la matriz. |
| vnfm | | | Configuración del Administrador de funciones de la red virtual. |

| | | |
|---|---|---|
| `syslog_server_address` | | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| `secure_syslog` | | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| `syslog_server_ca_cert_file_path` | | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| `syslog_format` | | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| `docker_memory_limit` | | Cantidad de RAM en megabytes para contenedores Docker del orquestador. |
| `JAVA_OPTS` | | Configuración de RAM de la máquina virtual Java. |
| | `Xms` | La cantidad mínima de memoria dinámica que la máquina virtual Java puede asignar al Administrador de funciones de la red virtual. Ingrese un valor en uno de los siguientes formatos:<br>• `< cantidad de RAM >m` es la cantidad de RAM en megabytes, por ejemplo: `512m`<br>• `< cantidad de RAM >g` es la cantidad de RAM en gigabytes, por ejemplo: `4g`<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de `Xmx`. |
| | `Xmx` | La cantidad máxima de memoria dinámica que la máquina virtual Java puede asignar al Administrador de funciones de la red virtual. Ingrese un valor en uno de los siguientes formatos:<br>• `<cantidad de RAM>m` es la cantidad de RAM en megabytes, por ejemplo: `512m`<br>• `<cantidad de RAM>g` es la cantidad de RAM en gigabytes, por ejemplo: `4g`<br>Recomendamos especificar un valor que sea la mitad de grande que la configuración de `docker_memory_limit`. |
| `vnfm_<1-2>` | | Configuración de implementación de los nodos del Administrador de funciones de la red virtual. Puede implementar un nodo del Administrador de funciones de la red virtual sin alta disponibilidad o dos nodos con alta disponibilidad. |

| | | | |
|---|---|---|---|
| | | `inventory_hostname` | Nombre de host del Administrador de funciones de la red virtual. Valor predeterminado: `vnfm-<1-2>`. |
| | | `state` | Implementación del Administrador de funciones de la red virtual en una máquina virtual o un servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el Administrador de funciones de la red virtual. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |
| `vnfm_proxy` | | | Configuración del Administrador de funciones de la red virtual del proxy. |

| | | | |
|---|---|---|---|
| | `syslog_server_address` | | Dirección web del servidor syslog al que los contenedores Docker del orquestador envían registros. El valor se especifica en el formato `< protocolo >://< dirección del host >:< número de puerto >.` Puede especificar la dirección IP o FQDN del host como la dirección del host.<br>Ejemplos:<br>`udp://192.168.2.15:1514`<br>`tcp+tls://my-syslog-server:1514`<br>Si la variable `secure_syslog` se establece en `true`, debe especificar `tcp+tls` como prefijo de protocolo, por ejemplo:<br>`tcp+tls://192.168.2.15:1514`<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique la dirección del host en formato FQDN.<br>Puede especificar la configuración del servidor syslog en la sección `syslog`. |
| | `secure_syslog` | | Habilita o deshabilita el cifrado de mensajes syslog enviados por el contenedor Docker. Valores posibles:<br>• `true`<br>• `false`<br>Valor predeterminado: `false`.<br>Si se establece en `false`, los mensajes de syslog se envían como texto sin formato a través de UDP. Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`. |
| | `syslog_server_ca_cert_file_path` | | Ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Obligatorio si `secure_syslog` se establece en `true`. |
| | `syslog_format` | | Formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:<br>`rfc3164` para formato compatible con RFC 3164.<br>`rfc5424` para formato compatible con RFC 5424.<br>`rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.<br>Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`. |
| | `docker_memory_limit` | | Cantidad de RAM en megabytes para los contenedores Docker del Administrador de funciones de la red virtual del proxy. |
| | `vnfm_proxy_<1-2>` | | Configuración de implementación de los nodos del Administrador de funciones de la red virtual del proxy. Puede implementar un nodo del Administrador de funciones de la red virtual del proxy sin alta disponibilidad o dos nodos con alta disponibilidad. |
| | | `inventory_hostname` | Nombre de host del Administrador de funciones de la red virtual del proxy. Valor predeterminado: `vnfm-proxy-<1-2>`. |
| | | `state` | Implementación del Administrador de funciones de red virtual proxy en una máquina virtual o servidor físico. Valores posibles:<br>• `enabled`<br>• `disabled` |
| | | `ansible_host` | Dirección IP de la máquina virtual o servidor físico de la sección `nodes` para implementar el Administrador de funciones de la red virtual del proxy. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>• Variable de Ansible, por ejemplo: `{{ nodes.node_1.ip }}` |

## Ejemplo del archivo de configuración

```
version: 2.24.03.0
nodes:
 node_1:
 ip: 192.168.2.1
 knaas_aio_int:
```

```
  base: 10.11.11
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
  node_2:
  ip: 192.168.2.2
  knaas_aio_int:
  base: 10.11.11
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
  node_3:
  ip: 192.168.2.3
  knaas_aio_int:
  base: 10.11.11
  mode: bridge
  knaas_os_man:
  base: 10.11.12
  mode: bridge
external:
  vault_passwords_dirname: ../passwords
  ansible_user: user
  ssl:
  san_list:
  ip:
  - 192.168.2.4
  dns:
  - sdwan.kaspersky.com
  path_local: ../ssl
  path_remote: /home/user/ssl
  docker:
  local_path_to_images: ../images
  remote_path_to_images: /tmp
  syslog:
  docker_memory_limit: 1024
  max_log_size: 32
  state: enabled
  zabbix:
  syslog_server_address: udp://192.168.2.5:1514
  db_docker_memory_limit: 1024
  srv_docker_memory_limit: 1024
  www_docker_memory_limit: 1024
  proxy_docker_memory_limit: 128
  cachesize: 512M
  zabbix_1:
  ansible_host: {{ nodes.node_1.ip }}
  db:
  inventory_hostname: zabbix-db-1
  state: enabled
  srv:
  inventory_hostname: zabbix-srv-1
  state: enabled
  www:
  inventory_hostname: zabbix-www-1
  state: enabled
  proxy:
```

```
inventory_hostname: zabbix-proxy-1
state: enabled
zabbix_2:
ansible_host: {{ nodes.node_2.ip }}
db:
inventory_hostname: zabbix-db-2
state: enabled
srv:
inventory_hostname: zabbix-srv-2
state: enabled
www:
inventory_hostname: zabbix-www-2
state: enabled
proxy:
inventory_hostname: zabbix-proxy-2
state: enabled
zabbix_3:
ansible_host: {{ nodes.node_3.ip }}
db:
inventory_hostname: zabbix-db-3
state: enabled
mongo:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 2048
mongo_1:
inventory_hostname: mongo-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
mongo_2:
inventory_hostname: mongo-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
mongo_3:
inventory_hostname: mongo-3
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
redis_1m:
inventory_hostname: redis-1m
state: enabled
ansible_host: {{ nodes.node_1.ip }}
redis_2m:
inventory_hostname: redis-2m
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_3m:
inventory_hostname: redis-3m
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_1s:
inventory_hostname: redis-1s
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_2s:
inventory_hostname: redis-2s
state: enabled
```

```
ansible_host: {{ nodes.node_3.ip }}
redis_3s:
inventory_hostname: redis-3s
state: enabled
ansible_host: {{ nodes.node_1.ip }}
ctl:
tenants:
- name: ha3
state: enabled
ctl_base: 10.11.11
mock_base: 10.11.12
hosts:
- inventory_hostname: ctl-1
ansible_host: {{ nodes.node_1.ip }}
- inventory_hostname: ctl-2
ansible_host: {{ nodes.node_2.ip }}
- inventory_hostname: ctl-3
ansible_host: {{ nodes.node_3.ip }}
docker_memory_limit: 8192
JAVA_OPTS:
Xms: 2g
Xmx: 4g
MaxDirectMemorySize: 4g
syslog_server_address: udp://192.168.2.5:1514
www:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
oem:
state: disabled
path_remote: /home/user/oem
path_local: ../../oem
title: OEM Title
support: https://support.support.com
assets: true
www_1:
inventory_hostname: www-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
www_2:
inventory_hostname: www-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
orc:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
JAVA_OPTS:
Xms: 2g
Xmx: 4g
orc_1:
inventory_hostname: orc-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
orc_2:
inventory_hostname: orc-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm:
syslog_server_address: udp://192.168.2.5:1514
```

```
docker_memory_limit: 1024
JAVA_OPTS:
Xms: 512m
Xmx: 1024m
vnfm_1:
inventory_hostname: vnfm-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_2:
inventory_hostname: vnfm-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm_proxy:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
vnfm_proxy_1:
inventory_hostname: vnfm-proxy-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_proxy_2:
inventory_hostname: vnfm-proxy-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
inventory_hostname: zabbix-db-2
state: enabled
srv:
inventory_hostname: zabbix-srv-2
state: enabled
www:
inventory_hostname: zabbix-www-2
state: enabled
proxy:
inventory_hostname: zabbix-proxy-2
state: enabled
zabbix_3:
ansible_host: {{ nodes.node_3.ip }}
db:
inventory_hostname: zabbix-db-3
state: enabled
mongo:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 2048
mongo_1:
inventory_hostname: mongo-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
mongo_2:
inventory_hostname: mongo-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
mongo_3:
inventory_hostname: mongo-3
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
redis_1m:
```

```
inventory_hostname: redis-1m
state: enabled
ansible_host: {{ nodes.node_1.ip }}
redis_2m:
inventory_hostname: redis-2m
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_3m:
inventory_hostname: redis-3m
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_1s:
inventory_hostname: redis-1s
state: enabled
ansible_host: {{ nodes.node_2.ip }}
redis_2s:
inventory_hostname: redis-2s
state: enabled
ansible_host: {{ nodes.node_3.ip }}
redis_3s:
inventory_hostname: redis-3s
state: enabled
ansible_host: {{ nodes.node_1.ip }}
ctl:
tenants:
- name: ha3
state: enabled
ctl_base: 10.11.11
mock_base: 10.11.12
hosts:
- inventory_hostname: ctl-1
ansible_host: {{ nodes.node_1.ip }}
- inventory_hostname: ctl-2
ansible_host: {{ nodes.node_2.ip }}
- inventory_hostname: ctl-3
ansible_host: {{ nodes.node_3.ip }}
docker_memory_limit: 8192
JAVA_OPTS:
Xms: 2g
Xmx: 4g
MaxDirectMemorySize: 4g
syslog_server_address: udp://192.168.2.5:1514
www:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
oem:
state: disabled
path_remote: /home/user/oem
path_local: ../../oem
title: OEM Title
support: https://support.support.com
assets: true
www_1:
inventory_hostname: www-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
www_2:
inventory_hostname: www-2
```

```
state: enabled
ansible_host: {{ nodes.node_2.ip }}
orc:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 4096
JAVA_OPTS:
Xms: 2g
Xmx: 4g
orc_1:
inventory_hostname: orc-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
orc_2:
inventory_hostname: orc-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
JAVA_OPTS:
Xms: 512m
Xmx: 1024m
vnfm_1:
inventory_hostname: vnfm-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_2:
inventory_hostname: vnfm-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
vnfm_proxy:
syslog_server_address: udp://192.168.2.5:1514
docker_memory_limit: 1024
vnfm_proxy_1:
inventory_hostname: vnfm-proxy-1
state: enabled
ansible_host: {{ nodes.node_1.ip }}
vnfm_proxy_2:
inventory_hostname: vnfm-proxy-2
state: enabled
ansible_host: {{ nodes.node_2.ip }}
```

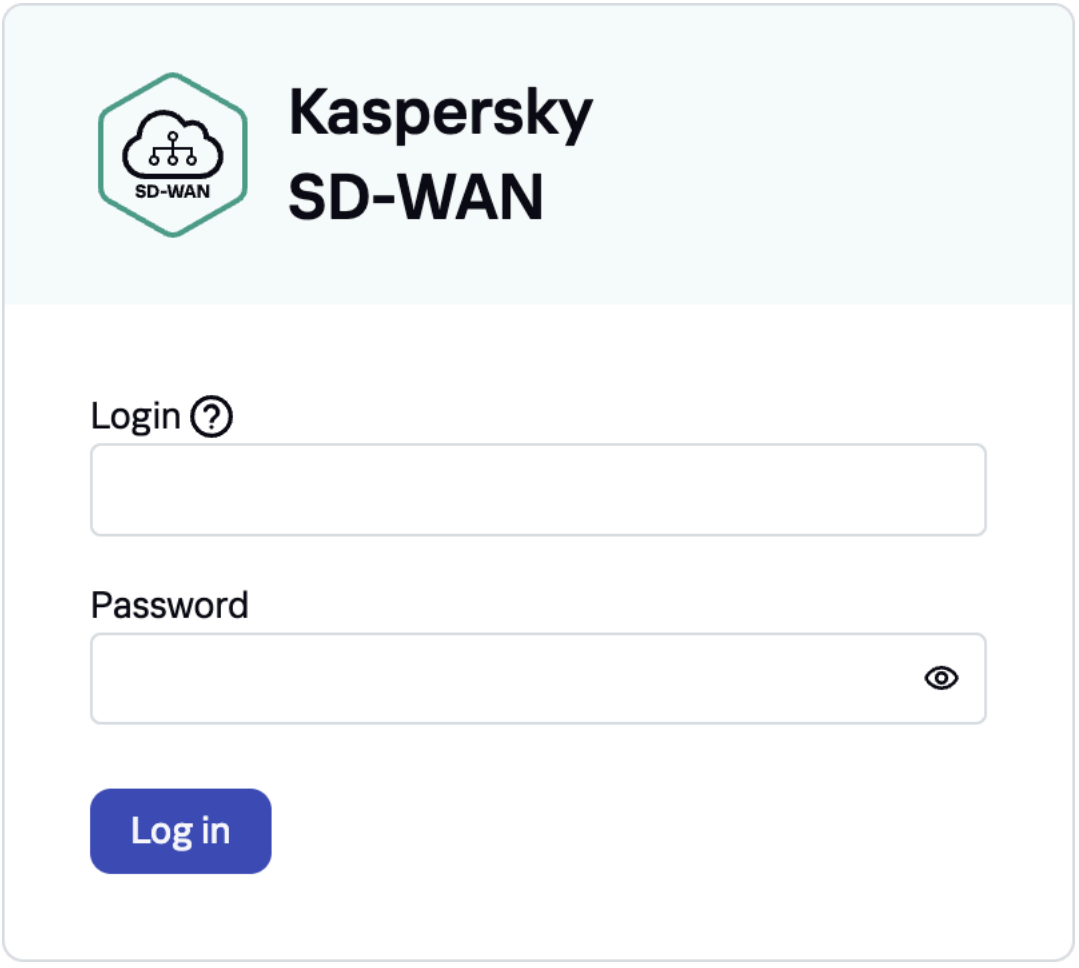
# Reemplazar los elementos gráficos de la interfaz web del orquestador

*Para reemplazar los gráficos de la interfaz web del orquestador:*

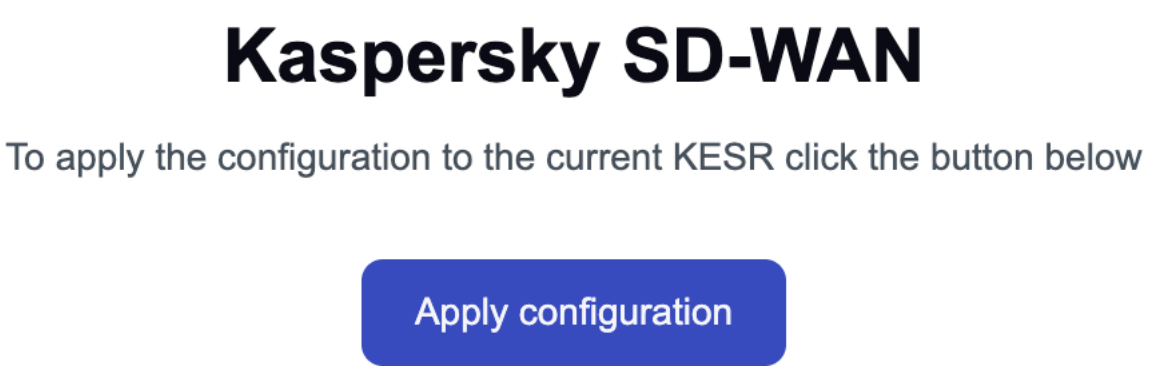
1. Configure la parte fronted de la solución en la sección `www` del archivo de configuración.
2. En el dispositivo del administrador, vaya al directorio /oem del archivo de instalación extraído. Este directorio contiene los gráficos predeterminados de la interfaz web del orquestador. Puede reemplazar los siguientes archivos:
   - favicon.png y favicon.svg son los íconos que se muestran en la pestaña de la interfaz web del orquestador.

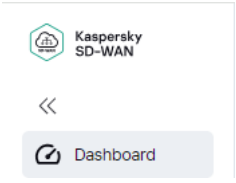
   - login_logo.svg es el ícono que se muestra en la parte superior de la ventana cuando inicia sesión en la interfaz web del orquestador.

- logo_activation.svg es el ícono que se muestra durante el registro automático de un dispositivo CPE.




- logo.svg y title.svg son el ícono y el título que se muestran en la parte superior del panel de navegación de la interfaz web del orquestador.




# Reemplazar un nodo de controlador fallido

Puede implementar un nuevo nodo de controlador para reemplazar un nodo de controlador que haya fallado y no pueda repararse. Si un nodo del controlador falla mientras está en un clúster con otros nodos, el nuevo nodo del controlador se agrega automáticamente a ese clúster y se sincroniza con los nodos existentes.

Antes de ejecutar este script, asegúrese de que la dirección IP de la máquina virtual o el servidor físico en el que está implementando el nuevo nodo del controlador sea la misma que la dirección IP de la máquina virtual o el servidor físico donde se implementó el nodo del controlador fallido. Especificó las direcciones IP de las máquinas virtuales o los servidores físicos para la implementación de los nodos del controlador cuando implementó la solución, en la sección `ctl` del archivo de configuración.

El escenario para reemplazar un nodo de controlador fallido implica los siguientes pasos:

1. **Preparar el dispositivo administrador**

   Prepare el dispositivo administrador para la implementación del nuevo nodo de controlador. Puede usar una máquina virtual local o remota, o una computadora personal como dispositivo administrador. Cuando implementa un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo-en-uno, debe usar una máquina virtual como dispositivo administrador.

**2 Asegurar la conexión de red entre el dispositivo administrador, los componentes de la solución y el nuevo nodo de controlador**

Asegúrese de la conexión de red entre el dispositivo administrador, los componentes de la solución y la máquina virtual o el servidor físico en el que desea implementar el nuevo nodo de controlador. Debe asegurarse de que los vínculos entre las máquinas virtuales o los servidores físicos cumplan con los requisitos de hardware y software.

> El servidor físico de la máquina virtual debe implementarse en un segmento de red de confianza para evitar comprometer el tráfico transmitido.

**3 Implementar un nodo de controlador**

Haga lo siguiente en el dispositivo administrador:

1. Acepte el Contrato de licencia de usuario final; para ello, ejecute el siguiente comando:

   ```
   export KNAAS_EULA_AGREED="true"
   ```

2. Vaya al directorio con el archivo de instalación extraído.

3. Si desea implementar el nuevo nodo del controlador en modo atendido, realice una de las siguientes acciones:

   - Si generó las contraseñas manualmente mientras implementaba la solución, ejecute el siguiente comando:

     ```
     ansible-playbook -i inventory/generic -e "@<ruta al archivo de configuración>" -e
     "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
     ```

     Cuando ejecute el comando, ingrese la contraseña de la cuenta raíz y la contraseña principal generada.

   - Si no generó las contraseñas manualmente mientras implementaba la solución, ejecute el siguiente comando:

     ```
     ansible-playbook -i inventory/generic -e "@<ruta al archivo de configuración>" -e
     "@inventory/external/images.yml" -K knaas/knaas-install.yml
     ```

4. Si desea implementar el nuevo nodo del controlador en modo desatendido, realice una de las siguientes acciones:

   > Recomendamos usar este modo solo en un entorno de confianza, ya que de lo contrario los piratas informáticos pueden interceptar sus contraseñas.

   - Si generó las contraseñas manualmente mientras implementaba la solución, ejecute el siguiente comando:

     ```
     ansible-playbook -i inventory/generic -e "@<ruta al archivo de configuración>" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
     vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
     ```

   - Si no generó las contraseñas manualmente mientras implementaba la solución, ejecute el siguiente comando:

     ```
     ansible-playbook -i inventory/generic -e "@<ruta al archivo de configuración>" -e
     "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword"
     knaas/knaas-install.yml
     ```

El nuevo nodo de controlador se implementa para reemplazar el nodo del controlador fallido. Se muestra un mensaje de implementación exitosa en la consola del dispositivo administrador.

Si ocurre un problema de conectividad de la red con una máquina virtual o un servidor físico mientras se implementa el nodo del controlador, se muestra un error en la consola del dispositivo administrador y el nuevo nodo del controlador no se implementa. En ese caso, debe restaurar la conectividad de la red, limpiar la máquina virtual o el servidor físico y luego volver a ejecutar el comando de implementación.

# Actualizar Kaspersky SD-WAN

LA FUNCIONALIDAD DE ACTUALIZACIÓN (INCLUIDAS LAS ACTUALIZACIONES DE FIRMA ANTIVIRUS Y LAS ACTUALIZACIONES DE BASE DE CÓDIGO), ASÍ COMO LA FUNCIONALIDAD DE KSN PUEDEN NO ESTAR DISPONIBLES EN EL SOFTWARE EN EL TERRITORIO DE EE. UU.

Antes de actualizar Kaspersky SD-WAN, asegúrese de que ninguno de los dispositivos CPE tenga el estado **Error**. Puede ver el estado de los dispositivos CPE en la tabla de dispositivos CPE. También recomendamos hacer copias de respaldo de los componentes de la solución:

- Si los componentes de su solución se implementan en máquinas virtuales, tome instantáneas de las máquinas virtuales. Después de actualizar Kaspersky SD-WAN, puede eliminar las instantáneas de las máquinas virtuales. Para obtener detalles sobre cómo tomar instantáneas de máquinas virtuales, consulte la documentación oficial de sus entornos de virtualización.

- Si los componentes de su solución se implementan en servidores físicos, debe realizar copias de seguridad de los discos duros de los servidores físicos. Si usa un controlador RAID (matriz redundante de discos independientes), puede obtener información sobre cómo crear copias de respaldo de sus discos duros en la documentación oficial proporcionada por el proveedor de su controlador RAID.

El escenario de actualización de Kaspersky SD-WAN implica los siguientes pasos:

1. **Preparar el dispositivo administrador**

   Prepare el dispositivo administrador para la actualización de la solución. Puede usar una máquina virtual local o remota, o una computadora personal como dispositivo administrador. Cuando implementa un banco de pruebas de Kaspersky SD-WAN de acuerdo con el escenario de implementación todo-en-uno, debe usar una máquina virtual como dispositivo administrador.

2. **Preparar el archivo de configuración**

   Ajuste el archivo de configuración de acuerdo con los cambios realizados en la nueva versión de Kaspersky SD-WAN. Puede ver los cambios en el archivo CHANGELOG.md en el directorio raíz del archivo de instalación.

   Cuando actualice Kaspersky SD-WAN, asegúrese de conservar los archivos con contraseñas y certificados SSL.

3. **Aceptar el Contrato de licencia de usuario final**

   Acepte el Contrato de licencia de usuario final; para ello, ejecute el siguiente comando:

   ```
   export KNAAS_EULA_AGREED="true"
   ```

4. **Actualizar Kaspersky SD-WAN**

Actualice Kaspersky SD-WAN de una de las siguientes maneras:

- Si desea actualizar la solución en modo atendido:

  ```
  ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
  "@inventory/external/images.yml" -K --ask-vault-pass knaas/knaas-install.yml
  ```

  Cuando ejecute el comando, ingrese la contraseña de la cuenta raíz en el dispositivo administrador y la contraseña principal generada.

- Si desea actualizar la solución en modo parcialmente atendido:

  ```
  ansible-playbook -i inventory/generic -e "@< path to configuration file >" -e
  "@inventory/external/images.yml" -K --vault-password-file
  ./passwords/vault_password.txt knaas/knaas-install.yml
  ```

  Ingrese la contraseña raíz del dispositivo administrador cuando ejecute el comando.

- Si desea actualizar la solución en modo desatendido:

  ```
  ansible-playbook -i inventory/generic -e "@< ruta al archivo de configuración >" -e
  "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword" --
  vault-password-file ./passwords/vault_password.txt knaas/knaas-install.yml
  ```

Los componentes de Kaspersky SD-WAN se actualizan en las máquinas virtuales o los servidores físicos que especificó en el archivo de configuración. Se muestra un mensaje de actualización exitosa en la consola del dispositivo administrador.

Si ocurre un problema de conectividad de la red con una de las máquinas virtuales o los servidores físicos durante la actualización de los componentes de la solución, se muestra un mensaje de error en la consola del dispositivo administrador y la solución no se actualiza. En ese caso, debe restaurar la conectividad de la red y luego volver a ejecutar el comando de actualización.

Después de actualizar la solución, debe borrar el historial de comandos Bash.

# Eliminar Kaspersky SD-WAN

La eliminación de Kaspersky SD-WAN no se puede revertir.

*Para eliminar Kaspersky SD-WAN, siga estos pasos:*

1. En el dispositivo administrador, vaya al archivo de instalación extraído.
2. Elimine Kaspersky SD-WAN de una de las siguientes maneras:

   - Si desea eliminar la solución en modo atendido:

     ```
     ansible-playbook -i inventory/generic -e "@< path to configuration file >" -e
     "@inventory/external/images.yml" -K knaas/knaas-teardown.yml
     ```

- Si desea eliminar la solución en modo desatendido:

  ```
  ansible-playbook -i inventory/generic -e "@<path to configuration file>" -e
  "@inventory/external/images.yml" -e "ansible_become_password=yourSudoPassword"
  knaas/knaas-teardown.yml
  ```

Los componentes de Kaspersky SD-WAN se eliminan de las máquinas virtuales o los servidores físicos. Se muestra un mensaje de eliminación exitosa en la consola del dispositivo administrador.

Si ocurre un problema de conectividad de la red con una de las máquinas virtuales o los servidores físicos durante la eliminación de los componentes de la solución, se muestra un mensaje de error en la consola del dispositivo administrador y la solución no se elimina. En ese caso, debe restaurar la conectividad de la red y luego volver a ejecutar el comando de eliminación.

# Iniciar y cerrar sesión en la interfaz web del orquestador

## Inicio de sesión en la interfaz web del orquestador

*Para iniciar sesión en la interfaz web del orquestador, haga lo siguiente:*

1. En la barra de direcciones de su navegador, ingrese una de las siguientes direcciones IP:

   - Si desea iniciar sesión en el portal del administrador, ingrese la dirección IP de la máquina virtual o el servidor físico en el que implementó el orquestador o el frontend de la solución. Usted especificó la dirección IP de la máquina virtual o el servidor físico para el orquestador o la implementación del frontend en las secciones `orc_<1-2>` y `www_<1-2>` del archivo de configuración mientras se implementaba la solución. También se puede ingresar la dirección IP virtual del orquestador.

   - Si desea iniciar sesión en el portal de autoservicio, ingrese la dirección IP que obtuvo del administrador de su plataforma.

2. De este modo, se abrirá la página de autenticación; en esa página, ingrese un nombre de usuario y una contraseña. La contraseña debe contener al menos una letra del alfabeto latino en mayúscula (A–Z), una letra en minúscula (a–z), un número y un carácter especial. Longitud de la contraseña: de 8 a 50 caracteres.

3. Haga clic en **Iniciar sesión**. Si se habilitó la autenticación de dos factores en su cuenta, haga lo siguiente:

   a. Escanee el código QR que aparece en pantalla con un autenticador físico o de software que admita el estándar RFC 6238.

   b. Ingrese y confirme el código único generado por el autenticador.

Después de haber hecho la autenticación correctamente, se lo dirigirá a la sección o subsección que haya configurado como página predeterminada.

## Cierre de sesión en la interfaz web del orquestador

*Para cerrar sesión en la interfaz web del orquestador, haga lo siguiente:*

1. En la parte inferior del menú, haga clic en el ícono de cierre de sesión .

2. En la ventana de confirmación, haga clic en **Aceptar**.

Ha cerrado sesión en la interfaz web del orquestador.

# Licencias de Kaspersky SD-WAN

En esta sección se contemplan los conceptos básicos de la licencia de Kaspersky SD-WAN. Si necesita escalar la solución, puede comprar licencias de software y hardware adicionales.

# Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula los términos según los cuales puede utilizar el programa. El texto del Contrato de licencia de usuario final en los idiomas admitidos se encuentra en los archivos *de licencia <código de idioma>.rtf* incluidos en el kit de distribución de Kaspersky SD-WAN.

Lea detenidamente y por completo los términos del Contrato de licencia de usuario final antes de empezar a usar Kaspersky SD-WAN.

Al confirmar que está de acuerdo con el Contrato de licencia de usuario final, usted manifiesta su aceptación de los términos del Contrato de licencia de usuario final. Puede hacer esto de una de las siguientes maneras:

- Inicialice la variable de entorno `KNAAS_EULA_AGREED` antes de iniciar el contenedor Docker de Kaspersky SD-WAN:

  ```
  export KNAAS_EULA_AGREED=yes
  ```

  En este caso, al iniciar el contenedor Docker de Kaspersky SD-WAN, pase la variable de entorno KNAAS_EULA_AGREED utilizando la opción `-e`:

  ```
  docker run -e KNAAS_EULA_AGREED [OPTIONS] IMAGE [COMMAND] [ARG...]
  ```

- Inicialice la variable de entorno `KNAAS_EULA_AGREED` directamente al iniciar el contenedor Docker de Kaspersky SD-WAN:

  ```
  docker run -e KNAAS_EULA_AGREED=yes [OPTIONS] IMAGE [COMMAND] [ARG...]
  ```

Si la variable de entorno `KNAAS_EULA_AGREED` no se inicializa o se inicializa con el valor `no` (`KNAAS_EULA_AGREED=no`), esto significa que no está de acuerdo con los términos del Contrato de licencia de usuario final. En este caso, al iniciar el contenedor Docker de Kaspersky SD-WAN, se muestra un mensaje de error y Kaspersky SD-WAN no se inicia.

# Acerca del suministro de datos

Las siguientes soluciones de terceros están integradas en Kaspersky SD-WAN:

- Sistema de supervisión Zabbix
- Plataforma OpenStack para crear servicios en la nube y almacenamiento
- Mapas geográficos de OpenStreetMap

La información personal que podría ingresarse en Zabbix, OpenStack u OpenStreetMap como resultado de la integración no se envía fuera del perímetro de la infraestructura de la organización.

Kaspersky protege la información recibida de acuerdo con los requisitos estipulados por la ley aplicable y las políticas de Kaspersky.

# Interfaz de usuario de la solución

Kaspersky SD-WAN se administra con la interfaz web del orquestador. Puede utilizar las secciones del menú para configurar los componentes de la solución. Cuando se navega a una sección, se muestra un menú adicional con subsecciones en forma contraída. Para expandir el menú, coloque el cursor del mouse sobre el ícono de una de las subsecciones. Puede hacer clic en el ícono de expandir » para deshabilitar la minimización automática del menú.

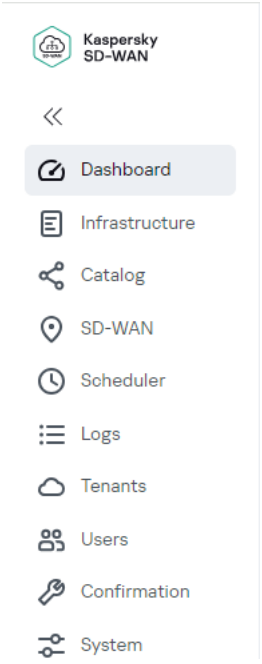
Se admiten dos variantes de la interfaz web del orquestador:

- El *portal del administrador* les otorga acceso total a los administradores para administrar los componentes de la solución.
- El *portal de autoservicio* les otorga acceso a los inquilinos para administrar las instancias SD-WAN que se implementan para ellos.

Los administradores pueden iniciar sesión en el portal de autoservicio de un inquilino.

## Portal del administrador

En la siguiente imagen, se muestra el menú del portal del administrador.

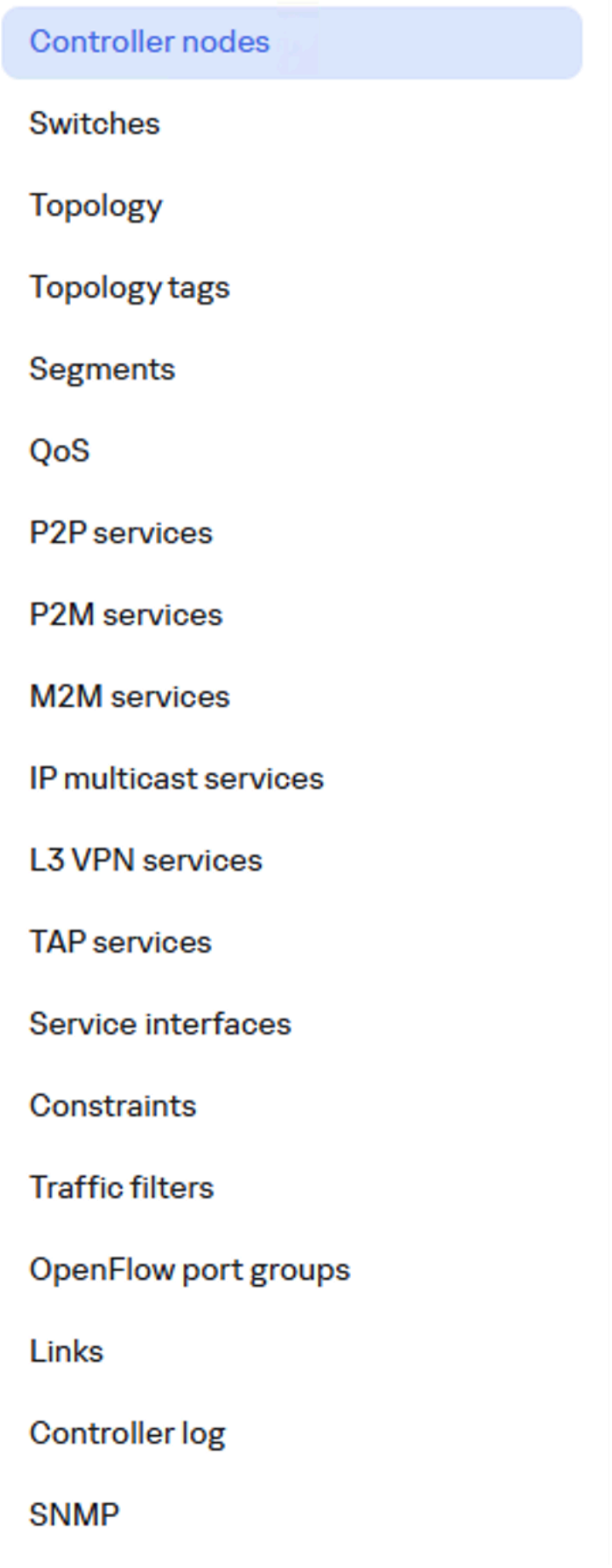



Menú del portal del administrador

| Sección | Descripción |
|---|---|
| **Panel** | Información sobre el estado actual de los componentes de la solución, como los dispositivos CPE, las funciones de la red virtual y las funciones de la red física. |
| **Infraestructura** | Infraestructura corporativa. En esta sección, puede configurar los siguientes componentes:<br>• Dominios<br>• Centros de datos<br>• Subredes de administración<br>• Controladores<br>• VIM |

| Sección | Descripción |
| --- | --- |
| **Catálogo** | Plantillas del servicio de red para la configuración centralizada de los servicios de red |
| **SD-WAN** | • **CPE**: dispositivos CPE para la retransmisión del tráfico.<br>• **Plantillas de CPE**: plantillas de CPE para la configuración centralizada de los dispositivos CPE.<br>• **Plantillas de firewall**: plantillas de firewall para la configuración centralizada del firewall en los dispositivos CPE.<br>• **Zonas de firewall**: zonas de firewall para las interfaces de red y las subredes de los dispositivos CPE.<br>• **Plantillas de NetFlow**: plantillas de NetFlow para el control de la información de los paquetes de tráfico en los dispositivos CPE.<br>• **Directorios de APN**: lista de directorios para la configuración automática de APN de las interfaces del tipo QMI en dispositivos CPE.<br>• **IPAM**: dirección IP y rangos de subred para los dispositivos CPE.<br>• **Firmware**: firmware del dispositivo CPE.<br>• **Certificados**: certificados de los dispositivos CPE.<br>• **Instancias SD-WAN**: instancias SD-WAN implementadas.<br>• **Plantillas de instancia SD-WAN**: plantillas de las instancias SD-WAN para la configuración e implementación centralizadas de las instancias SD-WAN.<br>• **Agrupaciones de instancias SD-WAN**: agrupaciones de las instancias SD-WAN.<br>• **Plantillas de UNI**: plantillas de UNI para la creación centralizada de las UNI en los dispositivos CPE. |
| **Programador** | Tareas programadas para que se ejecuten más tarde. |
| **Registros** | Registros de los componentes de la solución, como los dispositivos CPE, las funciones de la red virtual y las funciones de la red física. |
| **Inquilinos** | Inquilinos de la solución. |
| **Usuarios** | Usuarios de la solución. En esta sección, puede configurar los siguientes componentes:<br>• Usuarios<br>• Permisos de acceso<br>• Grupos de usuarios de LDAP<br>• Conexiones de LDAP |
| **Confirmación** | Solicitudes de confirmación para las acciones del usuario. |
| **Sistema** | • **Supervisión** contiene la configuración del servidor de Zabbix para el control de los componentes de la solución.<br>• **Notificación** contiene la configuración para enviar notificaciones por correo electrónico a los usuarios.<br>• **Registro del orquestador** es la verbosidad en el registro del contenedor Docker.<br>• **Sesiones del usuario** contiene la configuración de la sesión del usuario.<br>• **API** es la API del orquestador.<br>• **Otra** contiene configuraciones adicionales. |

El controlador tiene su propio menú de configuración (consulte la siguiente imagen). Para obtener información detallada sobre el menú de configuración del controlador, consulte el artículo Cómo visualizar la información sobre los nodos del controlador.

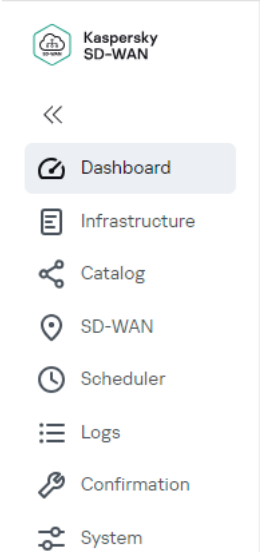



Menú de configuración del controlador en el portal del administrador

| Sección | Descripción |
| --- | --- |
| **Nodos del controlador** | Información sobre el estado actual de los nodos del controlador. |
| **Conmutadores** | Configuración avanzada de los dispositivos y conmutadores CPE. |
| **Topología** | Topología gráfica de una instancia SD-WAN. |
| **Etiquetas de topología** | Etiquetas de topología para establecer vínculos entre los dispositivos CPE. |
| **Segmentos** | Segmentos formados a partir de los dispositivos y conmutadores CPE. |
| **QoS** | Configuración de la calidad del servicio. En esta sección, puede configurar los siguientes componentes:<br>• Clases de tráfico<br>• Clasificadores de tráfico<br>• Reglas de la calidad del servicio |
| **Servicios de P2P** | Servicios de transporte punto a punto. |
| **Servicios de P2M** | Servicios de transporte de punto a multipunto. |
| **Servicios de M2M** | Servicios de transporte de multipunto a multipunto. |
| **Servicios de multidifusión de IP** | Servicios de transporte de multidifusión IP. |
| **Servicios de VPN L3** | Servicios de transporte de VPN L3. |
| **Servicios de TAP** | Servicios de TAP (punto de acceso de prueba) para duplicar el tráfico. |
| **Interfaces del servicio** | Interfaces de servicio de los dispositivos y conmutadores CPE. |
| **Restricciones** | Restricciones de Manual-TE y restricciones de umbral para garantizar la calidad del servicio. |
| **Filtros de tráfico** | Filtros de tráfico para aplicar la calidad del servicio. |
| **Grupos de puertos OpenFlow** | Grupos de puertos OpenFlow. |
| **Enlaces** | Vínculos entre los dispositivos y conmutadores CPE, y vínculos entre los dispositivos CPE. |
| **Registros** | Nivel de verbosidad en el registro del contenedor Docker. |
| **SNMP** | Configuración para el control de los dispositivos CPE, las funciones de la red virtual y las funciones de la red física mediante SNMP. |

## Portal de autoservicio

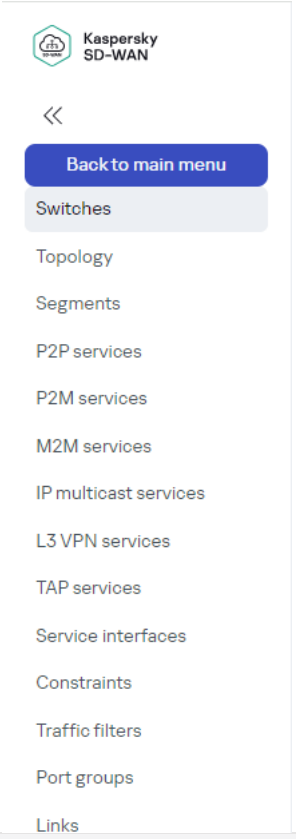
En la siguiente imagen, se muestra el menú del portal de autoservicio.




Menú del portal de autoservicio

| Sección | Descripción |
|---|---|
| **Panel** | Información sobre el estado actual de los componentes de la solución, como los dispositivos CPE y las funciones de la red. |
| **Infraestructura** | Infraestructura corporativa. En esta sección, puede configurar los controladores. |
| **Catálogo** | Servicios de red para la transmisión de tráfico y la virtualización de las funciones de la red. |
| **SD-WAN** | • **CPE**: dispositivos CPE para la retransmisión del tráfico.<br>• **Plantillas de CPE**: plantillas de CPE para la configuración centralizada de los dispositivos CPE.<br>• **Plantillas de firewall**: plantillas de firewall para la configuración centralizada del firewall en los dispositivos CPE.<br>• **Zonas de firewall**: zonas de firewall para las interfaces de red y las subredes de los dispositivos CPE.<br>• **Plantillas de NetFlow**: plantillas de NetFlow para el control de la información de los paquetes de tráfico en los dispositivos CPE.<br>• **IPAM**: dirección IP y rangos de subred para los dispositivos CPE.<br>• **Plantillas de UNI**: plantillas de UNI para la creación centralizada de las UNI en los dispositivos CPE. |
| **Programador** | Tareas programadas para que se ejecuten más tarde. |
| **Registros** | Registros de los componentes de la solución, como los dispositivos CPE, las funciones de la red virtual y las funciones de la red física. |
| **Confirmación** | Solicitudes de confirmación para las acciones del usuario. |
| **Sistema** | • **Notificación** contiene la configuración para enviar notificaciones por correo electrónico a los usuarios.<br>• **Sesiones del usuario** contiene la configuración de la sesión del usuario. |

El controlador tiene su propio menú de configuración (consulte la siguiente imagen).




| Sección | Descripción |
|---|---|
| **Conmutadores** | Configuración avanzada de los dispositivos y conmutadores CPE. |
| **Topología** | Topología gráfica de una instancia SD-WAN. |
| **Segmentos** | Segmentos formados a partir de los dispositivos y conmutadores CPE. |
| **Servicios de P2P** | Servicios de transporte punto a punto. |
| **Servicios de P2M** | Servicios de transporte de punto a multipunto. |
| **Servicios de M2M** | Servicios de transporte de multipunto a multipunto. |
| **Servicios de multidifusión de IP** | Servicios de transporte de multidifusión IP. |
| **Servicios de VPN L3** | Servicios de transporte de VPN L3. |

| Sección | Descripción |
| --- | --- |
| **Servicios de TAP** | Servicios de TAP para duplicar el tráfico. |
| **Interfaces del servicio** | Interfaces de servicio de los dispositivos y conmutadores CPE. |
| **Restricciones** | Restricciones de Manual-TE y restricciones de umbral para garantizar la calidad del servicio. |
| **Filtros de tráfico** | Filtros de tráfico para aplicar la calidad del servicio. |
| **Grupos de puertos OpenFlow** | Grupos de puertos OpenFlow. |
| **Enlaces** | Vínculos entre los dispositivos y conmutadores CPE, y vínculos entre los dispositivos CPE. |

# Configurar y restablecer la página predeterminada

*La página predeterminada* es una sección o subsección del menú que se muestra automáticamente después de iniciar sesión en la interfaz web del orquestador.

*Para configurar o restablecer la página predeterminada:*

1. Vaya a la sección o subsección de la interfaz web del orquestador que desee establecer como página predeterminada.
2. Abra el menú de configuración de la interfaz web en la esquina superior derecha de la página.
3. En el menú, seleccione **Página predeterminada → Configurar una página predeterminada**.

   En la parte superior de la página, se muestra el mensaje *Se configuró la página predeterminada*.
4. Si desea restablecer la página predeterminada, seleccione**Página predeterminada → Restablecer página predeterminada**.

   En la parte superior de la página, se muestra el mensaje *Se restableció la página predeterminada*. La sección **Panel** se convierte en la página predeterminada.

# Alternar entre los modos claro y oscuro de la interfaz web del orquestador

*Para alternar entre los modos claro y oscuro de la interfaz web del orquestador, siga estos pasos:*

1. Abra el menú de configuración de la interfaz web en la esquina superior derecha de la página.
2. En el menú, habilite o deshabilite el botón de alternancia **Modo oscuro**.

# Cambiar el idioma de la interfaz web del orquestador

La interfaz web del orquestador admite los siguientes idiomas:

- English
- Ruso
- Español (México)
- Portugués (Brasil)

*Para cambiar el idioma de la interfaz web del orquestador:*

1. Abra el menú de configuración de la interfaz web en la esquina superior derecha de la página.
2. En el menú, seleccione el elemento con el símbolo del mundo y el nombre del idioma de la interfaz actual. Luego, seleccione un idioma de la lista desplegable.

# Administrar tablas de componentes de la solución

Los componentes de la solución, como los usuarios, las interfaces de red y los pares de BGP, se muestran en tablas. Puede usar los siguientes controles para administrar las tablas:

- El ícono de configuración, que puede utilizar para hacer lo siguiente:
  - Actualice la tabla haciendo clic en el ícono de configuración → **Volver a cargar**. También puede actualizar la tabla con el ícono de actualización.
  - Restaure los anchos predeterminados de las columnas de la tabla haciendo clic en el ícono de configuración → **Restablecer ancho de columnas**.
  - Seleccione las columnas que se muestran en la tabla. Para hacerlo, haga clic en el ícono de configuración y seleccione las casillas de verificación junto a las columnas que desea mostrar.
- El ícono de búsqueda en el que puede hacer clic e ingresar sus criterios de búsqueda. Después de ingresar los criterios de búsqueda, la tabla muestra las entradas relevantes.
- Filtros de estado para mostrar las entradas con el estado seleccionado.
- Filtros de tiempo para mostrar entradas para el período seleccionado:
  - **Todo el tiempo**
  - **Último año**
  - **Último mes**

- **Última semana**
- **Último día**

  Puede especificar manualmente el período utilizando los campos en la parte superior de la tabla.

- El botón **Acciones** para aplicar una acción simultáneamente en todas las entradas con casillas de verificación seleccionadas. Por ejemplo, en la tabla de dispositivos CPE, puede eliminar varios dispositivos CPE al mismo tiempo.

Puede ajustar el ancho de cada columna de la tabla con los íconos de tres puntos ⋮ entre los nombres de las columnas.

# Navegar a la API de orquestador

*Para navegar a la API de orquestador,*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **API**.

Esto abre una lista de comandos de la API que se pueden usar para administrar el orquestador.

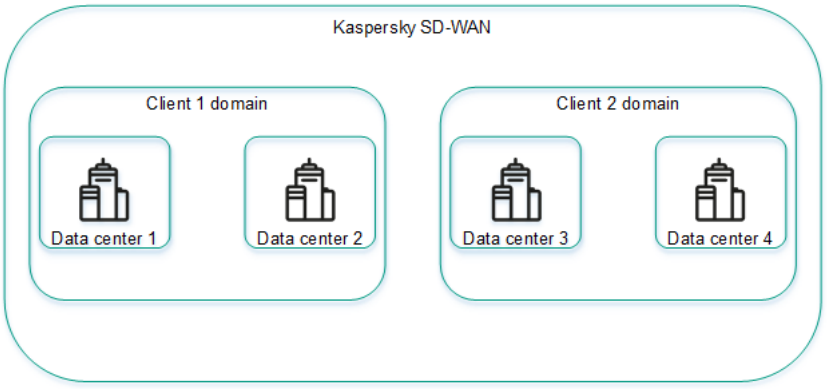
# Administrar la infraestructura de Kaspersky SD-WAN

Las ubicaciones en las que se implementan todos los componentes de Kaspersky SD-WAN que no son dispositivos CPE se denominan *centros de datos*. Debe agregar los centros de datos a la interfaz web del orquestador para administrar los controladores y los VIM, y especificar el servidor proxy Zabbix para configurar la supervisión de los componentes de la solución.

Si tiene una gran cantidad de centros de datos, puede agregarlos a los dominios. Los *dominios* son agrupaciones lógicas de centros de datos basadas en un criterio determinado, como la ubicación geográfica. Antes de agregar centros de datos, debe crear al menos un dominio. Puede mover centros de datos entre dominios.

En cada centro de datos, debe crear al menos una subred de administración para asignar direcciones IP, servidores DNS y rutas estáticas a dispositivos CPE y funciones de red virtual.

En la siguiente figura se muestra un diagrama de una organización. Los componentes de Kaspersky SD-WAN se implementan en cuatro centros de datos. La organización está proporcionando la solución a dos clientes, cada uno de los cuales tiene una instancia SD-WAN implementada. Se utilizan dos centros de datos para implementar cada instancia SD-WAN. Los centros de datos se agregan a los dominios que corresponden a los clientes.




Ejemplo de una organización con dominios y centros de datos

# Administrar dominios

Puede ver la lista de dominios en la sección **Infraestructura** del panel **Recursos**. Debajo de los dominios, la lista muestra los centros de datos agregados a los dominios.

## Crear un dominio

*Para crear un dominio, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En la parte superior de la página, haga clic en **+Dominio**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del dominio. La longitud máxima del nombre es de 50 caracteres.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del dominio. La longitud máxima de la descripción es de 100 caracteres.

5. Haga clic en **Crear**.

   El dominio se crea y se muestra en el panel **Recursos**.

Puede agregar centros de datos a un dominio cuando agrega centros de datos.

# Editar un dominio

*Para editar un dominio, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, haga clic en el ícono de configuración → **Editar** junto al dominio que desea editar.

3. En la ventana que se abre, si es necesario, edite el nombre o la descripción del dominio.

4. Haga clic en **Guardar**.

   El dominio se modifica y se muestra en el panel **Recursos**.

# Eliminar un dominio

Antes de eliminar un dominio, debe eliminar los centros de datos que se agregaron al dominio.

Los dominios eliminados no se pueden restaurar.

*Para eliminar un dominio, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, haga clic en el ícono de configuración → **Eliminar** junto al dominio que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El dominio se elimina y ya no se muestra en el panel **Recursos**.

# Administrar centros de datos

Las listas de centros de datos se muestran en el **Infraestructura** del panel **Recursos** en dominios. Antes de agregar centros de datos, debe crear al menos un dominio.

## Agregar un centro de datos

*Para agregar un centro de datos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En la parte superior de la página, haga clic en **+ Centro de datos**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del centro de datos. La longitud máxima del nombre es de 50 caracteres.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del centro de datos. La longitud máxima de la descripción es de 100 caracteres.

5. En la lista desplegable **Dominio**, seleccione el dominio creado al que desea agregar el centro de datos. Después de agregar el centro de datos, puede migrarlo a un dominio diferente.

6. Si desea implementar funciones de red virtual y ejecutar scripts en dispositivos CPE, en el campo **URL de VNFM**, ingrese la dirección web del administrador de funciones de red virtual al que se conecta el orquestador. Para verificar que el VNFM está disponible, puede hacer clic en **Probar conexión**.

7. Si es necesario, en el campo **Ubicación**, ingrese la dirección geográfica del centro de datos.

8. Haga clic en **Crear**.

El centro de datos se agrega y se muestra en el panel **Recursos**.

## Editar un centro de datos

*Para editar un centro de datos, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, haga clic en el ícono de configuración ⚙ → **Editar** junto al centro de datos que desea editar.

3. En la ventana que se abre, si es necesario, edite la siguiente configuración:
   - Nombre del centro de datos
   - Breve descripción del centro de datos
   - URL del Administrador de funciones de la red virtual
   - Dirección del centro de datos
4. Haga clic en **Guardar**.

El centro de datos se modifica y actualiza en el panel **Recursos**.

# Migrar un centro de datos a un dominio diferente

*Para migrar un centro de datos a un dominio diferente, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, haga clic en el ícono de configuración → **Migrar** junto al centro de datos que desea migrar a un dominio diferente.
3. En la ventana que se abre, seleccione el dominio creado al que desea migrar su centro de datos.
4. Haga clic en **Migrar**.

El centro de datos se migra al nuevo dominio y se muestra bajo el nuevo dominio en el panel **Recursos**.

# Eliminar un centro de datos

La eliminación de un centro de datos imposibilita la administración de controladores, VIM y subredes de administración dentro del centro de datos. También le impide especificar el servidor proxy Zabbix para configurar la supervisión de los componentes de la solución.

Los centros de datos eliminados no se pueden restaurar.

*Para eliminar un centro de datos, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, haga clic en el ícono de configuración → **Eliminar** junto al centro de datos que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

El centro de datos se elimina y ya no se muestra en el panel **Recursos**.

# Administrar subredes de administración

Para ver la tabla de subredes de administración, vaya a la sección del menú **Infraestructura**, haga clic en el centro de datos agregado y seleccione la pestaña **IPAM**. La información sobre las subredes de administración se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la subred de administración.
- **Tipo** es el tipo de subred. Actualmente, solo se admiten subredes de administración.
- **CIDR** es el prefijo IPv4 de la subred de administración.
- **Gateway** son direcciones IPv4 de las puertas de enlace que la subred de administración asigna a las funciones de red virtual.
- **Rango de IP** son rangos de direcciones IP desde los cuales la subred de administración asigna direcciones IP a los dispositivos CPE y las funciones de red virtual.
- **DNS** son direcciones IPv4 de los servidores DNS que la subred de administración asigna a las funciones de la red virtual.
- **Rutas estáticas** son direcciones IPv4 de origen y destino de rutas estáticas que la subred de administración asigna a las funciones de red virtual.
- **Uso** es la cantidad de direcciones IP que la subred de administración asignó a los dispositivos CPE y las funciones de red virtual.

Puede ver una tabla de los dispositivos CPE y las funciones de red virtual a las que la subred de administración asignó direcciones IP. Para hacerlo, seleccione la pestaña **Uso**. La información sobre los dispositivos CPE y las funciones de la red virtual se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la subred de administración que asignó una dirección IP al CPE o la función de red virtual.
- **Dirección IP** es la dirección IP asignada al dispositivo CPE o la función de red virtual.
- **Nombre de cliente** es el nombre del dispositivo CPE o la función de red virtual.
- **Tipo de cliente** es información sobre si la subred de control asignó una dirección IP al dispositivo CPE o a la función de red virtual:
  - **VNF**
  - **CPE**
- **Inquilino**es el inquilino al que se agregó el dispositivo CPE o se asignó la función de red virtual.

Las acciones que puede realizar con las tablas se describen en las instrucciones de Administración de las tablas de componentes de la solución.

# Crear una subred de administración

*Para crear una subred de administración, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que desea crear la subred de administración. Una vez que se crea la subred de administración, no se puede mover a un centro de datos diferente.

3. Seleccione la pestaña **IPAM**.

   De manera predeterminada, está seleccionada la pestaña **Subred**, que muestra la tabla de subredes de administración.

4. En la parte superior de la página, haga clic en **+ Subred**.

5. En el campo **Nombre**, escriba el nombre de la subred de administración.

6. En la lista desplegable **Versión de IP**, seleccione la versión de las direcciones IP en la subred de administración:

   - **IPv4**. Esta es la configuración predeterminada.
   - **IPv6**.

7. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de administración.

8. Si desea que la subred de administración asigne una puerta de enlace particular a las funciones de la red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

9. Especifique el rango de direcciones IP desde el cual la subred de administración asigna direcciones IP a los dispositivos CPE y las funciones de la red virtual. Para hacerlo, en **Rango de IP**, haga clic en **+ Agregar** y, en los campos que se muestran, ingrese los valores inicial y final del rango de direcciones IP.

   El rango de direcciones IP se especifica y se muestra en la sección **Rango de IP**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en el ícono de eliminar ✕ junto a él.

10. Especifique el servidor DNS que la subred de administración asigna a las funciones de la red virtual. Para hacerlo, en **DNS**, haga clic en **+ Agregar** y, en el campo que se muestra, ingrese la dirección IPv4 del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

11. Especifique la ruta estática que la subred de administración asigna a las funciones de la red virtual. Para hacerlo, en **Rutas estáticas**, haga clic en **+ Agregar** y, en los campos que se muestran, ingrese las direcciones IPv4 de origen y destino de la ruta estática.

    La ruta estática se especifica y se muestra en la sección **Rutas estáticas**. Puede especificar varias rutas estáticas o eliminar rutas estáticas. Para eliminar una ruta estática, haga clic en el ícono de eliminar ✕ junto a ella.

12. Haga clic en **Crear**.

La subred de administración se crea y se muestra en la tabla.

# Editar una subred de administración

*Para editar una subred de administración, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que creó la subred de administración.

3. Seleccione la pestaña **IPAM**.

   De manera predeterminada, está seleccionada la pestaña **Subred**, que muestra la tabla de subredes de administración.

4. Haga clic en **Administración** → **Editar** junto a la subred de administración que desea editar.

5. En la ventana que se abre, si es necesario, edite la siguiente configuración:

   - Nombre de la subred de administración
   - Prefijo IPv4 de la subred de administración
   - Direcciones IPv4 de las puertas de enlace que la subred de administración asigna a las funciones de red virtual
   - Rangos de direcciones IP desde los cuales la subred de administración asigna direcciones IP a los dispositivos CPE y funciones de red virtual
   - Servidores DNS que la subred de administración asigna a las funciones de red virtual
   - Rutas estáticas que la subred de administración asigna a las funciones de red virtual

6. Haga clic en **Guardar**.

La subred de administración se modifica y se actualiza en la tabla.

# Eliminar una subred de administración

Las subredes de administración eliminadas no se pueden restaurar.

*Para eliminar una subred de administración, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que creó la subred de administración.

3. Seleccione la pestaña **IPAM**.

   De manera predeterminada, está seleccionada la pestaña **Subred**, que muestra la tabla de subredes de administración.

4. Haga clic en **Administración** → **Eliminar** junto a la subred de administración que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

La subred de administración se elimina y ya no se muestra en la tabla.

# Administrar controladores

Para ver la tabla de controladores, vaya a la sección del menú **Infraestructura**, haga clic en el centro de datos creado y seleccione la pestaña **Recursos de la red**. La información sobre los controladores se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del controlador.
- **Estrategia de servicio/transporte** es la estrategia de transporte que se utiliza.
- **Tipo de conexión** es el tipo de conexión de los dispositivos CPE al controlador:
  - **Unidifusión**
  - **Multidifusión**
- **Estado del clúster** es el estado del clúster de los nodos del controlador:
  - **Arriba** significa que el clúster está funcionando normalmente.
  - **Degradado** significa que se produjo un error durante el funcionamiento del clúster.
  - **Abajo** significa que el clúster no está funcionando.
- **Nodos del controlador** son las direcciones IP de los nodos del controlador.

- **Estados de los nodos** es el estado de los nodos del controlador:
  - **Conectados** significa que el nodo está conectado al controlador.
  - **Desconectado** significa que el nodo no está conectado al controlador.
  - **No disponible** significa que el nodo no está disponible.
  - **Desconocido** significa que se desconoce el estado del nodo.
- **Rol en el clúster** es la función del nodo en el clúster:
  - **Principal** significa que el nodo está conectado al controlador y es el nodo principal del clúster.
  - **Secundario** significa que el nodo está conectado al controlador y es el nodo secundario del clúster.
  - **Único** significa que el nodo está conectado al controlador y es el único nodo del clúster.
  - **Arbitraje** significa que el nodo es el árbitro.
  - **Conectado (transición)** significa que se está modificando la función del nodo en el clúster.
  - **En ningún clúster** significa que el nodo no se agrega a un clúster.
  - **No disponible** significa que el nodo no está disponible.
  - **Desconocido** significa que se desconoce el estado del nodo.
- **Nodo de lectura de gRPC activo** indica si el nodo se selecciona como el nodo de prioridad para las operaciones de lectura con el fin de equilibrar la carga.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Editar un controlador

*Para editar un controlador, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Editar** junto al controlador que desea editar.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del controlador. Rango de valores: de 1 a 128 caracteres.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del controlador.

5. En el campo **Instalación del controlador en servidores <1>/<3>/<5>**, seleccione el número de nodos del controlador.

6. En la lista desplegable **Tipo de conexión**, seleccione el tipo de conexión de los dispositivos CPE al controlador:

   - **Unidifusión**
   - **Multidifusión**

7. Configure el nodo del controlador:

   a. En el campo **Dirección IP o nombre de host**, ingrese la dirección IP o el nombre de host del nodo del controlador.

   b. En el campo **Puerto gRPC**, ingrese el número de puerto gRPC del nodo del controlador.

   c. En el campo **Puerto JGroups**, ingrese el número de puerto jGroups del nodo del controlador.

   d. Si desea que el nodo del controlador sea el nodo principal, seleccione la opción **Principal**.

   Puede configurar varios nodos de controlador.

8. Si desea cambiar la forma en que se distribuye la carga entre los nodos en el clúster del controlador cuando se leen datos, en la lista desplegable **Modo de equilibrio de carga de lectura gRPC**, seleccione un modo de equilibrio:

   - **Solo nodo principal**.

     Las operaciones de lectura se realizan exclusivamente a través del nodo del clúster principal.

   - **Priorizar nodo secundario aleatorio**.

     Las operaciones de lectura se realizan dando prioridad a un nodo de clúster secundario elegido al azar.

   - **Seleccionar manualmente**.

     Las operaciones de lectura se realizan a través de un nodo de clúster priorizado que se especifica explícitamente.

   Si selecciona el modo **Seleccionar manualmente**, en la lista **Nodo seleccionado** que aparece, seleccione el nodo de prioridad a través del cual desea leer las operaciones a realizar.

9. Haga clic en **Guardar**.

El controlador se modifica y actualiza en la tabla.

# Reaprovisionar un controlador

Durante el reaprovisionamiento, las propiedades del controlador se restablecen a sus valores predeterminados. Esto puede ayudar a resolver errores.

*Para reaprovisionar el controlador, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Reaprovisionar** junto al controlador que desea reaprovisionar.
3. En la ventana de confirmación, haga clic en **Reaprovisionar**.

Se reaprovisiona el controlador.

# Restaurar la configuración del controlador

Puede descargar un archivo con la configuración del controlador que especificó en el menú de configuración del controlador. Por ejemplo, este archivo contiene la configuración de los servicios de transporte y la configuración de la calidad del servicio. Si es necesario, puede restaurar la configuración del controlador mediante el uso del archivo descargado.

*Para restaurar la configuración del controlador, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.
2. Haga clic en **Administración** → **Descargar archivo de respaldo** junto al controlador cuyo archivo de configuración desea descargar.

   Se guarda un archivo con la configuración del controlador en formato YAML en su dispositivo local.
3. Haga clic en **Administración** → **Restaurar** junto al controlador para el que desea restaurar la configuración.
4. En la ventana que se abre, especifique la ruta al archivo descargado que tiene la configuración del controlador.
5. Haga clic en **Restaurar**.

El controlador se restaura con la configuración del archivo de configuración del controlador.

# Habilitar o deshabilitar el modo de mantenimiento en un controlador

Puede habilitar el modo de mantenimiento en el controlador cuando se lleve a cabo trabajo de mantenimiento relacionado con la red de SD-WAN para minimizar el impacto del controlador en partes de la red de SD-WAN que no se vean afectadas por el trabajo de mantenimiento. En el modo de mantenimiento, el controlador supervisa el estado de la red de SD-WAN, pero no realiza ninguna acción cuando los parámetros de la red de SD-WAN cambian. Por ejemplo, en el modo de mantenimiento, el controlador no vuelve a compilar los vínculos y las rutas, no vuelve a escribir las direcciones MAC de las interfaces de servicio ni cambia los servicios de transporte.

Cuando se deshabilita el modo de mantenimiento, el controlador realiza acciones correspondientes a los cambios que hizo en los parámetros de la red SD-WAN.

*Para habilitar o deshabilitar el modo de mantenimiento en el controlador, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Realice una de las siguientes acciones:

   - Si desea habilitar el modo de mantenimiento en el controlador, haga clic en **Administración** → **Habilitar mantenimiento** junto a él.
   - Si desea deshabilitar el modo de mantenimiento en el controlador, haga clic en **Administración** → **Deshabilitar mantenimiento** junto a él.

El modo de mantenimiento se habilitará o deshabilitará en el controlador.

# Eliminar un controlador

Los controladores eliminados no se pueden restaurar.

*Para eliminar un controlador:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Eliminar** junto al controlador que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

El controlador se elimina y ya no se muestra en la tabla.

# Administrar las propiedades del controlador

Las propiedades regulan el funcionamiento del controlador. Cada propiedad tiene un *método de cambio* que determina si el valor de la propiedad se puede cambiar y cuándo el cambio entra en vigencia. Están disponibles los siguientes métodos de cambio:

- **Solo lectura** significa que la propiedad no se puede cambiar.
- **Recarga** significa que cuando se cambia una propiedad, el orquestador confirma el nuevo valor en la base de datos del controlador. El nuevo valor se aplicará después de reiniciar el controlador.

  Un valor de propiedad que está en la base de datos, pero que aún no se aplicó, se denomina *valor planificado*. Puede eliminar el valor planificado antes de reiniciar el controlador para mantener el valor actual.
- **Tiempo de ejecución** significa que el nuevo valor se aplicará apenas modifique la propiedad.

Modificar las propiedades puede provocar que el controlador funcione de forma inestable, por lo que le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky antes de hacerlo.

Puede ver la tabla de todas las propiedades del controlador o solo las propiedades del controlador modificables:

- Para ver la tabla de todas las propiedades del controlador, navegue hasta la sección **Infraestructura**, haga clic en el centro de datos agregado, seleccione la pestaña **Recursos de la red** y haga clic en **Administración** → **Propiedades** junto al controlador.
- Para ver la tabla de propiedades modificables del controlador, vaya a la sección **Infraestructura**, haga clic en el centro de datos agregado, seleccione la pestaña **Recursos de la red**, haga clic en **Administración** → **Propiedades** junto al controlador y seleccione la pestaña **Propiedades modificables**.

La información sobre las propiedades del controlador se muestra en las siguientes columnas de la tabla:

- **Cambiar método** es el método de cambio de la propiedad.
- **Propiedad** es el nombre de la propiedad.
- **Valor actual** es el valor actual de la propiedad.
- **Valor planificado** es el valor planificado de la propiedad. Esta columna solo se muestra en la pestaña **Propiedades modificables**.

Las acciones que puede realizar con la tabla se describen en el artículo Administración de las tablas de componentes de la solución.

## Descripción de las propiedades editables del controlador

Modificar las propiedades puede provocar que el controlador funcione de forma inestable, por lo que le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky antes de hacerlo.

| Propiedad | Descripción |
|---|---|
| `controller.buffers.in` | Tamaño del búfer, en bytes, para mensajes provenientes de los conmutadores del controlador. |
| `controller.buffers.out` | Tamaño del búfer, en bytes, para los mensajes que se envían a los conmutadores del controlador. |
| `controller.listen.port` | El número de puerto inicial en el rango de puertos del conmutador. Los puertos con los siguientes tres números consecutivos se agregan al rango. Por ejemplo, si escribe `6553`, el rango de puertos del conmutador incluye los puertos 6553, 6554, 6555, 6556. |
| `controller.sockets.config.nodelay` | Si el parámetro `TCP_NODELAY` se utiliza para las sesiones de administración entre los conmutadores y el controlador. Valores posibles:<br>• `true`<br>• `false` |
| `controller.sockets.mode.epoll` | Si el controlador utiliza el sistema epoll durante la administración de los conmutadores. Valores posibles:<br>• `true`<br>• `false` |
| `controller.sockets.timeouts.idle.both` | Tiempo en milisegundos después del cual las sesiones de administración entre los conmutadores y el controlador quedan inactivas ante la ausencia de operaciones de lectura o escritura. La cuenta regresiva comienza de nuevo cada vez que se realiza una operación de lectura o escritura. |
| `controller.sockets.timeouts.idle.read` | Tiempo en milisegundos después del cual las sesiones de administración entre los conmutadores y el controlador quedan inactivas ante la ausencia de operaciones de lectura. La cuenta regresiva comienza de nuevo cada vez que se realiza una operación de lectura. |

| Propiedad | Descripción |
| --- | --- |
| `controller.sockets.timeouts.idle.write` | Tiempo en milisegundos después del cual las sesiones de administración entre los conmutadores y el controlador quedan inactivas ante la ausencia de operaciones de escritura. La cuenta regresiva comienza de nuevo cada vez que se realiza una operación de escritura. |
| `controller.threads.affinity` | Los subprocesos de Netty se ejecutan preferentemente en núcleos de CPU independientes para conmutadores independientes. Valores posibles:<br>• `true`<br>• `false` |
| `controller.threads.boss` | Número de subprocesos de Netty para gestionar las nuevas conexiones del conmutador. |
| `controller.tls.ca.certificate.path` | Ruta al archivo PEM del certificado raíz que se utilizó para firmar el certificado de OpenFlow. |
| `controller.tls.certificate.path` | Ruta al archivo PEM del certificado de cifrado para el tráfico de OpenFlow entre el controlador y los conmutadores. |
| `controller.tls.private.key.path` | Ruta al archivo PEM con la clave privada del certificado de OpenFlow. |
| `controller.watermark.high` | Cuando el búfer de Netty de la sesión de administración entre los conmutadores y el controlador contiene este número de bytes, la cola se usa para escribir en la sesión. |
| `controller.watermark.low` | Cuando el búfer de Netty de la sesión de administración entre los conmutadores y el controlador contiene este número de bytes, la cola ya no se usa para escribir en la sesión.<br>Esta propiedad se utiliza cuando el número de bytes alcanza el valor `controller.watermark.high`. |
| `core.catcher.meter.value.kbits` | El rendimiento del regulador en los conmutadores durante el envío de paquetes de tráfico a través de la sesión de administración entre los conmutadores y el controlador. Los paquetes de tráfico se copian mediante reglas de flujo de interceptación. |
| `core.drop.rule.idle.sec` | Tiempo, en segundos, después del cual las reglas de flujo creadas automáticamente por el controlador durante el procesamiento del primer paquete de tráfico interceptado se eliminan en los conmutadores para bloquear los paquetes posteriores. La cuenta regresiva comienza de nuevo cada vez que se aplica la regla de flujo. |
| `core.link.bonding.enable` | Unión de vínculos paralelos entre dos conmutadores. Valores posibles:<br>• `true`<br>• `false` |
| `core.link.bonding.equal.cost` | Si se utiliza el algoritmo de igual costo durante la unión de vínculos. Valores posibles:<br>• `true`<br>• `false`<br>Si especifica `false`, se utiliza el algoritmo de costo desigual. |
| `core.link.bonding.max.links` | Número máximo de vínculos en un vínculo unido. |
| `core.link.bonding.mode` | Tipo de grupo de vínculos unidos. Valores posibles:<br>• `BALANCING` significa que el tráfico se equilibra entre los vínculos de acuerdo con un valor hash. El hash se calcula en función de los campos `IP Proto`, `IP src-dst` y `Port src-dst` de los paquetes de tráfico.<br>• `BROADCAST` significa que el tráfico se duplica a través de todos los vínculos. |
| `core.link.check.ports.status` | Si el controlador envía periódicamente paquetes LLDP solo a los puertos habilitados para detectar vínculos entre conmutadores. Valores posibles:<br>• `true`<br>• `false` |
| `core.link.enabled.ports.only` | Si los conmutadores transmiten paquetes LLDP al controlador solo desde los puertos habilitados cuando el controlador intenta descubrir vínculos entre los conmutadores. Valores posibles:<br>• `true`<br>• `false` |
| `core.link.liveness.interval` | Intervalo en milisegundos para que el controlador envíe paquetes LLDP a través de los vínculos del conmutador. |

| Propiedad | Descripción |
| --- | --- |
| `core.link.liveness.timeout` | Intervalo en milisegundos para que el lado receptor de los vínculos del conmutador reciba paquetes LLDP y reenvíe los paquetes LLDP al controlador. Si no llegan paquetes LLDP a través del vínculo dentro del tiempo especificado, el controlador considera que el vínculo no está disponible. |
| `core.lldp.sendrem.enabled` | Indica si los conmutadores envían notificaciones al controlador cada vez que se eliminan las reglas de flujo que envían paquetes de tráfico al controlador. Valores posibles:<br>• `true`<br>• `false` |
| `core.switch.liveness.interval` | Intervalo en milisegundos para verificar la conexión de los conmutadores al controlador. |
| `core.switch.liveness.timeout` | Tiempo en milisegundos dentro del cual los conmutadores desconectados deben volver a conectarse al controlador. |
| `core.tunnel.port.end` | Número de la última interfaz de red virtual (VNI) en el rango de interfaces de conmutador. |
| `core.tunnel.port.start` | Número de la primera interfaz de red virtual en el rango de interfaces de conmutador. |
| `dampening.link.enabled` | Indica si se utiliza la amortiguación de vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `dampening.link.maxSuppressTime.ms` | Tiempo máximo en milisegundos durante el cual se puede restringir el acceso al vínculo. Cuando transcurre el tiempo especificado, todos los contadores de amortiguación se restablecen. |
| `dampening.link.penalty` | El número en el que se incrementa la penalización cuando el vínculo cambia de estado. |
| `dampening.link.suppressLevel` | El valor de penalización en el que se restringe el acceso al vínculo. |
| `dampening.link.updateInterval.ms` | Tiempo en milisegundos dentro del cual la penalización debe alcanzar el valor de `dampening.link.suppressLevel` para restringir el acceso al vínculo. |
| `eth.s.type` | El valor de TPID IEEE 802.1Q que se especifica como la etiqueta interna para paquetes de tráfico con clasificación de tráfico Q-in-Q. |
| `eth.t.type` | El valor de TPID IEEE 802.1Q que se especifica como la etiqueta externa para paquetes de tráfico con clasificación de tráfico Q-in-Q. |
| `inband.statistics.enabled` | Obtención de estadísticas sobre conmutadores. Las estadísticas contienen información sobre los dispositivos de red a los que está conectado el conmutador, así como sobre las conexiones de los puertos que se utilizan. Valores posibles:<br>• `true`<br>• `false` |
| `inband.swos.cookie` | Valor del campo `cookie` en el mensaje para solicitar estadísticas de los conmutadores. Valores posibles:<br>• `true`<br>• `false`<br>Esta propiedad debe especificarse si, para `inband.statistics.enabled`, especificó `true`. |
| `network.control.queue.id` | ID de la cola de paquetes LLDP en los conmutadores. |
| `notification.all.queue.max.size` | Tamaño máximo de la cola de notificaciones push en los conmutadores. Si se excede este tamaño, se elimina la primera notificación emergente de la cola. |
| `openflow.fail2ban.banTimeSec` | Duración en segundos durante la cual las direcciones IP y los puertos de los conmutadores se bloquean después de un intento de conexión al controlador con un certificado TLS no válido. |
| `openflow.fail2ban.enabled` | Indica si las direcciones IP y los puertos de los conmutadores se bloquean después de un intento de conexión al controlador con un certificado TLS no válido. Valores posibles:<br>• `true`<br>• `false` |

| Propiedad | Descripción |
| --- | --- |
| `openflow.fail2ban.findTimeSec` | Tiempo en segundos dentro del cual los conmutadores deben realizar el número de intentos (especificado en la propiedad `openflow.fail2ban.maxRetry`) para establecer la conexión al controlador con un certificado TLS no válido, lo que hace que las direcciones IP y los puertos de estos conmutadores se bloqueen. |
| `openflow.fail2ban.maxRetry` | El número de intentos de los conmutadores para establecer una conexión al controlador con un certificado TLS no válido, después de lo cual se bloquean las direcciones IP y los puertos de los conmutadores. |
| `openflow.io.cpe.rate.limiter.read.byteps` | Esta propiedad ya no se utiliza. |
| `openflow.io.cpe.rate.limiter.write.byteps` | Esta propiedad ya no se utiliza. |
| `openflow.io.ovs.meters.enabled` | Indica si las reglas de flujo envían paquetes de tráfico al controlador. Valores posibles:<br>• `true`<br>• `false` |
| `openflow.io.rate.limiter.switch.type-to-rate` | Esta propiedad ya no se utiliza. |
| `openflow.io.switch.latency.monitoring.delay.ms` | Intervalo en milisegundos para comprobar la latencia entre el controlador y los conmutadores. |
| `openflow.io.switch.latency.monitoring.enabled` | Indica si se comprueba la latencia entre el controlador y los conmutadores. Valores posibles:<br>• `true`<br>• `false` |
| `openflow.io.switch.latency.sma.initial.drop.size` | Número de paquetes de tráfico principales en los conmutadores, que no se cuentan para las estadísticas. |
| `openflow.io.switch.latency.sma.window.size` | Número de paquetes de tráfico de seguimiento en los conmutadores, que no se cuentan para las estadísticas. |
| `openflow.io.switch.messages.chunk.bytes` | Tamaño, en bytes, de los fragmentos de mensajes de OpenFlow serializados que el controlador envía a los conmutadores. |
| `openflow.io.switch.messages.window.size` | Número máximo de bloques de mensajes de OpenFlow serializados en la cola del controlador. |
| `openflow.io.switch.rate.limiter.read.byteps` | Esta propiedad ya no se utiliza. |
| `openflow.io.switch.rate.limiter.write.byteps` | Esta propiedad ya no se utiliza. |
| `openflow.io.vtep.rate.limiter.read.byteps` | Esta propiedad ya no se utiliza. |
| `openflow.io.vtep.rate.limiter.write.byteps` | Esta propiedad ya no se utiliza. |
| `segment.path.num.max` | Número máximo de rutas en un segmento. |
| `segment.path.spf.num.max` | Número máximo de rutas SPF para el equilibrio automático. |
| `table-miss.mode` | Acción que realizan los conmutadores con paquetes de tráfico que no están en ninguna de las tablas de OpenFlow. Valores posibles:<br>• `DROP` para descartar los paquetes de tráfico.<br>• `TO_CTL` para enviar los paquetes de tráfico al controlador. |
| `topology.cfm.enabled` | Indica si se utiliza la Administración de fallas de conectividad (CFM) en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.debug.enabled` | Indica si se utilizan rutinas de depuración del controlador que involucran el protocolo gRPC. Valores posibles:<br>• `true`<br>• `false` |
| `topology.intervtep.links.enabled` | Establecimiento de vínculos entre VTEP. Valores posibles:<br>• `true`<br>• `false` |

| Propiedad | Descripción |
| --- | --- |
| `topology.link.charged` | Uso de todos los vínculos como último recurso para enrutar el tráfico, independientemente de la calidad del vínculo. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.discovery.groups.enabled` | Descubrimiento de vínculos por grupos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.encryption.enabled` | Cifrado de tráfico en vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.encryption.key.update.interval.minutes` | Intervalo en minutos para actualizar la clave de descifrado en los vínculos. |
| `topology.link.error.monitoring.enabled` | Supervisión de errores en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.error.threshold.eps` | Valor de umbral del número de errores por segundo en los vínculos. |
| `topology.link.eu.monitoring.delay.sec` | Intervalo en segundos para medir el número de errores en los vínculos y la utilización del vínculo. |
| `topology.link.fec.enable` | Indica si se utiliza la corrección de errores de reenvío (FEC) en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.fec.ratio` | Proporción de los paquetes de tráfico originales respecto de los paquetes de tráfico adicionales con código redundante. Ingrese un valor en el formato `<número de paquetes originales>:<número de paquetes adicionales>`. |
| `topology.link.fec.timeout` | El tiempo máximo, en milisegundos, durante el cual un paquete de tráfico puede permanecer en la cola para que se aplique FEC. |
| `topology.link.jitter.monitoring.enabled` | Supervisión de fluctuación en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.jitter.threshold.ms` | Umbral de tiempo de fluctuación en los vínculos, en milisegundos. |
| `topology.link.latency.monitoring.enabled` | Supervisión de latencia en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.latency.threshold.ms` | Umbral de latencia en los vínculos, en milisegundos. |
| `topology.link.ljp.monitoring.delay.sec` | Intervalo en segundos para comparar las cifras de supervisión recibidas con los umbrales especificados de latencia, fluctuación y pérdida de paquetes en los vínculos. |
| `topology.link.ljp.stats.collecting.enabled` | Supervisión de latencia, fluctuación y pérdida de paquetes de tráfico en los vínculos. Valores posibles:<br>• `true`<br>• `false`<br>Puede especificar el protocolo de supervisión mediante la propiedad `topology.link.ljp.stats.collecting.method`. |
| `topology.link.ljp.stats.collecting.lldp.window` | Tamaño en bytes del búfer adicional en cada paquete LLDP para las cifras de supervisión de latencia, jitter y pérdida de paquetes.<br>Esta propiedad debe especificarse si, para `topology.link.ljp.stats.collecting.method`, especificó `GENEVE`. |
| `topology.link.ljp.stats.collecting.method` | Protocolo para supervisar la latencia, fluctuación y pérdida de paquetes de tráfico en los vínculos. Valores posibles:<br>• `LLDP`<br>• `GENEVE` |

| Propiedad | Descripción |
| --- | --- |
| `topology.link.ljp.stats.collecting.multiplicity` | El multiplicador que aplica el controlador a las cifras de supervisión de retraso, fluctuación y pérdida de paquetes.<br>Esta propiedad debe especificarse si, para `topology.link.ljp.stats.collecting.method`, especificó `GENEVE`. |
| `topology.link.packet.loss.monitoring.enabled` | Supervisión de la pérdida de paquetes de tráfico en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.packet.loss.threshold.percents` | Valor de umbral del porcentaje de pérdida de paquetes de tráfico en los vínculos. |
| `topology.link.pmtud.scheduler.interval.sec` | Intervalo en segundos para la detección automática de la cifra MTU en los vínculos. |
| `topology.link.pmtud.wait.time.ms` | Cuánto tiempo espera el controlador un paquete PMTUD LLDP, en milisegundos. Si el controlador no recibe un paquete PMTUD LLDP dentro de este tiempo, concluye que un paquete de este tamaño no se puede transmitir a través del vínculo. |
| `topology.link.threshold.monitoring.delay.sec` | Intervalo en segundos para la supervisión de los umbrales del vínculo. |
| `topology.link.threshold.monitoring.enabled` | Supervisión de umbral en los vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.threshold.monitoring.unban.periods` | Número de comprobaciones seguidas con éxito para desbloquear un vínculo. Se realiza una comprobación una vez por segundo. |
| `topology.link.util.monitoring.enabled` | Supervisión de la utilización del vínculo (uso del ancho de banda). Valores posibles:<br>• `true`<br>• `false` |
| `topology.link.util.threshold.percents` | Valor de umbral de utilización del vínculo como porcentaje del ancho de banda de las interfaces de servicio. |
| `topology.overlay.lldp.sender.concurrent` | Envío simultáneo de paquetes LLDP por parte del controlador para el descubrimiento de vínculos. Valores posibles:<br>• `true`<br>• `false` |
| `topology.overlay.lldp.sender.core.pool.size` | Número mínimo de secuencias para el envío simultáneo de paquetes LLDP por parte del controlador.<br>Esta propiedad debe especificarse si, para `topology.overlay.lldp.sender.concurrent`, especificó `true`. |
| `topology.overlay.lldp.sender.max.pool.size` | Número máximo de secuencias para el envío simultáneo de paquetes LLDP por parte del controlador.<br>Esta propiedad debe especificarse si, para `topology.overlay.lldp.sender.concurrent`, especificó `true`. |
| `topology.overlay.lldp.sender.max.queue.capacity` | Tamaño máximo de la cola cuando el controlador envía paquetes LLDP al mismo tiempo.<br>Esta propiedad debe especificarse si, para `topology.overlay.lldp.sender.concurrent`, especificó `true`. |
| `topology.reserve.si.auto.revert.enabled` | La interfaz de servicio de reserva vuelve a ser reserva si la interfaz de servicio anterior vuelve a estar operativa. Valores posibles:<br>• `true`<br>• `false` |
| `topology.throttler.timeout.hard.enabled` | Acumulación de operaciones físicas en el controlador, como conectarse a un conmutador o un puerto, para realizar las operaciones cuando transcurre el tiempo especificado. Valores posibles:<br>• `true`<br>• `false`<br>Puede especificar la hora mediante las propiedades `topology.throttler.timeout.hard.ms` y `topology.throttler.timeout.idle.ms`. |

| Propiedad | Descripción |
| --- | --- |
| `topology.throttler.timeout.hard.ms` | Tiempo en segundos tras el cual se llevan a cabo las operaciones físicas acumuladas en el controlador.<br>Esta propiedad debe especificarse si, para `topology.throttler.timeout.hard.enabled`, especificó `true`. |
| `topology.throttler.timeout.idle.ms` | Tiempo en segundos tras el cual se llevan a cabo las operaciones físicas acumuladas en el controlador. La cuenta atrás comienza de nuevo cada vez que aparece una operación física.<br>Esta propiedad se puede especificar si, para `topology.throttler.timeout.hard.enabled`, especificó `true`. |
| `topology.throttler_future.enable` | Propiedad del sistema.<br>La edición de esta propiedad puede hacer que el controlador no funcione. |
| `topology.throttler_future.timeout.sec` | Propiedad del sistema.<br>La edición de esta propiedad puede hacer que el controlador no funcione. |

## Editar una propiedad del controlador

Los cambios realizados en las propiedades del controlador con el método de cambio de tiempo de ejecución se aplican de inmediato. Los cambios realizados en las propiedades del controlador con el método de cambio de recarga se aplican después de que se reinicia el controlador.

*Para cambiar una propiedad del controlador, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Propiedades** junto al controlador para el que desea cambiar una propiedad.

   Se muestra la página de propiedades del controlador. De manera predeterminada, la pestaña **Todas las propiedades** está seleccionada, que muestra una tabla de todas las propiedades del controlador.

3. Seleccione la pestaña **Propiedades modificables**.

   Se muestra una tabla de propiedades editables del controlador.

4. Haga clic en **Administración** → **Editar** junto a la propiedad del controlador que desea editar.

5. En la ventana que se abre, en el campo **Valor planificado**, ingrese el nuevo valor de la propiedad del controlador.

6. Haga clic en **Guardar**.

El nuevo valor de una propiedad con el método de tiempo de ejecución se muestra en la columna **Valor actual**. El nuevo valor de una propiedad con el método de recarga se muestra en la columna **Valor planificado**.

## Eliminar valores planificados de las propiedades del controlador

Puede eliminar un valor de planificación para deshacer un cambio de propiedad del controlador. Esta acción solo se aplica a las propiedades que tienen el método de recarga.

Los valores de planificación eliminados de las propiedades del controlador no se pueden restaurar.

*Para eliminar los valores de planificación de las propiedades del controlador, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. Haga clic en **Administración** → **Propiedades** junto al controlador para el que desea eliminar los valores de planificación de las propiedades.

   Se muestra la página de propiedades del controlador. De manera predeterminada, la pestaña **Todas las propiedades** está seleccionada, que muestra una tabla de todas las propiedades del controlador.

3. Seleccione la pestaña **Propiedades modificables**.

   Se muestra una tabla de propiedades editables del controlador.

4. Elimine los valores de planificación de las propiedades del controlador de una de las siguientes maneras:

   - Si desea eliminar el valor de planificación de una propiedad individual del controlador, haga clic en **Administración** → **Eliminar valor planificado** junto a esa propiedad.

   - Si desea eliminar los valores de planificación de todas las propiedades del controlador, en la parte superior de la tabla, haga clic en el ícono de configuración → **Eliminar todos los valores planificados**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

Se eliminan los valores de planificación de las propiedades del controlador.

## Restablecer las propiedades del controlador a los valores predeterminados

*Para restablecer las propiedades del controlador a los valores predeterminados, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Propiedades** junto al controlador cuyas propiedades desea restablecer a los valores predeterminados.

   Se muestra la página de propiedades del controlador. De manera predeterminada, la pestaña **Todas las propiedades** está seleccionada, que muestra una tabla de todas las propiedades del controlador.

3. Seleccione la pestaña **Propiedades modificables**.

   Se muestra una tabla de propiedades editables del controlador.

4. Restablezca las propiedades del controlador de una de las siguientes maneras:

   - Si desea restablecer una propiedad individual del controlador a su valor predeterminado, haga clic en **Administración** → **Restablecer propiedad** junto a esa propiedad.

   - Si desea restablecer todas las propiedades del controlador a sus valores predeterminados, haga clic en el ícono de configuración en la parte superior de la tabla → **Restablecer todas las propiedades**.

5. En la ventana de confirmación, haga clic en **Restablecer**.

Las propiedades del controlador se restablecerán a sus valores predeterminados.

# Ver información acerca de los nodos del controlador

- Para ver información sobre los nodos del controlador, siga estos pasos:

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador para el que desea ver información sobre los nodos.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador. La información sobre los nodos del controlador se muestra en las siguientes columnas de la tabla:

   - **Dirección** es la dirección IP del nodo del controlador.

   - **Estados de los nodos** es el estado de los nodos del controlador:

     - **Conectados** significa que el nodo está conectado al controlador.

     - **Desconectado** significa que el nodo no está conectado al controlador.

     - **No disponible** significa que el nodo no está disponible.

     - **Desconocido** significa que se desconoce el estado del nodo.

   - **Rol en el clúster** es la función del nodo en el clúster:

     - **Principal** significa que el nodo está conectado al controlador y es el nodo principal del clúster.

     - **Secundario** significa que el nodo está conectado al controlador y es el nodo secundario del clúster.

     - **Único** significa que el nodo está conectado al controlador y es el único nodo del clúster.

     - **Arbitraje** significa que el nodo es el árbitro.

     - **Conectado (transición)** significa que se está modificando la función del nodo en el clúster.

     - **En ningún clúster** significa que el nodo no se agrega a un clúster.

- **No disponible** significa que el nodo no está disponible.
- **Desconocido** significa que se desconoce el estado del nodo.

- **Nodo de lectura de gRPC activo** indica si el nodo se selecciona como el nodo de prioridad para las operaciones de lectura con el fin de equilibrar la carga.
- **Puerto gRPC** es el número de puerto gRPC del nodo del controlador.
- **Puerto JGroups** es el número de puerto JGroups del nodo del controlador.
- **Versión** es la versión de software del nodo del controlador.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

3. Si desea ver las estadísticas de un nodo del controlador, haga clic en **Administración** → **Estadísticas** junto al nodo.
4. Si desea ver las propiedades de un nodo de controlador, haga clic en **Administración** → **Propiedades del nodo** junto al nodo.

# Administrar un VIM

Puede implementar un VIM en uno de sus centros de datos o en un dispositivo uCPE. La implementación del VIM en un centro de datos implica la administración centralizada del ciclo de vida de la función de la red virtual. La implementación del VIM en un dispositivo uCPE le permite entregar funciones de la red virtual a centros de datos remotos y administrarlas localmente.

Para ver la tabla de VIM, vaya a la sección del menú **Infraestructura**, haga clic en el centro de datos creado y seleccione la pestaña **IPAM** → **Recursos de cómputo**. La información sobre los VIM se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del VIM.
- **Tipo** es el tipo de VIM. Kaspersky SD-WAN utiliza la plataforma en la nube de OpenStack como VIM.
- **Función** es el centro de datos o dispositivo uCPE en el que se implementa el VIM.
- **IP de VIM** es la dirección IP del VIM.
- **Estado** es el estado de conexión del VIM a la plataforma en la nube de OpenStack:
  - **Conectados**.
  - **Desconectado**.
- **Clúster de SDN** es el clúster SDN al que está conectado OpenStack.
- **Detrás de NAT** le permite especificar si el VIM está detrás de NAT (traducción de direcciones de red):
  - **Sí**.
  - **No**.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Configurar un VIM implementado en un centro de datos

*Para configurar un VIM implementado en un centro de datos, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que implementó el VIM.

3. Seleccione la pestaña **Recursos de cómputo**.

   Se muestra una tabla de los VIM.

4. En la parte superior de la página, haga clic en **+ VIM**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del VIM.

6. En el campo **Dirección IP**, ingrese la dirección IP o el nombre de dominio para la conexión del orquestador al VIM.

7. En el campo **Puerto**, ingrese el número de puerto para la conexión del orquestador al servicio de identificación del VIM. El valor predeterminado es `5000`.

8. En la lista desplegable **Protocolo**, seleccione el protocolo para la conexión del orquestador al VIM:

   - **http** es la configuración predeterminada.
   - **https**.

9. En los campos **Nombre de usuario** y **Contraseña**, ingrese el nombre de usuario y la contraseña de una cuenta con privilegios de administrador para autenticar al orquestador en la plataforma en la nube de OpenStack. Si la autenticación es correcta, el orquestador obtiene acceso a la administración de la infraestructura virtual que está disponible para el administrador.

10. Especifique la configuración de autenticación avanzada del orquestador en la plataforma en la nube de OpenStack:

    a. En el campo **Proyecto de administrador**, ingrese el nombre del proyecto del administrador para la autenticación del orquestador en el proyecto del administrador.

    b. En el campo **Dominio**, ingrese el nombre de dominio de OpenStack para la autenticación del orquestador en el dominio de OpenStack.

11. En la lista desplegable **Detrás de NAT**, seleccione si el VIM está detrás de NAT:

    - **Habilitado** para indicar que el VIM está detrás de NAT y la traducción de direcciones de red ocurre cuando el VIM interactúa con la instancia SD-WAN.
    - **Deshabilitado** para indicar que el VIM no está detrás de NAT. Esta es la opción predeterminada.

12. Especifique las relaciones de sobrecompromiso para los recursos físicos:

    a. En el campo **Sobrecompromiso de CPU**, ingrese la relación de sobrecompromiso del núcleo de la CPU. El valor predeterminado es `1`.

    b. En el campo **Sobrecompromiso de RAM**, ingrese la relación de sobrecompromiso de la memoria RAM. El valor predeterminado es `1`.

    c. En el campo **Sobrecompromiso de disco**, ingrese la relación de sobrecompromiso de espacio en disco. El valor predeterminado es `1`.

    *Las relaciones de sobrecompromiso* le permiten aprovisionar máquinas virtuales con más recursos virtuales que los que están físicamente presentes. Esto es posible porque las máquinas virtuales no utilizan al máximo todos los recursos físicos disponibles al mismo tiempo. Por ejemplo, si especifica un factor de sobrecompromiso de espacio en disco de `3`, el espacio disponible en el disco virtual puede ser tres veces mayor que el espacio en disco disponible físicamente en el host.

    Cuando configura el sobrecompromiso, debe considerar cómo se relacionan las capacidades de su hardware con los requisitos de las máquinas virtuales. Si especifica una relación alta de sobrecompromiso para los recursos físicos y las máquinas virtuales los agotan, esto puede provocar un retraso en la red o la falta de disponibilidad de partes de la red.

13. En el campo **Paralelismo**, ingrese el número máximo de operaciones simultáneas entre el orquestador y el VIM. El valor predeterminado es `1`. Esta configuración le permite reducir el tiempo de procesamiento general para las operaciones, pero crea una carga adicional en la infraestructura virtual.

    Recomendamos no cambiar el valor predeterminado a menos que la velocidad de procesamiento general de la operación sea crítica para usted.

14. En la lista desplegable **Clúster de SDN**, seleccione el clúster SDN al que está conectado OpenStack. Si OpenStack no está conectado con un clúster SDN, seleccione **Ninguna**.

15. En el campo **Cantidad máxima de VLAN**, ingrese la cantidad máxima de VLAN que el VIM puede usar. Esta configuración permite al orquestador realizar un seguimiento del número de segmentos disponibles para su uso. Rango de valores: de 0 a 4094.

16. Si el VIM es compatible con SR-IOV, ingrese el nombre de la red física en el campo **Red física de SR-IOV**. El orquestador utiliza el nombre de la red física SR-IOV para conectarse a las máquinas virtuales con el tipo de interfaz SR-IOV.

17. Si está utilizando una red con el tipo de segmentación de VLAN para la administración, en el campo **Red física de VLAN**, ingrese la etiqueta VLAN.

18. Si seleccionó un clúster SDN en la lista desplegable **Clúster de SDN**, configure la conexión a ese clúster:

    a. Si desea asignar las redes lógicas de la instancia SD-WAN a una red física, ingrese el nombre de la red física en el campo **Red física de OpenStack**.

    b. En la lista desplegable **Grupo de puertos**, seleccione el grupo de puertos a través del cual todos los nodos de OpenStack se conectan con el clúster SDN.

c. En la lista desplegable **Grupo de control**, seleccione el grupo de puertos a través del cual los nodos de control de OpenStack se conectan con el clúster SDN.

d. Si es necesario, en la lista desplegable **Grupo de cómputo**, seleccione el grupo de puertos a través del cual los nodos de cómputo de OpenStack se conectan con el clúster SDN.

19. Si, en la lista desplegable **Clúster de SDN**, seleccionó **Ninguna**, configure la red:

a. Si desea asignar las redes planas de la instancia SD-WAN a una red física, ingrese el nombre de la red física en el campo **Red física plana**.

b. Si desea asignar la VXLAN de la instancia SD-WAN a una red física, ingrese el nombre de la red física en el campo **Red física de VXLAN**.

c. En la lista desplegable **Segmentación de red de control**, seleccione el tipo de segmentación para aislar y asegurar el tráfico del plano de control en la estructura SD-WAN:

- **VLAN**
- **VXLAN**

d. En el campo **ID del segmento de control**, ingrese el ID de segmento de la red de administración. El rango de valores depende del valor seleccionado en la lista desplegable **Segmentación de red de control**:

- Si seleccionó **VLAN**, el rango de valores es de 0 a 4095.
- Si seleccionó **VXLAN**, el rango de valores es de 0 a 16 000 000.

e. En la lista desplegable **Seguridad de puerto**, seleccione si desea habilitar la función de seguridad del puerto:

- **Habilitado**
- **Deshabilitado**

f. En el campo **Permitir CIDR**, ingrese el prefijo IPv4 de la subred permitida para la red de administración.

20. Haga clic en **Crear**.

El VIM se crea y se muestra en la tabla de la pestaña **Recursos de cómputo**.

# Configurar un VIM implementado en un dispositivo uCPE

Para configurar un VIM implementado en un dispositivo uCPE, debe especificar la configuración del VIM en una plantilla de uCPE. La configuración del VIM especificada en una plantilla de uCPE se aplica automáticamente a todos los dispositivos CPE que utilizan esta plantilla de uCPE.

*Para configurar un VIM implementado en un dispositivo uCPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de uCPE en la que desea configurar un VIM.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **VIM**.

   Se muestra la configuración del VIM.

4. En el campo **Puerto**, ingrese el número de puerto para la conexión del orquestador al servicio de identificación del VIM. El valor predeterminado es `5000`.

5. En la lista desplegable **Protocolo**, seleccione el protocolo para la conexión del orquestador al VIM:

   - **http** es la configuración predeterminada.
   - **https**.

6. En los campos **Nombre de usuario** y **Contraseña**, ingrese el nombre de usuario y la contraseña de una cuenta con privilegios de administrador para autenticar al orquestador en la plataforma en la nube de OpenStack. Si la autenticación es correcta, el orquestador obtiene acceso a la administración de la infraestructura virtual que está disponible para el administrador.

7. Especifique la configuración de autenticación avanzada del orquestador en la plataforma en la nube de OpenStack:

   a. En el campo **Proyecto de administrador**, ingrese el nombre del proyecto del administrador para la autenticación del orquestador en el proyecto del administrador.

   b. En el campo **Dominio**, ingrese el nombre de dominio de OpenStack para la autenticación del orquestador en el dominio de OpenStack.

8. Si está utilizando una red con el tipo de segmentación de VLAN para la administración, en el campo **Red física de VLAN**, ingrese la etiqueta VLAN.

9. En la lista desplegable **Detrás de NAT**, seleccione si el VIM está detrás de NAT:

   - **Habilitado** para indicar que el VIM está detrás de NAT y la traducción de direcciones de red ocurre cuando interactúa con el instancia SD-WAN.
   - **Deshabilitado** para indicar que el VIM no está detrás de NAT. Esta es la opción predeterminada.

10. Especifique las relaciones de sobrecompromiso para los recursos físicos:

    a. En el campo **Sobrecompromiso de CPU**, ingrese la relación de sobrecompromiso del núcleo de la CPU. El valor predeterminado es `1`.

    b. En el campo **Sobrecompromiso de RAM**, ingrese la relación de sobrecompromiso de la memoria RAM. El valor predeterminado es `1`.

    c. En el campo **Sobrecompromiso de disco**, ingrese la relación de sobrecompromiso de espacio en disco. El valor predeterminado es `1`.

*Las relaciones de sobrecompromiso* le permiten aprovisionar máquinas virtuales con más recursos virtuales que los que están físicamente presentes. Esto es posible porque las máquinas virtuales no utilizan al máximo todos los recursos físicos disponibles al mismo tiempo. Por ejemplo, si especifica un factor de sobrecompromiso de espacio en disco de 3, el espacio disponible en el disco virtual puede ser tres veces mayor que el espacio en disco disponible físicamente en el host.

Cuando configura el sobrecompromiso, debe considerar cómo se relacionan las capacidades de su hardware con los requisitos de las máquinas virtuales. Si especifica una relación alta de sobrecompromiso para los recursos físicos y las máquinas virtuales los agotan, esto puede provocar un retraso en la red o la falta de disponibilidad de partes de la red.

11. En el campo **Cantidad máxima de VLAN**, ingrese la cantidad máxima de VLAN que el VIM puede usar. Esta configuración permite al orquestador realizar un seguimiento del número de segmentos disponibles para su uso. Rango de valores: de 0 a 4094.

12. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Editar un VIM implementado en un centro de datos

*Para editar un VIM implementado en un centro de datos, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que implementó el VIM.

3. Seleccione la pestaña **Recursos de cómputo**.

   Se muestra una tabla de los VIM.

4. Haga clic en **Administración** → **Editar** junto al VIM que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del VIM. Para obtener una descripción de la configuración, consulte las instrucciones para configurar un VIM implementado en un centro de datos.

6. Haga clic en **Guardar**.

El VIM se modifica y actualiza en la tabla.

# Ver los recursos informáticos que utiliza un VIM

Puede ver la utilización de los siguientes recursos informáticos por parte del VIM:

- CPU
- RAM

- Espacio en disco
- Segmentos de red

*Para ver los recursos informáticos utilizados por el VIM, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que implementó el VIM.

3. Seleccione la pestaña **Recursos de cómputo**.

   Se muestra una tabla de los VIM.

4. Haga clic en **Administración** → **Mostrar uso** junto al VIM.

Se abre una ventana con información sobre los recursos informáticos utilizados por el VIM.

# Eliminar un VIM

Los VIM eliminados no se pueden restaurar.

*Para eliminar un VIM:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. En el panel **Recursos**, seleccione el dominio creado y, a continuación, seleccione el centro de datos agregado en el que implementó el VIM.

3. Seleccione la pestaña **Recursos de cómputo**.

   Se muestra una tabla de los VIM.

4. Haga clic en **Administración** → **Eliminar** junto al VIM que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El VIM se elimina y ya no se muestra en la tabla.

# Administrar usuarios y sus permisos de acceso

Para restringir el acceso al portal del administrador y al portal de autoservicio, así como a las secciones, subsecciones y funciones, la solución implementa un modelo de control de acceso basado en roles (RBAC). Las cuentas de usuario pueden tener los siguientes roles:

- Un administrador tiene acceso al portal del administrador y al portal de autoservicio.
- Un inquilino solo tiene acceso al portal de autoservicio.

Al implementar la solución, se crea el usuario **Administrador** con el rol de administrador y el usuario **Usuario** con el rol de inquilino.

Puede crear usuarios locales, usuarios LDAP y grupos de usuarios LDAP. La solución no admite la creación de grupos de usuarios locales. Las credenciales de los usuarios locales se almacenan en la base de datos del orquestador. Las credenciales de los usuarios LDAP y los grupos de usuarios LDAP se almacenan en un servidor remoto. Los servidores compatibles incluyen el servidor OpenLDAP remoto con autenticación SSL simple, así como Microsoft Active Directory con autenticación Kerberos y autenticación Kerberos SSL.

Primero debe crear una conexión LDAP que el orquestador usa para conectarse al servidor remoto y luego crear usuarios LDAP o grupos de usuarios LDAP. Los usuarios LDAP y los grupos de usuarios LDAP creados pueden iniciar sesión en la interfaz web del orquestador con sus credenciales.

## Autenticación de dos factores

Para mejorar el nivel de seguridad general de la solución, puede requerir la autenticación de dos factores de los usuarios mediante el algoritmo de contraseña de un solo uso basada en el tiempo (TOTP). Puede habilitar o deshabilitar la autenticación de dos factores para todos los usuarios. También puede habilitar o deshabilitar la autenticación de dos factores cuando crea o edita usuarios locales, usuarios LDAP y grupos LDAP.

Si la autenticación de dos factores está habilitada para un usuario, se genera un código QR único la próxima vez que el usuario inicia sesión en la interfaz web del orquestador. El usuario debe escanear un código QR utilizando un software o hardware RFC 6238 autenticador compatible, como Kaspersky Password Manager, Google Authenticator, Yandex Key y Microsoft Authenticator. El autenticador genera un código único que el usuario debe ingresar para completar la autenticación de dos factores e iniciar sesión en la interfaz web del orquestador. Si el usuario ingresa el código único incorrectamente más de cinco veces, ese usuario se bloquea durante 30 minutos.

Después de completar la autenticación de dos factores, el usuario debe ingresar un nombre de usuario, una contraseña y un código único para iniciar sesión en la interfaz web del orquestador. Si es necesario, puede hacer que el usuario complete la autenticación de dos factores nuevamente.

> Si la discrepancia de tiempo entre el orquestador y el autenticador es superior a 30 segundos, la autenticación de dos factores puede fallar. Recomendamos sincronizar la hora en el orquestador y el autenticador mediante un servidor NTP.

### Permisos de acceso

Si es necesario, puede crear permisos de acceso que determinen las secciones y subsecciones de la interfaz web del orquestador y las acciones que están disponibles para los usuarios, y asignar permisos de acceso cuando crea o edita usuarios y grupos LDAP. Por ejemplo, puede crear un permiso de acceso que prohíba el acceso a la sección **Catálogo** y la creación de plantillas de servicios de red.

De manera predeterminada, los usuarios y grupos de LDAP tienen el permiso de **acceso completo**, que otorga acceso completo a todas las funciones de la solución.

### Solicitudes de confirmación

Cuando crea o edita un usuario, debe especificar si desea que se cree una solicitud de confirmación cada vez que este usuario realiza una acción. Las solicitudes de confirmación se pueden confirmar, denegar o eliminar. Cuando se confirma una solicitud, se realiza la acción asociada. Las solicitudes de confirmación denegadas se guardan en la interfaz web del orquestador.

### Sesiones del usuario

La siguiente funcionalidad se utiliza para administrar las sesiones de los usuarios:

- Limitar la duración de las sesiones de los usuarios. Si un usuario permanece inactivo durante 3600 segundos (una hora) después de realizar el registro en la interfaz web del orquestador, la sesión del usuario finaliza automáticamente. Puede especificar manualmente el tiempo de inactividad antes del cierre de sesión automático.

- Finalizar las sesiones de usuario. Si varios empleados utilizan las mismas credenciales de cuenta de usuario para iniciar sesión en la interfaz web del orquestador, cualquiera de estos empleados puede finalizar las sesiones de los demás.

# Administrar permisos de acceso

Puede mostrar la lista de permisos de acceso en la sección **Usuarios**, en la pestaña **Permisos**. De manera predeterminada, se crea el permiso de **acceso completo**, que otorga acceso completo a la interfaz web del orquestador y se asigna automáticamente a los usuarios y grupos de usuarios LDAP si no les asigna un permiso de acceso diferente.

En las instrucciones de Administrar las tablas de los componentes de la solución, se describen las acciones que puede realizar con la lista.

# Crear permisos de acceso

*Para crear un permiso de acceso, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Permisos**.

   Se muestra la lista de permisos de acceso.

3. En la parte superior de la lista, haga clic en **+ Permiso**.

4. En el área de configuración que se muestra, en el campo **Nombre**, ingrese el nombre del permiso de acceso. La longitud máxima del nombre es de 250 caracteres.

5. En la sección **Derechos de acceso** junto a las secciones y subsecciones de la interfaz web del orquestador, seleccione uno de los siguientes valores:

   - **Edición** para permitir que los usuarios vean la sección o subsección y ejecuten todas las tareas disponibles.
   - **Visualización** para permitir que los usuarios solo vean la sección o subsección.
   - **Sin acceso** para evitar que los usuarios vean la sección o subsección.

   Si desea que las subsecciones hereden el valor seleccionado para la sección, seleccione la casilla **Aplicar a subsecciones**. Esta casilla está desactivada por defecto.

6. Haga clic en **Crear**.

El permiso de acceso se crea y se muestra en la lista.

Puede asignar un permiso de acceso durante la creación o edición de un usuario o durante la creación o edición de un grupo de usuarios LDAP.

# Editar permisos de acceso

*Para editar un permiso de acceso, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Permisos**.

   Se muestra la lista de permisos de acceso.

3. Haga clic en el permiso de acceso que desea editar.

4. En el área de configuración que se muestra, edite la siguiente configuración, si es necesario:

   - Nombre del permiso de acceso
   - Secciones y subsecciones de la interfaz web del orquestador y acciones disponibles para los usuarios

5. Haga clic en **Guardar**.

El permiso de acceso se modifica y se actualiza en la lista.

# Clonar permisos de acceso

Puede clonar un permiso de acceso para crear un permiso de acceso idéntico con un nombre diferente.

*Para clonar un permiso de acceso, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Permisos**.

   Se muestra la lista de permisos de acceso.

3. Haga clic en el permiso de acceso que desea clonar.

4. En la parte superior del área de configuración que se muestra, haga clic en **Administración** → **Clonar**.

5. En la ventana que se abre, ingrese el nombre del nuevo permiso de acceso.

6. Haga clic en **Clonar**.

Se crea un clon del permiso de acceso con el nuevo nombre y se agrega a la lista.

# Eliminar un permiso de acceso

Los permisos de acceso eliminados no se pueden restaurar.

*Para eliminar un permiso de acceso:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Permisos**.

   Se muestra la lista de permisos de acceso.

3. Haga clic en el permiso de acceso que desea eliminar.

4. En la parte superior del área de configuración que se muestra, haga clic en **Administración**→ **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El permiso de acceso se elimina y ya no se muestra en la lista.

# Administrar conexiones de LDAP

Puede consultar la tabla de conexiones de LDAP en la sección **Usuarios**, en la pestaña **Conexiones de LDAP**. La información sobre las conexiones de LDAP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la conexión de LDAP.
- **Tipo** es el tipo de conexión. Esta columna siempre muestra **LDAP**.
- **Host** es el nombre de host del servidor remoto.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una conexión de LDAP

Si desea que los usuarios de LDAP o los grupos de usuarios de LDAP puedan iniciar sesión en la interfaz web del orquestador con sus credenciales, primero debe crear una conexión de LDAP que el orquestador use para conectarse al servidor remoto y luego crear sus usuarios de LDAP o grupos de usuarios de LDAP.

*Para crear una conexión de LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Conexiones de LDAP**.

   Se muestra una tabla de conexiones de LDAP.

3. Haga clic en **+ LDAP**.

4. En el área de configuración que se muestra, en el campo **Nombre**, ingrese el nombre de la conexión de LDAP.

5. En el campo **Dominio**, ingrese el FQDN del dominio del servidor remoto.

6. En el campo **Alias del dominio**, ingrese el alias o el nombre NETBIOS del dominio. Los usuarios ingresan el alias, el nombre NETBIOS o el FQDN del dominio cuando inician sesión en la interfaz web del orquestador.

   Por ejemplo, si el FQDN del dominio es "ejemplo.com" y el alias es "ejemplo", un usuario llamado "admin" puede ingresar las siguientes credenciales cuando inicia sesión en la interfaz web del orquestador:

   - `admin@ejemplo.com`
   - `admin@ejemplo`
   - `ejemplo.com\admin`
   - `ejemplo\admin`

7. En el campo **Host de LDAP**, ingrese el nombre de host del servidor remoto. Se admiten los siguientes formatos de nombre de host:

   - `ldap://<nombre de host>:<número de puerto>` para un servidor LDAP estándar. El puerto predeterminado es 389.

   - `ldaps://<nombre de host>:<número de puerto>` para un servidor LDAP con autenticación SSL. El puerto predeterminado es 636.

   Por ejemplo, si ingresa `ldap://ejemplo.com:100`, el nombre de host del servidor remoto es "ejemplo.com" y el número de puerto es 100.

8. En el campo **Base DN**, ingrese el nombre distinguido base que utiliza el orquestador como punto de partida para buscar cuentas de usuario en el directorio del servidor remoto. Se admiten los siguientes formatos de nombre distinguido base:

   - Para buscar en OpenLDAP, ingrese el nombre distinguido base en el formato `OU=<valor>,OU=<valor>`m donde `OU` es la estructura de las unidades organizativas en el directorio del servidor remoto. Por ejemplo, si escribe `OU=OU_ejemplo1,OU=OU_ejemplo2`, el punto de partida para buscar cuentas de usuario es la unidad organizativa OU_ejemplo2, que está anidada en OU_ejemplo1.

   - Para buscar en Microsoft Active Directory, ingrese el nombre distinguido base en `DC=<valor>,DC=<valor>`, donde los `DC` son los componentes de dominio del servidor remoto. Por ejemplo, si escribe `DC=ejemplo,DC=com`, el punto de partida para buscar cuentas de usuario es el dominio "ejemplo.com".

9. En la lista desplegable **Atributo de búsqueda**, seleccione el atributo que el orquestador utiliza para buscar cuentas de usuario en el directorio del servidor remoto:

   - **uid (OpenLDAP)** es el UID (usuario ID) para buscar en OpenLDAP. Esta es la configuración predeterminada.

   - **sAMAccountName (Active Directory)** es el nombre de inicio de sesión anterior a Windows 2000 para realizar búsquedas en Microsoft Active Directory.

10. En el campo **Bind DN**, ingrese el nombre distinguido para autenticar el orquestador en el servidor remoto. Se admiten los siguientes formatos de nombre distinguido:

    - Para la autenticación en openLDAP, ingrese un valor en el formato `UID=<valor>,OU=<valor>`, donde `UID` es el ID de usuario y OU es la estructura de la unidad organizativa en el directorio del servidor remoto donde se encuentra el usuario. Por ejemplo, si ingresa `UID=usuario_ejemplo,OU=OU_ejemplo`, el usuario usuario_ejemplo de la unidad organizativa OU_ejemplo se usa para autenticar el orquestador en el servidor remoto.

    - Para la autenticación en Microsoft Active Directory, ingrese un valor en el formato `CN=<valor>,OU=<valor>,DC=<valor>,DC=<valor>`, donde `CN`es el nombre común del usuario, `OU` es la estructura de la unidad organizativa en el directorio del servidor remoto al que pertenece el usuario, y los `DC` son los componentes de dominio del usuario. Por ejemplo, si ingresa `CN=usuario_ejemplo,OU=OU_ejemplo,DC=ejemplo,DC=com`, el usuario usuario_ejemplo en la unidad organizativa OU_ejemplo en el dominio ejemplo.com se usa para autenticar el orquestador en el servidor remoto.

11. En el campo **Contraseña de Bind DN**, ingrese la contraseña del servidor remoto para autenticar al orquestador en el servidor remoto. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar 👁.

12. Para comprobar si el servidor remoto está disponible, haga clic en **Probar autenticación**.

13. Haga clic en **Crear**.

La conexión de LDAP se crea y se muestra en la tabla.

# Editar una conexión de LDAP

*Para editar una conexión de LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Conexiones de LDAP**.

   Se muestra una tabla de conexiones de LDAP.

3. Haga clic en la conexión de LDAP que desea editar.

4. En el área de configuración que se muestra, edite la siguiente configuración de conexión de LDAP , si es necesario: para obtener una descripción de la configuración, consulte las instrucciones para crear una conexión de LDAP.

5. Haga clic en **Guardar**.

La conexión de LDAP se modifica y se actualiza en la tabla.

# Cambiar la contraseña de una conexión de LDAP

Puede cambiar la contraseña del servidor remoto que se especificó cuando se creó la conexión LDAP y hacer que el orquestador use la nueva contraseña para autenticarse con el servidor remoto.

*Para cambiar la contraseña de una conexión LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Conexiones de LDAP**.

   Se muestra una tabla de conexiones de LDAP.

3. Haga clic en la conexión LDAP para la que desea cambiar la contraseña.

4. En la parte superior del área de configuración que se muestra, haga clic en el botón **Administración → Cambiar contraseña**.

5. Se abre una ventana; escriba la nueva contraseña en los cuadros de texto **Contraseña nueva** y **Confirmar contraseña**.

6. Haga clic en **Guardar**.

Se cambia la contraseña de la conexión de LDAP.

# Eliminar una conexión de LDAP

Las conexiones de LDAP eliminadas no se pueden restaurar.

*Para eliminar una conexión de LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Conexiones de LDAP**.

   Se muestra una tabla de conexiones de LDAP.

3. Haga clic en la conexión de LDAP que desea eliminar.

4. En la parte superior del área de configuración que se muestra, haga clic en **Administración→ Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

La conexión de LDAP se elimina y ya no se muestra en la tabla.

# Administrar usuarios

Puede ver la tabla de usuarios en la sección **Usuarios**. La información sobre los usuarios se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de usuario.
- **Inquilino** es el inquilino al que está asignado el usuario.
- **Rol** es el rol del usuario:
  - **Administrador**
  - **Inquilino**
- **Origen** es el tipo de usuario:
  - **Local**es un usuario local.
  - **LDAP** es un usuario LDAP.
- **Grupo** es el grupo del usuario LDAP. Si el usuario es local, esta columna muestra **Predeterminado**.

- **Estado**es el estado del usuario:
  - **En línea**
  - **Sin conexión**
  - **Bloqueado**
- **Autenticación de dos factores** especifica si la autenticación de dos factores está habilitada para el usuario:
  - **Habilitado** significa que la autenticación de dos factores está habilitada para el usuario.
  - **Deshabilitado** significa que se deshabilitó la autenticación de dos factores para el usuario.
  - **Reinicio** significa que se realiza una autenticación de dos factores repetida para el usuario.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un usuario

Puede crear usuarios locales y de LDAP. Las credenciales de los usuarios locales se almacenan en la base de datos del orquestador. Las credenciales de los usuarios de LDAP se almacenan en el servidor remoto. Si desea que los usuarios de LDAP puedan iniciar sesión en la interfaz web del orquestador con sus credenciales, primero debe crear una conexión de LDAP que el orquestador usará para conectarse al servidor remoto y luego crear sus usuarios o grupos de usuarios de LDAP.

*Para crear un usuario:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Haga clic en **+ Usuario**.

3. En el área de configuración que se muestra, en la lista desplegable **Tipo de cuenta**, seleccione el tipo de usuario:
   - **Local**. Esta es la configuración predeterminada. Si se selecciona este valor en los campos **Contraseña** y **Confirmar contraseña**, ingrese la contraseña del usuario. La contraseña debe contener al menos una letra del alfabeto latino en mayúscula (A-Z), una letra en minúscula (a-z), un número y un carácter especial. Longitud de la contraseña: de 8 a 50 caracteres. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar .
   - **LDAP**.
   - **Servicio**

4. En el campo **Nombre de usuario**, escriba el nombre de usuario. El nombre de usuario del servidor remoto se especifica en el formato `usuario@dominio` o `dominio\usuario`.

5. En la lista desplegable **Rol**, seleccione la función del usuario:

   - **Administrador**
   - **Inquilino**
   - **Restricted-API-extern-ISU**

     Este rol se utiliza para integrar Kaspersky SD-WAN con herramientas de seguridad de la información externas a través de la API del orquestador.

6. En la lista desplegable **Permisos**, seleccione el permiso de acceso creado que desea asignar al usuario. De manera predeterminada, el usuario obtiene el permiso de **acceso completo**, que otorga acceso completo a la interfaz web del orquestador.

7. Si desea habilitar la autenticación de dos factores para el usuario, seleccione la casilla **Autenticación de dos factores**. Esta casilla está desactivada por defecto. El usuario debe completar la autenticación de dos factores la próxima vez que inicie sesión en la interfaz web del orquestador.

   No puede habilitar la autenticación de dos factores para un usuario individual si la autenticación de dos factores está deshabilitada para todos los usuarios.

8. Si desea crear una solicitud de confirmación cada vez que el usuario realiza una acción, seleccione la casilla **Es obligatorio confirmar la solicitud**. Esta casilla está desactivada de manera predeterminada y el usuario puede realizar acciones sin confirmación.

9. En el campo **Nombre**, escriba el nombre del empleado.

10. En el campo **Apellido**, escriba el apellido del empleado.

11. Si es necesario, ingrese información adicional sobre el usuario:

    a. En el campo **Correo electrónico**, ingrese la dirección de correo electrónico.

    b. En el campo **Descripción**, ingrese una breve descripción del usuario.

12. Haga clic en **Crear**.

El usuario se crea y se muestra en la tabla. De manera predeterminada, el usuario está bloqueado.

Debe desbloquear al usuario para otorgarle acceso a la interfaz web del orquestador.

# Activar o bloquear un usuario

De manera predeterminada, los usuarios creados están bloqueados. Debe desbloquear al usuario para otorgarle acceso a la interfaz web del orquestador.

*Para bloquear o desbloquear a un usuario:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Haga clic en el usuario que desea desbloquear o bloquear.

3. En la parte superior del área de configuración que se muestra, haga clic en **Administración** → **Desbloquear** o **Bloquear**.

El usuario se bloquea o desbloquea.

# Editar un usuario

No puede cambiar el tipo y el nombre de usuario del usuario. Se proporcionan instrucciones independientes para cambiar la contraseña de un usuario local.

*Para editar un usuario:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione el usuario que desea editar.

3. En el área de configuración que se muestra, edite la siguiente configuración de usuario, si es necesario: para obtener una descripción de la configuración, consulte las instrucciones para crear un usuario.

4. Haga clic en **Guardar**.

El usuario se modifica y se actualiza en la tabla.

# Cambiar la contraseña de un usuario local

Las contraseñas de usuario de LDAP se almacenan en servidores remotos y no se pueden cambiar en la interfaz web del orquestador.

*Para cambiar la contraseña de un usuario local, siga estos pasos:*

1. Cambie la contraseña del usuario local:

   - Si tiene el rol de administrador de la plataforma y desea cambiar la contraseña del usuario local creado, vaya a la sección del menú **Usuarios**, haga clic en el usuario local y haga clic en **Administración** → **Cambiar contraseña**.

   - Si tiene el rol de inquilino y desea cambiar su propia contraseña, en la parte inferior del menú, haga clic en el ícono de configuración → **Cambiar contraseña**.

2. Se abre una ventana; escriba la nueva contraseña en los cuadros de texto **Contraseña nueva** y **Confirmar contraseña**. La contraseña debe contener al menos una letra del alfabeto latino en mayúscula (A-Z), una letra en minúscula (a-z), un número y un carácter especial. Longitud de la contraseña: de 8 a 50 caracteres. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar .

3. Haga clic en **Guardar**.

Se cambia la contraseña del usuario local.

# Autenticación de dos factores repetida de un usuario

Puede hacer que el usuario repita la autenticación si ese usuario perdió el acceso al código único para iniciar sesión en la interfaz web del orquestador que se generó como resultado de la autenticación de dos factores anterior.

*Para repetir la autenticación del usuario, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Haga clic en el usuario que desea volver a autenticar con la autenticación de dos factores.

3. En la parte superior del área de configuración que se muestra, haga clic en **Administración** → **Reiniciar autenticación de dos factores**.

El usuario debe completar la autenticación de dos factores la próxima vez que inicie sesión en la interfaz web del orquestador.

# Eliminar un usuario

Los usuarios eliminados no se pueden restaurar.

*Para eliminar un usuario, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Haga clic en el usuario que desea eliminar.

3. En la parte superior del área de configuración que se muestra, haga clic en **Administración** → **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

El usuario se elimina y ya no se muestra en la tabla.

# Administrar grupos de usuarios de LDAP

Puede ver la tabla de grupos de usuarios LDAP en la sección **Usuarios**, en la pestaña **Grupos**. La información sobre los grupos de usuarios LDAP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del grupo de usuarios LDAP.
- **Inquilino** es el inquilino al que está asignado el grupo de usuarios LDAP.

- **Rol** es el rol de los usuarios LDAP.
- **Tipo** es el tipo de grupo de usuarios. Kaspersky SD-WAN solo admite grupos de usuarios LDAP.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un grupo de usuarios de LDAP

Las credenciales del grupo de usuarios LDAP se almacenan en el servidor remoto. Si desea que los usuarios del grupo de usuarios LDAP puedan iniciar sesión en la interfaz web del orquestador con sus credenciales, primero debe crear una conexión LDAP que el orquestador use para conectarse al servidor remoto y luego crear sus usuarios LDAP o grupos de usuarios LDAP.

> Si el usuario es miembro de varios grupos de usuarios LDAP en el servidor remoto, recomendamos crear solo uno de esos grupos de usuarios LDAP en la interfaz web del orquestador. Si se crearon varios grupos de usuarios LDAP en la interfaz web del orquestador, un usuario que sea miembro de todos estos grupos de usuarios LDAP inicia sesión en la interfaz web del orquestador como miembro del grupo de usuarios LDAP que se creó en primer lugar.

*Para crear un grupo de usuarios LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Grupos**.

   Se muestra una tabla de grupos de usuarios LDAP.

3. Haga clic en **+ Agregar**.

4. En el área de configuración que se muestra, en el campo **Nombre**, ingrese el nombre del grupo de usuarios LDAP en el servidor remoto en el formato `usuario@dominio` o `dominio\usuario`.

5. En la lista desplegable **Rol**, seleccione la función de los usuarios LDAP en el grupo:

   - **Administrador**
   - **Inquilino**

6. En la lista desplegable **Permisos**, seleccione el permiso de acceso creado que desea asignar al grupo de usuarios LDAP. De manera predeterminada, el grupo de usuarios LDAP obtiene el permiso de **acceso completo**, que otorga acceso completo a la interfaz web del orquestador.

7. Si desea habilitar la autenticación de dos factores para el grupo de usuarios LDAP, seleccione la casilla **Autenticación de dos factores**. Esta casilla está desactivada por defecto. Los usuarios del grupo de usuarios LDAP deben completar la autenticación de dos factores la próxima vez que inicien sesión en la interfaz web del orquestador.

   Cuando se habilita la autenticación de dos factores para un grupo de usuarios LDAP, los usuarios LDAP autenticados se muestran en la tabla de usuarios. Para deshabilitar la autenticación de dos factores para un usuario LDAP, edite el usuario.

No puede habilitar la autenticación de dos factores para un grupo de usuarios LDAP si la autenticación de dos factores está deshabilitada para todos los usuarios.

8. Haga clic en **Crear**.

El grupo de usuarios LDAP se crea y se muestra en la tabla.

# Editar un grupo de usuarios de LDAP

No puede cambiar el tipo y el nombre del grupo de usuarios de LDAP.

*Para editar un grupo de usuarios, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Grupos**.

   Se muestra una tabla de grupos de usuarios LDAP.

3. Haga clic en el grupo de usuarios de LDAP que desea editar.

4. En el área de configuración que se muestra, edite la siguiente configuración del grupo de usuarios de LDAP, si es necesario. Para obtener una descripción de la configuración, consulte las instrucciones para crear un grupo de usuarios de LDAP.

5. Haga clic en **Guardar**.

El grupo de usuarios LDAP se modifica y se actualiza en la tabla.

# Eliminar un grupo de usuarios de LDAP

Los grupos de usuarios LDAP eliminados no se pueden restaurar.

*Para eliminar un grupo de usuarios LDAP, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Grupos**.

   Se muestra una tabla de grupos de usuarios LDAP.

3. Haga clic en el grupo de usuarios LDAP que desea eliminar.

4. En la parte superior del área de configuración que se muestra, haga clic en **Administración**→ **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El grupo de usuarios LDAP se elimina y ya no se muestra en la tabla.

# Habilitar o deshabilitar la autenticación de dos factores para todos los usuarios

Puede habilitar o deshabilitar la autenticación de dos factores para todos los usuarios. Si la autenticación de dos factores está deshabilitada para todos los usuarios, no puede habilitar la autenticación de dos factores para usuarios locales y LDAP o grupos de usuarios LDAP. De manera predeterminada, la autenticación de dos factores está deshabilitada.

*Para habilitar o deshabilitar la autenticación de dos factores para todos los usuarios, siga estos pasos:*

1. En el menú, vaya a la sección **Usuarios**.

   Se muestra la página de administración de usuarios. La pestaña **Usuarios**, que está seleccionada de manera predeterminada, muestra la tabla de usuarios.

2. Seleccione la pestaña **Autenticación de dos factores**.

3. Realice una de las siguientes acciones:

   - Si desea habilitar la autenticación de dos factores para todos los usuarios, marque la casilla **Autenticación de dos factores para todos los usuarios**. Todos los usuarios deben completar la autenticación de dos factores la próxima vez que un usuario inicie sesión en la interfaz web del orquestador.

   - Si desea deshabilitar la autenticación de dos factores para todos los usuarios, desmarque la casilla **Autenticación de dos factores para todos los usuarios**.

   Esta casilla está seleccionada por defecto.

La autenticación de dos factores se habilita o deshabilita para todos los usuarios.

# Administrar solicitudes de confirmación

Si durante la creación o edición de un usuario, seleccionó la casilla **Es obligatorio confirmar la solicitud**, se crea automáticamente una solicitud de confirmación para cada acción del usuario. Puede confirmar, rechazar o eliminar la solicitud de confirmación. Cuando se confirma una solicitud, se aplica la acción correspondiente; las solicitudes de confirmación denegadas se guardan en la interfaz web del orquestador.

*Para confirmar, rechazar o eliminar una solicitud de confirmación, siga estos pasos:*

1. En el menú, vaya a la sección **Confirmación**.

Se muestra una tabla de solicitudes de confirmación. La información sobre las solicitudes de confirmación se muestra en las siguientes columnas de la tabla:

- **Método** es el método de API que se utilizó para crear la solicitud de confirmación.
- **URL** es la URL de la API.
- **Nota** es una descripción breve de la solicitud de confirmación.
- **Usuario** es el nombre del usuario cuya acción resultó en la creación de una solicitud de confirmación.
- **Encabezados** son encabezados de API.
- **Creado** es la fecha y la hora en que se creó la solicitud de confirmación.
- **Estado** es el estado de la solicitud de confirmación:
  - **Confirmado**
  - **Denegado**
  - **Error**
  - **Esperando confirmación**

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

2. Si es necesario, realice una de las siguientes acciones:
   - Para confirmar la solicitud, haga clic en **Permitir** junto a ella.
   - Para rechazar la solicitud, haga clic en **Denegar** junto a ella.
   - Para eliminar la solicitud, haga clic en **Eliminar** junto a ella.

   Si desea confirmar, rechazar o eliminar varias solicitudes de confirmación al mismo tiempo, seleccione las casillas junto a las solicitudes y seleccione una acción haciendo clic en el botón **Acción** en la parte superior de la tabla.

Las solicitudes de confirmación se confirman, rechazan o eliminan.

# Administrar las sesiones de usuario

Puede hacer lo siguiente con las sesiones de usuario:

- Limitar la duración de las sesiones de usuario. De manera predeterminada, si un usuario permanece inactivo durante 3600 segundos (una hora) después de iniciar sesión en la interfaz web del orquestador, la sesión del usuario finaliza.
- Ver y, si es necesario, finalizar las sesiones de usuario activas.

*Para administrar sesiones de usuario, siga estos pasos:*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **Sesiones del usuario**.

   Se muestra una tabla de sesiones de usuario. La información sobre las sesiones de usuario se muestra en las siguientes columnas de la tabla:

   - **Dirección IP** es la dirección IP del usuario.
   - **Agente de usuario** es información sobre el navegador y el sistema operativo del usuario.
   - **Fecha** es la fecha de inicio de la sesión del usuario.

   Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

3. Si es necesario, realice una de las siguientes acciones:

   - Si desea limitar la duración de las sesiones de usuario, en el campo **Cuando la sesión está inactiva, finalizarla después de (s)**, ingrese el tiempo en segundos después del cual debe finalizar una sesión de usuario inactiva. Rango de valores: de 60 a 86 400. El valor predeterminado es `3600`.
   - Si desea finalizar una sesión de usuario específica, haga clic en**Finalizar sesión**.
   - Si desea finalizar varias sesiones de usuario, seleccione las casillas junto a ellas y, en la parte superior de la tabla, haga clic en **Acciones** → **Finalizar sesión**.

4. Haga clic en **Guardar**.

# Tenencia múltiple

Puede implementar Kaspersky SD-WAN para múltiples *inquilinos*, que pueden ser clientes independientes, oficinas o departamentos de su organización. La solución implementada para un inquilino se denomina *instancia SD-WAN*. Después de implementar la solución, debe crear al menos un inquilino e implementar una instancia SD-WAN para él.

Cuando crea un inquilino, el inquilino obtiene su propio portal de autoservicio para administrar la instancia SD-WAN. Los inquilinos creados están aislados, por lo que no pueden acceder a los portales de autoservicio de los demás y sus redes IP pueden superponerse. La cantidad de inquilinos creados no debe exceder la cantidad de inquilinos que especificó en la sección `external` del archivo de configuración durante la implementación de la solución.

Para implementar una instancia SD-WAN para un inquilino, debe crear una plantilla de instancia SD-WAN. En la plantilla de la instancia SD-WAN, debe especificar la configuración básica de la instancia SD-WAN, como la configuración de la calidad del servicio y el servicio de transporte. También debe agregar el inquilino a la plantilla de la instancia SD-WAN para que la configuración de la plantilla de la instancia SD-WAN se aplique a la instancia SD-WAN cuando la implemente para ese inquilino.

Si el inquilino no se agregó a ninguna plantilla de instancia SD-WAN, se usa la **plantilla de SD-WAN predeterminada** cuando se implementa una instancia SD-WAN para ese inquilino. Puede asignar una plantilla de instancia de SD-WAN diferente como la predeterminada.

Si la configuración que especificó en la plantilla de instancia SD-WAN no coincide con los parámetros reales de la instancia SD-WAN, esa instancia SD-WAN no se implementa para el inquilino. Por ejemplo, una instancia SD-WAN no se implementa si el número de nodos de controlador especificado en la plantilla de instancia SD-WAN no coincide con el número real de nodos de controlador de la instancia SD-WAN.

Después de implementar la instancia SD-WAN, puede ver los resultados de la supervisión y las solicitudes de servicio de esa instancia SD-WAN, así como configurar sus nodos de controlador. También puede agregar inquilinos a una instancia SD-WAN implementada para permitirles usar el controlador de esa instancia SD-WAN. Esto evita la necesidad de implementar una instancia SD-WAN independiente para cada inquilino.

Puede agrupar instancias SD-WAN en grupos de instancias SD-WAN para equilibrar la carga cuando se usa una gran cantidad de CPE. Puede agregar dispositivos CPE a un grupo de instancias SD-WAN. Si agregó un dispositivo CPE a un grupo de instancias SD-WAN, el orquestador selecciona automáticamente la instancia SD-WAN con el número más bajo de dispositivos CPE y agrega el dispositivo CPE a esa instancia SD-WAN. Si las instancias SD-WAN en el grupo de instancias SD-WAN tienen la misma cantidad de dispositivos CPE, el orquestador agrega el dispositivo CPE a una instancia SD-WAN seleccionada al azar.

# Escenario: implementación de una instancia SD-WAN para un inquilino

El escenario de implementación de la instancia SD-WAN para un inquilino incluye los siguientes pasos:

1. **Crear un inquilino**

   Cree el inquilino para el que desea implementar una instancia SD-WAN.

2. **Crear una plantilla de instancia SD-WAN**

   Cree y configure una plantilla de instancia SD-WAN. Para obtener detalles sobre la administración de las plantillas de las instancias SD-WAN, consulte la sección Administrar plantillas de instancias SD-WAN. Puede usar la plantilla de instancia SD-WAN creada para implementar otras instancias SD-WAN.

3. **Agregar un inquilino a una plantilla de instancia SD-WAN**

   Agregue el inquilino a la plantilla de instancia SD-WAN para que la configuración de la plantilla de la instancia SD-WAN se aplique a la instancia SD-WAN cuando implemente la instancia SD-WAN para ese inquilino.

4. **Preparar las máquinas virtuales o los servidores físicos para la implementación del controlador**

   Cuando implementó Kaspersky SD-WAN, preparó las máquinas virtuales o los servidores físicos para la implementación de todos los componentes de la solución, incluido el controlador.

   Si no preparó las máquinas virtuales o los servidores físicos para el controlador, puede especificarlos en la sección `nodes` del archivo de configuración y luego ejecutar el comando de implementación de la solución nuevamente. Cuando vuelva a ejecutar el comando de implementación de la solución, se prepararán las máquinas virtuales o los servidores físicos que faltan. Los componentes de la solución que ya están implementados no se ven afectados.

5. **Preparar el paquete PNF del controlador**

   Prepare el paquete PNF del controlador de la instancia SD-WAN en su dispositivo local:

   1. Extraiga el archivo de instalación y vaya a uno de los siguientes directorios:

      - Si desea implementar un solo nodo del controlador, vaya al directorio /pnfs/pnf_sdwan_ctl.
      - Si desea implementar tres nodos de controlador, vaya al directorio /pnfs/pnf_sdwan_ctl_3.
      - Si desea implementar cinco nodos de controlador, vaya al directorio /pnfs/pnf_sdwan_ctl_5.

   2. Si desea cambiar el descriptor PNF del controlador, vaya al directorio /src del archivo de instalación extraído y edite el archivo pnfd.xml.

   3. Ejecute el siguiente comando para crear el paquete PNF:

      ```
      make
      ```

   El paquete PNF se coloca en el directorio /build del archivo de instalación extraído.

6. **Cargar el paquete PNF del controlador a la interfaz web del orquestador**

   Cargue el paquete PNF del controlador de instancias SD-WAN a la interfaz web del orquestador.

7. **Configurar el PNF del controlador**

   Configure el PNF del controlador de la instancia SD-WAN:

   1. En el menú, vaya a la sección **Catálogo** y, en el panel **Catálogo**, haga clic en el PNF del controlador.

   2. En el área de configuración que se muestra, seleccione la pestaña **Ubicación del DC** y, en el campo **Centro de datos**, especifique el centro de datos agregado en el que desea implementar el controlador.

   3. Seleccione la pestaña **IP de administración** y especifique las direcciones IP de los nodos del controlador. Especifique las direcciones IP estándar o virtuales de las máquinas virtuales o los servidores físicos para la implementación del controlador que especificó en la sección `nodes` del archivo de configuración cuando implementó la solución.

8. **Asignar el PNF del controlador al inquilino**

   Asigne el PNF del controlador de instancias SD-WAN al inquilino.

9. **Iniciar sesión en el portal de autoservicio de inquilinos**

   Inicie sesión en el portal de autoservicio de inquilinos

10. **Crear un servicio de red de SD-WAN**

    Cree un servicio de red de SD-WAN. Cuando crea el servicio de red de SD-WAN, debe agregar el PNF del controlador de la instancia SD-WAN a la topología y, a continuación, hacer lo siguiente:

    1. En la topología, haga clic en el PNF del controlador.
    2. En el área de configuración que se muestra, seleccione la pestaña **CA_certificates** y, en el campo **Certificado de CA**, ingrese el certificado raíz en formato PEM con el que está firmado el certificado del orquestador. Se admiten certificados raíz independientes, así como cadenas de certificados que constan de un certificado raíz y varios certificados intermedios. Si especifica una cadena de certificados, debe iniciar cada certificado en una nueva línea.
    3. Seleccione la pestaña **Orquestador** y, en el campo **IP de la API del orquestador**, ingrese la dirección IP de uno de los nodos del orquestador. Debe especificar una de las direcciones IP estándar o virtuales de las máquinas virtuales o los servidores físicos para la implementación del orquestador que especificó en la sección `nodes` del archivo de configuración.
    4. Seleccione las pestañas **CTL1–5** e ingrese la información del nodo del controlador:
        1. En el campo **IP para la conexión ORC**, ingrese la dirección IP del nodo del controlador para conectar el orquestador. Debe especificar una de las direcciones IP estándar o virtuales de las máquinas virtuales o los servidores físicos para la implementación del controlador que especificó en la sección `nodes` del archivo de configuración.
        2. En el campo **IP para conexiones CPE**, ingrese la dirección IP del nodo del controlador para conectar dispositivos CPE.
        3. En el campo **PUERTO para conexiones CPE**, ingrese el puerto TCP del nodo del controlador para conectar dispositivos CPE.

11. **Implementar el servicio de red de SD-WAN**

    Implemente el servicio de red de SD-WAN.

La instancia SD-WAN se implementa para el inquilino y el controlador de la instancia SD-WAN se muestra en el portal del administrador y el portal de autoservicio del inquilino en la sección **Infraestructura**.

Si en el paso 10 de este escenario, especificó un certificado raíz incorrecto:

1. Conéctese a la máquina virtual o al servidor físico en el que está implementado el nodo del controlador. Junto con cada nodo del controlador, el componente MOCKPNF se implementa automáticamente en la máquina virtual o el servidor físico para garantizar la seguridad de la configuración del contenedor Docker del nodo del controlador.
2. Inicie sesión en la cuenta de usuario que tiene acceso al grupo Docker, luego inicie sesión en el contenedor Docker del componente MOCKPNF ejecutando el siguiente comando:

   ```
   docker exec -it mockpnf-<número de nodo del controlador> /bin/ash
   ```

3. Ejecute el script `cleanup.sh`. Puede descargar el script del directorio /pnfs/pnf_sdwan_ctl<número de nodos de controlador>/scr/scripts del archivo de instalación.

   > Debe completar los pasos 2 y 3 para cada nodo del controlador.

4. Repita el paso 10 de este escenario con el certificado raíz correcto.

# Administrar inquilinos

Puede ver la tabla de inquilinos en la sección **Inquilinos**. La información acerca de los inquilinos se muestra en las siguientes columnas de la tabla:

- **Nombre**
- **Descripción**
- **ID de la instancia SD-WAN**
- **Estado de la instancia SD-WAN**
- **VIM**
- **UNI**

# Crear un inquilino

La cantidad de inquilinos creados no debe exceder la cantidad de inquilinos que especificó en la sección `external` del archivo de configuración durante la implementación de la solución.

*Para crear un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. Comience a crear el inquilino de una de las siguientes maneras:

   - Si está creando el primer inquilino, en **Inquilinos**, en el campo **Nombre**, ingrese el nombre del inquilino.
   - Si está creando el segundo inquilino o los siguientes, en la parte superior de la sección **Inquilinos**, haga clic en **+ Inquilino** y, en el campo **Nombre**, ingrese el nombre del inquilino.

3. Si es necesario, en el área correspondiente en la parte inferior de la página, ingrese una breve descripción del inquilino.

4. Haga clic en el ícono Crear +.

El inquilino se crea y se muestra en **Inquilinos**.

# Agregar un usuario a un inquilino

Puede asignar usuarios a un inquilino para permitirles iniciar sesión en el portal de autoservicio del inquilino y administrar la instancia SD-WAN que se implementa para el inquilino. Para asignar un usuario a un inquilino, primero debe asignar el rol de inquilino **Inquilino** al usuario durante la creación o edición del usuario. Puede asignar un usuario con el rol **Inquilino** a varios inquilinos y, a la inversa, puede asignar varios usuarios con el rol **Inquilino** a un inquilino.

*Para asignar usuarios a un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. Haga clic en el nombre del inquilino al que desea asignar usuarios o selecciónelo en la tabla y haga clic en el botón **Editar inquilino**.

   Se abre el área de configuración de inquilinos.

3. Vaya a la pestaña **Usuarios** y habilite el botón de alternancia **Utilizar** para uno o más usuarios que desee asignar a un inquilino.

   Si desea asignar todos los grupos de la tabla a un inquilino, haga clic en el botón **Utilizar todo**.

Los usuarios se asignan al inquilino. El inquilino al que asignó usuarios se muestra en la sección **Usuarios** de la tabla de usuarios en la columna **Inquilino**.

# Asignar un grupo de usuarios LDAP a un inquilino

Puede asignar grupos de LDAP a un inquilino para permitirles a los usuarios del grupo iniciar sesión en el portal de autoservicio del inquilino y administrar la instancia SD-WAN que se implementa para el inquilino. Para asignar un grupo de usuarios de LDAP a un inquilino, primero debe asignar el rol **Inquilino** al grupo de usuarios de LDAP al crear o editar el grupo de usuarios LDAP. Puede asignar un grupo de usuarios de LDAP con el rol **Inquilino** a varios inquilinos y, a la inversa, puede asignar varios grupos de usuarios de LDAP con el rol **Inquilino** a un inquilino.

*Para asignar un grupo de usuarios de LDAP a un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. Haga clic en el nombre del inquilino al que desea asignar un grupo de usuarios de LDAP o selecciónelo en la tabla y haga clic en el botón **Editar inquilino**.

   Se abre el área de configuración de inquilinos.

3. Vaya a la pestaña **Grupos de usuarios** y habilite el botón de alternancia **Utilizar** para uno o más grupos de usuarios de LDAP que desea asignar a un inquilino.

   Si desea asignar todos los grupos de la tabla a un inquilino, haga clic en el botón **Utilizar todo**.

Los grupos de usuarios de LDAP se asignan al inquilino. El inquilino al que asignó los grupos de usuarios de LDAP se muestra en la sección **Usuarios** → **Grupos** en la tabla de usuarios de la columna **Inquilino**.

# Asignar recursos informáticos a un inquilino

Puede asignar recursos informáticos a un inquilino para configurar el rendimiento de la instancia SD-WAN que desea implementar para el inquilino. La cantidad de recursos informáticos disponibles se determina durante la implementación de la solución.

*Para asignar recursos informáticos a un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. En **Inquilinos**, seleccione el inquilino al que desea asignar recursos informáticos.

3. En la parte superior de la sección **Recursos**, haga clic en el ícono de configuración ⚙.

4. Haga clic en el ícono de cambio de tamaño ∞ junto a uno de los siguientes recursos informáticos:

   - **CPU**: núcleos de CPU virtuales
   - **RAM**: RAM
   - **Disco**: espacio en el disco

5. En el campo que se muestra, ingrese la cantidad de recursos informáticos que desea asignar al inquilino.

6. Haga clic en el ícono de guardar ✓.

La cantidad especificada de recursos informáticos se asigna al inquilino.

# Asignar componentes de servicio de red a un inquilino

Puede asignar componentes de servicio de red a un inquilino para permitir que el inquilino los use para administrar los servicios de red.

*Para asignar componentes de servicio de red a un inquilino:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. En **Inquilinos**, seleccione el inquilino al que desea asignar los componentes del servicio de red.

3. En **Catálogo**, seleccione las casillas junto a los componentes del servicio de red que desea asignar al inquilino.

Los componentes del servicio de red se asignan al inquilino y se muestran en el portal de autoservicio del inquilino en la sección **Catálogo**.

# Asignar un VIM a un inquilino

Puede asignar uno o más VIM a un inquilino para permitir que el inquilino use estos VIM para administrar las funciones de la red virtual dentro de la infraestructura virtual.

*Para asignar un VIM a un inquilino, sifa estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. En **Inquilinos**, seleccione el inquilino al que desea asignar los VIM y haga clic en el botón **+ Editar VIM**.

   Se abre el área de configuración de VIM para el inquilino.

3. En la pestaña **Lista**, en la tabla, habilite el botón de alternancia **Utilizar** para uno o más VIM que desee asignar a un inquilino.

4. Puede filtrar la lista de VIM con las listas desplegables **Dominio** y **Centro de datos** seleccionando el dominio creado y el centro de datos agregado en el que implementaron los VIM.

Los VIM se asignan al inquilino y se muestran en la tabla de inquilinos de la columna **VIM**.

# Iniciar sesión en el portal de autoservicio de inquilinos

*Para iniciar sesión en el portal de autoservicio del inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. En **Inquilinos**, seleccione el inquilino en cuyo portal de autoservicio desea iniciar sesión.

3. Haga clic en **Conectar como inquilino**.

Se abre el portal de autoservicio del inquilino en una nueva pestaña del navegador. Inició sesión en el portal de autoservicio.

# Editar un inquilino

*Para editar un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.

2. En la sección **Inquilinos**, haga clic en el ícono de configuración ⚙ → **Editar** junto al inquilino que desea editar.

3. Si es necesario, edite el nombre o agregue una breve descripción del inquilino.
4. Haga clic en el ícono de guardar ✓.

El inquilino se modifica y se actualiza en **Inquilinos**.

## Eliminar un inquilino

Cuando elimina un inquilino, la instancia SD-WAN implementada para él se elimina automáticamente. Al mismo tiempo, todos los objetos creados dentro del inquilino, como las zonas y las plantillas de firewall, se guardan en el portal del administrador.

Los inquilinos eliminados no se pueden restaurar.

*Para eliminar un inquilino, siga estos pasos:*

1. En el menú, vaya a la sección **Inquilinos**.

   Se muestra la página de administración de inquilinos.
2. En la sección **Inquilinos**, haga clic en el ícono de configuración ⚙ → **Eliminar** junto al inquilino que desea eliminar.
3. En la ventana de confirmación, haga clic en **Eliminar**.

El inquilino se elimina y ya no se muestra en **Inquilinos**.

# Administrar plantillas de instancia SD-WAN

Puede ver la tabla de plantillas de instancias SD-WAN en la sección **SD-WAN** → **Plantillas de instancia SD-WAN**. **La plantilla de SD-WAN predeterminada** es la plantilla de instancia SD-WAN que se crea de manera predeterminada. La información sobre las plantillas de instancias SD-WAN se muestra en las siguientes columnas de la tabla:

- **Id** es el ID de la plantilla de instancias SD-WAN.
- **Nombre** es el nombre de la plantilla de instancia SD-WAN.
- **Utilizada** especifica si la plantilla de instancia SD-WAN está siendo utilizada por instancias SD-WAN:
  - **Sí**.
  - **No**.
- **Actualizado** es la fecha y la hora en que se modificó por última vez la configuración de la plantilla de instancia SD-WAN.
- **Usuario** es el nombre del usuario que creó la plantilla de instancia SD-WAN.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede administrar la configuración de la plantilla de instancia SD-WAN en las siguientes pestañas:

- **Información** contiene información básica sobre la plantilla de instancia SD-WAN. Puede editar el nombre de la plantilla de SD-WAN en el campo **Nombre**.
- **Clases de tráfico** contiene la configuración de las clases de tráfico.
- **Clasificadores de tráfico** contiene la configuración de los clasificadores de tráfico.
- **Reglas de QoS** contiene la configuración de las reglas de calidad de servicio.
- **Servicios de transporte** contiene la configuración de los servicios de transporte.
- **Inquilinos** contiene los inquilinos que se agregaron a la plantilla de instancia SD-WAN.
- **Alta disponibilidad** es el número de nodos de controlador de la instancia SD-WAN.
- **Estrategia de servicio/transporte** es la estrategia de transporte utilizada en la instancia SD-WAN.

# Crear una plantilla de instancia SD-WAN

*Para crear una plantilla de una instancia SD-WAN, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.
   Se muestra una tabla de plantillas de instancias SD-WAN.
2. En la parte superior de la página, haga clic en **+ Agregar**.
3. En la ventana que se abre, ingrese el nombre de la plantilla de la instancia SD-WAN.
4. Haga clic en **Crear**.

   Se crea la plantilla de la instancia SD-WAN y se muestra en la tabla.

Debe configurar la plantilla de la instancia SD-WAN que se creó. En la plantilla de la instancia SD-WAN, debe especificar la configuración básica de la instancia SD-WAN, como la configuración de la calidad del servicio y el servicio de transporte. También debe agregar el inquilino a la plantilla de la instancia SD-WAN para que la configuración de la plantilla de la instancia SD-WAN se aplique a la instancia SD-WAN cuando la implemente para ese inquilino. Para obtener detalles sobre la administración de las plantillas de las instancias SD-WAN, consulte la sección Administrar plantillas de instancias SD-WAN.

# Configurar la plantilla de instancia SD-WAN predeterminada

Si el inquilino no se agregó a ninguna plantilla de instancia SD-WAN, se usa la **plantilla de SD-WAN predeterminada** cuando se implementa una instancia SD-WAN para ese inquilino. Puede asignar una plantilla de instancia SD-WAN diferente como la predeterminada.

*Para configurar la plantilla de instancia SD-WAN predeterminada, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN que desea convertir en la plantilla de instancia SD-WAN predeterminada.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Configurar como plantilla predeterminada**.

La plantilla de instancia SD-WAN se convertirá en la plantilla de instancia SD-WAN predeterminada.

# Seleccionar el número de nodos de controlador para una instancia SD-WAN

Una instancia SD-WAN no se implementa si el número de nodos de controlador especificado en la plantilla de la instancia SD-WAN no coincide con el número real de nodos de controlador de la instancia SD-WAN.

*Para seleccionar la cantidad de nodos de controlador de instancias SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de la instancia SD-WAN para la que desea seleccionar el número de nodos de controlador.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Seleccione la pestaña **Alta disponibilidad**.

4. Seleccione el número de nodos del controlador

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Agregar un inquilino a una plantilla de instancia SD-WAN

Debe agregar al inquilino a la plantilla de instancia SD-WAN para que la configuración de la plantilla de instancia SD-WAN se aplique a la instancia SD-WAN cuando implemente la instancia SD-WAN para ese inquilino.

*Para agregar un inquilino a una plantilla de instancia SD-WAN:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN a la que desea agregar un inquilino.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Seleccione la pestaña **Inquilinos**.

   Se muestra una tabla de inquilinos.

4. Haga clic en **+ Inquilino**.

5. En la ventana que se abre, seleccione el inquilino creado que desea agregar a la plantilla de instancia SD-WAN.

6. Haga clic en **Agregar**.

   El inquilino se agrega a la plantilla de instancia SD-WAN y se muestra en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancia SD-WAN.

# Eliminar un inquilino de una plantilla de instancia SD-WAN

Puede eliminar un inquilino de una plantilla de instancia SD-WAN. Si lo hace, esta plantilla de instancia SD-WAN no se usará en la implementación de la instancia SD-WAN para el inquilino.

*Para eliminar un inquilino de una plantilla de instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN de la que desea eliminar un inquilino.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Seleccione la pestaña **Inquilinos**.

   Se muestra una tabla de inquilinos.

4. Haga clic en **Eliminar** junto al inquilino que desea eliminar de la plantilla de instancia SD-WAN.

   El inquilino se elimina de la plantilla de instancia SD-WAN y ya no se muestra en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Eliminar una plantilla de instancia SD-WAN

No puede eliminar la plantilla de la instancia SD-WAN predeterminada.

Las plantillas de instancias SD-WAN eliminadas no se pueden restaurar.

*Para eliminar una plantilla de instancia SD-WAN, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN que desea eliminar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

Se eliminará la plantilla de instancia SD-WAN y ya no se mostrará en la tabla.

# Administrar instancias SD-WAN

Puede ver la tabla de instancias SD-WAN en la sección **SD-WAN** → **Instancias SD-WAN**. La información sobre las instancias SD-WAN se muestra en las siguientes columnas de la tabla:

- **Id** es el ID de la instancia SD-WAN.
- **Inquilino** es el inquilino para el que se implementa la instancia SD-WAN.
- **Estado** es el estado de la instancia SD-WAN:
  - **Aceptar** significa que la instancia SD-WAN está funcionando normalmente.
  - **El controlador está ausente** significa que la instancia SD-WAN no tiene un controlador.
  - **Error** significa que ocurrió un error durante el funcionamiento de la instancia SD-WAN.
  - **Eliminando** significa que la instancia SD-WAN está en proceso de ser eliminada.
  - **Eliminado** significa que se eliminó la instancia SD-WAN.
- **CPE** es la cantidad de dispositivos CPE que se agregaron a la instancia SD-WAN.
- **Controladores** son las direcciones IP y los números de puerto de los controladores de la instancia SD-WAN.
- **DC** es el centro de datos en el que se implementa la instancia SD-WAN.

- **VIM** es el VIM de la instancia SD-WAN.
- **Creado** es la fecha y la hora en que se implementó la instancia SD-WAN.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede administrar la configuración de la instancia SD-WAN en las siguientes pestañas:

- **Configuración** contiene información básica sobre la instancia SD-WAN y la configuración de los nodos del controlador de la instancia SD-WAN. Puede ingresar una breve descripción de la instancia SD-WAN en el campo **Descripción**.
- **Supervisión** contiene los resultados de la supervisión de la instancia SD-WAN.
- **Solicitudes del servicio** contiene las solicitudes de servicio de la instancia SD-WAN.
- **Autoservicio del inquilino** contiene los inquilinos que se agregaron a la instancia SD-WAN.

# Configurar nodos de controlador de una instancia SD-WAN

Cuando configura los nodos del controlador de la instancia SD-WAN, puede cambiar sus direcciones IP y números de puerto TCP. Esto cambia automáticamente las direcciones IP y los números de puerto TCP de los nodos del controlador en todos los dispositivos CPE que se agregan a la instancia SD-WAN. Si las interfaces de SD-WAN del tipo WAN del dispositivo CPE están conectadas a diferentes redes, por ejemplo, Internet y una red MPLS privada, puede cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador en las interfaces de SD-WAN individuales del tipo WAN cuando crea o edita interfaces de SD-WAN del tipo WAN. Las direcciones IP y los números de puerto TCP especificados en una interfaz de SD-WAN individual del tipo WAN tienen prioridad sobre las direcciones IP y los números de puerto TCP especificados cuando configura los nodos del controlador de la instancia SD-WAN.

Si implementó varios nodos de controlador cuando implementó la instancia SD-WAN, puede especificar qué nodo de controlador es el nodo árbitro mientras configura los nodos de controlador de la instancia SD-WAN. Cuando se especifica un nodo árbitro en la interfaz web del orquestador, los dispositivos CPE no establecen sesiones de administración con ese nodo controlador, lo que reduce la carga sobre los dispositivos CPE.

> Después de configurar los nodos del controlador de la instancia SD-WAN, para aplicar los cambios, debe reiniciar los dispositivos CPE que ya se registraron.

*Para configurar los nodos del controlador de una instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

2. Haga clic en la instancia SD-WAN cuyos nodos de controlador desea configurar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra información general sobre la instancia SD-WAN.

3. Si es necesario, realice una de las siguientes acciones:

   - Si desea cambiar la dirección IP de un nodo del controlador, en el campo **Dirección IP**, ingrese una dirección IPv4. El número de campos corresponde al número de nodos del controlador.

   - Si desea cambiar el número de puerto TCP de un nodo del controlador, en el campo **Puerto**, ingrese el número del puerto base. Rango de valores: de 1 a 65 535. El valor predeterminado es `6653`. El número de campos corresponde al número de nodos del controlador.

     Junto con el puerto base del nodo del controlador, los puertos con los siguientes tres números consecutivos se especifican automáticamente. Por ejemplo, si ingresa `6653` como número de puerto base, los puertos 6654, 6655 y 6656 se especifican automáticamente.

   - Si desea especificar un nodo árbitro, seleccione la casilla de verificación **Arbitraje** junto al nodo del controlador. No puede especificar un nodo árbitro si solo implementó un nodo de controlador cuando implementó la instancia SD-WAN.

4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la instancia SD-WAN.

# Ver el uso de una instancia SD-WAN

Si es necesario, puede verificar qué dispositivos CPE se agregaron para la instancia SD-WAN.

*Para ver si se está utilizando una instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

2. Haga clic en la instancia SD-WAN para la que desea ver la información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra información general sobre la instancia SD-WAN.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar CPE asociados**.

Esto abre la sección **CPE**, que muestra una tabla de dispositivos CPE agregados a la instancia SD-WAN.

# Ver la topología de una instancia SD-WAN

*Para ver la topología de una instancia SD-WAN, siga estos pasos:*

1. Inicie sesión en el portal de autoservicio del inquilino para el que se implementó la instancia SD-WAN.

2. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

3. Haga clic en **Administración → Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

4. Vaya a la sección **Topología**.

   Se muestra la topología de la instancia SD-WAN.

5. Si es necesario, seleccione las siguientes casillas:

   - Seleccione la casilla **Utilización del vínculo** para ver la utilización de los vínculos. El nivel de utilización del vínculo está representado por los siguientes colores:

     - Verde: utilización baja del vínculo.
     - Amarillo: utilización media del vínculo.
     - Rojo: utilización alta del vínculo.

   - Seleccione la casilla **Segmentos** y, en la lista desplegable **Conmutadores de segmento**, seleccione dos dispositivos CPE para ver todos los vínculos entre esos dispositivos.
   - Seleccione la casilla **Nombre** para ver los nombres de los dispositivos CPE.
   - Seleccione la casilla **Dirección IP** para ver las direcciones IP de los dispositivos CPE.

   De manera predeterminada, todas las casillas de verificación están desactivadas.

# Agregar un inquilino a una instancia SD-WAN

Si desea usar el controlador de una sola instancia SD-WAN para varios inquilinos, debe agregar inquilinos a esa instancia SD-WAN. El uso de un solo controlador de instancia SD-WAN para varios inquilinos elimina la necesidad de implementar una instancia SD-WAN independiente para cada inquilino.

*Para agregar un inquilino a una instancia SD-WAN:*

1. En el menú, vaya a la sección **SD-WAN** → **Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

2. Haga clic en la instancia SD-WAN a la que desea agregar un inquilino.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra información general sobre la instancia SD-WAN.

3. Seleccione la pestaña **Autoservicio del inquilino**.

   Se muestra una tabla de inquilinos.

4. Haga clic en **+ Agregar**.

5. En la ventana que se abre, seleccione el inquilino creado que desea agregar a la instancia SD-WAN.

6. En el campo **Cantidad máxima de CPE**, ingrese el número máximo de dispositivos CPE disponibles para el inquilino.

7. Haga clic en **Agregar**.

El inquilino se agrega a la instancia SD-WAN y se muestra en la tabla.

# Eliminar un inquilino de una instancia SD-WAN

Puede eliminar un inquilino que se agregó a una instancia SD-WAN para evitar que el inquilino use el controlador de esa instancia SD-WAN.

*Para eliminar un inquilino de una instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

2. Haga clic en la instancia SD-WAN de la que desea eliminar un inquilino.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra información general sobre la instancia SD-WAN.

3. Seleccione la pestaña **Autoservicio del inquilino**.

   Se muestra una tabla de inquilinos.

4. Haga clic en **Eliminar** junto al inquilino que desea eliminar de la instancia SD-WAN.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El inquilino se elimina de la instancia SD-WAN y ya no se muestra en la tabla.

# Eliminar una instancia SD-WAN

Cuando elimina una instancia SD-WAN, los dispositivos CPE que se le agregaron y el servicio de red SD-WAN implementado para la instancia SD-WAN también se eliminan automáticamente. Sin embargo, el inquilino para el que se implementa la instancia SD-WAN no se elimina. Una forma alternativa de eliminar una instancia SD-WAN es eliminar el servicio de red SD-WAN.

Las instancias SD-WAN eliminadas no se pueden restaurar.

*Para eliminar una instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Instancias SD-WAN**.

   Se muestra una tabla de instancias de SD-WAN.

2. Haga clic en la instancia SD-WAN que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra información general sobre la instancia SD-WAN.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

La instancia SD-WAN se elimina y ya no se muestra en la tabla.

# Administrar agrupaciones de instancias SD-WAN

Puede ver la tabla de grupos de instancias SD-WAN en la sección **SD-WAN → Agrupaciones de instancias SD-WAN**. La información sobre los grupos de instancias SD-WAN se muestra en las siguientes columnas de la tabla:

- **Id** es el ID del grupo de instancias SD-WAN.
- **Nombre** es el nombre del grupo de instancias SD-WAN.
- **Cantidad de instancias** es el número de instancias SD-WAN en el grupo de instancias SD-WAN.
- **CPE** es la cantidad de dispositivos CPE que se agregaron a las instancias SD-WAN.
- **Creado** es la fecha y la hora en que se creó el grupo de instancias SD-WAN.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede administrar la configuración del grupo de instancias SD-WAN en las siguientes pestañas:

- **Información** contiene información básica sobre el grupo de instancias SD-WAN. Puede cambiar el nombre del grupo de instancias SD-WAN en el campo **Nombre** e ingresar una breve descripción en el campo **Descripción**.
- **Instancias SD-WAN** contiene instancias SD-WAN que se agregaron al grupo de instancias SD-WAN.

# Crear un grupo de instancias SD-WAN

*Para crear un grupo de instancias SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Agrupaciones de instancias SD-WAN**.

   Se muestra una tabla de grupos de instancias de SD-WAN.

2. En la parte superior de la página, haga clic en **+ Agrupación de instancias SD-WAN**.
3. En la ventana que se abre, ingrese el nombre del grupo de instancias SD-WAN.
4. Haga clic en **Crear**.

El grupo de instancias SD-WAN se crea y se muestra en la tabla.

Debe agregar instancias SD-WAN al grupo de instancias SD-WAN creado.

# Agregar una instancia SD-WAN a una agrupación de instancias SD WAN

*Para agregar una instancia SD-WAN a un grupo de instancias SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Agrupaciones de instancias SD-WAN**.

   Se muestra una tabla de grupos de instancias SD-WAN.

2. Haga clic en el grupo de instancias SD-WAN al que desea agregar una instancia SD-WAN.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Información** está seleccionada y muestra información general sobre el grupo de instancias SD-WAN.

3. Seleccione la pestaña **Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

4. Haga clic en **+ Agregar**.

5. En la ventana que se abre, seleccione la instancia SD-WAN implementada que desea agregar al grupo de instancias SD-WAN.

6. Haga clic en **Agregar**.

   La instancia SD-WAN se agrega al grupo de instancias SD-WAN y se muestra en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del grupo de instancias SD-WAN.

Si agrega un dispositivo CPE al grupo de instancias SD-WAN, puede agregar ese dispositivo CPE a la instancia SD-WAN que agregó al grupo de instancias SD-WAN. Esto sucede si se agregó la menor cantidad de dispositivos CPE a la instancia SD-WAN en comparación con las otras instancias SD-WAN en el grupo de instancias SD-WAN.

# Eliminar una instancia SD-WAN de una agrupación de instancias SD-WAN

*Para eliminar una instancia SD-WAN de un grupo de instancias SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Agrupaciones de instancias SD-WAN**.

   Se muestra una tabla de grupos de instancias SD-WAN.

2. Haga clic en el grupo de instancias SD-WAN del que desea eliminar una instancia SD-WAN.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Información** está seleccionada y muestra información general sobre el grupo de instancias SD-WAN.

3. Seleccione la pestaña **Instancias SD-WAN**.

   Se muestra una tabla de instancias SD-WAN.

4. Haga clic en **Eliminar** junto a la instancia SD-WAN que desea eliminar del grupo de instancias SD-WAN.

   La instancia SD-WAN se elimina del grupo de instancias SD-WAN y ya no se muestra en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del grupo de instancias SD-WAN.

# Eliminar una agrupación de instancias SD-WAN

Cuando elimina un grupo de instancias SD-WAN, todos los dispositivos CPE agregados a ese grupo de instancias SD-WAN se eliminan automáticamente. Esto no elimina las instancias SD-WAN.

Los grupos de instancias SD-WAN eliminados no se pueden restaurar.

*Para eliminar un grupo de instancias SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Agrupaciones de instancias SD-WAN**.

   Se muestra una tabla de grupos de instancias SD-WAN.

2. Haga clic en el grupo de instancias SD-WAN que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Información** está seleccionada y muestra información general sobre el grupo de instancias SD-WAN.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

El grupo de instancias SD-WAN se elimina y ya no se muestra en la tabla.

# Administrar dispositivos CPE

Los dispositivos CPE transmiten el tráfico entre las ubicaciones de su organización y los clientes, y también tienen acceso directo a Internet (DIA) sin transmitir el tráfico a la oficina central. De manera predeterminada, para crear la red SD-WAN, se instala un conmutador virtual de OpenFlow (conmutador virtual; vSwitch) en los dispositivos CPE. Puede utilizar dispositivos CPE de los siguientes tipos:

- Dispositivos CPE del modelo KESR (Kaspersky SD-WAN Edge Service Router) comprados a Kaspersky.
- Dispositivos CPE virtuales (dispositivos vCPE) implementados en máquinas virtuales. Cuando usa dispositivos vCPE, debe asegurarse de que las máquinas virtuales cumplan con los requisitos de hardware y software.
- Dispositivos CPE universales (dispositivos uCPE) que admiten la implementación de funciones de la red virtual y el VIM.

Para administrar dispositivos CPE, debe registrarlos.

Puede utilizar la *autenticación de dos factores* para registrar el dispositivo CPE de forma segura. Cuando se habilita la autenticación de dos factores, se registra un token (clave de seguridad) en la base de datos del orquestador. Luego, debe colocar este token en el dispositivo CPE cuando se registre con la tecnología de aprovisionamiento sin intervención. El registro se realiza de forma correcta si, cuando el dispositivo CPE se conecta automáticamente al orquestador, el token colocado en el dispositivo coincide con el token de CPE en la base de datos del orquestador.

Para la configuración centralizada de dispositivos CPE, puede usar plantillas de CPE. Para evitar configurar cada dispositivo CPE individualmente, puede especificar la configuración en la plantilla de CPE y luego aplicar la plantilla de CPE a los dispositivos CPE cuando agrega o registra dispositivos CPE manualmente. Si edita una configuración en una plantilla de CPE, la configuración se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. Si edita una configuración en el dispositivo CPE, la configuración se vuelve independiente de la plantilla de CPE, y si la configuración se modifica en la plantilla CPE, permanece sin cambios en el dispositivo CPE.

Algunas configuraciones del dispositivo CPE solo se pueden especificar en una plantilla de CPE, por ejemplo, el número de puerto para la conexión al orquestador.

Cuando elimina un dispositivo CPE de la interfaz web del orquestador, la configuración básica se conserva en el dispositivo CPE. Puede volver a registrar el dispositivo CPE. Cuando vuelve a registrar un dispositivo CPE, no puede usar la autenticación de dos factores.

Cuando agrega y registrar un dispositivo CPE, puede seleccionar si desea que el dispositivo CPE se habilite automáticamente después del registro. Cuando se habilita un dispositivo CPE, se le aplica la plantilla de CPE y el dispositivo CPE está disponible para retransmitir tráfico.

Puede restablecer el dispositivo CPE a los valores predeterminados de fábrica sin eliminarlo del orquestador; para ello, presione el botón Restablecer en el dispositivo. Para hacerlo, mantenga presionado el botón durante 10 segundos. Esta funcionalidad está disponible para los modelos KESR M1, M2 y M3.

# Acerca de la interacción del dispositivo CPE y el orquestador

Después del registro, el dispositivo CPE envía solicitudes de API REST al orquestador para obtener tareas con un período especificado cuando configura la conexión del dispositivo CPE al orquestador y al controlador. Las *tareas* son acciones que los usuarios realizan con el dispositivo CPE, como reiniciar el dispositivo CPE y actualizar el firmware. Se necesitan solicitudes de API REST para obtener tareas que no están asociadas con el conmutador virtual del dispositivo CPE.

Para ver la tabla de tareas realizadas por el orquestador en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE** y haga clic en el dispositivo CPE. La información sobre las tareas se muestra en las siguientes columnas de la tabla:

- **Tipo** es el tipo de tarea.
- **Estado** es el estado de la tarea:
  - **Esperar** significa que la tarea está guardada en la base de datos del orquestador y está a la espera de ser recibida por el dispositivo CPE.
  - **Ejecutando** significa que la tarea se está ejecutando.
  - **Se completó** significa que la tarea se completó correctamente.
  - **Error** significa que se produjo un error durante la ejecución de la tarea.
- **Última actualización** es la fecha y la hora de la última actualización de la tarea.

El orquestador ejecuta tareas en el dispositivo CPE de la siguiente manera:

1. Usted ejecuta una tarea, como modificar la configuración de BGP, en el dispositivo CPE mediante la interfaz web del orquestador.
2. El orquestador guarda la tarea en la base de datos. En la tabla, la tarea se muestra con el estado **Esperar**.
3. El dispositivo CPE recibe la tarea cuando envía una solicitud de API REST al orquestador. En la tabla, la tarea se muestra con el estado **Ejecutando**.
4. Si la tarea finaliza correctamente, el dispositivo CPE lo informa al orquestador. En la tabla, la tarea se muestra con el estado **Se completó**.

   Si la tarea falla, se muestra en la tabla con el estado **Error**.

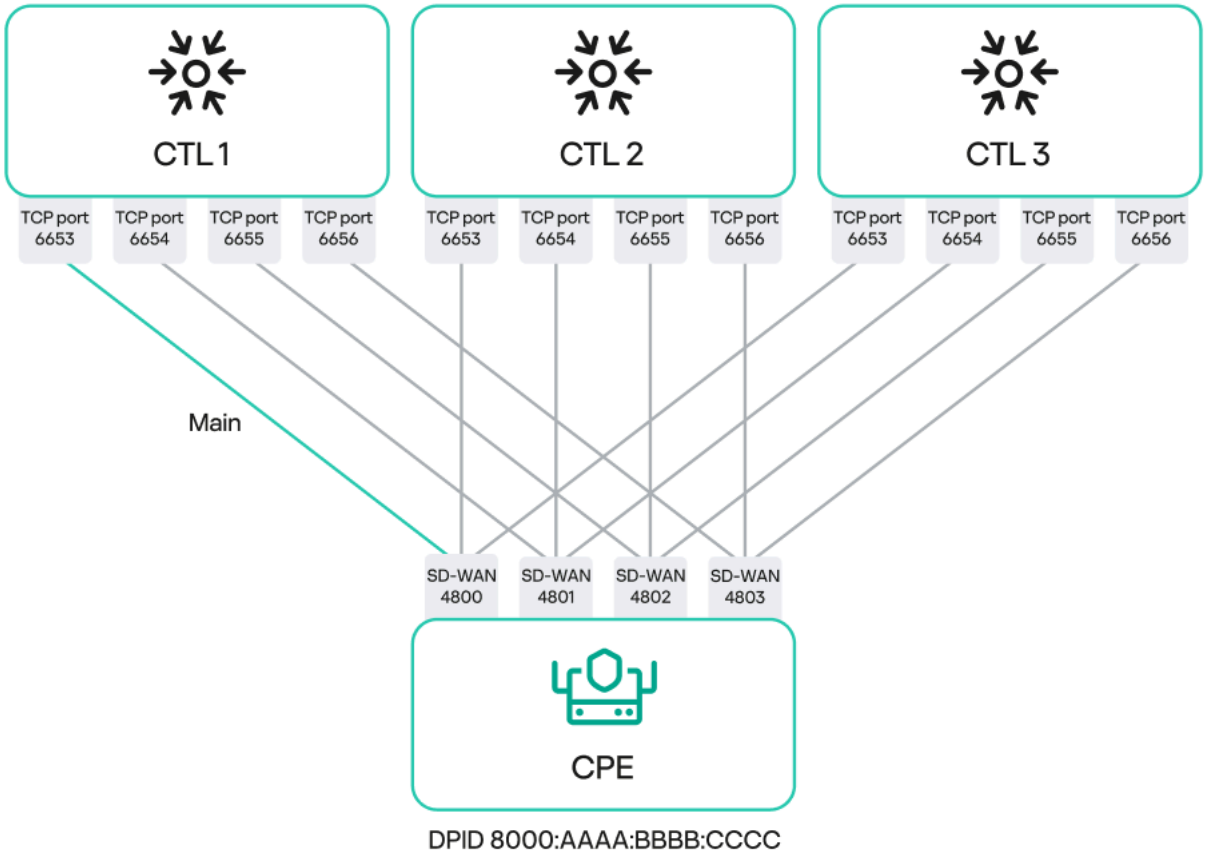
Antes de ejecutar la tarea, se guarda la configuración actual en el dispositivo CPE. Si el dispositivo CPE no puede enviar un mensaje de confirmación al orquestador después de completar con éxito la tarea, después de tres intentos, la configuración anterior se restaura en el dispositivo CPE y la tabla muestra la tarea con el estado **Error**.

# Acerca de la interacción del dispositivo CPE y el controlador

Una vez que se registra el dispositivo CPE, las *sesiones de administración* se establecen entre sus interfaces de SD-WAN del tipo WAN y los puertos TCP de los nodos del controlador. Una de las sesiones de administración es la sesión principal y las otras están en modo de espera. La sesión de administración principal se utiliza para transmitir tareas relacionadas con la administración del conmutador virtual del dispositivo CPE, como la modificación de la configuración de la ruta. Si se termina la sesión de administración principal, se elige una nueva sesión de administración principal al azar de las sesiones de administración establecidas anteriormente.

Las sesiones de administración se establecen haciendo coincidir los números de puerto de OpenFlow a los que hacen referencia las interfaces de SD-WAN del tipo WAN con los números de puerto TCP de los nodos del controlador, según su orden. Por ejemplo, en la siguiente figura, el dispositivo CPE tiene cuatro interfaces SD-WAN que hacen referencia a los puertos de OpenFlow 4800, 4801, 4802 y 4803. Los nodos del controlador CTL 1-3 tienen los puertos TCP 6653, 6654, 6655, 6656. En este caso, las sesiones de administración se establecen de la siguiente manera:

- SD-WAN 4800 → 6653
- SD-WAN 4801 → 6654
- SD-WAN 4802 → 6655
- SD-WAN 4803 → 6656




Sesiones de administración entre un dispositivo CPE y tres nodos del controlador

Las sesiones de administración se pueden configurar mientras se configura la conexión del dispositivo CPE al orquestador y al controlador. Por ejemplo, puede seleccionar una interfaz de SD-WAN del tipo WAN para priorizarla con el fin de establecer la sesión de administración principal. También puede habilitar o deshabilitar el cifrado para las sesiones de administración.

Puede cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador mientras configura los nodos del controlador de una instancia SD-WAN. Esto cambia automáticamente las direcciones IP y los números de puerto TCP de los nodos del controlador en todos los dispositivos CPE que se agregan a la instancia SD-WAN. Si las interfaces de SD-WAN del tipo WAN del dispositivo CPE están conectadas a diferentes redes, por ejemplo, Internet y una red MPLS privada, puede cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador en las interfaces de SD-WAN individuales del tipo WAN cuando crea o edita interfaces de SD-WAN del tipo WAN. Las direcciones IP y los números de puerto TCP especificados en una interfaz de SD-WAN individual del tipo WAN tienen prioridad sobre las direcciones IP y los números de puerto TCP especificados cuando configura los nodos del controlador de la instancia SD-WAN.

Para ver la tabla de dispositivos CPE con información sobre las sesiones de administración, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Conmutadores**. La información sobre las sesiones de administración se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del dispositivo CPE.
- **Orden** es el número de secuencia del dispositivo CPE. El número más pequeño se asigna al dispositivo CPE que se conecta primero al controlador.
- **Estado** es el estado del dispositivo CPE en relación con el controlador:
  - **Activa** significa que el dispositivo CPE se puede utilizar para retransmitir tráfico.
  - **Inactiva** significa que el dispositivo CPE no se puede utilizar para retransmitir tráfico.
- **Conexión** es el estado de la conexión del dispositivo CPE al controlador:
  - **Conectados** significa que las sesiones de administración se establecen entre el dispositivo CPE y los nodos del controlador.
  - **Desconectado** significa que no se establecen sesiones de administración entre el dispositivo CPE y los nodos del controlador.
- **MAC** es la dirección MAC del dispositivo CPE.
- **Interfaz** son las interfaces de SD-WAN del tipo WAN a partir de las cuales se establecen las sesiones de administración.
- **Sesión principal** es la interfaz de SD-WAN del tipo WAN desde la cual se establece la sesión de administración principal:
  - **Sí**.
  - **No**.
- **Dirección IP** es la dirección IP que la interfaz de SD-WAN del tipo WAN utilizó para establecer la sesión de administración.
- **Puerto** es el puerto TCP que la interfaz de SD-WAN del tipo WAN utilizó para establecer la sesión de administración.

- **Creado** es la fecha y la hora en que se registró el dispositivo CPE.
- **Ubicación** es la dirección de la ubicación del dispositivo CPE.
- **Latencia (ms)** es la latencia en milisegundos de la sesión de administración.
- **Descripción** es una breve descripción del dispositivo CPE.

# Credenciales predeterminadas de dispositivos CPE de KESR

Todos los dispositivos CPE del modelo KESR (Kaspersky SD-WAN Edge Service Router) tienen las mismas credenciales predeterminadas:

- Nombre de usuario: `root`
- Contraseña: `123-qwe`

Debe ingresar estas credenciales para conectarse a un dispositivo CPE de KESR no registrado a través de SSH o para establecer una sesión de consola con él. Después del registro, se cambiará automáticamente la contraseña predeterminada del dispositivo CPE. Puede ver la contraseña del dispositivo CPE en la interfaz web del orquestador.

# Comprobación de integridad

Esta función permite verificar de forma automática o manual la integridad de los archivos que son de importancia crítica para el funcionamiento de todo el sistema y el firewall en particular, comparando estos archivos con sumas de control de referencia. Puede detectar cambios no autorizados y garantizar que los scripts del sistema y los archivos ejecutables coincidan con el firmware publicado.

Puede ejecutar un análisis a pedido o configurar un análisis programado.

Un análisis a pedido solo se puede llevar a cabo en un dispositivo CPE.

Para hacerlo, vaya al menú de **plantillas de CPE** del orquestador, seleccione una plantilla, luego en el menú SD-WAN, vaya a la pestaña "Comprobaciones de CPE", haga clic en el botón "Ejecutar" en la sección "Comprobación de integridad" en "Análisis manual".

Se inicia una herramienta en el CPE que realiza la comprobación y envía la información al registro del sistema CPE.

Al mismo tiempo, en la sección "Análisis de integridad", en "Análisis manual", se indica que la tarea se ejecutó y se indica la fecha y hora de la ejecución. El estado también se muestra aquí.

El orquestador también muestra el estado y el resultado del análisis en la interfaz de usuario del dispositivo CPE en el menú "Principal", en la sección "Administración fuera de banda". Una vez iniciada, la tarea "Análisis de integridad" tiene el estado "En ejecución". Luego, según el resultado, el CPE envía el estado "Correcto" o "Error" al orquestador.

Un análisis programado se puede configurar tanto en una plantilla de CPE como en un dispositivo CPE.

Para configurarlo, vaya al menú "Plantillas CPE" del orquestador, seleccione una plantilla, luego vaya al menú SD-WAN → pestaña "Comprobaciones de CPE" y habilite el botón de alternancia "Comprobación de integridad" en "Programación de comprobaciones".

En un dispositivo CPE, primero debe habilitar el botón de alternancia "Anular".

Ahora puede establecer el intervalo entre comprobaciones.

Se inicia una herramienta en el CPE que realiza la comprobación y envía la información al registro del sistema CPE.

El orquestador también muestra el estado y el resultado del análisis en la interfaz de usuario del dispositivo CPE en el menú "Principal", en la sección "Administración fuera de banda". ????

Además, puede bloquear la transmisión del tráfico en caso de que las comprobaciones no se realicen correctamente.

# Registrar dispositivos CPE

Existen los siguientes escenarios para el registro de los dispositivos CPE:

- Registro de un dispositivo CPE mediante la tecnología de aprovisionamiento sin intervención (ZTP). Este escenario se aplica a los nuevos dispositivos CPE que no se han registrado anteriormente.
- Implementación de un dispositivo vCPE en la plataforma de virtualización de VMware y registro del dispositivo con la tecnología de aprovisionamiento sin intervención. Este escenario se aplica a los dispositivos CPE virtuales que se implementan en las máquinas virtuales.
- Registro repetido de un dispositivo CPE. Este escenario se aplica a los dispositivos CPE registrados anteriormente que se han eliminado.

Cuando registre un dispositivo CPE, no es necesario que se conecte a los servidores de activación y actualización de licencias de Kaspersky, ni a los servidores de KSN (Kaspersky Security Network). Si se produce un error durante el registro de un dispositivo CPE, puede reanudar el registro del dispositivo CPE.

## Escenario: registro automático de un dispositivo CPE con la tecnología de aprovisionamiento sin intervención.

Puede registrar nuevos dispositivos CPE mediante el aprovisionamiento sin intervención (ZTP). ZTP permite que un dispositivo CPE se conecte automáticamente al orquestador.

Si utiliza ZTP, debe generar una URL con la configuración básica del dispositivo CPE. La *configuración básica* es aquella que es necesaria para conectar automáticamente un dispositivo CPE al orquestador. Para completar el registro, debe conectar el dispositivo administrador al dispositivo CPE y visitar la URL de configuración básica generada en el dispositivo administrador.

El escenario de registro de ZTP para un dispositivo CPE implica los siguientes pasos:

1. **Crear una plantilla de CPE**

   Cree y configure una plantilla de CPE. Para obtener detalles sobre la administración de plantillas de CPE, consulte Administración de plantillas de CPE. Puede utilizar la plantilla de CPE creada para configurar otros dispositivos CPE.

2. **Agregar un dispositivo CPE**

   Agregue un dispositivo CPE. Si agrega el dispositivo CPE, asígnele la plantilla de CPE creada y seleccione si el dispositivo CPE debe encenderse automáticamente después del registro. El dispositivo CPE agregado tiene el estado **Esperando**. Para obtener detalles sobre la administración de dispositivos CPE, consulte Administración de dispositivos CPE.

3. **Autenticación de dos factores (paso opcional)**

   Si desea registrar su dispositivo CPE de forma segura, utilice la autenticación de dos factores.

4. **Generar una URL con la configuración básica**

   Genere una URL con la configuración básica del dispositivo CPE.

5. **Registrar el dispositivo CPE**

   Haga lo siguiente:

   1. Conecte el dispositivo administrador al puerto LAN del dispositivo CPE.

      El dispositivo administrador obtiene una dirección IP y la dirección IP de la puerta de enlace predeterminada a través de DHCP. La dirección IP recibida de la puerta de enlace predeterminada es la dirección IP del dispositivo CPE.

   2. Visite la URL de configuración básica generada del dispositivo CPE en el dispositivo administrador de una de las siguientes maneras:

      - En la barra de direcciones del navegador, ingrese la URL de configuración básica del dispositivo CPE y presione **`Intro`**.
      - Abra el archivo HTML que guardó cuando generó la URL de configuración básica del dispositivo CPE.

   3. En la página que se abre, haga clic en el botón **Aplicar configuración**.

   El dispositivo CPE se conecta automáticamente al orquestador, se une al dispositivo CPE agregado en la interfaz web del orquestador y se registra. Un dispositivo CPE registrado tiene el estado **Registrado** y está en el estado **Habilitado** o **Deshabilitado**.

6. **Habilitar el dispositivo CPE (paso opcional)**

   Si, cuando agregó el dispositivo CPE, especificó que no debe habilitarse automáticamente, habilite el dispositivo CPE. Un dispositivo CPE habilitado tiene el estado **Registrado** y está en el estado **Habilitado**.

7. **Habilitar el cifrado de tráfico en el dispositivo CPE (paso opcional)**

   Si desea utilizar el cifrado de tráfico en el dispositivo CPE, habilítelo para todo el dispositivo o para un vínculo específico.

# Escenario: implementación de un dispositivo vCPE en la plataforma de virtualización de VMware y registro del mismo con la tecnología de aprovisionamiento sin intervención

Puede implementar un dispositivo vCPE en la plataforma de virtualización de VMware mediante una plantilla OVF y, luego, registrar el dispositivo vCPE mediante ZTP.

La *plantilla OVF* es el archivo comprimido knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.combined.adm64-legacy.vKESR-M1-esxi.tar.gz que puede encontrar en el directorio /cpe del kit de distribución; el archivo comprimido incluye los siguientes archivos:

- vKESR.mf contiene el hash SHA256 de los archivos de la plantilla OVF.
- vKESR.nvram contiene el estado del BIOS de la máquina virtual.
- vKESR.ovf es el descriptor que contiene información sobre la configuración de la máquina virtual.
- vKESR.vmdk es la imagen de disco de la máquina virtual.

Debe descargar la plantilla OVF y extraerla en su dispositivo local antes de realizar este escenario.

El escenario para la implementación en la plataforma de virtualización de VMware y el registro ZTP de un dispositivo vCPE implica los siguientes pasos:

1. **Crear una plantilla de vCPE**

   Cree y configure una plantilla de vCPE. Para obtener detalles sobre la administración de plantillas de vCPE, consulte Administración de plantillas de vCPE. Puede usar la plantilla de vCPE creada para configurar otros dispositivos vCPE.

2. **Agregar un dispositivo vCPE**

   Agregue un dispositivo vCPE. Cuando agregue un dispositivo vCPE:

   - Especifique la plantilla de vCPE creada.
   - Seleccione si desea que el dispositivo vCPE se encienda automáticamente después del registro.
   - Especifique un DPID temporal del dispositivo vCPE, por ejemplo, `DPID temporal`.

   El dispositivo vCPE agregado tiene el estado **Esperando**. Para obtener detalles sobre la administración de dispositivos vCPE, consulte Administración de dispositivos CPE.

3. **Autenticación de dos factores (paso opcional)**

   Si desea registrar su dispositivo vCPE de forma segura, utilice la autenticación de dos factores.

4. **Generar una URL con la configuración básica**

   Genere una URL con la configuración básica del dispositivo vCPE.

5. **Implementar un dispositivo vCPE en la plataforma de virtualización de VMware**

En la interfaz web de la plataforma de virtualización de VMware, cree una máquina virtual para implementar el dispositivo vCPE. Asegúrese de que la máquina virtual que está creando cumpla con los requisitos de hardware y software. Cuando cree la máquina virtual:

1. Seleccione cómo desea crear la máquina virtual, mediante el estándar OVF o un archivo OVA.
2. Cuando seleccione archivos VDMK, especifique los archivos de la plantilla OVF extraídos en el dispositivo local.
3. Al momento de ajustar la configuración avanzada, especifique la URL generada con la configuración básica.

Para obtener más información sobre la creación de máquinas virtuales, consulte la documentación oficial de VMware.

Si la configuración se aplica correctamente, el dispositivo vCPE se conecta de forma automática al orquestador y se muestra en la interfaz web del orquestador con el estado **Desconocido**.

6. **Registrar un dispositivo vCPE**

   Cambie el DPID temporal que especificó cuando agregó el dispositivo vCPE al DPID real del dispositivo vCPE. El DPID real del dispositivo vCPE es el nombre de host de la máquina virtual en la que se implementa el dispositivo vCPE. El nombre de host de la máquina virtual se muestra en la interfaz web de la plataforma de virtualización de VMware.

   El dispositivo vCPE se vincula al dispositivo vCPE agregado en la interfaz web del orquestador y se registra a sí mismo. Un dispositivo vCPE registrado tiene el estado **Registrado** y está en el estado **Habilitado** o **Deshabilitado**.

7. **Habilitar el vCPE (paso opcional)**

   Si, cuando agregó el dispositivo vCPE, especificó que no debe habilitarse automáticamente, habilite el dispositivo vCPE. Un dispositivo vCPE habilitado tiene el estado **Registrado** y está en el estado **Habilitado**.

# Escenario: volver a registrar un dispositivo CPE

Si elimina un dispositivo CPE, la configuración básica se conserva en él. Puede volver a registrar un CPE remoto sin utilizar ZTP.

> Cuando vuelve a registrar un dispositivo CPE, no puede usar la autenticación de dos factores. Si desea utilizar la autenticación de dos factores, registre su dispositivo CPE mediante ZTP.

El escenario en el que se vuelve a registrar el dispositivo CPE implica los siguientes pasos:

1. **Restaurar el firmware del dispositivo CPE a la condición inicial**

   Conéctese al dispositivo CPE a través de SSH. Para hacerlo, especifique la dirección IP e ingrese las credenciales del dispositivo CPE. Luego, ejecute el siguiente comando:

   ```
   firstboot && reboot
   ```

2. **Crear una plantilla de CPE**

   Cree y configure una plantilla de CPE. Para obtener detalles sobre la administración de plantillas de CPE, consulte Administración de plantillas de CPE. Puede utilizar la plantilla de CPE creada para configurar otros dispositivos CPE.

3. **Conectar el dispositivo CPE al orquestador**

   Desconecte y vuelva a conectar el cable de alimentación del dispositivo CPE para que el dispositivo CPE se reinicie y establezca la conexión con el orquestador. Si se realiza la conexión adecuadamente, el dispositivo CPE se muestra en la interfaz web del orquestador con el estado **Desconocido**.

4. **Registrar un dispositivo CPE manualmente**

   Registre manualmente el dispositivo CPE . Cuando registre manualmente el dispositivo CPE, asígnele la plantilla de CPE creada y seleccione si el dispositivo CPE debe encenderse automáticamente después del registro. Un dispositivo registrado tiene el estado **Registrado** y está en el estado **Habilitado** o **Deshabilitado**. Para obtener detalles sobre la administración de dispositivos CPE, consulte Administración de dispositivos CPE.

5. **Habilitar el dispositivo CPE (paso opcional)**

   Si, cuando registró manualmente el dispositivo CPE, especificó que no debe habilitarse automáticamente, encienda el dispositivo CPE. Un dispositivo CPE habilitado tiene el estado **Registrado** y está en el estado **Habilitado**.

# Reanudar el registro del dispositivo CPE en caso de error

Si se produce un error durante el registro de un dispositivo CPE, el estado del dispositivo CPE cambia a **Suspendida** y el registro no se completa.

*Para reanudar el registro de un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. En la columna **Estado**, haga clic en el estado del dispositivo CPE.

   Se muestra el registro de la solicitud de servicio.

3. Haga clic en el paso en el que se produjo el error para ver información sobre las posibles causas, así como los pasos para corregir el error.

4. Si desea cancelar el registro del dispositivo CPE, haga clic en **Cancelar**.

5. Después de completar los pasos para corregir el error, haga clic en **Reanudar** para reanudar el registro del dispositivo CPE. En algunos casos, el dispositivo CPE debe reiniciarse después de reanudar el proceso de registro.

El dispositivo CPE se vuelve a registrar.

Si no puede registrar un dispositivo CPE, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.

# Administrar plantillas de CPE

Puede ver la tabla de plantillas de CPE en la sección **SD-WAN → Plantillas de CPE**. La información sobre las plantillas de CPE se muestra en las siguientes columnas de la tabla:

- **Id** es el Id. de la plantilla de CPE.
- **Nombre** es el nombre de la planilla de CPE.
- **Uso** especifica si los dispositivos CPE utilizan una plantilla de CPE:
  - **Sí**.
  - **No**.
- **Actualizado** es la fecha y la hora en que se modificó por última vez la configuración de la plantilla de CPE.
- **Usuario** es el nombre del usuario que creó la plantilla de CPE.
- **Propietario** es el inquilino al que pertenece la plantilla de CPE.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede administrar la configuración de la plantilla de CPE en las siguientes pestañas:

- **Información** es la información básica sobre la plantilla de CPE. Puede editar el nombre de la plantilla de CPE en el campo **Nombre**.
- **Rutas múltiples** es la configuración de la ruta.
- **Desactivación** es la configuración para eliminar y deshabilitar automáticamente el dispositivo CPE.
- **Cifrado** es la configuración de cifrado del tráfico.
- **Scripts** son scripts para la configuración adicional del dispositivo CPE.
- **SD-WAN** es la configuración de conexión de un dispositivo CPE a la red SD-WAN. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración de conexión del dispositivo CPE al orquestador y al controlador.
  - **Interfaces** contiene interfaces SD-WAN.
- **Topología** contiene etiquetas de topología para establecer vínculos entre dispositivos CPE.
- **Red** contiene interfaces de red.
- **BGP** contiene la configuración del protocolo BGP para intercambiar rutas entre dispositivos CPE y dispositivos de red externos.

- **VRF** contiene tablas de enrutamiento y reenvío virtuales.
- **OSPF** abarca el protocolo OSPF para el intercambio de rutas entre dispositivos CPE y dispositivos de red externos. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración básica del protocolo OSPF.
  - **Áreas de OSPF** contiene áreas de OSPF.
  - **Interfaces de OSPF** contiene interfaces de OSPF.
- **Filtros de enrutamiento** contiene la configuración para filtrar rutas y paquetes de tráfico entre dispositivos CPE y dispositivos de red externos. Las siguientes pestañas se muestran en esta pestaña:
  - **Listas de control de acceso** contiene listas de control de acceso (ACL).
  - **Listas de prefijos** contiene listas de prefijos.
  - **Mapas de ruta** contiene mapas de ruta.
- **BFD** abarca el protocolo BFD para detectar fallas de enrutamiento entre dispositivos CPE y dispositivos de red externos.
- **Rutas estáticas** contiene rutas estáticas.
- **Multidifusión** contiene la configuración para la transmisión de tráfico de multidifusión entre dispositivos CPE y dispositivos de red externos que utilizan los protocolos PIM e IGMP. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración básica de PIM.
  - **Interfaces** contiene interfaces de multidifusión.
- **VRRP** abarca el protocolo VRRP para alta disponibilidad de dispositivos CPE. Las siguientes pestañas se muestran en esta pestaña:
  - **Instancias de VRRP** contiene instancias de VRRP.
  - **Grupos de instancias de VRRP** contiene grupos de instancias de VRRP.
- **CFM** contiene la configuración de la funcionalidad de administración de fallas de conexión (CFM).
- **Supervisión** contiene la configuración de supervisión del dispositivo CPE.
- **Servicios de transporte** contiene servicios de transporte.
- **Registro** contiene la configuración de registro.
- **NTP** contiene servidores NTP para la sincronización horaria.
- **VIM** contiene la configuración de VIM. Esta ficha solo se muestra si se selecciona el tipo **uCPE** al crear la plantilla.

# Crear una plantilla de CPE

*Para crear una plantilla de CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. En la parte superior de la página, haga clic en **+ Plantilla de CPE**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la plantilla de CPE.

4. En la lista desplegable **Tipo**, seleccione el tipo de plantilla de CPE:

   - **CPE** para una plantilla de dispositivo CPE estándar. Esta es la configuración predeterminada.
   - **uCPE** para una plantilla de dispositivo uCPE. Los dispositivos uCPE incluyen un hipervisor, que le permite implementar funciones de la red virtual y el VIM en el dispositivo uCPE.

5. Haga clic en **Crear**.

La plantilla de CPE se crea y se muestra en la tabla.

Debe configurar la plantilla de CPE creada. Para obtener detalles sobre la administración de plantillas de CPE, consulte Administración de plantillas de CPE.

# Importar una plantilla de CPE

Puede exportar una plantilla de CPE y luego importarla a otra plantilla de CPE. La configuración de la plantilla de CPE se especifica de acuerdo con la configuración de la plantilla de CPE importada. Durante la importación, puede seleccionar las pestañas que desea dejar sin cambios.

*Para importar una plantilla de CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE que desea exportar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar**.

Un archivo comprimido TAR.GZ con los siguientes datos se guarda en su dispositivo local:

- Un archivo con la descripción de la plantilla de CPE en formato XML. La versión de la plantilla se indica en la descripción.
- Archivos de script.
- Archivos necesarios para ejecutar scripts, como certificados SSL.

El archivo comprimido no contiene información sobre los dispositivos CPE que utilizan la plantilla de CPE.

4. Haga clic en la plantilla de CPE a la que desea importar la plantilla de CPE.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

5. En la parte superior del área de configuración, en **Acciones**, haga clic en **Importar**.

6. En la ventana que se abre, desactive las casillas de verificación junto a las pestañas de la plantilla de CPE que desea dejar sin cambios después de la importación.

7. En el campo **Archivo**, especifique la ruta al archivo comprimido TAR.GZ.

8. Haga clic en **Importar**.

La configuración de la plantilla de CPE se modifica de acuerdo con la configuración de la plantilla de CPE importada.

# Clonar una plantilla de CPE

Puede clonar una plantilla de CPE para crear una plantilla de CPE idéntica con un nombre diferente.

*Para clonar una plantilla de CPE:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE que desea clonar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Clonar**.

4. En la ventana que se abre, ingrese el nombre de la nueva plantilla de CPE.

5. Haga clic en **Clonar**.

Se crea un clon de la plantilla de CPE con el nuevo nombre y se muestra en la tabla.

# Exportar la configuración de conexión del orquestador y del controlador y las interfaces SD-WAN desde una plantilla de CPE

*Para exportar la configuración de conexión del orquestador y el controlador y las interfaces SD-WAN desde una plantilla de CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE desde la cual desea exportar la configuración de conexión del orquestador y del controlador y las interfaces SD-WAN.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar configuración de SD-WAN**.

Un archivo JSON llamado <nombre de plantilla>sdwan-config se guarda en su dispositivo local.

# Exportar interfaces de red desde una plantilla de CPE

*Para exportar interfaces de red desde una plantilla CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE desde la que desea exportar las interfaces de red.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar interfaces de red**.

Un archivo en formato JSON con el nombre <nombre de plantilla>-network-config se guarda en su dispositivo local.

# Ver el uso de una plantilla de CPE

Si es necesario, puede verificar qué dispositivos CPE están utilizando la plantilla de CPE. Por ejemplo, si una plantilla de CPE está en uso, no se puede eliminar.

*Para ver si se está utilizando una plantilla de CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea ver su información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar CPE asociados**.

Se mostrará la sección **CPE** con una tabla de los dispositivos CPE que están utilizando la plantilla de CPE.

## Eliminar una plantilla de CPE

No puede eliminar una plantilla de CPE si al menos un dispositivo de CPE la está utilizando. Para eliminar una plantilla de CPE que está siendo utilizada por dispositivos CPE, primero debe eliminar los dispositivos CPE. Puede verificar qué dispositivos CPE están usando la plantilla de CPE.

Las plantillas de CPE eliminadas no se pueden restaurar.

*Para eliminar una plantilla de CPE:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Seleccione la plantilla de CPE que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

La plantilla de CPE se elimina y ya no se muestra en la tabla.

# Administrar dispositivos CPE

Puede ver la tabla de dispositivos CPE en la sección **SD-WAN → CPE**.

Puede usar filtros en la parte superior de la tabla para filtrar por estado del dispositivo, estado de conexión, estado de energía y período de tiempo.

La información sobre los dispositivos CPE se muestra en las siguientes columnas de la tabla:

- **DPID** es el DPID del dispositivo CPE.
- **S/N** es el número de serie del dispositivo CPE.
- **Modelo** es el modelo del dispositivo CPE.

- **Tipo de conmutador** es el tipo de conmutador de software en el que se basa el firmware del dispositivo CPE (OVS o SWOS).
- **Versión de software** es la versión de firmware del dispositivo CPE. El firmware desactualizado se resalta en naranja.
- **Nombre** es el nombre del dispositivo CPE.
- **Rol** es la función del dispositivo CPE:
  - **CPE**
  - **Gateway**
- **Estado** es el estado del dispositivo CPE.
  - **Desconocido** significa que el dispositivo CPE está conectado al orquestador pero no está registrado.
  - **Esperando** significa que el dispositivo CPE se agregó a la interfaz web del orquestador, pero no está conectado al orquestador.
  - **Registrando** significa que el dispositivo CPE se está registrando.
  - **Error** significa que se produjo un error al registrar el dispositivo CPE.
  - **Registrado** significa que el dispositivo CPE se registró correctamente.
  - **Configuración** significa que los scripts se están ejecutando en el dispositivo CPE.
  - **Suspendida** significa que al registrar el dispositivo CPE, se produjo un error y el registro no se completó.
- **Estado** es el estado del dispositivo CPE:
  - **Habilitado** significa que la plantilla de CPE asignada se aplicó al dispositivo CPE en el lado del orquestador. En el lado del controlador, el dispositivo CPE se puede usar para retransmitir el tráfico.
  - **Deshabilitado** (en el estado **Esperando**) significa que la plantilla de CPE asignada no se aplicó al dispositivo CPE en el lado del orquestador. En el lado del controlador, el dispositivo CPE no se puede usar para retransmitir el tráfico.
  - **Deshabilitado** (en el estado **Registrado**) significa que el orquestador no responde a las solicitudes de la API REST del dispositivo CPE. En el lado del controlador, la transmisión de tráfico a través de vínculos está bloqueada para el dispositivo CPE.
- **Conexión** contiene información sobre si el dispositivo CPE está conectado al controlador:
  - **Conectados**
  - **Desconectado**
- **Etiquetas de topología** contiene etiquetas de topología que se asignaron al dispositivo CPE.

- **Fragmentación** es el resultado de verificar la fragmentación de paquetes de tráfico en el dispositivo CPE:
  - **No admitido** significa que el dispositivo CPE no puede transmitir paquetes fragmentados.
  - **Desconocido** significa que no se puede verificar la fragmentación de paquetes en el dispositivo CPE.
  - **Admitido** significa que el dispositivo puede transmitir paquetes fragmentados.
- **Inquilino de transporte** es el inquilino de transporte al que se agrega el dispositivo CPE. El dispositivo CPE se conecta al controlador de la instancia SD-WAN que se implementa para el inquilino de transporte.
- **Inquilino del cliente** es el inquilino del cliente al que se agrega el dispositivo CPE. El inquilino del cliente puede administrar el dispositivo CPE en su portal de autoservicio.
- **Plantilla de CPE** es la plantilla de CPE utilizada por el dispositivo CPE.
- **Ubicación** es la dirección de ubicación del dispositivo CPE.
- **IP de administración** es la dirección IP asignada al dispositivo CPE por la subred de administración.
- **Controladores** son las direcciones IP y el número de puerto de los nodos del controlador a los que está conectado el dispositivo CPE.
- **Gateways** son las direcciones IP y los números de puerto de las puertas de enlace a las que está conectado el dispositivo CPE.
- **Red móvil** es la red móvil a la que está conectado el dispositivo CPE.
- **Registrado** es la fecha y la hora en que se registró el dispositivo CPE.
- **Actualización** es la fecha y hora en que se modificó por última vez la configuración del dispositivo CPE.
- **Usuario** es el nombre del usuario que creó el dispositivo CPE.
- **Estado de encendido** es el estado de energía del dispositivo CPE:
  - **Aceptar**
  - **Falla de la fuente de alimentación**
  - **Batería**
  - **Desconocido**

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede ver y administrar la configuración del dispositivo CPE haciendo clic en su nombre en la tabla para abrir una ventana y seleccionar una sección de la barra lateral:

- **Configuración** es la información básica sobre el dispositivo CPE. Puede ver información en las siguientes columnas de la tabla **Información del dispositivo**:
  - **Modelo** es el modelo del dispositivo CPE.
  - **Versión de software** es la versión de firmware del dispositivo CPE. El firmware desactualizado se resalta en naranja.
  - **Controlador** son las direcciones IP y el número de puerto de los nodos del controlador a los que está conectado el dispositivo CPE.
  - **Gateways** son las direcciones IP y los números de puerto de las puertas de enlace a las que está conectado el dispositivo CPE.
  - **Usuario** es el nombre del usuario que creó el dispositivo CPE.
  - **Registrado** es la fecha y la hora en que se registró el dispositivo CPE.
  - **Actualización** es la fecha y hora en que se modificó por última vez la configuración del dispositivo CPE.
  - **IP de administración** es la dirección IP asignada al dispositivo CPE por la subred de administración.
  - **Estado** es el estado del dispositivo CPE:
    - **Habilitado** significa que la plantilla de CPE asignada se aplicó al dispositivo CPE en el lado del orquestador. En el lado del controlador, el dispositivo CPE se puede usar para retransmitir el tráfico.
    - **Deshabilitado** (en el estado **Esperando**) significa que la plantilla de CPE asignada no se aplicó al dispositivo CPE en el lado del orquestador. En el lado del controlador, el dispositivo CPE no se puede usar para retransmitir el tráfico.
    - **Deshabilitado** (en el estado **Registrado**) significa que el orquestador no responde a las solicitudes de la API REST del dispositivo CPE. En el lado del controlador, la transmisión de tráfico a través de vínculos está bloqueada para el dispositivo CPE.
  - **Conexión** contiene información sobre si el dispositivo CPE está conectado al controlador:
    - **Conectados**
    - **Desconectado**

  Puede ingresar una breve descripción del dispositivo CPE en el campo **Descripción** y ver las tareas que realiza el orquestador en la tabla **Administración fuera de banda**.
- **Supervisión** son los resultados del control del dispositivo CPE.
- **Problemas** son problemas que ocurrieron mientras el dispositivo CPE estaba en funcionamiento. En caso de que haya ocurrido un problema, se muestra un signo de exclamación rojo junto a la pestaña.
- **Cifrado** es la configuración de cifrado del tráfico.
- **Solicitudes del servicio** son solicitudes de servicio del dispositivo CPE.

- **Etiquetas** son etiquetas para agrupar dispositivos CPE.
- **Scripts** son scripts para la configuración adicional del dispositivo CPE.
- **SD-WAN** es la configuración de conexión de un dispositivo CPE a la red SD-WAN. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración de conexión del dispositivo CPE al orquestador y al controlador.
  - **Interfaces** contiene interfaces SD-WAN.
- **Topología** contiene etiquetas de topología para establecer vínculos entre dispositivos CPE.
- **Red** contiene interfaces de red.
- **DHCP** contiene la configuración del DHCP.
- **Firewall** contiene la configuración del firewall.
- **VRF** contiene tablas de enrutamiento y reenvío virtuales.
  - **BGP** contiene la configuración del protocolo BGP para intercambiar rutas entre dispositivos CPE y dispositivos de red externos.
- **OSPF** abarca el protocolo OSPF para el intercambio de rutas entre dispositivos CPE y dispositivos de red externos. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración básica del protocolo OSPF.
  - **Áreas de OSPF** contiene áreas de OSPF.
  - **Interfaces de OSPF** contiene interfaces de OSPF.
- **Filtros de enrutamiento** contiene la configuración para filtrar rutas y paquetes de tráfico entre dispositivos CPE y dispositivos de red externos. Las siguientes pestañas se muestran en esta pestaña:
  - **Listas de control de acceso** contiene listas de control de acceso (ACL).
  - **Listas de prefijos** contiene listas de prefijos.
  - **Mapas de ruta** contiene mapas de ruta.
- **PBR** contiene la configuración del enrutamiento basado en directivas (PBR).
- **BFD** abarca el protocolo BFD para detectar fallas de enrutamiento entre dispositivos CPE y dispositivos de red externos.
- **Rutas estáticas** contiene rutas estáticas.

- **Multidifusión** contiene la configuración para la transmisión de tráfico de multidifusión entre dispositivos CPE y dispositivos de red externos que utilizan los protocolos PIM e IGMP. Las siguientes pestañas se muestran en esta pestaña:
  - **Configuración general** contiene la configuración básica de PIM.
  - **Interfaces** contiene interfaces de multidifusión.
- **VRRP** abarca el protocolo VRRP para alta disponibilidad de dispositivos CPE. Las siguientes pestañas se muestran en esta pestaña:
  - **Instancias de VRRP** contiene instancias de VRRP.
  - **Grupos de instancias de VRRP** contiene grupos de instancias de VRRP.
- **CFM** contiene la configuración de la funcionalidad de administración de fallas de conexión (CFM).
- **UNI** son las UNI en el dispositivo CPE.
- **Módems** son configuraciones del módem del dispositivo CPE.
- **Enlaces** contiene la configuración del vínculo.
- **Rutas múltiples** es la configuración de la ruta.
- **Activación** es la configuración de la autenticación de dos factores del dispositivo CPE.
- **Desactivación** es la configuración para eliminar y deshabilitar automáticamente el dispositivo CPE.
- **Registro** contiene la configuración de registro.
- **NetFlow** contiene la configuración básica de NetFlow.
- **NTP** muestra los servidores NTP utilizados para la sincronización horaria.
- **Información de diagnóstico** muestra solicitudes de información de diagnóstico del dispositivo CPE.
- **Utilidades** muestra utilidades para diagnosticar dispositivos CPE.

# Agregar dispositivos CPE

Debe agregar un dispositivo CPE si lo registra automáticamente (ZTP). Al agregar un dispositivo CPE, debe especificar el DPID que se utilizará para hacer coincidir el registro agregado con el dispositivo CPE que se conectará más adelante. Puede agregar un dispositivo CPE para la instancia SD-WAN actual, un inquilino o una instancia SD-WAN diferente. Puede agregar un dispositivo individual o dispositivos de importación masiva con la configuración de un archivo CSV.

*Para agregar un dispositivo CPE:*

1. Agregue un dispositivo CPE de una de las siguientes maneras:

   - Si desea agregar un dispositivo CPE a la instancia SD-WAN actual, en el menú, vaya a la sección **SD-WAN** → **CPE** y, en la parte superior de la página, haga clic en **+ Agregar**.

   - Si desea agregar un dispositivo CPE para un inquilino, vaya a la sección **Inquilinos**, haga clic en el inquilino creado y, en la pestaña **CPE**, haga clic en el botón **+ Agregar**.

   - Si desea agregar un dispositivo CPE a una instancia SD-WAN diferente, vaya a la subsección **SD-WAN** → **Instancias SD-WAN**, haga clic en una instancia SD-WAN implementada y, en la parte superior del área de configuración, en **Acciones**, haga clic en **Agregar CPE**.

2. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del dispositivo CPE.

3. En el campo **DPID**, ingrese el DPID del dispositivo CPE. Puede encontrar el DPID en la caja del dispositivo CPE.

   Si el dispositivo CPE no tiene un DPID, puede especificar un DPID temporal, por ejemplo, `un DPID temporal`. Puede reemplazar el DPID temporal con el DPID real.

4. En la lista desplegable **Estado**, seleccione el estado del dispositivo CPE después del registro:

   - **Habilitado** para aplicar una plantilla CPE al dispositivo CPE y usarla para retransmitir el tráfico. Esta es la configuración predeterminada.

   - **Deshabilitado** para no aplicar una plantilla CPE al dispositivo CPE.

5. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del dispositivo CPE.

6. Si está agregando un dispositivo CPE a una instancia SD-WAN, en la lista desplegable **Inquilino**, seleccione el inquilino de transporte al que desea agregar el dispositivo CPE. El dispositivo CPE se conecta al controlador de la instancia SD-WAN que se implementa para el inquilino de transporte. Puede seleccionar un grupo de instancias SD-WAN.

7. En la lista desplegable **Inquilino del cliente**, seleccione el inquilino del cliente al que desea agregar el dispositivo CPE. El inquilino del cliente puede administrar el dispositivo CPE en su portal de autoservicio.

8. Si desea crear una UNI en el dispositivo CPE utilizando una plantilla UNI, en la lista desplegable **Plantilla de UNI**, seleccione la plantilla UNI creada.

9. En la lista desplegable **Plantilla de CPE**, seleccione la plantilla CPE creada que desea usar para configurar el dispositivo CPE.

10. En la lista desplegable **Plantilla de NetFlow**, seleccione la plantilla NetFlow creada que desea utilizar para establecer la configuración básica de NetFlow en el dispositivo CPE.

11. En la lista desplegable **Plantilla de firewall**, seleccione la plantilla de firewall creada que desea usar para configurar el firewall del dispositivo CPE.

12. Haga clic en **Siguiente** y especifique la dirección de la ubicación del dispositivo CPE en el campo **Dirección**. Cuando ingrese la dirección, se le pedirá que seleccione una dirección de una lista desplegable.

    La dirección se muestra en el mapa.

13. Haga clic en **Realizado**.

El dispositivo se agrega, su estado cambia a **Esperando** y obtiene uno de los siguientes resultados:

- Si agregó el dispositivo CPE para la instancia SD-WAN actual, el dispositivo se muestra en la tabla.
- Si agregó un dispositivo CPE para un inquilino, este dispositivo CPE aparece en el área de configuración del inquilino en la pestaña **CPE**.
- Si agregó un dispositivo CPE para una instancia SD-WAN diferente, el portal de autoservicio se abre en una nueva pestaña del navegador. Iniciará sesión en el portal de autoservicio automáticamente y se le dirigirá a la subsección **CPE**. El dispositivo CPE se agrega a la tabla.

# Importación masiva de dispositivos CPE desde un archivo CSV

Si necesita agregar una gran cantidad de dispositivos CPE al mismo tiempo, puede usar la función de importación masiva. Antes de importar dispositivos CPE, debe especificar su configuración en un archivo CSV. El archivo CSV para la importación debe cumplir con los siguientes requisitos:

- La primera fila del archivo CSV contiene los encabezados.
- El orden de los encabezados no es importante.
- El archivo importado debe tener la extensión `csv`.
- El tamaño máximo del archivo es 10 485 760 bytes.
- El número máximo de filas en el archivo es 25 001 (25 000 filas de datos + 1 fila de encabezado).

Si realiza la operación de importación dentro de un inquilino, el orquestador especifica automáticamente los inquilinos de transporte y cliente, y los valores correspondientes del archivo CSV se ignoran.

Para obtener una descripción detallada de las columnas del archivo, consulte la tabla de este artículo. También puede descargar un archivo de ejemplo en la ventana de importación.

*Para importar dispositivos CPE desde un archivo, siga estos pasos:*

1. Prepare el archivo CSV para la importación.
2. En el menú, vaya a la sección **SD-WAN** → **CPE**; en la parte superior de la página, haga clic en el ícono ⌄ en la parte derecha de **+ CPE** para abrir la lista desplegable, luego seleccione **Importación masiva de CSV**.
3. En la ventana que se abre, seleccione su archivo CSV preparado y cárguelo en el orquestador.

    Después de cargar el archivo CSV, el orquestador valida las filas del archivo.

4. Cualquier error que encuentre se enumerará en la ventana de importación. La lista de errores se divide en pestañas según el tipo de error:

   - **Formato de línea no válido**
   - **Sin supervisión**
   - **Objeto no encontrado**
   - **Errores de validación**

   Si hay algún error de importación, corríjalo en el archivo y vuelva a intentarlo.

5. Si el archivo pasa la validación sin errores, comienza la importación. Durante toda la validación e importación, el dispositivo CPE está bloqueado (el tiempo máximo de bloqueo es de 30 segundos).

Después de una importación exitosa, se muestra el mensaje correspondiente que indica la cantidad de dispositivos agregados. Los dispositivos se agregan y se muestran en la tabla; su estado cambia a **Esperando**.

Descripción de las columnas del archivo CSV para la importación por lotes de dispositivos CPE

| Nombre de la columna | Contenido de la columna | Proceso de validación | Requeridos |
|---|---|---|---|
| `Nombre` | Nombre del dispositivo CPE. Cadena de texto arbitraria. | Lo mismo que para agregar un dispositivo CPE individual. | Requeridos |
| `MACAddress` | 6 grupos de 2 números hexadecimales, que pueden estar separados por guiones, dos puntos o nada.<br>Ejemplos:<br>• `DE-AD-BE-EF-11-22`<br>• `DE:AD:BE:EF:11:22`<br>• `DEADBEEF1122` | El valor resultante se convierte al formato DPID:<br>• Se agrega 8000 al principio de la línea<br>• Los separadores, si los hubiera, se eliminan<br>• Las letras `a–f` se convierten a mayúsculas si están en minúsculas.<br>La validación del DPID obtenido es la misma que para agregar un dispositivo CPE individual. | Requeridos |
| `Estado` | Cadena. Valores posibles:<br>• `enabled`<br>• `disabled` | Lo mismo que para agregar un dispositivo CPE individual. | Requeridos |
| `Inquilino de transporte` | Nombre del inquilino del transporte. | Este valor se usa para buscar el inquilino de transporte. | Requeridos |
| `Plantilla de CPE` | Nombre de la plantilla de CPE. | Este valor se usa para buscar la plantilla de CPE con un propietario que corresponda al inquilino desde el cual se está importando el CSV. | Requeridos |
| `Plantilla de NetFlow` | Nombre de la plantilla de NetFlow. | Este valor se usa para buscar la plantilla de NetFlow con un propietario que corresponda al inquilino desde el cual se está importando el CSV. | Requeridos |
| `Plantilla de firewall` | Nombre de la plantilla de firewall. | Este valor se usa para buscar la plantilla de firewall con un propietario que corresponda al inquilino desde el cual se está importando el CSV. | Requeridos |
| `Descripción` | Descripción del dispositivo CPE. Cadena de texto arbitraria. | Lo mismo que para agregar un dispositivo CPE individual. | Opcional |
| `Inquilino del cliente` | Nombre del inquilino del cliente. | Este valor se usa para buscar el inquilino del cliente. | Opcional |
| `Plantilla de UNI` | Nombre de la plantilla de UNI. | Este valor se usa para buscar la plantilla de UNI con un propietario que corresponda al inquilino desde el cual se está importando el CSV. | Opcional |

# Generar una URL con la configuración básica del dispositivo CPE

Para el registro automático de un dispositivo CPE, debe generar una dirección web con la configuración básica del dispositivo CPE. Puede especificar la plantilla de la URL generada cuando se configure la conexión del dispositivo CPE al orquestador y controlador. La URL generada contiene la siguiente información:

- Servidores NTP
- Interfaces de red
- Configuración para la conexión del dispositivo CPE al orquestador y controlador y las interfaces de SD-WAN
- Certificados
- Configuración de BGP
- El token si se está utilizando la autenticación de dos factores
- Tablas de enrutamiento y reenvío virtuales
- Directorios de APN

El tamaño máximo de una URL con la configuración básica del dispositivo CPE no puede exceder los 64 KB.

*Para generar una URL con la configuración básica del dispositivo CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el que desea generar una URL con la configuración básica.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Obtener URL de configuración**.

4. En la ventana que se abre, en la lista desplegable **Versión**, especifique la versión de firmware del dispositivo CPE para el que desea generar una dirección web con la configuración básica:

   - **Actual**
   - **23.07**

5. Guarde la URL con la configuración básica del dispositivo CPE de una de las siguientes maneras:

   - Si desea copiar la URL, haga clic en **Copiar** junto a ella.
   - Si desea guardar la dirección web como un archivo HTML, haga clic en **Guardar** junto a ella.

   Debe conectar un dispositivo administrador al puerto LAN del dispositivo CPE y usar la URL guardada con la conexión básica para registrar automáticamente el dispositivo CPE.

Si necesita instalar certificados en un dispositivo CPE con la versión de firmware 23.07, siga los pasos descritos en el artículo Escenario: instalación de certificados en un dispositivo CPE con la versión de firmware 23.07.

# Registrar un dispositivo CPE manualmente

Debe registrar manualmente el dispositivo CPE en la interfaz web cuando vuelva a registrar el dispositivo CPE. El registro no requiere conexión a los servicios en la nube de Kaspersky.

*Para registrar manualmente un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE que desea registrar manualmente.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Registrar**.

4. En la ventana que se abre, en la lista desplegable **Estado**, seleccione el estado del dispositivo CPE después del registro:

   - **Habilitado** para aplicar una plantilla CPE al dispositivo CPE y usarla para retransmitir el tráfico. Esta es la configuración predeterminada.
   - **Deshabilitado** para no aplicar una plantilla CPE al dispositivo CPE.

5. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del dispositivo CPE.

6. En la lista desplegable **Inquilino**, seleccione el inquilino de transporte al que desea agregar el dispositivo CPE. El dispositivo CPE se conecta al controlador de la instancia SD-WAN que se implementa para el inquilino de transporte. Puede seleccionar un grupo de instancias SD-WAN.

7. En la lista desplegable **Inquilino del cliente**, seleccione el inquilino del cliente al que desea agregar el dispositivo CPE. El inquilino del cliente puede administrar el dispositivo CPE en su portal de autoservicio.

8. Si desea crear una UNI en el dispositivo CPE utilizando una plantilla UNI, en la lista desplegable **Plantilla de UNI**, seleccione la plantilla UNI creada.

9. En la lista desplegable **Plantilla de CPE**, seleccione la plantilla CPE creada que desea usar para configurar el dispositivo CPE.

10. En la lista desplegable **Plantilla de NetFlow**, seleccione la plantilla NetFlow creada que desea utilizar para establecer la configuración básica de NetFlow en el dispositivo CPE.

11. En la lista desplegable **Plantilla de firewall**, seleccione la plantilla de firewall creada que desea usar para configurar el firewall del dispositivo CPE.

12. Haga clic en **Siguiente** y especifique la dirección de la ubicación del dispositivo CPE en el campo **Dirección**. Cuando ingrese la dirección, se le pedirá que seleccione una dirección de una lista desplegable.

    La dirección se muestra en el mapa.

13. Haga clic en **Registrar**.

El estado del dispositivo CPE cambia primero a **Registrando**, luego a **Registrado**.

# Anular el registro de un dispositivo CPE

*Para anular el registro de un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el desea anular el registro.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Dar de baja**.

4. En la ventana de confirmación, haga clic en **Dar de baja**.

El dispositivo CPE no está registrado y el estado del dispositivo CPE cambia a **Esperando**.

# Especificar la dirección de un dispositivo CPE

*Para especificar la dirección de un dispositivo CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE cuya dirección desea especificar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Configurar ubicación**.

4. En la ventana que se abre, ingrese la dirección de la ubicación del dispositivo CPE. Cuando ingrese la dirección, se le pedirá que seleccione una dirección de una lista desplegable.

   La dirección se muestra en el mapa.

5. Haga clic en **Guardar**.

Se especificará la dirección del dispositivo CPE.

# Activar y desactivar un dispositivo CPE

Cuando se habilita un dispositivo CPE, se le aplica una plantilla de CPE. Los dispositivos CPE deshabilitados no se pueden usar para retransmitir el tráfico.

*Para habilitar o deshabilitar un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE que desea habilitar o deshabilitar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Habilitar** o **Deshabilitar**.

El dispositivo CPE se habilita o deshabilita.

# Reiniciar un dispositivo CPE

*Para reiniciar un dispositivo CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE que desea reiniciar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Reiniciada**.

4. En la ventana de confirmación, haga clic en **Reiniciada**.

Se reiniciará el dispositivo CPE.

# Apagar un dispositivo CPE

Puede apagar el dispositivo CPE en la interfaz web del orquestador o desconectando el cable de alimentación del dispositivo CPE. Cuando se apaga la alimentación en la interfaz web del orquestador, el comando de `apagado` se envía al sistema operativo del dispositivo CPE.

*Para apagar el dispositivo CPE en la interfaz web del orquestador, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE que desea apagar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Apagar**.

4. En la ventana de confirmación, haga clic en **Apagar**.

El dispositivo CPE se apagará.

# Conectarse a la consola del dispositivo CPE

*Para conectarse a la consola de un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE a cuya consola desea conectarse.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Abrir consola SSH**.

Se abre la ventana de la consola del dispositivo CPE en una nueva pestaña del navegador.

# Visualizar la contraseña de un dispositivo CPE

*Para visualizar la contraseña de un dispositivo CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE cuya contraseña desea ver.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar contraseña**.

Esto abre una ventana con la contraseña del dispositivo CPE.

# Exportar la configuración de conexión del orquestador y del controlador y las interfaces SD-WAN desde un dispositivo CPE

*Para exportar la configuración de conexión del orquestador y del controlador y las interfaces de SD-WAN desde un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE desde el que desea exportar la configuración de conexión del orquestador y del controlador y las interfaces de SD-WAN.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar configuración de SD-WAN**.

Un archivo JSON llamado <nombre de plantilla>sdwan-config se guarda en su dispositivo local.

# Exportar interfaces de red desde un dispositivo CPE

*Para exportar interfaces de red desde un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE desde el que desea exportar las interfaces de red.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior, debajo de **Acciones**, haga clic en **Exportar interfaces de red**.

Un archivo en formato JSON con el nombre <nombre de plantilla>-network-config se guarda en su dispositivo local.

# Cambiar el DPID de un dispositivo CPE

Es posible que deba editar el DPID en las siguientes situaciones:

- Implementación de un dispositivo vCPE en la plataforma de virtualización VMware con registro automático
- Reemplazo de un dispositivo CPE registrado existente con un nuevo dispositivo CPE mientras se mantiene la configuración de red anterior (por ejemplo, si un dispositivo deja de funcionar).

*Para cambiar el DPID de un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE cuyo DPID desea cambiar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Cambiar DPID**.

4. En la ventana que se abre, ingrese el nuevo DPID del dispositivo CPE.

5. Haga clic en **Guardar**.

Se cambia el DPID del dispositivo CPE.

# Editar la configuración del dispositivo CPE

Si es necesario, puede editar la configuración del dispositivo CPE. Puede hacer que la configuración modificada se aplique inmediatamente o después de un retraso mediante el programador de tareas.

*Para editar la configuración del dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE cuya configuración desea editar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Después de seleccionar las pestañas con la configuración del dispositivo CPE que desea editar, proceda a editar la configuración.

4. Seleccione una de las opciones para guardar la configuración:

- Si desea que los cambios se apliquen instantáneamente, haga clic en el botón **Guardar**.

  Se guarda la configuración del dispositivo CPE.

- Si desea programar la configuración para que se aplique en un momento específico:

  1. Use el ícono ⌄ en la parte derecha del botón **Guardar**, abra el menú del modo de guardado y seleccione **Guardado programado**.

     Se abre la barra lateral para crear una tarea.

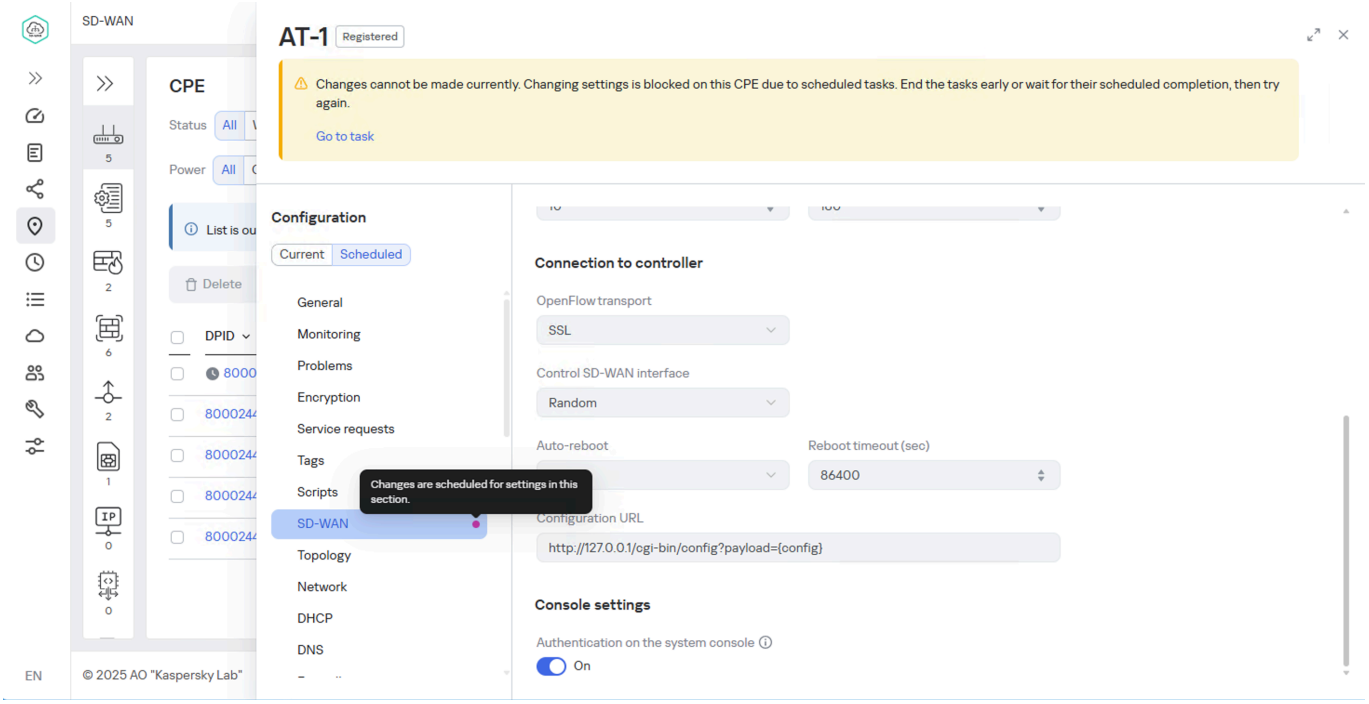
  2. En el campo **Fecha de ejecución de la tarea programada**, ingrese la fecha y la hora en que desea ejecutar la tarea. La configuración predeterminada es la fecha y la hora en que comenzó a crear la tarea.

  3. Si es necesario, en el campo **Nombre de la tarea**, ingrese el nombre de la tarea. De manera predeterminada, el nombre "Actualización de la configuración del programa" se ingresa en este campo.

  4. Haga clic en **Programar**.

  Se crea una tarea programada para modificar la configuración del dispositivo CPE. Puede ver el estado de la tarea en la tabla **Programador**.

  El dispositivo CPE en el que se programan los cambios se muestra en la tabla de la sección **SD-WAN → CPE** con el ícono 🕒 junto a su DPID. En el área de configuración del dispositivo CPE, aparecen nuevas pestañas que le permiten ver la configuración actual del dispositivo y la configuración programada del dispositivo. Las secciones con configuraciones que están programadas para cambiar como parte de una tarea creada se resaltan visualmente. No puede editar ninguna configuración del CPE o su plantilla de CPE hasta que se complete la tarea programada. Para ir a la tarea, haga clic en **Ir a la tarea** y complete la tarea antes de lo programado o elimine la tarea.




Se muestra el CPE junto con los cambios programados

# Eliminar dispositivos CPE

Cuando elimina un dispositivo CPE, todas las interfaces de servicio creadas en él se eliminan automáticamente.

Los dispositivos CPE eliminados no se pueden restaurar.

*Para eliminar dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Para eliminar un dispositivo CPE individual, siga estos pasos:

   a. Haga clic en el dispositivo CPE que desea eliminar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

   b. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

3. Para eliminar varios dispositivos CPE, siga estos pasos:

   a. Seleccione las casillas que hay junto a los dispositivos CPE que desee eliminar.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

4. En la ventana de confirmación que se abre, seleccione el método para eliminar el dispositivo CPE:

   - **Eliminar, dar de baja y restablecer contraseña** para eliminar el dispositivo CPE de la interfaz web del orquestador. Cuando se enciende, el dispositivo CPE se vuelve a conectar al orquestador y se muestra en la interfaz web del orquestador con el estado **Desconocido**.
   - **Restablecer ajustes de fábrica** para eliminar el dispositivo CPE de la interfaz web del orquestador y restablecer la configuración del dispositivo CPE a los valores predeterminados de fábrica. Cuando se enciende, el dispositivo CPE no se vuelve a conectar al orquestador y no se muestra en la interfaz web del orquestador.
   - **Forzar eliminación** para eliminar el dispositivo CPE de la interfaz web del orquestador. Puede seleccionar esta opción para eliminar un CPE no disponible o una entrada redundante de la interfaz web del orquestador.

5. Haga clic en **Eliminar**.

Los dispositivos CPE se eliminan y ya no se muestran en la tabla.

# Autenticación de dos factores de un dispositivo CPE

Puede utilizar la *autenticación de dos factores* para registrar el dispositivo CPE de forma segura. Cuando se habilita la autenticación de dos factores, se registra un token (clave de seguridad) en la base de datos del orquestador. Luego, debe colocar este token en el dispositivo CPE cuando se registre con la tecnología de aprovisionamiento sin intervención. El registro se realiza de forma correcta si, cuando el dispositivo CPE se conecta automáticamente al orquestador, el token colocado en el dispositivo coincide con el token de CPE en la base de datos del orquestador.

No puede usar la autenticación de dos factores para un dispositivo CPE que ya está registrado.

*Para usar la autenticación de dos factores para un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el que desea usar la autenticación de dos factores.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Activación**.

   Se muestra la configuración de la autenticación de dos factores.

4. En la lista desplegable **Autenticación de dos factores**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

5. Si desea generar un nuevo token, haga clic en **Generate** debajo del campo **Token**.

6. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Administrar certificados

Al comunicarse con el orquestador, el dispositivo CPE verifica si se puede confiar en los certificados del orquestador para evitar ataques MITM. De manera predeterminada, el dispositivo CPE confía en las autoridades de certificación públicas.

Si el orquestador utiliza certificados firmados por una autoridad de certificación personalizada, debe cargar estos certificados en la interfaz web del orquestador e instalarlos en los dispositivos CPE. Se admiten certificados raíz independientes, así como cadenas de certificados que constan de un certificado raíz y varios certificados intermedios.

30 días antes de que caduque el certificado, se muestra una notificación cuando inicia sesión en la interfaz web del orquestador.

Puede ver la tabla de certificados en la sección **SD-WAN → Certificados**. La información sobre los certificados se muestra en las siguientes columnas de la tabla:

- **Nombre común** es el nombre de dominio o nombre de host para el cual se emite el certificado.
- **Organización** es el nombre de la organización que emitió el certificado.
- **Distribuir a CPE** es la casilla de verificación para instalar el certificado en dispositivos CPE. Los certificados que tienen sus casillas de verificación seleccionadas se instalan en los dispositivos CPE en los siguientes casos:
  - Registro automático (ZTP) de un dispositivo CPE
  - Reinicio del dispositivo CPE
  - Instalación manual de certificados en el dispositivo CPE

  La selección incorrecta de certificados puede hacer que el dispositivo CPE deje de confiar en el certificado del orquestador y se desconecte de él.
- **Remitente** es la fecha de inicio de la validez del certificado.
- **Destinatario** es la fecha de caducidad del certificado.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Cargar un certificado mediante la interfaz web del orquestador

*Para cargar un certificado en la interfaz web del orquestador, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Certificados**.

   Se muestra una tabla de certificados.
2. En la parte superior de la página, haga clic en **+ Certificado**.
3. Especifique la ruta al archivo del certificado en formato PEM. Tamaño máximo del archivo: 16 KB.

El certificado se carga y se muestra en la tabla. Aparece el mensaje *Certificado <nombre del certificado> cargado*.

## Instalar certificados manualmente en dispositivos CPE

*Para instalar certificados en dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Certificados**.

   Se muestra una tabla de certificados.

2. Seleccione las casillas de verificación **Distribuir a CPE** junto a los certificados cargados que desea instalar en los dispositivos CPE.

3. Haga clic en **Aplicar a CPE**.

Los certificados se instalan en los dispositivos CPE. Se muestra el mensaje *Los certificados se aplican a los CPE*.

# Escenario: instalación de certificados en un dispositivo CPE con la versión de firmware 23.07

Puede instalar un certificado raíz o una cadena de certificados firmada por una autoridad de certificación personalizada en un dispositivo CPE con la versión de firmware 23.07.

La versión del firmware 23.07 no es completamente compatible con la versión actual del orquestador; por lo tanto, es probable que se produzcan problemas técnicos cuando se utilice esta versión del firmware. Recomendamos actualizar el firmware de todos los dispositivos CPE a la última versión.

El escenario para instalar certificados en los dispositivos CPE con la versión del firmware 23.07 conlleva los siguientes pasos:

1. **Cargar certificados con la interfaz web del orquestador**

   Cargue un certificado con la interfaz web del orquestador.

2. **Generar una URL con la configuración básica del dispositivo CPE**

   Para generar una URL con la configuración básica del dispositivo CPE, haga lo siguiente:

   1. En la lista desplegable **Versión**, seleccione **23.07**.

      Se generarán las direcciones web de la configuración para cada uno de los certificados cargados.

   2. Haga clic en **Copiar** junto a todas las URL generadas.

   3. Guarde las direcciones web que se copiaron.

3. **Instalar los certificados en un dispositivo CPE**

   Haga lo siguiente:

   1. Conecte el dispositivo administrador al puerto LAN del dispositivo CPE.

      El dispositivo administrador obtiene una dirección IP y la dirección IP de la puerta de enlace predeterminada a través de DHCP. La dirección IP recibida de la puerta de enlace predeterminada es la dirección IP del dispositivo CPE.

   2. Desde el dispositivo administrador, visite cada dirección web generada, una por una.

      El dispositivo CPE se reinicia después de instalar cada certificado. Tenga en cuenta que el dispositivo CPE puede obtener una dirección IP nueva después del reinicio, por lo que es posible que deba modificar la dirección web copiada anteriormente para instalar el siguiente certificado.

# Exportar un certificado

*Para exportar un certificado, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Certificados**.

   Se muestra una tabla de certificados.

2. Haga clic en el certificado que desea exportar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar**.

Se guarda un archivo de certificado en formato PEM en su dispositivo local.

# Eliminar certificados

Los certificados eliminados no se pueden restaurar.

*Para eliminar certificados, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **Certificados**.

   Se muestra una tabla de certificados.

2. Para eliminar un certificado individual, haga lo siguiente:

   a. Haga clic en el certificado que desea eliminar.

      Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

   b. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

3. Para eliminar varios certificados, haga lo siguiente:

   a. Seleccione las casillas de verificación junto a los certificados que desea eliminar.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

Los certificados se eliminarán y ya no se mostrarán en la tabla.

# Administrar directorios de APN

Para ver la tabla de directorios de APN, vaya a la sección del menú **SD-WAN → Plantillas de NetFlow**. De manera predeterminada, el directorio de APN **DefaultAPNDir** se crea en el portal del administrador.

La información sobre los directorios de APN se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del directorio de APN.
- **Uso** indica si el directorio de APN está siendo utilizado por dispositivos CPE:
  - **Sí**.
  - **No**.
- **Propietario** es el inquilino al que pertenece el directorio de APN.
- **Actualizado** es la fecha y la hora en que se modificó por última vez la configuración del directorio de APN.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un directorio de APN

*Para crear un directorio de APN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Directorios de APN**.

   Se muestra la tabla de directorios de APN.

2. Si desea agregar un directorio APN manualmente:

   a. En la parte superior de la página, haga clic en **+ Crear**.

   Esto abre la ventana para agregar el directorio APN con una tabla de registros APN.

   b. En el campo **Nombre**, ingrese el directorio APN.

   c. Agregue uno o más registros APN haciendo clic en el botón **Agregar**. Para cada registro, complete los siguientes campos:

   - **PLMN** es el identificador PLMN de su operador. Los primeros tres dígitos del identificador de PLMN son el código de país móvil (MCC) y los dos o tres dígitos siguientes son el código de red móvil (MNC). Por ejemplo, para la red Vimpelcom en el territorio ruso, PLMN =25099: MCC = 250 (Federación de Rusia), MNC = 99 (Vimpelcom).

     Configuración requerida.

   - **APN** es la cadena APN de su operador. Los caracteres permitidos son `[0-9A-Za-z-.]`. La cadena debe comenzar y finalizar con una letra o un número. Puede ser una cadena vacía. La longitud máxima es de 100 caracteres.

     Configuración requerida.

- **Nombre de usuario de APN** es el nombre de usuario de APN para la autenticación con el operador. Longitud máxima: 32 caracteres. Caracteres permitidos: `[0-9A-Za-z-._#$%*]`.

  Configuración opcional.

- **Contraseña de APN** es la contraseña de APN para la autenticación con el operador. Longitud máxima: 32 caracteres. Caracteres permitidos: `[0-9A-Za-z~`!@#$%^&*()_-+={[}]|\:;"'<,>.?/]`.

  Configuración opcional.

Para eliminar un registro APN , haga clic en **Eliminar** junto a él.

d. Haga clic en **Crear**.

3. Si desea agregar el directorio APN desde un archivo:

   a. En la parte superior de la página, haga clic en **+ Cargar a partir de un archivo**.

   b. En la ventana que se abre, seleccione el archivo JSON desde el que desea importar un directorio APN. El archivo debe tener la siguiente estructura:

```
{
 "name": "MyCustomDirectory",
 "entriesAmount": 150,
 "entries": [
 {"plmn": "25099", "apn": "internet.beeline.ru"},
 {"plmn": "25002", "apn": "internet"},
 {"plmn": "250201","apn": "some.private.apn","username": "apn-user","password": "********"}
 ]
}
```

El directorio APN se crea y se muestra en la tabla.

# Ver y restablecer sesiones en dispositivos CPE

Los dispositivos CPE rastrean y almacenan información acerca de las conexiones entrantes y salientes en forma de sesiones. Una sesión es un conjunto de atributos relacionados que permiten combinar paquetes individuales en una entidad lógica y rastrear su estado.

Puede descargar y ver la lista de sesiones para un dispositivo CPE utilizando la interfaz web del orquestador, por ejemplo, para diagnosticar rápidamente problemas de conexión del usuario, analizar la actividad de la red o supervisar el uso de recursos CPE en tiempo real. También puede restablecer la lista de sesiones en un dispositivo.

*Para ver o restablecer la lista de sesiones en un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el que desea ver la lista de sesiones.

3. Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

4. Vaya a la sección **Firewall** y seleccione la pestaña **Sesiones**.

   Se muestra la tabla de sesiones. De manera predeterminada, la tabla de sesiones está vacía porque las sesiones no se descargaron del dispositivo CPE.

5. Solicite sesiones desde el dispositivo; para ello, haga clic en el botón **Solicitar del CPE**.

   Espere hasta que se recupere la lista de sesiones del dispositivo CPE.

   La información acerca de las sesiones se muestra en las siguientes columnas de la tabla:

   - **Protocolo**
   - **Tiempo de espera (s)**
   - **Estado**
   - **IP de origen**
   - **Puerto de origen**
   - **IP de destino**
   - **Puerto de destino**
   - **IP de origen equivalente**
   - **Puerto de origen equivalente**
   - **IP de destino equivalente**
   - **Puerto de destino equivalente**
   - **Paquetes salientes**
   - **Paquetes entrantes**
   - **Tráfico saliente (bytes)**
   - **Tráfico entrante (bytes)**
   - **Marca de sesión**
   - **Marca**

   Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

6. Si desea filtrar las sesiones que se muestran en la tabla:

   a. Haga clic en el ícono de filtro ▽ cerca del borde derecho del panel de acción sobre la tabla.

      Se abre la ventana de creación de filtros.

   b. Agregue filtros para los campos que necesita: para cada filtro, haga clic en el botón **Agregar**, seleccione un campo y especifique un valor por el que desea filtrar.

   c. Para aplicar el filtro, haga clic en el botón **Aplicar**.

   Se filtran las sesiones de la tabla.

7. Si desea restablecer la lista de sesiones en el dispositivo, haga clic en el botón **Borrar sesiones en CPE**.

Se muestra una advertencia:

> El borrado de sesiones puede causar una pérdida temporal de la conexión del controlador, lo que restablece los vínculos de este CPE y, como consecuencia, genera una pérdida temporal de tráfico.

Confirme el restablecimiento de las sesiones; para ello, haga clic en **Borrar sesiones en la tabla**.

# Eliminar y deshabilitar automáticamente los dispositivos CPE

En la plantilla de CPE o en el dispositivo CPE, puede especificar el tiempo después del que el dispositivo CPE se elimina o se deshabilita si se termina la sesión de administración con el controlador. Ambas funciones se utilizan para evitar el robo de los dispositivos CPE. La función de eliminación automática también se utiliza para hacer una limpieza de las entradas obsoletas de la interfaz web del orquestador. Ambas funciones están deshabilitadas de manera predeterminada.

El tiempo de eliminación o deshabilitación automática que está especificado en una plantilla de CPE se aplica automáticamente a todos los dispositivos CPE que usen esta plantilla de CPE.

*Para configurar la eliminación y deshabilitación automática de los dispositivos CPE, haga lo siguiente:*

1. Proceda a configurar la eliminación y la deshabilitación automática de una de las siguientes maneras:

   - Si desea configurar la eliminación y deshabilitación automática en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Desactivación**.

   - Si desea configurar la eliminación y deshabilitación automática en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Desactivación** y seleccione las casillas de verificación **Anular**.

   Se mostrará la configuración de la eliminación y deshabilitación automática del dispositivo CPE.

2. Habilite la eliminación automática del dispositivo CPE:

   a. Seleccione la casilla de verificación **Habilitar** junto al campo **Eliminar tiempo de espera (s)**.

   b. En el campo **Eliminar tiempo de espera (s)**, ingrese el tiempo en segundos después del cual el dispositivo CPE se elimina si no es posible la comunicación con el controlador. Rango de valores: 60 a 31 536 000. El valor ingresado no puede ser menor al valor especificado para la deshabilitación automática.

3. Habilite la deshabilitación automática del dispositivo CPE:

   a. Seleccione la casilla de verificación **Habilitar** junto al campo **Deshabilitar tiempo de espera (s)**.

   b. En el campo **Deshabilitar tiempo de espera (s)**, ingrese el tiempo en segundos después del cual el dispositivo CPE se deshabilita si no es posible la comunicación con el controlador. Rango de valores: 60 a 31 536 000. El valor ingresado no puede ser mayor al valor especificado para la eliminación automática.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Agrupar dispositivos CPE mediante etiquetas

Las *etiquetas* describen la configuración del dispositivo CPE, como el modelo, la versión de firmware y la dirección de ubicación. Cuando agrega un dispositivo CPE, se le asignan etiquetas automáticamente, que describen su modelo y el inquilino al que se agregó el dispositivo CPE.

Puede usar etiquetas para agrupar dispositivos CPE y realizar acciones en grupos. Por ejemplo, puede asignar la misma etiqueta a los dispositivos CPE que se encuentran en la misma ubicación y luego actualizar el firmware en todos ellos.

Para que se le asigne una etiqueta, el dispositivo CPE debe tener el estado **Registrado**. No se pueden asignar dos etiquetas idénticas al mismo dispositivo CPE.

## Asignar una etiqueta a dispositivos CPE

*Para asignar una etiqueta a dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Para asignar una etiqueta a un dispositivo CPE individual:

   a. Haga clic en el dispositivo CPE al que desea asignar una etiqueta.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

   b. Seleccione la pestaña **Etiquetas**.

   Se muestran las etiquetas asignadas.

   c. Ingrese la etiqueta y haga clic en el ícono de asignar +.

   d. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

3. Para asignar una etiqueta a varios dispositivos CPE:

   a. Seleccione las casillas de verificación junto a los dispositivos CPE a los que desea asignar una etiqueta.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Asignar etiquetas**.

   c. En la ventana que se abre, ingrese la etiqueta y haga clic en el ícono de asignación +.

   d. Haga clic en **Agregar**.

La etiqueta se asigna a los dispositivos CPE.

# Eliminar una etiqueta de dispositivos CPE

*Para eliminar una etiqueta de dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Para eliminar una etiqueta de un dispositivo CPE individual:

   a. Haga clic en el dispositivo CPE del que desea eliminar una etiqueta.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

   b. Seleccione la pestaña **Etiquetas**.

   Se muestran las etiquetas asignadas.

   c. Haga clic en el ícono de eliminar ✕ junto a la etiqueta que desea eliminar.

   d. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

3. Para eliminar una etiqueta de varios dispositivos CPE:

   a. Seleccione las casillas de verificación junto a los dispositivos CPE de los que desea eliminar una etiqueta.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar etiquetas**.

   c. En la ventana que se abre, elimine las etiquetas de una de las siguientes maneras:

   - Haga clic en el ícono de eliminar ✕ junto a la etiqueta que desea eliminar.
   - Ingrese la etiqueta que desea eliminar y selecciónela de la lista desplegable.

   d. Haga clic en **Eliminar**.

Se elimina la etiqueta del dispositivo CPE.

# Configurar registros en dispositivos CPE

Los registros generados en los dispositivos CPE se almacenan localmente o se envían a un servidor syslog externo. Cuando almacena registros localmente, puede especificar un tamaño máximo. Puede especificar un prefijo que se asignará a los registros antes de que se envíen al servidor syslog externo.

Para ver el registro local en el dispositivo CPE, debe solicitar información de diagnóstico.

Puede especificar la configuración del registro en una plantilla de CPE o en el dispositivo CPE. La configuración de registro especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para configurar los registros en los dispositivos CPE, siga estos pasos:*

1. Si desea que el dispositivo CPE envíe registros a un servidor syslog externo en forma cifrada, primero cargue el certificado CA del servidor syslog al dispositivo CPE:

   1. Abra la pestaña **SD-WAN** → **Certificados**, haga clic en **+ Agregar** y, en el formulario que se muestra, haga clic en **Cargar** y seleccione el archivo del certificado.

      El certificado cargado aparece en la tabla de certificados.

   2. En la tabla de certificados, seleccione la casilla **Distribuir a CPE** para el certificado agregado.

   3. Haga clic en **Aplicar a CPE**.

2. Configure los registros de una de las siguientes maneras:

   - Si desea configurar los registros en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y, en el área de configuración que se muestra, seleccione la sección **Registro** y, en el área de configuración, seleccione la pestaña **General**.

   - Si desea configurar los registros en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE, seleccione la sección **Registro** y, en el área de configuración, seleccione la pestaña **General** y habilite el botón de alternancia **Anular**.

   Se muestra la configuración del registro.

3. En el campo **IP/FQDN**, ingrese la dirección IP o el nombre de dominio completo del servidor syslog.

   Si desea utilizar una conexión cifrada para enviar mensajes de syslog y se emitió el certificado CA correspondiente para un nombre de dominio, en el campo **IP/FQDN**, debe especificar el nombre de dominio completo (FQDN). Este nombre de dominio debe resolverse a través del servidor DNS especificado al configurar el DNS en el dispositivo CPE.

4. En el campo **Puerto**, ingrese el número de puerto del servidor syslog. Rango de valores: de 0 a 65 353.

5. En la lista desplegable **Protocolo**, seleccione el protocolo para enviar registros al servidor syslog:

   - **UDP**. Esta es la configuración predeterminada.

   - **TCP**.

- **TLS**. Seleccione esta opción si desea que el dispositivo CPE envíe registros al servidor syslog externo en forma cifrada.

  El servidor syslog determina los parámetros del algoritmo de cifrado para la comunicación entre el cliente y el servidor syslog. Las siguientes versiones de cifrado y TLS son compatibles con los dispositivos CPE:

  - `TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD`
  - `TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any Enc=CHACHA20/POLY1305(256) Mac=AEAD`
  - `TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD`
  - `ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256) Mac=AEAD`
  - `ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD`
  - `ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD`
  - `ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(256) Mac=AEAD`
  - `DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD`

6. En el campo **Tamaño del archivo (KB)**, ingrese el tamaño máximo de los registros del dispositivo CPE en kilobytes. Rango de valores: de 64 a 2048. El valor predeterminado es `64`. Si se excede el tamaño máximo de registro, los registros nuevos sobrescriben los registros más antiguos.

7. Si desea que el dispositivo CPE agregue un prefijo a los registros, especifique este prefijo en el campo **Prefijo del nombre del archivo**. La longitud máxima del prefijo es de 256 caracteres.

8. Si es necesario, configure el filtrado de mensajes enviados al servidor syslog mediante el campo **Filtrar mensajes**. Cuando se utiliza un filtro de mensajes, solo los registros que contienen las cadenas especificadas en el filtro se envían al servidor syslog. Puede especificar hasta diez cadenas individuales. Las cadenas se combinan con el operador lógico OR. Caracteres permitidos para las cadenas de filtro:

   - Letras latinas mayúsculas (A–Z)
   - Letras latinas minúsculas (a–z)
   - Números (0-9)
   - Caracteres especiales : - . _
   - El carácter de espacio

9. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar módems

Esta funcionalidad no es compatible con algunos modelos. Para obtener consejos, comuníquese con el Servicio de soporte técnico de Kaspersky.

Un dispositivo CPE puede tener hasta cuatro módems para establecer una conexión a la red celular. Para ver la tabla de los módems, vaya a la sección **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Módems**. La información sobre los módems se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del módem.
- **Dirección IP** es la dirección IP del módem.
- **Subred** es la subred a la que está conectada el módem.
- **Gateway** es la puerta de enlace a la que está conectada el módem.
- **DNS 1** y **DNS 2** son servidores DNS que utiliza el módem.
- **Señal** es la intensidad de la señal del módem.
- **Formato de los datos** es el protocolo de transferencia de datos del módem.
- **Registro** es el estado de registro del módem.
- **Red** es la red a la que está conectado el módem.
- **País** es el país en el que está registrado el módem.
- **MCC de PLMN** es el código de país del operador móvil.
- **MNC de PLMN** es el código de la red móvil.
- **Roaming** indica si se está utilizando roaming en el módem:
  - **Sí**.
  - **No**.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Actualizar el firmware

Kaspersky distribuye las nuevas versiones del software del dispositivo CPE en forma de firmware. Se admite el firmware basado en los siguientes conmutadores de software:

- Open vSwitch (OVS) es una implementación de conmutador de software con procesamiento de paquetes a nivel de kernel. Este tipo de conmutador es adecuado para la mayoría de los dispositivos y está seleccionado de manera predeterminada.

- Switch Operating System (SWOS) es una implementación de conmutador de software alternativa con procesamiento de paquetes basado en DPDK. Puede ofrecer un mayor rendimiento gracias al procesamiento de paquetes que omite el kernel.

Puede descargar un archivo comprimido TAR.GZ con el firmware del directorio /cpe del kit de distribución.

Puede actualizar el firmware en un dispositivo CPE de tres maneras:

- Actualización manual del firmware del dispositivo CPE sin usar la interfaz web del orquestador.

- Programación de actualizaciones de firmware en dispositivos CPE seleccionados. En este caso, debe cargar el firmware en la interfaz web del orquestador, seleccionar los dispositivos CPE en los que desea actualizar el firmware y luego actualizar el firmware. Se crea automáticamente una tarea de actualización de firmware en el programador de tareas.

- Programación de actualizaciones de firmware en dispositivos CPE con etiquetas específicas. En este caso, debe cargar el firmware en la interfaz web del orquestador, asignar etiquetas a los dispositivos CPE en los que desea actualizar el firmware y luego crear una tarea de actualización de firmware en el programador de tareas. Cuando crea la tarea, debe especificar las etiquetas que asignó a los dispositivos CPE.

El dispositivo CPE se reinicia durante el proceso de actualización del firmware.

Puede ver la tabla de firmware cargada en la interfaz web en la sección **SD-WAN** → **Firmware**. La información sobre el firmware se muestra en las siguientes columnas de la tabla:

- **Versión** es la versión del firmware.

- **Tamaño (MB)** es el tamaño del archivo de firmware en megabytes.

- **SHA256** es el hash del firmware.

- **Arquitectura** es la arquitectura del conjunto de instrucciones (ISA) del firmware.

- **Fecha de lanzamiento** es la fecha de lanzamiento del firmware.

- **Modelo** es el modelo de dispositivos CPE con los que el firmware es compatible.

- **Tipo de conmutador** es el tipo de conmutador de software en el que se basa el firmware (OVS o SWOS).

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Actualizar manualmente el firmware en un dispositivo CPE

Cuando siga estos pasos, se le solicitará que ingrese las credenciales del dispositivo CPE. Después del registro, se cambiará automáticamente la contraseña predeterminada del dispositivo CPE. Puede ver la contraseña del dispositivo CPE en la interfaz web del orquestador.

*Para actualizar manualmente el firmware en un dispositivo CPE, haga lo siguiente:*

1. Descargue el archivo comprimido de firmware del directorio /cpe del kit de distribución al dispositivo administrador, por ejemplo, su computadora portátil. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

2. Conecte el dispositivo administrador al puerto LAN del dispositivo CPE.

   El dispositivo administrador obtiene la dirección IP de la puerta de enlace predeterminada a través de DHCP. La dirección IP recibida de la puerta de enlace predeterminada es la dirección IP del dispositivo CPE.

3. Conéctese al dispositivo CPE a través de SCP, por ejemplo, con WinSCP. Para conectarse a través de SCP, especifique la dirección IP e ingrese las credenciales del dispositivo CPE.

4. Coloque el archivo comprimido del firmware en el directorio /tmp.

5. Conéctese al dispositivo CPE a través de SSH. Para conectarse a través de SSH, especifique la dirección IP e ingrese las credenciales del dispositivo CPE.

6. Cambie al directorio /tmp:

   ```
   cd /tmp/
   ```

7. Actualice el firmware del dispositivo CPE de una de las siguientes maneras:

   - Si desea dejar la configuración del dispositivo CPE sin cambios después de la actualización del firmware, ejecute el siguiente comando:

     ```
     sysupgrade knaas-<nombre del archivo comprimido del firmware>
     ```

   - Si desea restablecer el dispositivo CPE a la configuración de fábrica después de la actualización del firmware, ejecute el siguiente comando:

     ```
     sysupgrade -n knaas-cpe<nombre del archivo comprimido del firmware>
     ```

   Cuando un dispositivo CPE se restablece a la configuración de fábrica, se desconecta del orquestador. Para volver a conectar el dispositivo CPE al orquestador, debe registrar automáticamente (ZTP) el dispositivo CPE.

La nueva versión de firmware se instala en el dispositivo CPE, que luego se reinicia. De manera predeterminada, la dirección del dispositivo CPE permanece sin cambios, y se habilita DHCP en los puertos LAN.

# Cargar el firmware a la interfaz web del orquestador

*Para cargar el firmware en la interfaz web de orquestador, haga lo siguiente:*

1. Descargue el archivo comprimido del firmware del directorio /cpe del kit de distribución a su dispositivo local. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

2. En el menú, vaya a la sección **SD-WAN** → **Firmware**.

   Se muestra una tabla de firmware.

3. En la parte superior de la página, haga clic en **+ Firmware**.

4. Ingrese la ruta al archivo comprimido con el firmware. Cuando se especifica una ruta, puede seleccionar varios archivos al mismo tiempo.

El firmware se cargará y se mostrará en la tabla.

# Programar actualizaciones de firmware en dispositivos CPE seleccionados

*Para crear una tarea de actualización de firmware programada en dispositivos CPE seleccionados:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Proceda con la actualización de firmware programada de una de las siguientes maneras:

   - Si desea realizar una actualización de firmware programada en un dispositivo CPE individual, haga clic en el dispositivo CPE para abrir la ventana de propiedades del dispositivo y, en esa ventana, abra el menú de acciones haciendo clic en el ícono ⋮ en la esquina superior derecha, luego seleccione **Actualizar firmware**.

   - Si desea realizar una actualización de firmware programada en varios dispositivos CPE, seleccione las casillas de verificación junto a los dispositivos CPE relevantes y, en la parte superior de la tabla, haga clic en **Acciones** → **Actualizar firmware**.

   El firmware obsoleto se resalta en naranja en la columna **Versión de software** de la tabla de dispositivos CPE. También puede encontrar dispositivos CPE con versiones de firmware desactualizadas utilizando el filtro **Se necesita actualización** en la parte superior de la tabla.

3. En la ventana que se abre, en el campo **Nombre de la tarea**, ingrese el nombre de la tarea programada.

4. Utilice el botón de alternancia **Tipo de conmutador** para seleccionar el tipo de conmutador de software para el nuevo firmware (OVS o SWOS).

Si está actualizando el firmware en varios dispositivos CPE al mismo tiempo, debe seleccionar el tipo de conmutador de software para que coincida con el firmware de todos los dispositivos seleccionados. Si el tipo de firmware en al menos un dispositivo no coincide con el tipo de conmutador de software seleccionado, se muestra el mensaje **El CPE se puede actualizar solo con firmware del mismo tipo de conmutador** en la ventana de creación de la tarea de actualización de firmware, y no se puede crear la tarea. Si está actualizando el firmware en un dispositivo individual, se muestra la advertencia **El tipo de conmutador que seleccionó no coincide con el tipo de conmutador del CPE. Es posible que no pueda accederse al dispositivo después de la actualización del firmware debido a posibles inconsistencias en la configuración** cuando se selecciona un tipo de conmutador no coincidente, pero es posible crear la tarea.

No recomendamos actualizar el firmware a una versión basada en un tipo de conmutador de software diferente.

5. En la lista desplegable **Versión**, seleccione la versión de su firmware cargado. La lista muestra las versiones de firmware que coinciden con el tipo de interruptor de software seleccionado en la configuración **Tipo de conmutador**. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

   Si la lista no contiene versiones de firmware coincidentes (no se encontraron versiones que coincidan con el tipo de conmutador de software seleccionado o no se cargaron versiones en el orquestador), entonces se muestra el mensaje **No hay un firmware disponible para los CPE seleccionados. Puede cargar un nuevo firmware** en la parte superior de la ventana con un vínculo a la sección **SD-WAN→ Firmware**.

6. En el campo **Fecha de ejecución de la tarea programada**, ingrese la fecha y la hora en que desea ejecutar la tarea. De manera predeterminada, la fecha y la hora especificadas son la fecha y la hora en que comenzó a crear la tarea.

7. Si desea restablecer la configuración de fábrica del dispositivo CPE después de actualizar el firmware, desmarque la casilla **Guardar configuración del CPE**. Si se selecciona la casilla, la configuración del dispositivo CPE existente no se modifica después de una actualización de firmware. Esta casilla está seleccionada por defecto.

   Cuando un dispositivo CPE se restablece a la configuración de fábrica, se desconecta del orquestador. Para volver a conectar el dispositivo CPE al orquestador, debe registrar automáticamente (ZTP) el dispositivo CPE.

8. La casilla **Forzar actualización** le permite forzar la actualización del firmware, incluso si la verificación interna del CPE muestra que el nuevo firmware es incompatible con el anterior. Esta casilla está desactivada por defecto.

9. Haga clic en **Siguiente**.

   Se muestran dos tablas de dispositivos CPE. Se actualiza el firmware de los dispositivos CPE en la tabla superior. El firmware de los dispositivos CPE en la tabla inferior no se actualiza. La información sobre los dispositivos CPE se muestra en las siguientes columnas de la tabla:

   - **DPID** es el DPID del dispositivo CPE.
   - **Modelo** es el modelo del dispositivo CPE.
   - **Tipo de conmutador** es el tipo de interruptor de software del firmware del dispositivo CPE (OVS o SWOS).
   - **Nombre** es el nombre del dispositivo CPE.
   - **Versión de software** es la versión de firmware del dispositivo CPE.

- **Inquilino** es el inquilino al que se agregó el dispositivo CPE.
- **Motivo** es el motivo por el cual no se puede actualizar el firmware. Esta columna se muestra solo en la tabla inferior.

Si la tabla superior contiene dispositivos CPE en los que no desea actualizar el firmware, puede mover estos dispositivos CPE a la tabla inferior.

10. Haga clic en **Programar**.

La tarea de actualización de firmware se crea y se muestra en la tabla de tareas. El estado de las tareas se muestra en la columna **Estado**. Si la tarea de actualización del firmware finaliza correctamente, su estado cambia a**Realizado**.

# Programar actualizaciones de firmware en dispositivos CPE con etiquetas específicas

*Para crear una tarea de actualización de firmware programada en dispositivos CPE con etiquetas específicas, siga estos pasos:*

1. En el menú, vaya a la sección **Programador**.

   Se muestra la tabla de tareas.

2. En la parte superior de la página, haga clic en **+ Tarea**.

3. En la ventana que se abre, en la lista desplegable **Tipo**, seleccione**Actualización de firmware**.

4. En el campo **Nombre de la tarea**, escriba el nombre de la tarea.

5. Utilice el botón de alternancia **Tipo de conmutador** para seleccionar el tipo de conmutador de software para el nuevo firmware (OVS o SWOS).

6. En la lista desplegable **Versión**, seleccione la versión de su firmware cargado. La lista muestra las versiones de firmware que coinciden con el tipo de interruptor de software seleccionado en la configuración **Tipo de conmutador**. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

   Si la lista no contiene versiones de firmware coincidentes (no se encontraron versiones que coincidan con el tipo de conmutador de software seleccionado o no se cargaron versiones en el orquestador), entonces se muestra el mensaje **No hay un firmware disponible para los CPE seleccionados. Puede cargar un nuevo firmware** en la parte superior de la ventana con un vínculo a la sección **SD-WAN→ Firmware**.

7. En el campo **Fecha de ejecución de la tarea programada**, ingrese la fecha y la hora en que desea ejecutar la tarea. De manera predeterminada, la fecha y la hora especificadas son la fecha y la hora en que comenzó a crear la tarea.

8. Si desea restablecer la configuración de fábrica del dispositivo CPE después de actualizar el firmware, desmarque la casilla **Guardar configuración del CPE**. Si se selecciona la casilla, la configuración del dispositivo CPE existente no se modifica después de una actualización de firmware. Esta casilla está seleccionada por defecto.

   Cuando un dispositivo CPE se restablece a la configuración de fábrica, se desconecta del orquestador. Para volver a conectar el dispositivo CPE al orquestador, debe registrar automáticamente (ZTP) el dispositivo CPE.

9. La casilla **Forzar actualización** le permite forzar la actualización del firmware, incluso si la verificación interna del CPE muestra que el nuevo firmware es incompatible con el anterior. Esta casilla está desactivada por defecto.

10. En el campo **Etiquetas**, ingrese las etiquetas asignadas a los dispositivos CPE en los que desea actualizar el firmware. El firmware obsoleto se resalta en naranja en la columna **Versión de software** de la tabla de dispositivos CPE. También puede encontrar dispositivos CPE con versiones de firmware desactualizadas utilizando el filtro **Se necesita actualización** en la parte superior de la tabla.

11. Haga clic en **Siguiente**.

    Se muestran dos tablas de dispositivos CPE. Se actualiza el firmware de los dispositivos CPE en la tabla superior. El firmware de los dispositivos CPE en la tabla inferior no se actualiza. La información sobre los dispositivos CPE se muestra en las siguientes columnas de la tabla:

    - **DPID** es el DPID del dispositivo CPE.
    - **Modelo** es el modelo del dispositivo CPE.
    - **Tipo de conmutador** es el tipo de interruptor de software del firmware del dispositivo CPE (OVS o SWOS).
    - **Nombre** es el nombre del dispositivo CPE.
    - **Versión de software** es la versión de firmware del dispositivo CPE.
    - **Inquilino** es el inquilino al que se agregó el dispositivo CPE.
    - **Motivo** es el motivo por el cual no se puede actualizar el firmware. Esta columna se muestra solo en la tabla inferior.

    Si la tabla superior contiene dispositivos CPE en los que no desea actualizar el firmware, puede mover estos dispositivos CPE a la tabla inferior.

12. Haga clic en **Crear**.

La tarea de actualización de firmware se crea y se muestra en la tabla. El estado de las tareas se muestra en la columna **Estado**. Si la tarea de actualización del firmware finaliza correctamente, su estado cambia a**Realizado**.

# Restaurar el firmware de un dispositivo CPE KESR-M1

Puede restaurar el firmware y restablecer la configuración de fábrica de un dispositivo CPE KESR-M1 si perdió las credenciales de ese CPE o si tiene un problema con el firmware.

Cuando un dispositivo CPE se restablece a la configuración de fábrica, se desconecta del orquestador. Para volver a conectar el dispositivo CPE al orquestador, debe registrar automáticamente (ZTP) el dispositivo CPE.

*Para restaurar el firmware de un dispositivo CPE KESR-M1, siga estos pasos:*

1. Descargue el archivo de firmware del directorio /cpe del kit de distribución al dispositivo administrador, por ejemplo, su computadora portátil. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

2. Extraiga el archivo de firmware para obtener el firmware en formato BIN.

3. Encienda el dispositivo CPE con el firmware de fábrica.

   a. Desconecte el cable de alimentación del dispositivo CPE.

   b. Conecte el cable de alimentación y mantenga presionado el botón **RESET** en el dispositivo CPE durante 10 segundos.

   El dispositivo CPE se enciende con el firmware de fábrica.

4. Conecte el dispositivo administrador al puerto LAN del dispositivo CPE.

   El dispositivo administrador obtiene una dirección IP y la dirección IP de la puerta de enlace predeterminada en la subred 192.168.1.0/24 a través de DHCP.

5. En la barra de direcciones del navegador en el dispositivo administrador, ingrese `192.168.1.1` y presione **Intro**.

   Se abre la página de carga de firmware del dispositivo CPE.

6. Haga clic en el botón de carga de firmware y especifique la ruta al firmware en formato BIN. Obtuvo el firmware en formato BIN en el paso 2 de estas instrucciones.

La nueva versión de firmware se instala en el dispositivo CPE, que luego se reinicia. De manera predeterminada, la dirección IP del dispositivo CPE es 192.168.7.1 y DHCP está habilitado en los puertos LAN.

# Restaurar el firmware de un dispositivo CPE KESR-M2-5

Puede restaurar el firmware y restablecer la configuración de fábrica de un dispositivo CPE KESR-M2-5 si perdió las credenciales de ese CPE o si tiene un problema con el firmware.

Cuando un dispositivo CPE se restablece a la configuración de fábrica, se desconecta del orquestador. Para volver a conectar el dispositivo CPE al orquestador, debe registrar automáticamente (ZTP) el dispositivo CPE.

*Para restaurar el firmware de un dispositivo CPE KESR-M2-5, siga estos pasos:*

1. Descargue el archivo comprimido de firmware del directorio /cpe del kit de distribución al dispositivo administrador, por ejemplo, su computadora portátil. Si no sabe qué versión de firmware necesita instalar en el dispositivo CPE, utilice la tabla de correspondencia de los modelos de dispositivos CPE con las versiones de firmware.

2. Extraiga el archivo comprimido del firmware para obtener un archivo en formato IMG.GZ.

3. Descomprima el archivo comprimido IMG.GZ para obtener la imagen del firmware en formato IMG.

4. Utilice el firmware IMG para crear una unidad USB de arranque mediante un software de escritura de imágenes de disco como BalenaEtcher.

5. Conecte el dispositivo administrador al dispositivo CPE con un cable de consola e inserte la unidad USB en el puerto USB del dispositivo CPE.

6. Especifique la configuración para establecer una sesión de consola con el dispositivo CPE en el dispositivo administrador, por ejemplo, utilizando la aplicación PuTTY, y haga lo siguiente:

   - Especifique el número de puerto de comunicaciones (puerto COM) del dispositivo administrador.
   - Especifique `115200` como la velocidad de la sesión.

7. Desconecte y vuelva a conectar el cable de alimentación del dispositivo CPE. Presione **F7** o **F11** mientras se enciende el dispositivo CPE.

8. En el menú que se abre, seleccione la unidad USB y presione **Intro**.

   El dispositivo CPE se inicia desde la unidad USB.

9. Conecte el dispositivo administrador al puerto LAN del dispositivo CPE.

   El dispositivo administrador obtiene una dirección IP y la dirección IP de la puerta de enlace predeterminada en la subred 192.168.7.0/24 a través de DHCP.

10. Conéctese al dispositivo CPE a través de SCP, por ejemplo, con WinSCP. Para conectarse a través de SCP, especifique la dirección IP e ingrese las credenciales predeterminadas del dispositivo CPE.

11. Coloque el firmware en formato IMG en el directorio /tmp.

12. Conéctese al dispositivo CPE a través de SSH o establezca una sesión de la consola con el dispositivo CPE. Para conectarse a través de SSH o iniciar una sesión de la consola, especifique la dirección IP e ingrese las credenciales predeterminadas del dispositivo CPE.

13. Cambie al directorio /tmp:

    ```
    cd /tmp/
    ```

14. Copie la imagen del firmware en formato IMG a /dev/sda:

    ```
    dd if=< nombre del archivo IMG del firmware > bs=1M of=/dev/sda
    ```

15. Reinicie el dispositivo CPE mediante el siguiente comando:

    ```
    reboot
    ```

La nueva versión de firmware se instala en el dispositivo CPE, que luego se reinicia. De manera predeterminada, la dirección IP del dispositivo CPE es 192.168.7.1 y DHCP está habilitado en los puertos LAN.

# Correspondencia de modelos de dispositivos CPE con versiones de firmware

La siguiente tabla muestra la correspondencia de los modelos de dispositivos CPE con las versiones de firmware compatibles.

| Modelo del dispositivo CPE | Archivo de firmware |
|---|---|
| KESR M1 (V1 TTK) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.firmware.kesr-m1-r-5g-1l-w-v1-ttk_en-US_ru-RU.tar.gz |
| KESR M1 (V2) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.firmware.kesr-m1-r-5g-2l-w-v2_en-US_ru-RU.tar.gz |
| KESR M1 (V3) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m1-k-4g-2l-w-v3_en-US_ru-RU.tar.gz |
| KESR M2 (Wi-Fi/LTE) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m2-k-5g-1l-w_en-US_ru-RU.tar.gz |
| KESR M2 (SFP) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m2-k-5g-1s_en-US_ru-RU.tar.gz |
| KESR M3 | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m3-k-4g-4s_en-US_ru-RU.tar.gz |
| KESR M4 (SFPx2) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m4-k-4g-2x_en-US_ru-RU.tar.gz |
| KESR M4 (SFPx4/RJ-45x8) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m4-k-8g-4x_en-US_ru-RU.tar.gz |
| KESR M5 (SFPx8) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m5-k-4g-8x_en-US_ru-RU.tar.gz |
| KESR M5 (SFPx4/RJ-45x8) | knaas-cpe_<versión de firmware>.release.<número de versión de la solución>.efi.amd64-kesr-m5-k-8g-4x_en-US_ru-RU.tar.gz |

# Eliminar firmware

No puede eliminar el firmware que se está utilizando en al menos una tarea. Para eliminar el firmware que se está utilizando en las tareas, primero debe eliminar las tareas.

El firmware eliminado no se puede restaurar.

*Para eliminar el firmware, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **Firmware**.

   Se muestra una tabla de firmware.

2. Seleccione las casillas de verificación junto al firmware que desea eliminar.

3. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

   El firmware se eliminará y ya no se mostrará en la tabla.

# Configuración adicional de dispositivos CPE mediante scripts

Puede utilizar scripts para la configuración adicional de dispositivos CPE. Puede agregar scripts a una plantilla de CPE. Los scripts agregados a la plantilla de CPE se agregan automáticamente a todos los dispositivos CPE que usan esta plantilla de CPE. Los scripts agregados se pueden ejecutar de manera automática o manual. Los scripts se ejecutan automáticamente cuando se cumplen las condiciones especificadas en la configuración del script, por ejemplo, cuando se registra un dispositivo CPE.

La ejecución de scripts es responsabilidad del VNFM, por lo que debe asegurarse la conexión de red entre los dispositivos VNFM y CPE antes de comenzar a trabajar con scripts. De manera predeterminada, el número de puerto para la conexión del VNFM al dispositivo y el nombre de usuario para ejecutar scripts se especifican en la plantilla de CPE. Puede cambiar el número de puerto y el nombre de usuario si es necesario.

Puede ver la tabla de scripts en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de scripts en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Scripts**.
- Para ver la tabla de scripts en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Scripts**.

La información sobre los scripts se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del script.
- **Ejecutor** es el intérprete.
- **Autenticación** es el tipo de autenticación VNFM en el dispositivo CPE.
- **Ejecutor personalizado** es la ruta al intérprete personalizado.
- **Tiempo de espera (s)** es el tiempo en segundos después del cual el VNFM deja de intentar ejecutar un script que no pudo ejecutarse la primera vez.
- **Repetir ejecución** indica si el script se puede volver a ejecutar:
  - **Sí**.
  - **No**.
- **Etapa** es la etapa de la operación del dispositivo CPE en la que el VNFM ejecuta el script.
- **Script** es el nombre del archivo de script o del archivo del playbook de Ansible.
- **Archivo** es el nombre del archivo con archivos adicionales que el script requiere para ejecutarse.
- **Acciones** contiene las acciones que se pueden realizar con el script.

# Agregar un script a dispositivos CPE

Puede agregar un script a una plantilla de CPE. Los scripts agregados a la plantilla de CPE se agregan automáticamente a todos los dispositivos CPE que usan esta plantilla de CPE.

*Para agregar un script a los dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE a la que desea agregar un script.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Scripts**.

   Esto muestra el número de puerto que VNFM usa para conectarse al dispositivo CPE, el nombre de usuario para ejecutar scripts y la tabla de scripts si se agregó al menos un script.

4. Haga clic en **+ Script**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del script. La longitud máxima del nombre es de 255 caracteres.

6. En el campo **Tiempo de espera (s)**, ingrese el tiempo en segundos después del cual VNFM deja de intentar ejecutar un script que no pudo ejecutarse la primera vez. El valor predeterminado es `360`.

7. En la lista desplegable **Ejecutor**, seleccione uno de los valores siguientes:

   - **Ansible**. Esta es la configuración predeterminada.
   - **Shell**
   - **Prever**
   - **Personalizado** para usar un intérprete en el dispositivo CPE. Si selecciona este valor, ingrese la ruta al intérprete personalizado en el campo **Ejecutor personalizado**.

8. En la lista desplegable **Etapa**, seleccione la etapa de operación del dispositivo CPE en la que VNFM ejecuta el script:

   - **Registro**. Esta es la configuración predeterminada.
   - **Eliminación**
   - **Manual** para ejecutar el script solo manualmente.

9. Si necesita volver a ejecutar el script, seleccione la casilla **Repetir ejecución**. Esta casilla está desactivada por defecto. Tenga en cuenta las siguientes consideraciones especiales para volver a ejecutar un script:

   - Si en la lista desplegable **Etapa**, seleccionó **Registro**, el script se vuelve a ejecutar en casos de registro, encendido y reinicio del dispositivo CPE.
   - Si en la lista desplegable **Etapa**, seleccionó **Eliminación**, el script no se ejecuta nuevamente.
   - Si en la lista desplegable **Etapa**, seleccionó **Manual**, el script se vuelve a ejecutar en los casos de encendido y reinicio del dispositivo CPE.

10. En el campo **Script**, ingrese la ruta al archivo de script o al archivo de script del manual de Ansible.

11. Si es necesario, en el campo **Archivo**, especifique la ruta al archivo comprimido que contiene los archivos adicionales necesarios para ejecutar el script. Formatos admitidos de archivos comprimidos que contienen archivos: TAR.GZ y ZIP.

12. Haga clic en **Guardar**.

    El script se crea y se muestra en la tabla.

13. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Ejecutar un script en dispositivos CPE manualmente

Puede ejecutar manualmente un script individual o todos los scripts en una plantilla de CPE o en un dispositivo CPE. Los scripts iniciados en una plantilla de CPE se ejecutan automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE o en dispositivos CPE con etiquetas específicas.

## Ejecutar scripts manualmente en una plantilla de CPE

*Para ejecutar scripts manualmente en una plantilla de CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea ejecutar los scripts manualmente.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Scripts**.

   Esto muestra el número de puerto que VNFM usa para conectarse al dispositivo CPE, el nombre de usuario para ejecutar scripts y la tabla de scripts si se agregó al menos un script.

4. Para ejecutar manualmente un script individual, siga estos pasos:

   a. Haga clic en **Ejecutar** junto al script que desea ejecutar manualmente.

   b. En la ventana que se abre, seleccione los dispositivos CPE en los que desea ejecutar el script:

   - **Ejecutar el script <nombre del script> en todos los CPE relacionados** ejecuta el script en todos los dispositivos CPE que utilizan la plantilla de CPE. Esta es la configuración predeterminada.

   - **Ejecutar <nombre del script> en todos los CPE relacionados con etiquetas especificadas** ejecuta el script en los dispositivos CPE que usan la plantilla de CPE y tienen etiquetas específicas asignadas. Si selecciona este valor, especifique las etiquetas en la parte inferior de la ventana.

5. Para ejecutar manualmente todos los scripts, siga estos pasos:

   a. En la parte superior del área de configuración, en **Acciones**, haga clic en **Ejecutar scripts**.

   b. En la ventana que se abre, seleccione los dispositivos CPE en los que desea ejecutar los scripts:

   - **Ejecutar todos los scripts en CPE relacionados** para ejecutar los scripts en todos los dispositivos CPE que utilizan la plantilla CPE. Esta es la configuración predeterminada.

   - **Ejecutar todos los scripts en CPE relacionados con etiquetas específicas** para ejecutar los scripts en los dispositivos CPE que usan la plantilla de CPE y tienen etiquetas específicas asignadas. Si selecciona este valor, especifique las etiquetas en la parte inferior de la ventana.

6. Haga clic en **Ejecutar**.

Se ejecutan los scripts.

## Ejecutar scripts manualmente en un dispositivo CPE

*Para ejecutar scripts manualmente en un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar los scripts manualmente.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Scripts**.

   Esto muestra el número de puerto que VNFM usa para conectarse al dispositivo CPE, el nombre de usuario para ejecutar scripts y la tabla de scripts si se agregó al menos un script.

4. Ejecute manualmente los scripts de una de las siguientes maneras:

   - Si desea ejecutar manualmente un script individual, haga clic en **Ejecutar** junto al script correspondiente.
   - Si desea ejecutar manualmente todos los scripts, en la parte superior del área de configuración, en **Acciones**, haga clic en **Ejecutar scripts**.

5. En la ventana que se abre, haga clic en **Ejecutar**.

Se ejecutan los scripts.

# Programar scripts en dispositivos CPE

Puede crear tareas de ejecución de scripts programadas en dispositivos CPE en el programador de tareas. Al crear una tarea, debe seleccionar la plantilla de CPE, los scripts y los dispositivos CPE en los que desea ejecutar los scripts.

Puede ejecutar scripts en todos los dispositivos CPE que usan una plantilla de CPE o restringir el número de dispositivos CPE especificando etiquetas o seleccionándolos manualmente.

*Para crear una tarea para ejecutar scripts en dispositivos CPE:*

1. En el menú, vaya a la sección **Programador**.

   Se muestra la tabla de tareas programadas.

2. En la parte superior de la página, haga clic en **+ Tarea**.
3. En la ventana que se abre, en la lista desplegable **Tipo**, seleccione **Ejecución de script**.
4. En el campo **Nombre**, escriba el nombre de la tarea.
5. En la lista desplegable **CPE donde se ejecutará el script**, seleccione los dispositivos CPE en los que desea ejecutar el script:

   - **Todos los CPE con plantilla seleccionada** para ejecutar los scripts en todos los dispositivos CPE que utilizan la plantilla de CPE.
   - **Todos los CPE con plantilla seleccionada y etiquetas específicas** para ejecutar los scripts en dispositivos CPE que utilizan la plantilla de CPE y tienen etiquetas específicas asignadas. Si selecciona este valor, especifique las etiquetas del dispositivo CPE en el campo **Etiquetas**.
   - **CPE específicos con plantilla seleccionada** para ejecutar los scripts en todos los dispositivos CPE seleccionados manualmente que utilizan la plantilla de CPE. Si selecciona este valor, seleccione los dispositivos CPE en **CPE**.

6. En **Plantilla de CPE**, seleccione la plantilla de CPE que contiene los scripts que desea ejecutar.
7. En **Scripts**, seleccione los scripts que desea ejecutar.

8. En el campo **Fecha de ejecución de la tarea programada**, ingrese la fecha y la hora en que desea ejecutar la tarea. De manera predeterminada, la fecha y la hora especificadas son la fecha y la hora en que comenzó a crear la tarea.

9. Haga clic en **Crear**.

Se crea una tarea de ejecución de script programada y se muestra en la tabla. El estado de las tareas se muestra en la columna **Estado**. Si la tarea para ejecutar un script finaliza con éxito, su estado cambia a**Realizado**.

# Editar un script en dispositivos CPE

Puede editar un script en la plantilla de CPE. Un script editado en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar un script en dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea editar un script.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Scripts**.

   Esto muestra el número de puerto que VNFM usa para conectarse al dispositivo CPE, el nombre de usuario para ejecutar scripts y la tabla de scripts si se agregó al menos un script.

4. Haga clic en **Editar** junto al script que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del script. Para obtener una descripción de la configuración, consulte las instrucciones para agregar un script en dispositivos CPE.

6. Haga clic en **Guardar**.

   El script se modifica y actualiza en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Eliminar un script en dispositivos CPE

Puede eliminar un script en la plantilla de CPE. Un script eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

Los scripts eliminados no se pueden restaurar.

*Para eliminar un script en los dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Scripts**.

   Esto muestra el número de puerto que VNFM usa para conectarse al dispositivo CPE, el nombre de usuario para ejecutar scripts y la tabla de scripts si se agregó al menos un script.

4. Haga clic en **Eliminar** junto al script que desea eliminar.

   El script se elimina y ya no se muestra en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Administrar la configuración de DNS en dispositivos CPE

## Habilitar DNS en interfaces de red

De manera predeterminada, los servidores DNS especificados cuando crea interfaces de red o en las reglas de reenvío de DNS condicional no están activos en ninguna interfaz. Para que el dispositivo CPE procese consultas DNS, debe habilitar DNS en ciertas interfaces en la plantilla de CPE o en el dispositivo CPE.

*Para habilitar DNS, siga estos pasos:*

1. Habilite DNS de una de las siguientes maneras:

   - Si desea habilitar DNS en interfaces en una plantilla de CPE, en el menú, vaya a la sección **SD-WAN → Plantillas de CPE** y haga clic en una plantilla de CPE.
   - Si desea habilitar DNS en las interfaces de un dispositivo CPE, en el menú, vaya a la sección **SD-WAN → CPE** y haga clic en un dispositivo CPE.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

2. En el menú de la izquierda, seleccione la sección **DNS** y, a continuación, seleccione la pestaña **Interfaces DNS**.

   Se muestra la tabla **Habilitar/deshabilitar el servidor DNS por interfaz**.

   Las interfaces que se utilizan en las tablas de enrutamiento y reenvío virtuales no se incluyen en esta tabla. Los dispositivos CPE no admiten dichas interfaces para procesar consultas DNS.

3. Habilite el botón de alternancia en la columna **Habilitado** para las interfaces para las que desea habilitar el procesamiento de consultas DNS.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

El DNS está habilitado en las interfaces y el dispositivo CPE usa los servidores DNS especificados cuando crea interfaces de red o en las reglas de reenvío condicional al procesar consultas DNS.

# Administrar el reenvío de DNS condicional

Puede configurar el reenvío de DNS condicional en un dispositivo CPE para reenviar las solicitudes de DNS recibidas en el CPE a los servidores DNS ascendentes según el sufijo del nombre especificado en la consulta de DNS (por ejemplo, para bloquear el acceso a recursos no deseados o para usar servidores DNS para solicitudes a recursos corporativos).

Si desea usar el reenvío de DNS condicional, debe configurar las reglas de reenvío para procesar las consultas de DNS y seleccionar un servidor DNS según el sufijo especificado en la regla.

El reenvío de DNS condicional no es compatible con el enrutamiento y reenvío virtuales y las tablas de reenvío: un dispositivo CPE no puede usar las interfaces utilizadas en una instancia de VRF para procesar consultas de DNS.

## Crear reglas de reenvío condicional

Puede crear reglas de reenvío condicional en una plantilla de CPE o en un dispositivo CPE. Las reglas creadas en la plantilla de CPE se crean automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

De manera predeterminada, los servidores DNS no están activos en ninguna interfaz. Para que el dispositivo CPE procese consultas de DNS, debe habilitar el DNS en ciertas interfaces.

*Para crear una regla de reenvío condicional:*

1. Cree un reenvío condicional de una de las siguientes maneras:

   - Si desea crear una regla de reenvío condicional en una plantilla de CPE, en el menú, vaya a la sección **SD-WAN → Plantillas de CPE** y haga clic en una plantilla CPE.

   - Si desea crear una regla de reenvío condicional en un dispositivo CPE, en el menú, vaya a la sección **SD-WAN → CPE** y haga clic en un dispositivo CPE.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

2. En el menú de la izquierda, seleccione la sección **DNS** y, a continuación, seleccione la pestaña **Reenvío de DNS condicional**.

   Se muestra la tabla de reglas de reenvío condicional.

3. En la parte superior de la tabla, haga clic en **+ Crear**.

4. En la ventana que se abre, administre la configuración de la regla de reenvío:

   a. Habilite el interruptor **Habilitado** si desea que la regla creada se use en el dispositivo CPE. Deje el interruptor deshabilitado si desea crear una regla sin aplicarla al dispositivo CPE.

   b. En el campo **Sufijo**, especifique el sufijo que reenviará las solicitudes DNS al servidor DNS con la dirección IP especificada.

   El sufijo de cada regla debe ser único. La longitud máxima es de 255 caracteres. El valor del campo debe ser una cadena con el siguiente formato:

   `<label1>[.<label>]`

   (el elemento `<label1>` seguido del conjunto opcional de elementos `<label>` separados por puntos), donde `<label>` es un subcadena compuesta por `[a-zA-Z0-9-]` caracteres de 1 a 63 caracteres de longitud, `<label1>` es una subcadena compuesta por los mismos caracteres permitidos con un comodín * opcional al principio.

   Si el sufijo incluye una o más `<label>` después de `<label1>` , entonces `<label1>` puede contener solo el carácter *; si el sufijo no tiene ningún elemento `<label>`, `<label1>` debe tener otros caracteres permitidos después de *.

   Ejemplos:

   Valores posibles:

   *.example.com

   *example.com

   Valores no válidos.

   *

   www.*.com

   www.*example.com

   c. Agregue uno o más servidores DNS ascendentes a los que desea reenviar consultas DNS:

   - En el campo **DNS ascendente**, ingrese la dirección IP del servidor DNS al que desea reenviar las consultas DNS cuando el sufijo de esta regla coincide.
   - En la lista **Alias**, seleccione el alias de la interfaz desde la cual desea enviar consultas DNS para esta regla.

   Si es necesario, haga clic en el botón **Agregar DNS ascendente** para agregar el siguiente servidor DNS ascendente. Puede agregar hasta 15 servidores DNS ascendentes para cada sufijo.

5. Haga clic en **Guardar**.

   La regla de reenvío condicional se crea y se muestra en la tabla.

6.

7. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Editar reglas de reenvío condicional

Puede editar las reglas de reenvío condicional en una plantilla de CPE o en un dispositivo CPE. Las reglas editadas en la plantilla de CPE se modifican automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una regla de reenvío condicional, siga estos pasos:*

1. Edite un reenvío condicional de una de las siguientes maneras:

   - Si desea editar una regla de reenvío condicional en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE** y haga clic en la plantilla de CPE en la que desea editar la regla de reenvío condicional.

   - Si desea editar una regla de reenvío condicional en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE** y haga clic en el dispositivo CPE en el que desea editar la regla de reenvío condicional.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

2. En el menú de la izquierda, seleccione la sección **DNS** y, a continuación, seleccione la pestaña **Reenvío de DNS condicional**.

   Se muestra la tabla de reglas de reenvío condicional.

3. Seleccione la regla de reenvío condicional que desea editar y haga clic en el botón **Editar**.

4. En la ventana que se abre, edite la configuración de la regla de reenvío según sea necesario. Para obtener una descripción de la configuración, consulte el artículo Crear de reglas de reenvío condicional.

5. Haga clic en **Guardar**.

   La regla de reenvío condicional se modifica y actualiza en la tabla.

6. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Eliminar reglas de reenvío condicional

*Para eliminar las reglas de reenvío condicional, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea eliminar las reglas.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En el menú de la izquierda, seleccione la sección **DNS** y, a continuación, seleccione la pestaña **Reenvío de DNS condicional**.

   Se muestra la tabla de reglas de reenvío condicional.

4. Seleccione una o varias reglas de reenvío condicional que desee eliminar y haga clic en el botón **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

Las reglas de reenvío condicional se eliminan y ya no se muestran en la tabla.

# Configurar la conexión de un dispositivo CPE al orquestador y al controlador

Cuando se registra un dispositivo CPE, se conecta al orquestador y al controlador. Puede especificar la configuración de conexión al orquestador y al controlador en una plantilla de CPE o en un dispositivo CPE. La configuración de conexión al orquestador y al controlador especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

Algunos modelos de CPE de hardware tienen LED adicionales que muestran el estado de la conexión al controlador, la conexión al orquestador y si hay túneles activos si la función CPE está habilitada. Para obtener más información sobre los LED, consulte la documentación de los dispositivos o comuníquese con el Servicio de soporte técnico.

*Para configurar la conexión de un dispositivo CPE al orquestador y al controlador, siga estos pasos:*

1. Configure la conexión al orquestador y al controlador del dispositivo CPE de una de las siguientes maneras:

   - Si desea configurar la conexión automática al orquestador y al controlador en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN→ Configuración general**.

   - Si desea configurar la conexión automática al orquestador y al controlador en una plantilla de CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **SD-WAN→ Configuración general** y marque la casilla de verificación **Anular**.

   Se muestra la configuración de conexión de un dispositivo CPE al orquestador y al controlador.

2. En **Conexión con el orquestador**, especifique la configuración de conexión del dispositivo CPE al orquestador:

   a. En el campo **Dirección IP/FQDN del orquestador**, ingrese la dirección IP o FQDN del orquestador. La longitud máxima del FQDN es de 50 caracteres.

   b. En el campo **Puerto del orquestador**, ingrese el número de puerto del orquestador. Rango de valores: de 0 a 65 535.

   c. Si desea que el dispositivo CPE obtenga el número de puerto del orquestador a través de DNS, habilite el conmutador **Obtener puerto del orquestador mediante DNS**. Para utilizar esta función, primero debe crear un registro TXT en el servidor DNS que almacene el número de puerto requerido en el formato `_port.<FQDN>`, donde `<FQDN>` es la dirección del orquestador especificado en el campo **Dirección IP/FQDN del orquestador**.

d. Si desea usar un orquestador de respaldo si el orquestador principal falla, en **Dirección IP y puerto del orquestador de respaldo**:

   1. Seleccione la casilla de verificación **Habilitado**. Esta casilla está desactivada por defecto.

   2. En el campo **Dirección IP/FQDN del orquestador de respaldo**, ingrese la dirección IP o el FQDN del orquestador de respaldo. La longitud máxima del FQDN es de 50 caracteres.

   3. En el campo **Puerto del orquestador de respaldo**, ingrese el número de puerto del orquestador de respaldo. Rango de valores: de 0 a 65 535.

e. En la lista desplegable **Protocolo del orquestador**, seleccione el protocolo para la conexión del dispositivo CPE al orquestador:

   - **http**.
   - **https**. Esta es la configuración predeterminada.

   Esta configuración solo se puede especificar en una plantilla de CPE.

f. En el campo **Intervalo de actualización (s)**, ingrese el período en segundos para enviar solicitudes de API REST del dispositivo CPE al orquestador. Rango de valores: de 5 a 300. El valor predeterminado es `30`.

g. En el campo **Intervalo de actualización del modo interactivo (s)**, ingrese el período en segundos para enviar solicitudes de API REST del dispositivo CPE al orquestador en modo interactivo. Rango de valores: de 1 a 10. Puede habilitar el modo interactivo para el diagnóstico del dispositivo CPE.

h. En el campo **Tiempo de espera del modo interactivo (s)**, ingrese el tiempo en segundos después del cual el modo interactivo se deshabilita automáticamente en el dispositivo CPE. Rango de valores: de 30 a 180.

3. En **Conexión con el controlador**, especifique la configuración de conexión del controlador del dispositivo CPE:

a. En la lista desplegable **Transporte de OpenFlow**, especifique si las sesiones de administración entre las interfaces SD-WAN del tipo WAN del dispositivo CPE y los nodos del controlador están cifradas:

   - **TCP** para sesiones de administración no cifradas.
   - **SSL** para sesiones de administración cifradas. Esta es la configuración predeterminada.

   Esta configuración solo se puede especificar en una plantilla de CPE.

b. En la lista desplegable **Interfaz de plano de control priorizada**, seleccione la interfaz SD-WAN del tipo WAN que se prioriza al establecer la sesión de administración principal:

   - **Aleatorio** significa que la sesión de administración principal se establece a partir de una interfaz SD-WAN del tipo WAN elegida al azar. Esta es la configuración predeterminada.
   - **<Interfaz SD-WAN del tipo WAN>** significa que la interfaz SD-WAN especificada del tipo WAN se utiliza para establecer la sesión de administración principal. Si la interfaz SD-WAN del tipo WAN especificada no está disponible, la sesión de administración principal se establece a partir de una interfaz SD-WAN del tipo WAN elegida al azar.

Si la interfaz SD-WAN del tipo WAN desde la cual se estableció la sesión de administración principal falla, se selecciona una nueva sesión de administración principal al azar de las sesiones de administración que se establecieron anteriormente. Si en la lista desplegable **Interfaz de plano de control priorizada**, seleccionó **<interfaz SD-WAN del tipo WAN>** y desea que la sesión de administración que se estableció desde la interfaz SD-WAN del tipo WAN especificada vuelva a ser la sesión principal cuando se recupere la interfaz, siga estos pasos:

1. Seleccione la casilla de verificación **Prioridad**. Esta casilla está desactivada por defecto.

2. En el campo **Tiempo de espera**, ingrese el tiempo en segundos después del cual la sesión de administración establecida desde la interfaz SD-WAN del tipo WAN especificada vuelve a ser la principal cuando esa interfaz se recupera. Rango de valores: de 0 a 86 400.

c. En la lista desplegable **Reinicio automático**, seleccione si desea que el dispositivo CPE se reinicie cuando las sesiones de administración con los nodos del controlador se interrumpan durante mucho tiempo:

- **Sí**. Si selecciona esta opción, en el campo **Tiempo de espera de reinicio (s)**, ingrese el tiempo en segundos después del cual el dispositivo CPE se reinicia automáticamente cuando se interrumpen las sesiones de administración con los nodos del controlador. Rango de valores: de 60 a 2 073 600.

- **No**. Esta es la configuración predeterminada.

d. En el campo **URL de configuración**, ingrese la plantilla de URL para la configuración básica del dispositivo CPE. Cuando ingrese una plantilla, tenga en cuenta las siguientes limitaciones:

- `{config}` es una parte obligatoria que se reemplaza con la configuración del dispositivo CPE cuando se genera un vínculo a partir de la plantilla.

- Longitud máxima: 128 caracteres.

- Debe especificar `http` o `https`.

De manera predeterminada, se utiliza la siguiente plantilla de URL: `http://192.168.7.1/cgi-bin/config?payload={config}`.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar la configuración de conexión del dispositivo CPE mediante la consola del sistema

Puede establecer una sesión de consola con un dispositivo CPE, por ejemplo, para restaurar el firmware o diagnosticar el dispositivo. Los modelos M2 y posteriores están equipados con un puerto serie externo para conectarse a la consola del sistema. Para el modelo M1, puede establecer una conexión con la consola del sistema a través del conector UART ubicado debajo de la cubierta del dispositivo, usando un adaptador.

Una vez que haya obtenido acceso a la consola del sistema, debe proporcionar sus credenciales de inicio de sesión. Puede configurar la autenticación en la consola del sistema mediante la interfaz web del orquestador en una plantilla de CPE o en el dispositivo CPE.

*Para configurar la autenticación en la consola del sistema:*

1. Configure la autenticación en la consola del sistema mediante uno de los siguientes métodos:

   - Si desea configurar la autenticación en la consola del sistema en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN → Configuración general**.

   - Si desea configurar la conexión a la consola del sistema en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **SD-WAN → Configuración general**pestaña y marque la casilla de verificación **Anular**.

   Se muestra la configuración de conexión del dispositivo CPE.

2. En **Configuración de la consola**, habilite el interruptor **Autenticación en la consola del sistema** para solicitar las credenciales del usuario cuando se conecte a través de la consola del sistema, o deshabilite el interruptor para deshabilitar la solicitud de credenciales. Este conmutador está desactivado de forma predeterminada.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

Para que este cambio surta efecto, debe reiniciar manualmente el dispositivo.

# Administrar interfaces de red

*Las interfaces de red* corresponden a los puertos e interfaces virtuales del sistema operativo del dispositivo CPE que se conectan a la WAN o LAN. Debe asignar las interfaces de red del dispositivo CPE a los puertos de OpenFlow del conmutador virtual mediante interfaces de SD-WAN.

Puede ver la tabla de interfaces de red en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de interfaces de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.

- Para ver la tabla de interfaces de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

La información sobre las interfaces de red se muestra en las siguientes columnas de la tabla:

- **Anular**:

  - **Sí** significa que la configuración de la interfaz de red no se hereda de una plantilla.

  - **No** significa que la configuración de la interfaz de red se hereda de una plantilla.

  Esta columna se muestra solo en el dispositivo CPE. Puede cambiar el valor en esta columna para cada interfaz de red directamente en la tabla.

- **Habilitado**:
  - **Sí** significa que la interfaz de red está habilitada.
  - **No** significa que la interfaz de red está deshabilitada.

  Puede cambiar el valor de esta columna para cada interfaz de red directamente en la tabla del dispositivo CPE después de seleccionar **Sí** en la columna **Anular**.
- **Heredado** indica si la interfaz de red se hereda de la plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Alias** es el alias de la interfaz de red para asignar la interfaz de red a un puerto de OpenFlow. Debe especificar este alias de interfaz de red cuando crea una interfaz de SD-WAN del tipo WAN.
- **Descripción** es una breve descripción de la interfaz de red.
- **Zona** es la zona del firewall.
- **NetFlow ifIndex** es el ID numérico permanente de la interfaz que se utiliza cuando se envían estadísticas a través del protocolo de NetFlow.

  De manera predeterminada, esta columna está oculta.
- **Nombre de interfaz** es el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE.
- **Protocolo** es el método para asignar una dirección IP a la interfaz de red:
  - **Cliente DHCP** significa que DHCP asigna automáticamente la dirección IP.
  - **Dirección IPv4 estática** significa que una dirección IPv4 se asigna de forma estática.
  - **Dirección IPv6 estática** significa que una dirección IPv6 se asigna de forma estática.
  - **QMI** significa que la configuración de la conexión de red LTE se especifica manualmente.
  - **PPPoE** significa que la configuración de la conexión del servidor PPPoE se especifica manualmente.
  - **Ninguna** significa que no se asignó una dirección IP.
- **Máscara/dirección IP** son la dirección IP, la máscara y la puerta de enlace predeterminada de la interfaz de red.
- **MTU** es el valor de MTU para la interfaz de red.
- **Habilitar automáticamente** indica si la interfaz de red se habilita automáticamente cuando se enciende el dispositivo CPE:
  - **Sí**.
  - **No**.

Las acciones que puede realizar con las tablas se describen en las instrucciones de Administración de las tablas de componentes de la solución.

# Crear interfaces de red

Puede crear una interfaz de red en una plantilla de CPE o en un dispositivo CPE. Una interfaz de red creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla.

## Crear una interfaz de red con asignación automática de una dirección IP mediante DHCP

*Para crear una interfaz de red con asignación automática de una dirección IP a través de DHCP, siga estos casos:*

1. Cree una interfaz de red de una de las siguientes maneras:

   - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.

3. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la interfaz de red para asignar la interfaz de red a un puerto OpenFlow. Debe especificar el nombre de esta interfaz de red cuando crea una interfaz SD-WAN del tipo WAN. La longitud máxima del nombre es de 15 caracteres.

4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.

5. En el campo **Nombre de interfaz**, ingrese el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE. La longitud máxima del nombre es de 256 caracteres. Por ejemplo, puede ingresar `eth0`, `eth1`, `eth2` o `tun0`. Para crear un puente a partir de varias interfaces, ingrese sus nombres separados por espacios.

   Si desea asignar una etiqueta de VLAN externa a una interfaz de red, ingrese un punto (.) después del puerto físico o el nombre de la interfaz virtual del sistema operativo y luego ingrese la etiqueta de VLAN externa. Por ejemplo, puede ingresar `eth2.150`.

6. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535. Si desea crear un puente a partir de interfaces físicas o virtuales cuyos nombres se especifican en el campo **Nombre de interfaz**, siga estos pasos:

   a. Seleccione la casilla **Puente**. Esta casilla está desactivada por defecto.

   b. Si desea utilizar STP en el puente para evitar bucles de enrutamiento, seleccione la casilla **STP**. Esta casilla está desactivada por defecto.

   c. En el campo **Antigüedad (segundos)**, ingrese la duración en segundos durante la cual los registros dinámicos se almacenan en la tabla MAC del puente. Si desea utilizar el puente como concentrador, ingrese `0` en este campo. Rango de valores: de 0 a 86 400.

7. Si desea habilitar el protocolo NetFlow en la interfaz de red, seleccione la casilla **NetFlow**. Esta casilla está desactivada por defecto.

8. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535.

9. En la lista desplegable **Protocolo**, seleccione **Cliente DHCP**.

10. Si no desea que la interfaz de red se habilite automáticamente cuando el dispositivo CPE esté habilitado, desmarque la casilla **Habilitar automáticamente**. Esta casilla está seleccionada por defecto.

11. Si desea que una dirección IP, una ruta y una puerta de enlace predeterminada se asignen automáticamente a la interfaz de red, seleccione la casilla **Forzar dirección IP, ruta y gateway**. Esta casilla está desactivada por defecto.

12. Si no desea que la ruta obtenida a través de DHCP sea utilizada por la interfaz de red de manera predeterminada, desmarque la casilla **Utilizar ruta predeterminada**. Esta casilla está seleccionada por defecto.

13. Si es necesario, especifique un servidor DNS para la interfaz de red:

    a. En **Servidores DNS**, haga clic en **+ Agregar**.

    b. En el campo que se muestra, ingrese la dirección IP del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **Servidores DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

14. En el campo **Anular MAC**, ingrese la dirección MAC de la interfaz de red. El valor ingresado reemplaza la dirección MAC real de la interfaz de red. El campo no se puede editar si la casilla de verificación **Generar dirección MAC automáticamente** está seleccionada.

15. En el campo **Anular MTU**, ingrese la MTU para la interfaz de red. El valor ingresado anula la MTU predeterminada.

16. Si desea que la dirección MAC de la interfaz de red se genere automáticamente, seleccione la casilla **Generar dirección MAC automáticamente** (desactivada de manera predeterminada).

17. Si es necesario, en el campo **Métrica de rutas**, ingrese la métrica de ruta predeterminada para la interfaz de red. El dispositivo CPE utiliza la ruta predeterminada con la métrica más baja.

La métrica de ruta para interfaces de red con los alias **sdwan0** - **sdwan3** se asigna automáticamente al inicio del CPE: **sdwan0** obtiene la prioridad más alta y la prioridad más baja es para **sdwan3.** En este caso, el dispositivo CPE utiliza la ruta predeterminada de la interfaz de red **sdwan0**. Si la interfaz de red **sdwan0** falla, la ruta predeterminada de la interfaz de red **sdwan1** se usa a continuación, seguida de la ruta predeterminada de la interfaz de red **sdwan2**. El valor del campo **Métrica de rutas** está bloqueado para la edición manual de interfaces con los alias **sdwan0** - **sdwan9**.

La métrica se calcula automáticamente a partir de los siguientes atributos:

- `1-4` si no hay errores y hay acceso a Internet
- `11-14` si no hay errores y no hay acceso a Internet
- `21-24` si hay errores y no hay acceso a Internet

Las métricas se asignan automáticamente a las interfaces según el número en el que termina el alias de la interfaz, de acuerdo con el siguiente esquema:

- **sdwan0**: `1, 11, 21`
- **sdwan1**: `2, 12, 22`
- **sdwan2**: `3, 13, 23`
- **sdwan3**: `4, 14, 24`

18. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.

19. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Crear una interfaz de red con una dirección IPv4 estática

*Para crear una interfaz de red con una dirección IPv4 estática, siga estos pasos:*

1. Cree una interfaz de red de una de las siguientes maneras:

   - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.

3. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la interfaz de red para asignar la interfaz de red a un puerto OpenFlow. Debe especificar el nombre de esta interfaz de red cuando crea una interfaz SD-WAN del tipo WAN. La longitud máxima del nombre es de 15 caracteres.

4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.

5. En el campo **Nombre de interfaz**, ingrese el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE. La longitud máxima del nombre es de 256 caracteres. Por ejemplo, puede ingresar `eth0`, `eth1`, `eth2` o `tun0`. Para crear un puente a partir de varias interfaces, ingrese sus nombres separados por espacios.

   Si desea asignar una etiqueta de VLAN externa a una interfaz de red, ingrese un punto (.) después del puerto físico o el nombre de la interfaz virtual del sistema operativo y luego ingrese la etiqueta de VLAN externa. Por ejemplo, puede ingresar `eth2.150`.

6. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535. Si desea crear un puente a partir de interfaces físicas o virtuales cuyos nombres se especifican en el campo **Nombre de interfaz**, siga estos pasos:

   a. Seleccione la casilla **Puente**. Esta casilla está desactivada por defecto.

   b. Si desea utilizar STP en el puente para evitar bucles de enrutamiento, seleccione la casilla **STP**. Esta casilla está desactivada por defecto.

   c. En el campo **Antigüedad (segundos)**, ingrese la duración en segundos durante la cual los registros dinámicos se almacenan en la tabla MAC del puente. Si desea utilizar el puente como concentrador, ingrese `0` en este campo. Rango de valores: de 0 a 86 400.

7. Si desea habilitar el protocolo NetFlow en la interfaz de red, seleccione la casilla **NetFlow**. Esta casilla está desactivada por defecto.

8. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535.

9. En la lista desplegable **Protocolo**, seleccione **Dirección IPv4 estática**.

10. Si no desea que la interfaz de red se habilite automáticamente cuando el dispositivo CPE esté habilitado, desmarque la casilla **Habilitar automáticamente**. Esta casilla está seleccionada por defecto.

11. Si desea que una dirección IP, una ruta y una puerta de enlace predeterminada se asignen automáticamente a la interfaz de red, seleccione la casilla **Forzar dirección IP, ruta y gateway**. Esta casilla está desactivada por defecto.

12. En la lista desplegable **Dirección IPv4 y tipo de entrada de máscara de subred**, seleccione el método para asignar una dirección IPv4 a la interfaz de red:

    - **Manual** para asignar manualmente una dirección IPv4. Si selecciona esta opción, haga lo siguiente:

      a. En el campo **Dirección IPv4**, ingrese la dirección IPv4 de la interfaz de red.

      b. En el campo **Máscara de red de IPv4**, ingrese la máscara de subred de la interfaz de red.

    Esta es la configuración predeterminada.

- **De la agrupación de IP** para asignar una dirección IPv4 del rango especificado de direcciones IP. Si selecciona este valor, en la lista desplegable **Agrupación de direcciones IP**, seleccione un rango creado de direcciones IP.

- **De la agrupación de subredes** para asignar una dirección IPv4 del rango de subredes especificado. Si selecciona este valor, en la lista desplegable **Agrupación de subredes**, seleccione un rango creado de subredes.

13. En el campo **Gateway de IPv4**, ingrese la dirección IPv4 de la puerta de enlace predeterminada.

14. En el campo **Transmisión de IPv4**, ingrese la dirección de transmisión de la interfaz de red. Si no especifica un valor para esta configuración, se genera automáticamente.

15. Si es necesario, especifique un servidor DNS para la interfaz de red:

    a. En **Servidores DNS**, haga clic en **+ Agregar**.

    b. En el campo que se muestra, ingrese la dirección IP del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **Servidores DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

16. En el campo **Anular MAC**, ingrese la dirección MAC de la interfaz de red. El valor ingresado reemplaza la dirección MAC real de la interfaz de red.

17. En el campo **Anular MTU**, ingrese la MTU para la interfaz de red. El valor ingresado anula la MTU predeterminada.

18. Si es necesario, en el campo **Métrica de rutas**, ingrese la métrica de ruta predeterminada para la interfaz de red. El dispositivo CPE utiliza la ruta predeterminada con la métrica más baja.

    La métrica de ruta para interfaces de red con los alias **sdwan0** - **sdwan3** se asigna automáticamente al inicio del CPE: **sdwan0** obtiene la prioridad más alta y la prioridad más baja es para **sdwan3.** En este caso, el dispositivo CPE utiliza la ruta predeterminada de la interfaz de red **sdwan0**. Si la interfaz de red **sdwan0** falla, la ruta predeterminada de la interfaz de red **sdwan1** se usa a continuación, seguida de la ruta predeterminada de la interfaz de red **sdwan2**. El valor del campo **Métrica de rutas** está bloqueado para la edición manual de interfaces con los alias **sdwan0** - **sdwan9**.

    La métrica se calcula automáticamente a partir de los siguientes atributos:

    - `1-4` si no hay errores y hay acceso a Internet
    - `11-14` si no hay errores y no hay acceso a Internet
    - `21-24` si hay errores y no hay acceso a Internet

    Las métricas se asignan automáticamente a las interfaces según el número en el que termina el alias de la interfaz, de acuerdo con el siguiente esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

19. En **Servidor DHCP**, en la lista desplegable **Tipo**, seleccione el modo de funcionamiento del servidor DHCP para la interfaz de red:

    - **Deshabilitado**. Esta es la configuración predeterminada.
    - **Relé** Si selecciona este valor, ingrese la dirección IP del servidor DHCP en el campo **IP del servidor DHCP**.
    - **Servidor**

20. Si en la lista desplegable **Tipo**, seleccionó **Servidor**, especifique la configuración del servidor DHCP:

    a. En el campo **Primera dirección IP**, ingrese el valor de desplazamiento de la dirección IP base de la interfaz de red para derivar la dirección IP más baja que se puede arrendar a los clientes. El valor predeterminado es `100`. Puede ingresar un valor superior a 255 para subredes grandes.

    b. En el campo **Límite**, ingrese la cantidad máxima de direcciones IP que se pueden arrendar a los clientes. Rango de valores: de 1 a 250. El valor predeterminado es `150`.

    c. En el campo **Tiempo de arrendamiento**, ingrese el tiempo máximo, en horas, durante el cual se puede arrendar una dirección IP individual a un cliente. Rango de valores: 1 a 250. El valor se especifica en el siguiente formato: `<cantidad de horas>h`. Por ejemplo, si desea que el tiempo máximo de arrendamiento sea de 5 horas, ingrese `5 h` . El valor predeterminado es `12h`.

    d. Si es necesario, especifique una opción de DHCP:

        1. En **Opciones de DHCP**, haga clic en **+ Agregar**.
        2. En el campo que se muestra, ingrese el número de la opción DHCP de conformidad con el estándar RFC 1533. Longitud máxima: 250 caracteres.

        La opción DHCP se especifica y se muestra en **Opciones de DHCP**. Puede especificar varias opciones DHCP o eliminar opciones DHCP. Para eliminar una opción DHCP, haga clic en el ícono de eliminar ✕ junto a ella.

21. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.

22. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Crear una interfaz de red con una dirección IPv6 estática

*Para crear una interfaz de red con una dirección IPv6 estática, siga estos pasos:*

1. Cree una interfaz de red de una de las siguientes maneras:

    - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
    - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.

3. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la interfaz de red para asignar la interfaz de red a un puerto OpenFlow. Debe especificar el nombre de esta interfaz de red cuando crea una interfaz SD-WAN del tipo WAN. La longitud máxima del nombre es de 15 caracteres.

4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.

5. En el campo **Nombre de interfaz**, ingrese el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE. La longitud máxima del nombre es de 256 caracteres. Por ejemplo, puede ingresar `eth0`, `eth1`, `eth2` o `tun0`. Para crear un puente a partir de varias interfaces, ingrese sus nombres separados por espacios.

   Si desea asignar una etiqueta de VLAN externa a una interfaz de red, ingrese un punto (.) después del puerto físico o el nombre de la interfaz virtual del sistema operativo y luego ingrese la etiqueta de VLAN externa. Por ejemplo, puede ingresar `eth2.150`.

6. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535. Si desea crear un puente a partir de interfaces físicas o virtuales cuyos nombres se especifican en el campo **Nombre de interfaz**, siga estos pasos:

   a. Seleccione la casilla **Puente**. Esta casilla está desactivada por defecto.

   b. Si desea utilizar STP en el puente para evitar bucles de enrutamiento, seleccione la casilla **STP**. Esta casilla está desactivada por defecto.

   c. En el campo **Antigüedad (segundos)**, ingrese la duración en segundos durante la cual los registros dinámicos se almacenan en la tabla MAC del puente. Si desea utilizar el puente como concentrador, ingrese `0` en este campo. Rango de valores: de 0 a 86 400.

7. Si desea habilitar el protocolo NetFlow en la interfaz de red, seleccione la casilla **NetFlow**. Esta casilla está desactivada por defecto.

8. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535.

9. En la lista desplegable **Protocolo**, seleccione **Dirección IPv6 estática**.

10. Si no desea que la interfaz de red se habilite automáticamente cuando el dispositivo CPE esté habilitado, desmarque la casilla **Habilitar automáticamente**. Esta casilla está seleccionada por defecto.

11. Si desea que una dirección IP, una ruta y una puerta de enlace predeterminada se asignen automáticamente a la interfaz de red, seleccione la casilla **Forzar dirección IP, ruta y gateway**. Esta casilla está desactivada por defecto.

12. En el campo **Dirección IPv6**, ingrese la dirección IPv6 de la interfaz de red. Puede especificar varias direcciones, separándolas con espacios.

13. En el campo **Sufijo de IPv6**, ingrese el sufijo IPv6 de la interfaz de red. Longitud máxima: 30 caracteres.

14. En el campo **Gateway de IPv6**, ingrese la dirección IPv6 de la puerta de enlace predeterminada.

15. En el campo **Longitud del prefijo**, ingrese la longitud del prefijo IPv6 de la interfaz de red. Rango de valores: de 12 a 127.

16. En el campo **Longitud del subprefijo DHCPv6**, ingrese el tamaño del subprefijo DHCPv6 de la interfaz de red. Longitud máxima: 256 caracteres.

17. En el campo **Prefijo de IPv6**, ingrese el prefijo IPv6 de la interfaz de red. Longitud máxima: 30 caracteres.

18. Si desea que la interfaz de red acepte la clase de prefijo IPv6 especificada, haga lo siguiente:

    a. En **Clase IPv6**, haga clic en **+ Agregar**.

    b. Ingrese el nombre de la clase de prefijo IPv6 en el campo que se muestra. Longitud máxima: 256 caracteres.

    La clase de prefijo IPv6 se especifica y se muestra en **Clase IPv6**. Puede especificar varias clases de prefijos IPv6 o eliminar clases de prefijos IPv6. Para eliminar una clase de prefijo IPv6, haga clic en el ícono de eliminar ✕ junto a él.

19. Si es necesario, especifique un servidor DNS para la interfaz de red:

    a. En **Servidores DNS**, haga clic en **+ Agregar**.

    b. En el campo que se muestra, ingrese la dirección IP del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **Servidores DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

20. En el campo **Anular MAC**, ingrese la dirección MAC de la interfaz de red. El valor ingresado reemplaza la dirección MAC real de la interfaz de red.

21. En el campo **Anular MTU**, ingrese la MTU para la interfaz de red. El valor ingresado anula la MTU predeterminada.

22. Si es necesario, en el campo **Métrica de rutas**, ingrese la métrica de ruta predeterminada para la interfaz de red. El dispositivo CPE utiliza la ruta predeterminada con la métrica más baja.

    La métrica de ruta para interfaces de red con los alias **sdwan0** - **sdwan3** se asigna automáticamente al inicio del CPE: **sdwan0** obtiene la prioridad más alta y la prioridad más baja es para **sdwan3.** En este caso, el dispositivo CPE utiliza la ruta predeterminada de la interfaz de red **sdwan0**. Si la interfaz de red **sdwan0** falla, la ruta predeterminada de la interfaz de red **sdwan1** se usa a continuación, seguida de la ruta predeterminada de la interfaz de red **sdwan2**. El valor del campo **Métrica de rutas** está bloqueado para la edición manual de interfaces con los alias **sdwan0** - **sdwan9**.

    La métrica se calcula automáticamente a partir de los siguientes atributos:

    - `1-4` si no hay errores y hay acceso a Internet
    - `11-14` si no hay errores y no hay acceso a Internet
    - `21-24` si hay errores y no hay acceso a Internet

    Las métricas se asignan automáticamente a las interfaces según el número en el que termina el alias de la interfaz, de acuerdo con el siguiente esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`

- **sdwan2**: `3, 13, 23`
- **sdwan3**: `4, 14, 24`

23. En **Servidor DHCP**, en la lista desplegable **Tipo**, seleccione el modo de funcionamiento del servidor DHCP para la interfaz de red:
    - **Deshabilitado**. Esta es la configuración predeterminada.
    - **Relé** Si selecciona este valor, ingrese la dirección IP del servidor DHCP en el campo **IP del servidor DHCP**.
    - **Servidor**
24. Si en la lista desplegable **Tipo**, seleccionó **Servidor**, especifique la configuración del servidor DHCP:
    a. En el campo **Primera dirección IP**, ingrese el valor de desplazamiento de la dirección IP base de la interfaz de red para derivar la dirección IP más baja que se puede arrendar a los clientes. El valor predeterminado es `100`. Puede ingresar un valor superior a 255 para subredes grandes.
    b. En el campo **Límite**, ingrese la cantidad máxima de direcciones IP que se pueden arrendar a los clientes. Rango de valores: de 1 a 250. El valor predeterminado es `150`.
    c. En el campo **Tiempo de arrendamiento**, ingrese el tiempo máximo, en horas, durante el cual se puede arrendar una dirección IP individual a un cliente. Rango de valores: 1 a 250. El valor se especifica en el siguiente formato: `<cantidad de horas>h`. Por ejemplo, si desea que el tiempo máximo de arrendamiento sea de 5 horas, ingrese `5 h` . El valor predeterminado es `12h`.
    d. Si es necesario, especifique una opción de DHCP:
        1. En **Opciones de DHCP**, haga clic en **+ Agregar**.
        2. En el campo que se muestra, ingrese el número de la opción DHCP de conformidad con el estándar RFC 1533. Longitud máxima: 250 caracteres.

    La opción DHCP se especifica y se muestra en **Opciones de DHCP**. Puede especificar varias opciones DHCP o eliminar opciones DHCP. Para eliminar una opción DHCP, haga clic en el ícono de eliminar ✕ junto a ella.
25. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.
26. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Crear una interfaz de red para conectarse a una red LTE

*Esta funcionalidad no es compatible con algunos modelos. Para obtener consejos, comuníquese con el Servicio de soporte técnico de Kaspersky.*

*Para crear una interfaz de red para conectarse a una red LTE:*

1. Cree una interfaz de red de una de las siguientes maneras:

   - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.
3. En la ventana que se abre, en el campo **Alias**, ingrese el alias de la interfaz de red para asignar la interfaz de red a un puerto de OpenFlow. Debe especificar este alias de interfaz de red cuando crea una interfaz de SD-WAN del tipo WAN. La longitud máxima del alias es de 15 caracteres.
4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.
5. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535.
6. En la lista desplegable **Protocolo**, seleccione **QMI**.
7. En el campo **Nombre de QMI**, ingrese la ruta al módem en el dispositivo CPE. La longitud máxima de la ruta es de 30 caracteres. Por ejemplo, puede escribir `/dev/cdc-wdm0`.
8. En la lista **Origen de APN**, seleccione cómo desea ingresar el ID de APN del operador de telecomunicaciones que emitió la tarjeta SIM instalada en el módem:

   - Si desea que el APN se inserte automáticamente desde el directorio de APN, seleccione**Directorio** y luego seleccione un directorio en la lista **Directorio de APN** que se muestra
   - Si desea especificar la cadena de APN manualmente, seleccione **Manual** y luego ingrese la cadena de APN en el campo **Cadena de APN**. La longitud máxima del ID es de 30 caracteres.

9. En la lista desplegable **Tipo de autenticación**, seleccione el tipo de autenticación en la interfaz de red:

   - **PAP** (Password Authentication Protocol).
   - **CHAP** (Challenge Handshake Authentication Protocol).
   - **PAP y CHAP** significa que ambos tipos de autenticación se utilizan en la interfaz de red .
   - **Ninguna** significa que la autenticación no se utiliza en la interfaz de red.

10. En el campo **Nombre de usuario de la autenticación de PAP/CHAP**, ingrese el nombre de usuario para la autenticación PAP/CHAP. La longitud máxima del nombre es de 30 caracteres. Si no desea utilizar la autenticación, no especifique un valor para esta configuración.

11. En el campo **Contraseña de la autenticación de PAP/CHAP**, ingrese la contraseña para la autenticación PAP/CHAP. La longitud máxima de la contraseña es de 30 caracteres. Si no desea utilizar la autenticación, no especifique un valor para esta configuración.

12. En el campo **Código PIN**, ingrese el código PIN de la tarjeta SIM instalada en el módem. Longitud máxima del PIN: 4 dígitos.

13. En el campo **Demora**, ingrese el tiempo en segundos después del cual la interfaz de red comienza a comunicarse con el módem. Valor máximo: 30. Esta configuración se utiliza cuando el módem tarda demasiado en iniciarse.

14. Si es necesario, especifique los modos de comunicación móvil en los que desea que funcione el módem:

    a. En **Modos**, haga clic en **+ Agregar**.

    b. En la lista desplegable, seleccione uno de los valores siguientes:

    - **Todo** para usar todos los modos de comunicación móvil disponibles
    - **LTE**
    - **UMTS**
    - **GSM**
    - **CDMA**
    - **TD-SCDMA**

    Los modos de comunicación móvil se configuran en el módem y se muestran en **Modos**. Puede especificar varios modos o eliminar modos. Para eliminar un modo, haga clic en el ícono de eliminar ✕ junto a él.

15. Si es necesario, especifique un servidor DNS para la interfaz de red:

    a. En **Servidores DNS**, haga clic en **+ Agregar**.

    b. En el campo que se muestra, ingrese la dirección IP del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **Servidores DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

16. En el campo **Perfil de conexión**, ingrese el índice del perfil de conexión que utiliza la interfaz de red en lugar del ID de APN. La longitud máxima del índice es de 30 caracteres.

17. En la lista desplegable **Pila de IP**, seleccione la pila de IP que se usa en la interfaz de red:

    - **IPv4** para usar la pila de protocolos IPv4 en la interfaz de red. Esta es la configuración predeterminada.
    - **IPV6** para usar la pila de protocolos IPv6 en la interfaz de red.
    - **Pila doble (IPv4 e IPv6)** para usar la pila dual IPv4 e IPv6 en la interfaz de red.

18. Desmarque la casilla **IPv4 sobre DHCP** si no desea asignar una dirección IPv4 a la interfaz de red a través de DHCP. Para seleccionar esta casilla simultáneamente con la casilla **IPv6 sobre DHCP**, seleccione **Pila doble (IPv4 e IPv6)** (para pila dual) en el menú desplegable **Pila de IP**. Esta casilla está seleccionada por defecto.

19. Seleccione la casilla **IPv6 sobre DHCP** para asignar una dirección IPv6 a la interfaz de red a través de DHCP. Para seleccionar esta casilla simultáneamente con la casilla **IPv4 sobre DHCP**, seleccione **Pila doble (IPv4 e IPv6)** en la lista desplegable **Pila de IP**. Esta casilla está desactivada por defecto.

20. Desmarque la casilla **Conexión automática** si no desea que el módem se conecte automáticamente a la red. Esta casilla está seleccionada por defecto.

21. En el campo **PLMN**, ingrese el ID de PLMN del proveedor de servicios. Los primeros tres dígitos del identificador de PLMN son el código de país móvil (MCC) y los dos o tres dígitos siguientes son el código de red móvil (MNC). Por ejemplo, para la red Vimpelcom en el territorio ruso, PLMN =25099: MCC = 250 (Federación de Rusia), MNC = 99 (Vimpelcom).

22. En el campo **Tiempo de espera**, ingrese el tiempo en segundos para que la interfaz de red espere la finalización de las operaciones de la tarjeta SIM en el módem. Valor máximo: 20. El valor predeterminado es `10`.

23. En el campo **Puerto serie**, ingrese el nombre del puerto serie del módem. La longitud máxima del nombre es de 50 caracteres.

24. Si es necesario, en el campo **Métrica de rutas**, ingrese la métrica de ruta predeterminada para la interfaz de red. El dispositivo CPE utiliza la ruta predeterminada con la métrica más baja.

    La métrica de ruta para interfaces de red con los alias **sdwan0** - **sdwan3** se asigna automáticamente al inicio del CPE: **sdwan0** obtiene la prioridad más alta y la prioridad más baja es para **sdwan3.** En este caso, el dispositivo CPE utiliza la ruta predeterminada de la interfaz de red **sdwan0**. Si la interfaz de red **sdwan0** falla, la ruta predeterminada de la interfaz de red **sdwan1** se usa a continuación, seguida de la ruta predeterminada de la interfaz de red **sdwan2**. El valor del campo **Métrica de rutas** está bloqueado para la edición manual de interfaces con los alias **sdwan0** - **sdwan9**.

    La métrica se calcula automáticamente a partir de los siguientes atributos:

    - `1-4` si no hay errores y hay acceso a Internet
    - `11-14` si no hay errores y no hay acceso a Internet
    - `21-24` si hay errores y no hay acceso a Internet

    Las métricas se asignan automáticamente a las interfaces según el número en el que termina el alias de la interfaz, de acuerdo con el siguiente esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

25. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.

26. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Crear una interfaz de red para conectarse a un servidor PPPoE

*Para crear una interfaz de red para conectarse a un servidor PPPoE:*

1. Cree una interfaz de red de una de las siguientes maneras:

   - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.
3. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la interfaz de red para asignar la interfaz de red a un puerto OpenFlow. Debe especificar el nombre de esta interfaz de red cuando crea una interfaz SD-WAN del tipo WAN. La longitud máxima del nombre es de 15 caracteres.
4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.
5. En el campo **Nombre de interfaz**, ingrese el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE. La longitud máxima del nombre es de 256 caracteres. Por ejemplo, puede ingresar `eth0`, `eth1`, `eth2` o `tun0`. Para crear un puente a partir de varias interfaces, ingrese sus nombres separados por espacios.

   Si desea asignar una etiqueta de VLAN externa a una interfaz de red, ingrese un punto (.) después del puerto físico o el nombre de la interfaz virtual del sistema operativo y luego ingrese la etiqueta de VLAN externa. Por ejemplo, puede ingresar `eth2.150`.
6. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65535. En la lista desplegable **Protocolo**, seleccione **PPPoE**.
7. En el campo **Acceder al concentrador**, ingrese la dirección IP o el nombre de host del concentrador de acceso al cual se conecta la interfaz de red. La longitud máxima del nombre de host es de 30 caracteres. Si no ingresa un valor en este campo, el demonio del protocolo punto a punto (PPPD) utilizará el primer concentrador de acceso que detecte.
8. En el campo **Servicio**, ingrese el nombre del servicio PPPoE al que se conecta la interfaz de red. La longitud máxima del nombre es de 30 caracteres. Si no ingresa un valor en este campo, PPPD utilizará el primer servicios PPPoE que detecte.

9. En la lista desplegable **Tipo de autenticación**, seleccione qué autenticación se usa en la interfaz de red:

   - **PAP y CHAP** si se usa la autenticación PAP y CHAP en la interfaz de red. Si selecciona esta opción, haga lo siguiente:

     a. En el campo **Nombre de usuario de la autenticación de PAP/CHAP**, ingrese el nombre de usuario para la autenticación PAP/CHAP. La longitud máxima del nombre es de 30 caracteres.

     b. En el campo **Contraseña de la autenticación de PAP/CHAP**, ingrese la contraseña para la autenticación PAP/CHAP. La longitud máxima de la contraseña es de 30 caracteres.

   - **Ninguna** significa que la autenticación no se utiliza en la interfaz de red.

10. En el campo **Cantidad máxima de pings con error**, ingrese el número de solicitudes ICMP fallidas antes de que la interfaz de red considere que el servidor PPPoE no está disponible. Rango de valores: 1 a 3600. El valor predeterminado es `5`.

11. En el campo **Intervalo de ping (s)**, ingrese el intervalo en segundos que la interfaz de red debe esperar antes de enviar solicitudes ICMP al servidor PPPoE. Rango de valores: 1 a 3600. El valor predeterminado es `1`.

12. Si desea que la interfaz de red finalice una conexión PPPoE inactiva después del tiempo especificado, en el campo **Tiempo de espera (s)**, ingrese el tiempo en segundos. Rango de valores: 1 a 3600.

13. Si es necesario, en el campo **Host-Uniq**, ingrese la etiqueta Host-Uniq para la conexión PPPoE. La longitud máxima de la etiqueta es de 30 caracteres. Si no ingresa un valor en este campo, el valor de la etiqueta Host-Uniq es el mismo que el del identificador de proceso PPPD.

14. En el campo **Anular MTU**, ingrese la MTU para la interfaz de red. El valor ingresado anula la MTU predeterminada.

15. Si es necesario, en el campo **Métrica de rutas**, ingrese la métrica de ruta predeterminada para la interfaz de red. El dispositivo CPE utiliza la ruta predeterminada con la métrica más baja.

    La métrica de ruta para interfaces de red con los alias **sdwan0** - **sdwan3** se asigna automáticamente al inicio del CPE: **sdwan0** obtiene la prioridad más alta y la prioridad más baja es para **sdwan3.** En este caso, el dispositivo CPE utiliza la ruta predeterminada de la interfaz de red **sdwan0**. Si la interfaz de red **sdwan0** falla, la ruta predeterminada de la interfaz de red **sdwan1** se usa a continuación, seguida de la ruta predeterminada de la interfaz de red **sdwan2**. El valor del campo **Métrica de rutas** está bloqueado para la edición manual de interfaces con los alias **sdwan0** - **sdwan9**.

    La métrica se calcula automáticamente a partir de los siguientes atributos:

    - `1-4` si no hay errores y hay acceso a Internet
    - `11-14` si no hay errores y no hay acceso a Internet
    - `21-24` si hay errores y no hay acceso a Internet

    Las métricas se asignan automáticamente a las interfaces según el número en el que termina el alias de la interfaz, de acuerdo con el siguiente esquema:

    - **sdwan0**: `1, 11, 21`
    - **sdwan1**: `2, 12, 22`
    - **sdwan2**: `3, 13, 23`
    - **sdwan3**: `4, 14, 24`

16. Si es necesario, desmarque las siguientes casillas:

    - Desmarque la casilla **Keepalive adaptado** si desea que la interfaz de red que no recibió paquetes de control del protocolo de control de vínculos (LCP) del servidor PPPoE para finalizar la conexión PPPoE, incluso si el tráfico proviene del servidor PPPoE.
    - Desmarque la casilla **Utilizar ruta predeterminada** si no desea utilizar la ruta obtenida del servidor PPPoE como ruta predeterminada en la interfaz de red.
    - Desmarque la casilla **Servidor DNS asignado por pares** si no desea que la interfaz de red utilice los servidores DNS asignados a sus vecinos.

    Las casillas están seleccionadas de manera predeterminada.

17. Si desea enviar argumentos de línea de comandos adicionales al iniciar el PPPD (demonio del protocolo punto a punto), en el campo **PPPD**, ingrese los argumentos de línea de comandos. Por ejemplo, puede enviar parámetros de autenticación, direcciones IP y scripts al PPPD.

18. Si es necesario, especifique un servidor DNS para la interfaz de red:

    a. En **Servidores DNS**, haga clic en **+ Agregar**.

    b. En el campo que se muestra, ingrese la dirección IP del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **Servidores DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en el ícono de eliminar ✕ junto a él.

19. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.

20. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Crear una interfaz de red sin dirección IP

*Para crear una interfaz de red sin una dirección IP, siga estos pasos:*

1. Cree una interfaz de red de una de las siguientes maneras:

    - Si desea crear una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
    - Si desea crear una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

    Se muestra la tabla de interfaces de red.

2. Haga clic en **+ Interfaz de red**.

3. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la interfaz de red para asignar la interfaz de red a un puerto OpenFlow. Debe especificar el nombre de esta interfaz de red cuando crea una interfaz SD-WAN del tipo WAN. La longitud máxima del nombre es de 15 caracteres.

4. Si desea agregar una interfaz de red a una zona de firewall, en la lista desplegable **Zona**, seleccione la zona de firewall creada.

5. En el campo **Nombre de interfaz**, ingrese el nombre del puerto físico o la interfaz virtual del sistema operativo del dispositivo CPE. La longitud máxima del nombre es de 256 caracteres. Por ejemplo, puede ingresar `eth0`, `eth1`, `eth2` o `tun0`. Para crear un puente a partir de varias interfaces, ingrese sus nombres separados por espacios.

   Si desea asignar una etiqueta de VLAN externa a una interfaz de red, ingrese un punto (.) después del puerto físico o el nombre de la interfaz virtual del sistema operativo y luego ingrese la etiqueta de VLAN externa. Por ejemplo, puede ingresar `eth2.150`.

6. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535. Si desea crear un puente a partir de interfaces físicas o virtuales cuyos nombres se especifican en el campo **Nombre de interfaz**, siga estos pasos:

   a. Seleccione la casilla **Puente**. Esta casilla está desactivada por defecto.

   b. Si desea utilizar STP en el puente para evitar bucles de enrutamiento, seleccione la casilla **STP**. Esta casilla está desactivada por defecto.

   c. En el campo **Antigüedad (segundos)**, ingrese la duración en segundos durante la cual los registros dinámicos se almacenan en la tabla MAC del puente. Si desea utilizar el puente como concentrador, ingrese `0` en este campo. Rango de valores: de 0 a 86 400.

7. Si desea habilitar el protocolo NetFlow en la interfaz de red, seleccione la casilla **NetFlow**. Esta casilla está desactivada por defecto.

8. Si es necesario, en el campo **NetFlow ifIndex**, ingrese un ID numérico permanente para la interfaz que se utilizará cuando se envían estadísticas a través del protocolo NetFlow. Rango de valores: de 1 a 65 535.

9. En la lista desplegable **Protocolo**, seleccione **Ninguna**.

10. Si desea establecer una conectividad L2 entre dispositivos CPE, seleccione la casilla **Modo L2**. Cuando se selecciona la casilla, se crea automáticamente un puerto de OpenFlow asignado a la interfaz de red en el conmutador virtual del dispositivo CPE. Esta casilla está desactivada por defecto. No puede seleccionar esta casilla en los siguientes casos:

    - Seleccionó una de las siguientes casillas cuando creó la interfaz de red:
        - **Puente**
        - **NetFlow**
        - **Forzar dirección IP, ruta y gateway**
    - La interfaz de red se utiliza en una ruta estática.
    - BGP utiliza la interfaz de red.
    - El protocolo OSPF utiliza la interfaz de red.
    - El protocolo VRRP utiliza la interfaz de red.
    - La interfaz de red se utiliza para transmitir tráfico de multidifusión.

- Una tabla de enrutamiento y reenvío virtuales (VRF) utiliza la interfaz de red.
- La interfaz de red se utiliza para el diagnóstico de dispositivos CPE mediante la utilidad ping, traceroute, tcpdump o sweep.

Si selecciona esta casilla, el puerto de OpenFlow creado automáticamente en el conmutador virtual del dispositivo CPE se muestra en el campo **Puerto OpenFlow**. Puede cambiar el número de puerto de OpenFlow. Rango de valores: de 11 a 20.

11. Si desea que la interfaz de red se habilite automáticamente cuando el dispositivo CPE esté habilitado, seleccione la casilla **Habilitar automáticamente**. Esta casilla está desactivada por defecto.
12. Si desea que una dirección IP, una ruta y una puerta de enlace predeterminada se asignen automáticamente a la interfaz de red, seleccione la casilla **Forzar dirección IP, ruta y gateway**. Esta casilla está desactivada por defecto.
13. En el campo **Anular MAC**, ingrese la dirección MAC de la interfaz de red. El valor ingresado reemplaza la dirección MAC real de la interfaz de red.
14. En el campo **Anular MTU**, ingrese la MTU para la interfaz de red. El valor ingresado anula la MTU predeterminada.
15. Haga clic en **Crear**.

    La interfaz de red se crea y se muestra en la tabla.
16. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Editar una interfaz de red

Puede editar una interfaz de red en una plantilla de CPE o en un dispositivo CPE. Una interfaz de red editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una interfaz de red, siga estos pasos:*

1. Edite una interfaz de red de una de las siguientes maneras:
   - Si desea editar una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea editar una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**. Si desea editar una interfaz de red heredada de la plantilla de CPE, seleccione la casilla de verificación **Anular** junto a la interfaz de red.

   Se muestra la tabla de interfaces de red.
2. Haga clic en **Editar** junto a la interfaz de red que desea editar.
3. En la ventana que se abre, si es necesario, edite la configuración de la interfaz de red. Para obtener una descripción de la configuración, consulte las instrucciones para crear una interfaz de red.

4. Haga clic en **Guardar**.

   La interfaz de red se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Deshabilitar o habilitar una interfaz de red

Puede deshabilitar o habilitar una interfaz de red en una plantilla de CPE o en un dispositivo CPE. Una interfaz de red habilitada o deshabilitada en una plantilla de CPE se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esa plantilla.

*Para deshabilitar o habilitar una interfaz de red:*

1. Deshabilite o habilite una interfaz de red de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Red**.
   - Si desea habilitar o deshabilitar una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**. Si desea deshabilitar o habilitar una interfaz de red heredada de la plantilla de CPE, seleccione la casilla **Anular** junto a la interfaz de red.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **Deshabilitar** o **Habilitar** junto a la interfaz de red que desea deshabilitar o habilitar.

   La interfaz de red se deshabilita o habilita.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Cancelar la aplicación de la configuración de la interfaz de red a un dispositivo CPE

*Si no desea aplicar la configuración de la interfaz de red a un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE al que no desea aplicar la configuración de la interfaz de red.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

4. Seleccione la casilla **Ignorar configuración de red**. Esta casilla está desactivada por defecto.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

La configuración de la interfaz de red no se aplica al dispositivo CPE.

Si desea aplicar la configuración de la interfaz de red al dispositivo CPE, desmarque la casilla **Ignorar configuración de red**.

# Eliminar una interfaz de red

Puede eliminar una interfaz de red en una plantilla CPE o en un dispositivo CPE. Una interfaz de red eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. No puede eliminar una interfaz de red heredada de una plantilla CPE en un dispositivo CPE.

Las interfaces de red eliminadas no se pueden restaurar.

*Para eliminar una interfaz de red:*

1. Elimine una interfaz de red de una de las siguientes maneras:

   - Si desea eliminar una interfaz de red en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Red**.

   - Si desea eliminar una interfaz de red en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Red**.

   Se muestra la tabla de interfaces de red.

2. Haga clic en **Eliminar** junto a la interfaz de red que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La interfaz de red se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Protección contra la suplantación de IP mediante uRPF

Esta función permite mitigar el impacto de los ataques de suplantación de direcciones IP mediante el uso del algoritmo Unicast Reverse Path Forwarding (uRPF) en las interfaces CPE.

## Principio de funcionamiento de uRPF

El algoritmo utiliza la tabla de enrutamiento y reenvío de la Base de información de reenvío (FIB) para analizar los paquetes de la siguiente manera:

1. Recepción de un paquete.

   El enrutador recibe un paquete en una interfaz.

2. Comprobación del origen.

   uRPF comprueba la dirección IP de origen del paquete.

3. Búsqueda inversa.

   El enrutador busca la interfaz que usaría para enviar un paquete de respuesta a este origen (ruta de retorno) en la tabla FIB.

4. Procesamiento del paquete. Otras acciones dependen del modo de funcionamiento seleccionado de uRPF:

   - Modo estricto

     El paquete debe llegar exactamente a través de esa interfaz que es la mejor ruta de retorno al origen. Si la ruta no coincide, el paquete se descarta.

     El modo estricto se utiliza para proteger contra la suplantación de IP en el perímetro de las redes con enrutamiento simétrico.

   - Modo laxo

     Se acepta un paquete si la tabla de enrutamiento y reenvío tiene al menos alguna ruta al origen, independientemente de la interfaz específica.

     El modo laxo se puede utilizar en redes con enrutamiento asimétrico (cuando la ruta de ida es diferente de la ruta de regreso).

Puede configurar uRPF de forma independiente para cada interfaz de red del dispositivo CPE. uRPF se puede utilizar tanto en interfaces normales como en interfaces de puente.

> uRPF está disponible para interfaces con los protocolos "cliente DHCP"/"dirección IPv4 estática"/"QMI"/"PPPoE" y no está disponible para interfaces con los protocolos "dirección IPv6 estática"/"Ninguno".

Puede configurar uFPF en dispositivos CPE o en plantillas CPE.

*Para configurar uRPF, siga estos pasos:*

1. Configure uRPF de una de las siguientes maneras:

   - Para configurar uRPF en un dispositivo CPE, en el menú del orquestador, vaya a la sección **SD-WAN**, seleccione el dispositivo CPE y vaya a la sección **Red** de configuración.

   - Para configurar uRPF en una plantilla de CPE, en el menú del orquestador, vaya a la sección `Plantillas CPE`, seleccione la plantilla de CPE y vaya a la sección **Red** de configuración.

2. Cree una nueva interfaz de red o edite una existente.

   Si la interfaz se usa en la plantilla de CPE, seleccione el botón de alternancia **Anular** para ella.

3. Si creará una nueva interfaz de red, seleccione uno de los protocolos admitidos en la lista desplegable **Protocolo**:

   - **Cliente DHCP**
   - **Dirección IPv4 estática**
   - **QMI**
   - **PPPoE**

4. En la lista desplegable **Modo uRPF**, seleccione el modo uRPF:

   - **Estricto**
   - **Laxo**

5. Guarde la configuración de la interfaz de red.

6. Aplique los cambios al dispositivo o plantilla de CPE.

# Administrar interfaces de SD-WAN

Las *interfaces de SD-WAN* son interfaces lógicas que están sobre las interfaces de red del dispositivo CPE y los puertos OpenFlow del conmutador virtual, que forman un nivel adicional de abstracción. Cada interfaz de SD-WAN se asigna a una interfaz de red por el nombre de la interfaz de red y un puerto OpenFlow por el número de puerto OpenFlow. Son posibles los siguientes tipos de interfaces de SD-WAN:

- Las interfaces de SD-WAN del tipo LAN son interfaces de SD-WAN creadas de manera predeterminada y asignadas a las interfaces de red que están conectadas al LAN. No puede eliminar y crear una interfaz de SD-WAN del tipo LAN, pero puede editarla para especificar la velocidad máxima y configurar las colas de tráfico.

- Las interfaces de SD-WAN del tipo WAN son interfaces de SD-WAN asignadas a las interfaces de red que están conectadas al WAN.

- Una interfaz de SD-WAN del tipo de administración es una interfaz de SD-WAN creada de manera predeterminada y asignada a una interfaz de red que es utilizada por el sistema de supervisión Zabbix para la supervisión pasiva del dispositivo CPE, así también como por el orquestador para conectar el dispositivo CPE a través del SSH. No puede eliminar y crear una interfaz de SD-WAN del tipo de administración.

Puede ver la tabla de interfaces de SD-WAN en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de las interfaces SD-WAN en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN → Interfaces**.

- Para ver la tabla de las interfaces de SD-WAN en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **SD-WAN → Interfaces**.

La información sobre las interfaces de SD-WAN se muestra en las siguientes columnas de la tabla:

- **Tipo** es el tipo de interfaz de SD-WAN:
  - **WAN**
  - **LAN**
  - **Administración**
- **Heredado** indica si la interfaz de SD-WAN es heredada desde una plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Puerto** es el número de puerto de OpenFlow.
- **Alias** es el nombre de la interfaz de red.
- **Tasa máxima** es la velocidad máxima de la interfaz de SD-WAN en Mbps.

En las siguientes columnas de la tabla, se muestra información adicional sobre las comprobaciones de WAN a las que están conectadas las interfaces de SD-WAN:

- **Dirección IP para seguimiento** son las direcciones IP de los hosts para comprobar la disponibilidad de WAN.
- **Confiabilidad** es la cantidad mínima de comprobaciones correctas que hace que la WAN esté disponible.
- **Conteo** es la cantidad de solicitudes a los hosts dentro de una comprobación de WAN.
- **Tiempo de espera** es el tiempo que hay que esperar una respuesta de los hosts, en milisegundos.
- **Intervalo (s)** es el intervalo de tiempo en segundos para la comprobación de WAN.
- **Abajo** es la cantidad de comprobaciones fallidas que hacen que la WAN no esté disponible.
- **Arriba** es la cantidad de comprobaciones correctas que hacen que la WAN esté disponible.
- **Supervisión de velocidad** indica si se está midiendo la velocidad de la interfaz de SD-WAN del tipo WAN:
  - **Sí**.
  - **No**.

# Acerca del envío de información sobre interfaces SD-WAN del tipo WAN al controlador

Cuando crea o edita interfaces de SD-WAN del tipo WAN, puede especificar qué información se debe enviar al controlador.

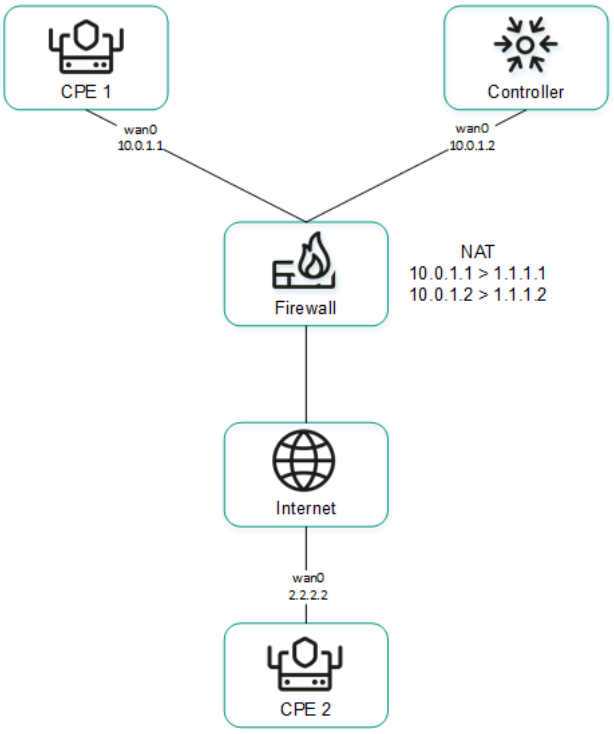
## Envío de direcciones IP públicas y puertos UDP de interfaces SD-WAN al controlador

Para establecer vínculos entre dispositivos CPE, el controlador debe obtener información sobre las direcciones IP públicas de las interfaces SD-WAN del tipo WAN. De manera predeterminada, el controlador obtiene esta información a través de una sesión de administración. En ese caso, la dirección IP de origen se utiliza como dirección IP pública.

Puede especificar manualmente las direcciones IP y los puertos UDP de la interfaz SD-WAN del tipo WAN. En la siguiente figura, el CPE 1 y el controlador están en la misma red local y obtienen acceso a Internet a través del mismo firewall que realiza el reenvío de direcciones IP.

Al establecer una sesión entre la interfaz SD-WAN del tipo WAN de CPE 1 y la dirección IP pública del controlador (1.1.1.2), si el firewall no se puede configurar de manera que el Controlador reenvíe la dirección IP privada a la dirección IP pública (10.0.1.1 > 1.1.1.1), el Controlador no podrá obtener información sobre la dirección IP pública de la interfaz SD-WAN del tipo WAN y proporcionarla a otros dispositivos CPE en la topología (CPE 2).

Como resultado, no se puede crear un vínculo entre CPE 1 y CPE 2; CPE 1 se aísla y no se puede agregar al plano de control común.




CPE 1 y el controlador están detrás de NAT y están conectados a CPE 2

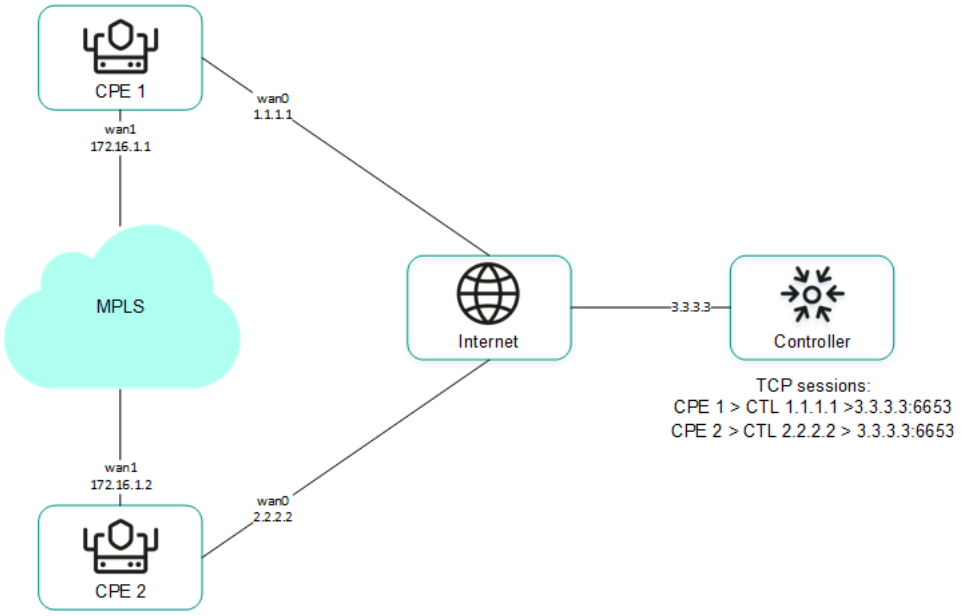
## Envío de direcciones IP de interfaces SD-WAN del tipo WAN ubicadas en una red aislada al controlador

Las interfaces SD-WAN del tipo WAN pueden estar en una red aislada sin la posibilidad de establecer una sesión de administración con el controlador, pero pueden usarse para establecer vínculos. En este caso, el controlador no puede obtener información sobre las direcciones IP de las interfaces SD-WAN aisladas del tipo WAN y usarla para establecer vínculos entre dispositivos CPE.

En la siguiente figura, CPE 1 y CPE 2 tienen dos interfaces SD-WAN del tipo WAN cada uno, pero pueden establecer una sesión de administración con el controlador solo a través de wan0 porque wan1 está en una red aislada (MPLS) que no tiene acceso al controlador. Sin embargo, ambas interfaces wan1 se pueden usar para establecer vínculos.

Si el vínculo utilizado para interactuar con el controlador falla para uno de los dispositivos CPE, todos los demás vínculos tampoco se pueden usar, incluso si permanecen operativos, porque el controlador excluye el dispositivo de la topología.

Las direcciones IP de las interfaces SD-WAN aisladas del tipo WAN se envían al controlador a través del orquestador.




CPE 1 y CPE 2 están conectados entre sí a través de MPLS y con el controlador a través de Internet.

# Fragmentación de paquetes

Kaspersky SD-WAN comprueba si los dispositivos CPE admiten la fragmentación de paquetes de tráfico. Se inicia automáticamente una prueba de fragmentación de paquetes. Cuando se habilita cada dispositivo CPE, envía dos solicitudes ICMP a las direcciones IP que especificó cuando creó o editó las interfaces de SD-WAN del tipo WAN.

Las solicitudes ICMP tienen un tamaño de paquete de 1600 bytes. Si al menos una de las solicitudes ICMP recibe una respuesta, se llega a la conclusión de que el dispositivo CPE admite la fragmentación de paquetes. Puede ver el resultado de la prueba de fragmentación en la columna **Fragmentación** de la tabla de dispositivos CPE o en la tabla de vínculos.

# Colas de tráfico en interfaces de SD-WAN

Se puede utilizar un máximo de 8 colas de tráfico en las interfaces de SD-WAN. Para cada cola de tráfico, debe especificar el ancho de banda mínimo y máximo como un porcentaje del ancho de banda total establecido para la interfaz de SD-WAN. La suma total de todos los valores de ancho de banda mínimos especificados para las colas de tráfico no puede exceder el 100 %.

Las colas de tráfico tienen prioridad estricta y el ancho de banda no reservado se ofrece primero al tráfico de la cola de mayor prioridad. A cada cola de tráfico se le garantiza un cierto ancho de banda mínimo de acuerdo con su valor de ancho de banda mínimo especificado. Se necesita un límite superior en el ancho de banda máximo para las colas de mayor prioridad a fin de permitir que el tráfico de las colas de menor prioridad se siga transmitiendo.

Puede configurar las colas de tráfico cuando se crea interfaz de SD-WAN del tipo WAN o se edita una interfaz de SD-WAN.

Los proveedores de servicios pueden usar diferentes directivas de calidad de servicio para marcar las colas de tráfico en sus redes y cumplir con los requisitos del SLA para el paso del tráfico del cliente. Por lo tanto, al establecer una conexión simultánea a las redes de diferentes proveedores de servicios, los dispositivos CPE pueden volver a marcar el tráfico de diferentes colas para cada interfaz de SD-WAN del tipo WAN. Para configurar el remarcado, debe cambiar el valor del tipo de servicio (ToS) cuando se configuran las colas de tráfico en una interfaz de SD-WAN.

Solo puede cambiar los valores de ToS de los encabezados externos de los paquetes de tráfico que se originan en las interfaces de SD-WAN del tipo WAN. Los valores de ToS de los encabezados de paquetes de tráfico interno no se pueden editar.

# Crear una interfaz SD-WAN del tipo WAN

Puede crear una interfaz de SD-WAN del tipo WAN en una plantilla de CPE o en un dispositivo CPE. Una interfaz de SD-WAN del tipo WAN creada en una plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una interfaz de SD-WAN del tipo WAN, siga estos pasos:*

1. Cree una interfaz de SD-WAN del tipo WAN de una de las siguientes maneras:

   - Si desea crear una interfaz de SD-WAN del tipo WAN en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN → Interfaces**.
   - Si desea crear una interfaz de SD-WAN del tipo WAN en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **SD-WAN→ Interfaces**.

   Se muestra una tabla de interfaces SD-WAN.

2. Haga clic en **+ Agregar**.
3. En la ventana que se abre, en el campo **Puerto OpenFlow**, ingrese el número del puerto de OpenFlow que está creando en el conmutador virtual.
4. En el campo **Interfaz (alias)**, ingrese el alias de la interfaz de red creada, a la que se asigna la interfaz de SD-WAN del tipo WAN.
5. En el campo **Tasa máxima**, ingrese la velocidad máxima de la interfaz de SD-WAN del tipo WAN en Mbps. Rango de valores: de 1 a 100 000. El valor predeterminado es `1000`.

6. Configure la verificación de disponibilidad de la WAN a la que está conectada la interfaz de SD-WAN del tipo WAN:

   a. Especifique el host para verificar la disponibilidad de la WAN. Para hacerlo, en **Dirección IP para seguimiento**, ingrese la dirección IP del host y haga clic en **+ Agregar**.

      El host se especifica y se muestra en **Dirección IP para seguimiento**. Puede especificar varios hosts o eliminarlos. Para eliminar un host, haga clic en el ícono de eliminar ✕ junto a él.

   b. En el campo **Dirección IP para comprobar la fragmentación**, ingrese la dirección IPv4 del host hasta la cual se comprueba el soporte de la fragmentación. Valor predeterminado: `1.1.1.1`.

   c. En el campo **Confiabilidad**, ingrese el número mínimo de comprobaciones correctas que hacen que la WAN esté disponible. El valor predeterminado es `1`.

      Asegúrese de que la cantidad de hosts no exceda la cantidad de direcciones IP especificadas en **Dirección IP para seguimiento**. De lo contrario, la WAN siempre se considerará no disponible.

   d. En el campo **Intervalo (s)**, ingrese el intervalo de tiempo en segundos para la comprobación de la WAN. Rango de valores: 1 a 600. El valor predeterminado es `2`.

   e. En el campo **Conteo**, ingrese el número de solicitudes que se realizan a los hosts dentro de una comprobación de la WAN. Rango de valores: 1 a 600. El valor predeterminado es `2`.

   f. En el campo **Tiempo de espera**, ingrese el tiempo de espera para recibir una respuesta de los hosts, en milisegundos. Rango de valores: de 1 a 100 000. El valor predeterminado es `2000`.

   g. En el campo **Abajo**, ingrese el número de comprobaciones fallidas que hacen que la WAN no esté disponible. Rango de valores: 1 a 600. El valor predeterminado es `3`.

   h. En el campo **Arriba**, ingrese el número de comprobaciones exitosas que hacen que la WAN esté disponible. Rango de valores: 1 a 600. El valor predeterminado es `2`.

   i. En la lista desplegable **Supervisión de velocidad**, seleccione si se está midiendo la velocidad de la interfaz de SD-WAN del tipo WAN:

      - **Sí**.
      - **No**. Esta es la configuración predeterminada.

7. Si desea configurar colas de tráfico en la interfaz de SD-WAN del tipo WAN:

   a. Seleccione la pestaña **QoS**.

      Se muestra una tabla de colas de tráfico.

   b. En la columna **Reasignar ToS**, seleccione el valor Tipo de servicio de los encabezados externos de los paquetes de tráfico para cada cola.

c. En la columna **Tasa mínima (%)**, especifique el ancho de banda de tráfico mínimo para la cola como un porcentaje de la velocidad máxima de la interfaz de SD-WAN del tipo WAN. La suma total en una columna no puede ser mayor que 100.

d. En la columna **Tasa máxima (%)**, especifique el ancho de banda de tráfico máximo para la cola como un porcentaje de la velocidad máxima de la interfaz de SD-WAN del tipo WAN. Esta configuración se utiliza para evitar que el tráfico de las colas de alta prioridad se apropie indefinidamente del tráfico de las colas de baja prioridad.

La velocidad máxima de la interfaz de SD-WAN del tipo WAN se especifica en el paso 5 de estas instrucciones.

8. Si desea configurar el envío de información acerca de la interfaz de SD-WAN del tipo WAN al controlador, siga estos pasos:

   a. Seleccione la pestaña **NAT e infraestructura subyacente de WAN discontinua**.

   b. En la lista desplegable **Estado**, seleccione uno de los valores siguientes:

      - **Deshabilitado** si no desea que se envíe información sobre la interfaz de SD-WAN del tipo WAN al controlador. Esta es la configuración predeterminada.
      - **NAT/PAT** si la interfaz de SD-WAN del tipo WAN está detrás de NAT o PAT y necesita asignarle una dirección IP pública y un número de puerto UDP, que deben enviarse al controlador.
      - **Infraestructura subyacente de WAN discontinua** significa que la interfaz de SD-WAN del tipo WAN está conectada a una red aislada y la dirección IP de la interfaz de SD-WAN del tipo WAN debe pasarse al controlador.

   c. Si, en la lista desplegable **Estado**, seleccionó **NAT/PAT**, siga estos pasos:

      1. En el campo **Dirección IP real**, ingrese la dirección IPv4 pública de la interfaz de SD-WAN del tipo WAN.
      2. En el campo **Puerto UDP GENEVE real**, ingrese el número de puerto UDP de la interfaz de SD-WAN del tipo WAN. Rango de valores: de 1 a 65 535.

   d. Si, en la lista desplegable **Estado** seleccionó **Infraestructura subyacente de WAN discontinua**, ingrese la dirección IPv4 de la interfaz de SD-WAN del tipo WAN en el campo **Dirección IP**.

   e. Si es necesario, anule la tabla de enrutamiento y reenvío virtuales para la interfaz de SD-WAN del tipo WAN. Para hacer esto, habilite el conmutador **Asignar VRF**, luego, en la lista desplegable **VRF**, seleccione una tabla de enrutamiento y reenvío virtuales.

      Anular el VRF le permite configurar una ruta alternativa para la comunicación con el controlador. Por ejemplo, puede usar una interfaz del tipo LAN en lugar de la WAN predeterminada. El valor que especifique en la lista **VRF** tendrá efecto solo después de reiniciar el CPE o deshabilitar y habilitar la interfaz de red correspondiente.

9. Si las interfaces de SD-WAN del tipo WAN del dispositivo CPE están conectadas a diferentes redes, por ejemplo, Internet y una red MPLS privada, puede cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador en una conexión de SD-WAN individual del tipo WAN. Para hacerlo, haga lo siguiente:

   a. Seleccione la pestaña **Controladores**.

   b. Seleccione la casilla **Volver a escribir la dirección IP o el puerto del controlador**. Esta casilla está desactivada por defecto.

c. En la lista desplegable **Cantidad de controladores**, seleccione la cantidad de nodos de controlador.

> Debe especificar la cantidad de nodos de controlador que implementó cuando implementó la instancia SD-WAN. De lo contrario, se produce un error y la configuración no se modifica.

d. En el campo **Dirección IP**, ingrese la dirección IPv4 del nodo del controlador. La cantidad de campos corresponde al valor que seleccionó en la lista desplegable **Cantidad de controladores**.

e. En el campo **Puerto**, ingrese el número de puerto base del nodo del controlador. Rango de valores: de 1 a 65 535. El valor predeterminado es `6653`. La cantidad de campos corresponde al valor que seleccionó en la lista desplegable **Cantidad de controladores**.

Junto con el puerto base del nodo del controlador, los puertos con los siguientes tres números consecutivos se especifican automáticamente. Por ejemplo, si ingresa `6653` como número de puerto base, los puertos 6654, 6655 y 6656 se especifican automáticamente.

> Para que los cambios surtan efecto, debe reiniciar el dispositivo CPE después de cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador en la interfaz de SD-WAN del tipo WAN.

Puede cambiar las direcciones IP y los números de puerto TCP de los nodos del controlador mientras configura los nodos del controlador de una instancia SD-WAN. Esto cambia automáticamente las direcciones IP y los números de puerto TCP de los nodos del controlador en todos los dispositivos CPE que se agregan a la instancia SD-WAN. Las direcciones IP y los números de puerto TCP especificados en una interfaz de SD-WAN individual del tipo WAN tienen prioridad sobre las direcciones IP y los números de puerto TCP especificados cuando configura los nodos del controlador de la instancia SD-WAN.

10. Si es necesario, habilite la función FEC en la pestaña **Configuración del vínculo**.

11. Haga clic en **Crear**.

    La interfaz de SD-WAN del tipo WAN se crea y se muestra en la tabla.

12. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Editar una interfaz SD-WAN

Puede editar una interfaz de SD-WAN en una plantilla de CPE o en un dispositivo CPE. No puede editar el nombre de una interfaz de SD-WAN. Cuando edita una interfaz de SD-WAN del tipo LAN, solo puede configurar la velocidad máxima y las colas de tráfico. Una interfaz de SD-WAN editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una interfaz de SD-WAN, siga estos pasos:*

1. Edite una interfaz de SD-WAN de una de las siguientes maneras:

   - Si desea editar una interfaz de SD-WAN en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN**→ **Interfaces**.

   - Si desea editar una interfaz SD-WAN en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **SD-WAN**→ **Interfaces**. Si desea editar una interfaz de SD-WAN heredada de la plantilla CPE, seleccione la casilla **Anular** junto a esa interfaz de SD-WAN.

   Se muestra una tabla de interfaces SD-WAN.

2. Haga clic en **Editar** junto a la interfaz de SD-WAN que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la interfaz de SD-WAN. Para obtener una descripción de la configuración, consulte las instrucciones para crear una interfaz del tipo WAN.

4. Haga clic en **Guardar**.

   La interfaz de SD-WAN se modifica y actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Deshabilitar o habilitar una interfaz SD-WAN

Puede deshabilitar o habilitar una interfaz de SD-WAN en una plantilla de CPE o en un dispositivo CPE. Una interfaz de SD-WAN habilitada o deshabilitada en una plantilla de CPE se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE.

*Para deshabilitar o habilitar una interfaz de SD-WAN, siga estos pasos:*

1. Deshabilite o habilite una interfaz de SD-WAN de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar una interfaz de SD-WAN en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN**→ **Interfaces**.

   - Si desea habilitar o deshabilitar una interfaz de SD-WAN en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **SD-WAN**→ **Interfaces**. Si desea deshabilitar o habilitar una interfaz de SD-WAN heredada de la plantilla de CPE, seleccione la casilla de verificación **Anular** junto a esa interfaz de SD-WAN.

   Se muestra una tabla de interfaces SD-WAN.

2. Haga clic en **Deshabilitar** o **Habilitar** junto a la interfaz de SD-WAN que desea deshabilitar o habilitar.

   La interfaz de SD-WAN se deshabilita o habilita y se actualiza en la tabla.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Eliminación de una interfaz SD-WAN de tipo WAN

Puede eliminar una interfaz de SD-WAN del tipo WAN en una plantilla de CPE o en un dispositivo CPE. Una interfaz SD-WAN del tipo WAN eliminada en una plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. No puede eliminar una interfaz SD-WAN heredada de la plantilla de CPE en un dispositivo CPE o eliminar una interfaz SD-WAN del tipo LAN.

Las interfaces SD-WAN eliminadas del tipo WAN no se pueden restaurar.

*Para eliminar una interfaz SD-WAN del tipo WAN:*

1. Elimine una interfaz SD-WAN del tipo WAN de una de las siguientes maneras:

   - Si desea eliminar una interfaz SD-WAN del tipo WAN en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **SD-WAN → Interfaces**.

   - Si desea eliminar una interfaz SD-WAN del tipo WAN en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **SD-WAN → Interfaces**.

   Se muestra una tabla de interfaces SD-WAN.

2. Haga clic en **Eliminar** junto a la interfaz SD-WAN del tipo de WAN que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La interfaz SD-WAN del tipo WAN se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar interfaces de servicio

Las interfaces de servicio se asignan a los puertos de OpenFlow y se utilizan para conectar un dispositivo CPE a los servicios de transporte. Una interfaz de servicio no se puede asignar a un puerto de OpenFlow que ya está asignado a una interfaz de SD-WAN del tipo WAN.

Si desea filtrar los paquetes de tráfico en una interfaz de servicio, puede crear una interfaz de Lista de control de acceso (ACL) que se asigne a esta interfaz de servicio. La interfaz de ACL aplica el filtro de tráfico especificado a la interfaz de servicio. Se puede asignar una única interfaz de servicio a un máximo de cuatro interfaces de ACL.

Para ver la tabla de interfaces de servicio, vaya a la sección del menú **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador y vaya a la sección **Interfaces del servicio**. La información sobre las interfaces de servicio se muestra en las siguientes columnas de la tabla:

- **Puerto** es el número del puerto de OpenFlow al que está asignada la interfaz de servicio.
- **Tipo** es el tipo de clasificación de tráfico en la interfaz de servicio.
  - **Acceso**
  - **VLAN**
  - **Q-in-Q**
  - **ACL**
- **Descripción** es una descripción breve de la interfaz de servicio.
- **VLAN** es la etiqueta de VLAN externa de la interfaz de servicio. El valor de esta columna solo se muestra para las interfaces de servicio con los tipos de clasificación de tráfico **VLAN** y **Q-in-Q**.
- **VLAN interna** es la etiqueta de VLAN interna de la interfaz de servicio. El valor de esta columna solo se muestra para las interfaces de servicio que tienen el tipo de clasificación de tráfico **Q-in-Q**.
- **Filtro** es el filtro de tráfico para la interfaz de ACL. El valor de esta columna solo se muestra para las interfaces de servicio que tienen el tipo de clasificación de tráfico **ACL**.
- **Nombre** es la información sobre la interfaz de servicio:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una interfaz de servicio

*Para crear una interfaz de servicio:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración → Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Interfaces del servicio**.

   Se muestra una tabla de interfaces de servicio e interfaces de ACL.

4. En las listas desplegables **Conmutador** y **Puerto**, seleccione el dispositivo CPE y el puerto OpenFlow al que está asignada la interfaz de servicio.

5. Haga clic en **Crear una nueva**.

6. En la ventana que se abre, en la lista desplegable **Tipo**, seleccione el tipo de clasificación de tráfico en la interfaz de servicio:

   - **Acceso** Esta es la configuración predeterminada.
   - **VLAN** Si selecciona esta opción, en el campo **ID de VLAN**, ingrese la etiqueta de la VLAN externa de la interfaz de servicio. Rango de valores: 1 a 4094.
   - **Q-in-Q** Si selecciona esta opción, haga lo siguiente:

     a. En el campo **ID de VLAN**, ingrese la etiqueta de la VLAN externa de la interfaz de servicio. Rango de valores: 1 a 4094.

     b. En el campo **ID de VLAN interna**, ingrese la etiqueta de la VLAN interna de la interfaz de servicio. Rango de valores: 1 a 4094.

   - **ACL** se utiliza al crear una interfaz de ACL.

7. Si es necesario, ingrese una breve descripción de la interfaz de servicio en el campo **Descripción**.

8. Haga clic en **Crear**.

La interfaz de servicio se crea y se muestra en la tabla.

# Crear una interfaz de ACL

*Para crear una interfaz de ACL, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración → Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Interfaces del servicio**.

   Se muestra una tabla de interfaces de servicio e interfaces de ACL.

4. En las listas desplegables **Conmutador** y **Puerto**, seleccione el dispositivo CPE y el puerto de OpenFlow al que se asigna la interfaz de servicio creada.

5. Haga clic en **Crear una nueva**.

6. En la ventana que se abre, en la lista desplegable **Tipo**, seleccione **ACL**.

7. En la lista desplegable **Interfaz del servicio**, seleccione la interfaz de servicio a la que está asignada la interfaz de ACL.

8. En la lista desplegable **Filtro de tráfico**, seleccione el filtro de tráfico creado para la interfaz de ACL. Puede utilizar el mismo filtro de tráfico para varias interfaces de ACL.

9. En la lista desplegable **Secuencia**, seleccione el número secuencial de la interfaz de ACL. El tráfico se dirige primero a la interfaz de ACL con el número más bajo. Si el filtro utilizado en una interfaz de ACL no acepta el tráfico, este se envía a la segunda interfaz de ACL y así sucesivamente.

   Rango de valores: de 1 a 4. No se pueden asignar dos interfaces de ACL con el mismo número de serie a la misma interfaz de servicio.

10. Si es necesario, ingrese una breve descripción de la interfaz de ACL en el campo **Descripción**.

11. Haga clic en **Crear**.

La interfaz de ACL se crea y se muestra en la tabla.

# Ver el uso de una interfaz de servicio y una interfaz de ACL

Si es necesario, puede verificar qué servicios de transporte están utilizando una interfaz de servicio o una interfaz de ACL. Por ejemplo, una interfaz de servicio o una interfaz de ACL que está en uso no se puede eliminar.

*Para ver si se está utilizando una interfaz de servicio o una interfaz de ACL, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Interfaces del servicio**.

   Se muestra una tabla de interfaces de servicio e interfaces de ACL.

4. Haga clic en **Administración** → **Mostrar uso** junto a la interfaz de servicio o la interfaz de ACL para la que desea ver la información de uso.

Se abre una ventana con una tabla de servicios de transporte que utilizan la interfaz de servicio o la interfaz de ACL.

# Eliminar una interfaz de servicio o una interfaz de ACL

No puede eliminar una interfaz de servicio o una interfaz de ACL si al menos un servicio de transporte la está utilizando. Para eliminar una interfaz de servicio o una interfaz de ACL utilizada por los servicios de transporte, primero debe eliminar la interfaz de servicio o la interfaz de ACL de la configuración de los servicios de transporte. Puede comprobar qué servicios de transporte utilizan una interfaz de servicio o una interfaz de ACL.

Las interfaces de servicio y las interfaces de ACL eliminadas no se pueden restaurar.

*Para eliminar una interfaz de servicio o una interfaz de ACL, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Interfaces del servicio**.

   Se muestra una tabla de interfaces de servicio e interfaces de ACL.

4. Haga clic en **Administración** → **Eliminar** junto a la interfaz de servicio o la interfaz de ACL que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

La interfaz de servicio o la interfaz de ACL se elimina y ya no se muestra en la tabla.

# Administrar grupos de puertos OpenFlow

Los *puertos OpenFlow* son interfaces de la superposición SDN que se crean automáticamente al mismo tiempo que las interfaces de SD-WAN. El controlador utiliza los puertos OpenFlow para controlar el tráfico de red. Puede crear las interfaces de servicio y las UNI que se asignan a los puertos OpenFlow.

Los puertos OpenFlow se pueden combinar en grupos de puertos OpenFlow y utilizar cuando se crean servicios de transporte P2M y M2M. Cuando agrega un grupo de puertos OpenFlow a un servicio de transporte, esto crea automáticamente las interfaces de servicio asignadas a los puertos OpenFlow y, luego, estas interfaces de servicio se agregan al servicio de transporte. El uso de los grupos de puertos OpenFlow elimina la necesidad de crear interfaces de servicio manualmente y agregarlas a los servicios de transporte.

Para ver la tabla de los grupos de puertos OpenFlow, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Grupos de puertos OpenFlow**. La información sobre los grupos de los puertos OpenFlow se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del grupo de puertos OpenFlow.
- **Puertos OpenFlow** son puertos OpenFlow que se han agregado al grupo de puertos OpenFlow.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un grupo de puertos OpenFlow

*Para crear un grupo de puertos de OpenFlow, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Grupos de puertos OpenFlow**.

   Se muestra una tabla de grupos de puertos OpenFlow.

4. En la parte superior de la página, haga clic en **+ Grupo de puertos OpenFlow**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del grupo de puertos de OpenFlow.

6. En las listas desplegables **Conmutador** y **Puerto**, seleccione el dispositivo CPE y el puerto de OpenFlow que desea agregar al grupo de puertos de OpenFlow.

   Puede agregar varios puertos de OpenFlow o eliminarlos. Para eliminar un puerto de OpenFlow, haga clic en **Eliminar** junto a él.

7. Haga clic en **Crear**.

El grupo de puertos de OpenFlow se crea y se muestra en la tabla.

# Editar un grupo de puertos OpenFlow

*Para editar un grupo de puertos OpenFlow, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Grupos de puertos OpenFlow**.

   Se muestra una tabla de grupos de puertos OpenFlow.

4. Haga clic en **Administración** → **Editar** junto al grupo de los puertos OpenFlow que desea editar.

5. En la ventana que se abre, si es necesario, edite el nombre del grupo de puertos OpenFlow y agregue o elimine los puertos OpenFlow.

6. Haga clic en **Guardar**.

El grupo de puertos OpenFlow se modificará y actualizará en la tabla.

## Eliminar un grupo de puertos OpenFlow

Los grupos eliminados de puertos de OpenFlow no se pueden restaurar.

*Para eliminar un grupo de puertos de OpenFlow, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Grupos de puertos OpenFlow**.

   Se muestra una tabla de grupos de puertos OpenFlow.

4. Haga clic en **Administración** → **Eliminar** junto al grupo de puertos de OpenFlow que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El grupo de puertos de OpenFlow se elimina y ya no se muestra en la tabla.

# Configurar una UNI para la conexión de dispositivos CPE a los servicios de red

Las UNI se asignan a puertos OpenFlow y se utilizan para la conexión de un dispositivo CPE a los servicios de red. Una UNI no se puede asignar a un puerto OpenFlow que ya está asignado a una interfaz SD-WAN del tipo WAN.

Las plantillas de UNI se utilizan para la configuración centralizada de las UNI en dispositivos CPE. Para no crear una UNI en cada dispositivo CPE individual, puede crear una UNI en una plantilla de UNI y luego aplicar la plantilla de UNI a los dispositivos CPE cuando los agregue o registre manualmente. Si edita una UNI en una plantilla de UNI, la UNI se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de UNI.

Al crear una UNI, se crea automáticamente una interfaz de servicio para ella.

# Administrar plantillas de UNI

Puede ver la tabla de plantillas de UNI en la sección **SD-WAN → Plantillas de UNI**. La información sobre las plantillas de UNI se muestra en las siguientes columnas de la tabla:

- **Id** es el ID de la plantilla de UNI.
- **Nombre** es el nombre de la plantilla de UNI.
- **Utilizada** indica si los dispositivos CPE están utilizando la plantilla de UNI:
  - **Sí**.
  - **No**.
- **Actualizado** es la fecha y la hora en que se modificó por última vez la configuración de la plantilla de UNI.
- **Usuario** es el nombre del usuario que creó la plantilla de UNI.
- **Propietario** es el inquilino al que pertenece la plantilla de UNI.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede administrar la configuración de la plantilla de UNI en las siguientes pestañas:

- **Información** es la información básica sobre la plantilla de UNI. Puede editar el nombre de la plantilla de UNI en el campo **Nombre**.
- **UNI** contiene las UNI que se crearon en la plantilla de UNI.

## Crear una plantilla de UNI

*Para crear una plantilla de UNI:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de UNI**.

   Se muestra una tabla de plantillas de UNI.

2. En la parte superior de la página, haga clic en **+ Plantilla de UNI**.
3. En la ventana que se abre, ingrese el nombre de la plantilla de UNI.
4. Haga clic en **Crear**.

Se crea la plantilla de UNI y se muestra en la tabla.

Debe configurar la plantilla de UNI creada. Para obtener más información sobre la administración de plantillas de UNI, consulte Administración de plantillas de UNI.

## Eliminar una plantilla de UNI

Las plantillas de UNI eliminadas no se pueden restaurar.

*Para eliminar una plantilla de UNI, siga estos pasos:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de UNI**.

   Se muestra una tabla de plantillas de UNI.

2. Seleccione la plantilla de UNI que desea eliminar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra el nombre de la plantilla de UNI y el inquilino al que está asignada la plantilla de UNI.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

La plantilla de UNI se elimina y ya no se muestra en la tabla.

# Administrar las UNI

### Administrar las UNI en una plantilla de UNI

Para ver la tabla de las UNI en una plantilla de UNI, vaya a la sección del menú **SD-WAN → Plantillas de UNI**, haga clic en la plantilla de UNI y seleccione la pestaña **UNI**. La información sobre las UNI se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la UNI.
- **Puerto OpenFlow** es el número del puerto de OpenFlow asignado a la UNI.
- **Clasificación** es el tipo de clasificación de tráfico en la UNI:
  - **Acceso**
  - **VLAN**
  - **Q-in-Q**
- **Acciones** contiene las acciones que se pueden realizar con la UNI.

### Administrar las UNI en un dispositivo CPE

Para ver la lista de las UNI en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **UNI**.

# Crear una UNI

Puede crear una UNI en una plantilla de UNI o en un dispositivo CPE. Una UNI creada en la plantilla de UNI se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de UNI.

*Para crear una UNI, siga estos pasos*

1. Cree una UNI de una de las siguientes maneras:

   - Si desea crear una UNI en una plantilla de UNI, vaya a la sección del menú **SD-WAN** → **Plantillas de UNI**, haga clic en la plantilla de UNI y seleccione la pestaña **UNI**.
   - Si desea crear una UNI en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **UNI**.

   Se muestra una tabla o lista de las UNI.

2. Haga clic en **+ UNI**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la UNI.
4. Especifique el puerto de OpenFlow al que se asigna la UNI de una de las siguientes maneras:

   - Si está creando una UNI en una plantilla de UNI, ingrese el número de puerto de OpenFlow en el campo **Puerto OpenFlow**.
   - Si creará una UNI en un dispositivo CPE, seleccione el puerto de OpenFlow en la lista desplegable **Puerto**.

5. En la lista desplegable **Clasificación**, seleccione el tipo de clasificación de tráfico de la UNI:

   - **Acceso** Esta es la configuración predeterminada.
   - **VLAN**Si selecciona esta opción, en el campo **ID de VLAN**, ingrese la etiqueta VLAN externa de la UNI. Rango de valores: 1 a 4094.
   - **Q-in-Q** Si selecciona esta opción, haga lo siguiente:

     a. En el campo **ID de VLAN**, ingrese la etiqueta de VLAN externa de la UNI. Rango de valores: 1 a 4094.

     b. En el campo **ID de VLAN interna**, ingrese la etiqueta de VLAN interna de la UNI. Rango de valores: 1 a 4094.

6. Si creará una UNI en un dispositivo CPE, en la lista desplegable **QoS**, seleccione una regla de calidad de servicio creada para la UNI.
7. Haga clic en **Crear**.

   La UNI se crea y se muestra en la tabla o lista.

8. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de UNI o el dispositivo CPE.

## Ver el uso de la UNI

Si es necesario, puede verificar qué servicios de red están utilizando la UNI en un dispositivo CPE. Por ejemplo, si se utiliza una plantilla de UNI, no se puede eliminar.

*Para ver si se está utilizando una plantilla UNI, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ver el uso de la UNI.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **UNI**.

   Se muestra una lista de UNI.

4. Haga clic en **Administración** → **Mostrar uso** junto a la UNI cuyo uso desea ver.

Se abre una ventana con una tabla de servicios de red que utilizan la UNI.

## Editar una UNI

Puede editar una UNI en una plantilla de UNI. Una UNI editada en la plantilla de UNI se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de UNI.

*Para editar una UNI, haga lo siguiente:*

1. En el menú, vaya a la subsección **SD-WAN** → **Plantillas de UNI**.

   Se muestra una tabla de plantillas de UNI.

2. Haga clic en la plantilla de UNI en la que desea editar una UNI.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra el nombre de la plantilla de UNI y el inquilino al que está asignada la plantilla de UNI.

3. Seleccione la pestaña **UNI**.

   Se muestra una tabla de UNI.

4. Haga clic en **Editar** junto a la UNI que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración de la UNI. Para obtener una descripción de la configuración, consulte las instrucciones para crear una UNI.

6. Haga clic en **Guardar**.

   La UNI se modificará y actualizará en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla UNI.

## Eliminar una UNI

Puede eliminar una UNI en una plantilla de UNI o en un dispositivo CPE. Una UNI eliminada en la plantilla UNI se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla UNI.

Las UNI eliminadas no se pueden restaurar.

### Eliminación de una UNI en una plantilla de UNI

*Para eliminar una UNI en una plantilla de UNI:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de UNI**.

   Se muestra una tabla de plantillas de UNI.

2. Haga clic en la plantilla de UNI en la que desea eliminar una UNI.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra el nombre de la plantilla de UNI y el inquilino al que está asignada la plantilla de UNI.

3. Seleccione la pestaña **UNI**.

   Se muestra una tabla de UNI.

4. Haga clic en **Eliminar** junto a la UNI que desea eliminar.

   La UNI se elimina y ya no se muestra en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla UNI.

### Eliminación de una UNI en un dispositivo CPE

No puede eliminar una UNI si está siendo utilizada por al menos un servicio de red. Para eliminar una UNI que están utilizando los servicios de red, primero debe eliminar la UNI de la topología de servicios de red. Puede comprobar qué servicios de red están utilizando la UNI.

*Para eliminar una UNI en un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea eliminar una UNI.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **UNI**.

   Se muestra una lista de UNI.

4. Haga clic en **Administración** → **Eliminar** junto a la UNI que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

   La UNI se elimina y ya no se muestra en la tabla.

6. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Agregar una ruta estática

Además del intercambio de rutas dinámicas entre los dispositivos CPE y los dispositivos de red externos mediante los protocolos de BGP y OSPF, Kaspersky SD-WAN admite las rutas IPv4 estáticas. Puede agregar una ruta estática a una plantilla de CPE o a un dispositivo CPE. La ruta estática que es agregada a la plantilla de CPE se agrega automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para agregar una ruta estática, haga lo siguiente:*

1. Agregue una ruta estática de una de las siguientes maneras:

   - Si desea agregar una ruta estática a una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Rutas estáticas**.
   - Si desea agregar una ruta estática a un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Rutas estáticas** y seleccione la casilla de verificación **Anular**.

   Se mostrará una tabla de rutas estáticas.

2. Haga clic en **+ Agregar**.

3. En la lista desplegable **VRF**, seleccione una tabla de enrutamiento y reenvío virtuales. Esta configuración es obligatoria.

4. En la lista desplegable **Interfaz**, seleccione la interfaz de red de origen creada de la ruta estática. Esta configuración es obligatoria si el VRF principal/254 se selecciona como la tabla de enrutamiento y reenvío virtuales.

   La lista de interfaces que se puede seleccionar depende del VRF seleccionado en el paso anterior. Puede seleccionar solamente aquellas interfaces que pertenezcan al VRF seleccionado que no sea principal/254, y cualquier interfaz de VRF principal/254.

5. En el campo **Destino**, ingrese la dirección IPv4 de destino de la ruta estática.

6. Si es necesario, en el campo **Máscara de red de IPv4**, ingrese la dirección IPv4 de la subred de destino de la ruta estática.

7. En el campo **Gateway**, ingrese la dirección IPv4 de la puerta de enlace de la ruta estática.

   No se puede especificar un valor en este campo si en la lista **Tipo** se seleccionó el tipo de ruta de **agujero negro**.

8. En el campo **Métrica**, ingrese una métrica para la ruta estática. El valor predeterminado es `0`.

   No se puede especificar un valor en este campo si en la lista **Tipo** se seleccionó el tipo de ruta de **agujero negro** o si la ruta estática se creó en una tabla de enrutamiento y reenvío virtuales que no sea el VRF principal/254.

9. En el campo **MTU**, ingrese el valor de MTU para la ruta estática.

   No se puede especificar un valor en este campo si en la lista **Tipo** se seleccionó el tipo de ruta de **agujero negro** o si la ruta estática se creó en una tabla de enrutamiento y reenvío virtuales que no sea el VRF principal/254.

10. En el campo **AD**, ingrese la distancia administrativa para la ruta estática.

    No se puede especificar un valor en este campo si la ruta estática se creó en el VRF principal/254. El valor predeterminado es `1`.

    Para ver la tabla de correspondencias entre las distancias administrativas y los protocolos de enrutamiento, consulte el artículo correspondiente.

11. En la lista desplegable **Tipo**, seleccione el tipo de la ruta estática:

    - **unidifusión**. Esta es la configuración predeterminada.
    - **local** Solo para el VRF principal/254.
    - **difusión** Solo para el VRF principal/254.
    - **multidifusión** Solo para el VRF principal/254.
    - **inalcanzable** Solo para el VRF principal/254.
    - **prohibido** Solo para el VRF principal/254.
    - **cualquier difusión** Solo para el VRF principal/254.
    - **agujero negro**

      Si selecciona el tipo de ruta de **agujero negro**, los campos **Gateway**, **Métrica** y **MTU** se deshabilitan.

      Si necesita utilizar la ruta de agujero negro predeterminada, 0.0.0.0/0, para aislar las rutas entre los VRF, agréguela al VRF correspondiente en la pestaña **VRF** en la sección **SD-WAN → Plantillas de CPE** o **SD-WAN → CPE** seleccionando **Agregar ruta de agujero negro**. Si intenta agregar dicha ruta en la pestaña **Rutas estáticas**, aparecerá un mensaje de error.

Se agrega la ruta estática y se muestra en la tabla. Puede agregar varias rutas estáticas o eliminar rutas estáticas. Para eliminar una ruta estática, haga clic en el ícono de eliminar ✕ junto a ella.

12. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Tabla de correspondencia de distancias administrativas y protocolos de enrutamiento

| Protocolo | Distancia |
|---|---|
| Sistema | 0 |
| Kernel | 0 |
| Conexión | 0 |
| Estática | 1 |
| NHRP | 10 |
| EBGP | 20 |
| EIGRP | 90 |
| BABEL | 100 |
| OSPF | 110 |
| ISIS | 115 |
| OPENFABRIC | 115 |
| RIP | 120 |
| Tabla | 150 |
| SHARP | 150 |
| IBGP | 200 |
| PBR | 200 |

# Filtrar rutas y paquetes de tráfico

Puede utilizar los siguientes mecanismos para filtrar rutas cuando se trabaja con los protocolos BGP y OSPF, y para filtrar paquetes de tráfico cuando se trabaja con el protocolo PIM:

- Las listas de control de acceso (ACL) permiten o deniegan los prefijos IPv4 especificados.
- Las listas de prefijos son una versión ampliada de las listas de control de acceso. Estas también permiten o bloquean prefijos IPv4 en el rango de longitud de prefijo especificado. Puede utilizar listas de prefijos en mapas de ruta.
- Las listas de comunidades permiten administrar prefijos en función de marcas. Puede utilizar listas de comunidades en mapas de ruta.
- Los mapas de ruta son una versión ampliada de las listas de prefijos. Los mapas de ruta modifican adicionalmente los valores de los atributos.

Puede crear reglas en listas de control de acceso, listas de prefijos, listas de comunidades y mapas de ruta. Cada regla está numerada. La regla con el número de secuencia más bajo es la primera que se aplica a un prefijo IPv4. Si no se puede aplicar ninguna de las reglas, se deniega el prefijo IPv4.

Los mecanismos de filtrado de rutas que se describen a continuación se pueden utilizar en diferentes escenarios de enrutamiento, por ejemplo:

- Para distribuir el tráfico a través de los vínculos, simplificar el equilibrio de carga y las directivas de conmutación por error
- Para enviar tráfico de diferentes subredes (o aplicaciones) a un vínculo decidido de antemano
- Para enrutar el tráfico a ciertos servicios corporativos (por ejemplo, centros de datos) a través de un vínculo más rápido/más costoso, y el resto del tráfico a través de un vínculo más económico
- Para hacer que uno de los vínculos sea menos atractivo para los proveedores externos mediante un AS-Path más largo a sus rutas

# Administrar listas de control de acceso (ACL)

Puede ver la tabla de listas de control de acceso en una plantilla de CPE y en un dispositivo CPE, siga estos pasos:

- Para ver la tabla de listas de control de acceso en una plantilla de CPE, vaya a la sección del menú **SD-WAN**→ **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento**→ **Listas de control de acceso**.
- Para ver la tabla de listas de control de acceso en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Filtros de enrutamiento**→ **Listas de control de acceso**.

La información sobre las listas de control de acceso se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la lista de control de acceso.
- **Heredado** indica si la lista de control de acceso se hereda de la plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Secuencia** es el número de secuencia de la regla en la lista de control de acceso. La regla con el número de secuencia más bajo es la primera que la lista de control de acceso aplica al prefijo IPv4.
- **Red** es el prefijo IPv4 al que la lista de control de acceso aplica la regla.
- **Acción** es la acción que realiza la regla en el prefijo IPv4:
  - **Permitir** permite el prefijo IPv4.
  - **Denegar** bloquea el prefijo IPv4.
- **Administración** contiene las acciones que se pueden realizar en la lista de control de acceso.

# Creación de una lista de control de acceso

Puede crear una lista de control de acceso en una plantilla de CPE o en un dispositivo CPE. Una lista de control de acceso creada en la plantilla CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla CPE.

*Para crear una lista de control de acceso:*

1. Cree una lista de control de acceso de una de las siguientes maneras:

   - Si desea crear una lista de control de acceso en una plantilla CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Filtros de enrutamiento→ Listas de control de acceso**.

   - Si desea crear una lista de control de acceso en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Filtros de enrutamiento→ Listas de control de acceso** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de listas de control de acceso.

2. Haga clic en **+ Lista de control de acceso**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la lista de control de acceso. La longitud máxima del nombre es de 50 caracteres. No utilice espacios en este campo.

4. Crear una regla en la lista de control de acceso:

   a. Haga clic en **+ Regla**.

   b. En el campo **Secuencia**, escriba el número de secuencia de la regla. La regla con el número de secuencia más bajo es la primera en ser aplicada al prefijo IPv4 por la lista de control de acceso. Rango de valores: 1 a 4,294,967,295.

   c. En la lista desplegable **Red**, seleccione el tipo de regla:

      - **Cualquier red** para una regla que permite o deniega todos los prefijos IPv4.

      - **Máscara/dirección IP** para una regla que permite o deniega el prefijo IPv4 especificado. Esta es la configuración predeterminada. Si selecciona este valor, ingrese el prefijo IPv4 en el campo que se muestra.

   d. En la lista desplegable **Acción**, seleccione la acción que realiza la regla con el prefijo IPv4:

      - **Permitir** permite el prefijo IPv4. Esta es la configuración predeterminada.

      - **Denegar** bloquea el prefijo IPv4.

   Se crea la regla. Puede crear varias reglas o eliminarlas. Para eliminar una regla, haga clic en el ícono de eliminar ✕ junto a él.

5. Haga clic en **Crear**.

   La lista de control de acceso se crea y se muestra en la tabla.

6. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar una lista de control de acceso

Puede editar una lista de control de acceso en una plantilla de CPE o en un dispositivo CPE. Una lista de control de acceso editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una lista de control de acceso, haga lo siguiente:*

1. Edite una lista de control de acceso de una de las siguientes maneras:

   - Si desea editar una lista de control de acceso en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento → Listas de control de acceso**.

   - Si desea editar una lista de control de acceso en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento → Listas de control de acceso** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de listas de control de acceso.

2. Haga clic en **Editar** junto a la lista de control de acceso que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la lista de control de acceso. Para obtener una descripción de la configuración, consulte las instrucciones para crear una lista de control de acceso.

4. Haga clic en **Guardar**.

   La lista de control de acceso se modificará y se actualizará en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una lista de control de acceso

Puede eliminar una lista de control de acceso en una plantilla de CPE o en un dispositivo CPE. Una lista de control de acceso eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos de CPE que usan esta plantilla de CPE.

Las listas de control de acceso eliminadas no se pueden restaurar.

*Para eliminar una lista de control de acceso:*

1. Elimine una lista de control de acceso de una de las siguientes maneras:

   - Si desea eliminar una lista de control de acceso en una plantilla CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento → Listas de control de acceso**.

   - Si desea eliminar una lista de control de acceso en un dispositivo CPE, vaya a la sección del menú**SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Filtros de enrutamiento → Listas de control de acceso** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de listas de control de acceso.

2. Haga clic en **Eliminar** junto a la lista de control de acceso que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La lista de control de acceso se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar listas de prefijos

Puede ver la tabla de listas de prefijos en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de listas de prefijos en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento→ Listas de prefijos**.

- Para ver la tabla de listas de prefijos en un dispositivo de CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Filtros de enrutamiento→ Listas de prefijos**.

La información sobre las listas de prefijos se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la lista de prefijos.

- **Heredado** indica si la lista de prefijos se hereda de la plantilla CPE:

  - **Sí**.

  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.

- **Secuencia** es el número de secuencia de la regla en la lista de prefijos. La regla con el número de secuencia más bajo es la primera que la lista de prefijos aplica al prefijo IPv4.

- **Red** es el prefijo IPv4 al que la lista de prefijos aplica la regla.

- **Acción** es la acción que realiza la regla en el prefijo IPv4:
  - **Permitir** permite el prefijo IPv4.
  - **Denegar** bloquea el prefijo IPv4.
- **Mayor o igual a** es el valor inicial del rango de longitud del prefijo al que la lista de prefijos aplica la regla.
- **Menor o igual a** es el valor final del rango de longitud del prefijo al que la lista de prefijos aplica la regla.
- **Administración** contiene las acciones que se pueden realizar en la lista de prefijos.

## Crear una lista de prefijos

Puede crear una lista de prefijos en una plantilla de CPE o en un dispositivo CPE. Una lista de prefijos creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una lista de prefijos, siga estos pasos:*

1. Cree una lista de prefijos de una de las siguientes maneras:
   - Si desea crear una lista de prefijos en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento→ Listas de prefijos**.
   - Si desea crear una lista de prefijos en un dispositivo CPE, vaya a la sección del menú **SD-WAN**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento→ Listas de prefijos** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de listas de prefijos.
2. Haga clic en **+ Lista de prefijos**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la lista de prefijos. La longitud máxima del nombre es de 50 caracteres. No utilice espacios en este campo.
4. Cree una regla en la lista de prefijos:
   a. haga clic en **+ Regla**.
   b. En el campo **Secuencia**, escriba el número de secuencia de la regla. La regla con el número de secuencia más bajo es la primera que la lista de prefijos aplica al prefijo IPv4. Rango de valores: 1 a 4,294,967,295.
   c. En la lista desplegable **Red**, seleccione el tipo de regla:
      - **Cualquier red** para una regla que permite o deniega todos los prefijos IPv4.
      - **Máscara/dirección IP** para una regla que permite o deniega el prefijo IPv4 especificado. Esta es la configuración predeterminada. Si selecciona este valor, ingrese el prefijo IPv4 en el campo que se muestra.

d. En la lista desplegable **Acción**, seleccione la acción que realiza la regla con el prefijo IPv4:

- **Permitir** permite el prefijo IPv4. Esta es la configuración predeterminada.
- **Denegar** bloquea el prefijo IPv4.

e. En el campo **Mayor o igual a**, ingrese el valor inicial del rango de longitud del prefijo al que la lista de prefijos aplica la regla. Rango de valores: de 0 a 32.

f. En el campo **Menor o igual a**, ingrese el valor final del rango de longitud del prefijo al que la lista de prefijos aplica la regla. Rango de valores: de 0 a 32.

Se crea la regla. Puede crear varias reglas o eliminarlas. Para eliminar una regla, haga clic en el ícono de eliminar ✕ junto a él.

5. Haga clic en **Crear**.

   La lista de prefijos se crea y se muestra en la tabla.

6. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar una lista de prefijos

Puede editar una lista de prefijos en una plantilla de CPE o en un dispositivo CPE. Una lista de prefijos editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una lista de prefijos, siga estos pasos:*

1. Edite una lista de prefijos de una de las siguientes maneras:

   - Si desea editar una lista de prefijos en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la ficha **Filtros de enrutamiento** → **Listas de prefijos**.
   - Si desea editar una lista de prefijos en un dispositivo CPE, vaya a la sección del menú **SD-WAN**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento**→ **Listas de prefijos**y marque la casilla de verificación **Anular**.

   Se muestra una tabla de listas de prefijos.

2. Haga clic en **Editar** junto a la lista de prefijos que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la lista de prefijos. Para obtener una descripción de la configuración, consulte las instrucciones para crear una lista de prefijos.

4. Haga clic en **Guardar**.

   La lista de prefijos se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una lista de prefijos

Puede eliminar una lista de prefijos en una plantilla de CPE o en un dispositivo CPE. Una lista de prefijos eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla.

Las listas de prefijos eliminadas no se pueden restaurar.

*Para eliminar una lista de prefijos:*

1. Elimine una lista de prefijos de una de las siguientes maneras:

   - Si desea eliminar una lista de prefijos en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Filtros de enrutamiento** → **Listas de prefijos**.

   - Si desea eliminar una lista de prefijos en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento**→ **Listas de prefijos** y la casilla **Anular**.

   Se muestra una tabla de listas de prefijos.

2. Haga clic en **Eliminar** junto a la lista de prefijos que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La lista de prefijos se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar listas de comunidades

Puede ver la tabla de listas de comunidad en una plantilla de CPE y en un dispositivo CPE:

Para ver la tabla de listas de comunidades en una plantilla de CPE, vaya a la sección de menú SD-WAN → Plantillas de CPE, haga clic en la plantilla de CPE y seleccione la pestaña Enrutamiento → Filtros de enrutamiento → Listas de comunidades.

Para ver la tabla de listas de comunidades en un dispositivo CPE, vaya a la sección de menú SD-WAN → CPE, haga clic en el dispositivo CPE y seleccione la pestaña Enrutamiento → Filtros de enrutamiento → Listas de comunidades.

La información acerca de las listas de comunidades se muestra en las siguientes columnas de la tabla:

"Nombre" es el nombre de la lista de comunidades

Anular:

"Sí" significa que la configuración de las listas de comunidades es única y no se hereda de una plantilla.

"No" significa que la configuración de la lista de comunidades se hereda de la plantilla.

Esta columna se muestra solo en el dispositivo CPE. Puede cambiar el valor de esta columna para cada lista de comunidades directamente en la tabla.

"Heredado" indica si la lista de comunidades se hereda de la plantilla de CPE:

Sí

No

Esta columna se muestra solo en el dispositivo CPE.

"Tipo" es el tipo de lista de la comunidades, estándar o avanzada.

"Secuencia" es el número de secuencia de la regla en la lista de comunidades. La lista de comunidades aplica la regla con el número más bajo primero.

"Acción" es la acción que realiza la regla con el valor de "comunidad":

"Permitir" permite la comunidad

"Denegar" deniega la comunidad

"Valor" marca el prefijo IPv4, lo que permite que se le apliquen directivas.

Crear una lista de comunidades

Puede crear una lista de comunidades en una plantilla de CPE o en un dispositivo CPE.

Cree una lista de comunidades de una de las siguientes maneras:

Si desea crear una lista de comunidades en una plantilla de CPE, vaya a la sección SD-WAN → Plantillas de CPE → Enrutamiento → Filtros de enrutamiento → Listas de comunidades, y en la parte superior de la página, haga clic en el botón "+ Agregar".

Si desea crear una lista de comunidades en un dispositivo CPE, vaya a la sección SD-WAN → CPE, seleccione la pestaña Enrutamiento → Filtros de enrutamiento → Listas de comunidades, y en la parte superior de la página, haga clic en el botón "+ Agregar".

Se muestra una tabla de listas de comunidades.

En la ventana que se muestra, en el campo "Nombre", ingrese el nombre de la lista de comunidades. La longitud máxima del nombre es de 50 caracteres.

Tenga en cuenta que el nombre de la lista de comunidades debe ser único dentro de un inquilino.

En el campo "Tipo", seleccione el tipo de comunidad estándar (coincidencia estricta de valor) o avanzada (coincidencia de expresión regular).

Ahora, haga clic en "+ Agregar" para agregar registros de la comunidad a la lista.

El campo "Orden de registros de la comunidad" genera automáticamente números con un paso de 10, comenzando con 10. Puede cambiar el número de secuencia (y el orden en que se aplican los registros) mediante el elemento de menú "Contador".

A continuación, seleccione una "Acción" para el registro de la comunidad: "Denegar" o "Permitir".

Tipo de comunidad estándar

Para ingresar los valores de la comunidad, selecciónelos de la lista desplegable o ingréselos como una lista de valores de texto. Una comunidad también se puede especificar como un valor numérico en el formato <número de 0 a 65535>:<número de 0 a 65535>. Es posible combinar valores personalizados y valores predeterminados.

Tipo de comunidad avanzada

A continuación, puede ingresar valores de comunidad como una expresión regular.

Si desea eliminar un registro de la comunidad de la lista, seleccione su casilla y haga clic en el botón "Eliminar".

Ahora, la lista de la comunidad creada se puede usar en las instrucciones "match" o "set" dentro del mapa de ruta para manipular los prefijos BGP (vínculo a la sección "Administrar mapas de ruta").

Editar una lista de comunidades

Para editar una lista de comunidades, seleccione su casilla y haga clic en el botón "Editar" o haga clic en el nombre de la lista de comunidades.

Ahora puede agregar o eliminar registros de la lista de comunidades.

Eliminar una lista de comunidades

Para eliminar una lista de comunidades, seleccione su casilla y haga clic en el botón "Eliminar". Solo puede eliminar una lista a la vez.

## Crear una lista de comunidades

Puede crear listas de comunidades en una plantilla de CPE o en un dispositivo CPE. Las listas de comunidades creadas en la plantilla de CPE se crean automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una lista de comunidades, siga estos pasos:*

1. Cree una lista de comunidades de una de las siguientes maneras:

   - Si desea crear una lista de comunidades en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.

   - Si desea crear una lista de comunidades en un dispositivo CPE, vaya a la sección del menú **SD-WAN**, haga clic en el dispositivo CPE, seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.

   Se muestra una tabla de listas de comunidades.

2. Haga clic en **+ Agregar**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la lista de comunidades. La longitud máxima del nombre es de 50 caracteres. No utilice espacios en este campo.

   El nombre de la lista de comunidades debe ser exclusivo dentro del inquilino.

4. En la lista desplegable **Tipo**, seleccione el tipo de lista de comunidades:

   - **Standard**

     Las rutas se vinculan en función de las coincidencias exactas de los valores de los atributos de la comunidad.

   - **Extended**

     Las rutas se vinculan según las expresiones regulares.

5. Cree una regla en la lista de comunidades:

   a. Haga clic en **+ Agregar**.

   b. En el campo **Secuencia**, escriba el número de secuencia de la regla. La regla con el número de secuencia más bajo es la primera que la lista de comunidades aplica al prefijo IPv4. Rango de valores: 1 a 4 294 967 295.

   c. En la lista desplegable **Acción**, seleccione la acción que realiza la regla en el prefijo IPv4:

      - **Permitir** permite el prefijo IPv4. Esta es la configuración predeterminada.

      - **Denegar** bloquea el prefijo IPv4.

   d. Especifique el criterio de filtrado que la regla aplicará a las rutas:

      - Para listas de comunidades estándar, en la columna **Comunidad**, especifique uno o más atributos de la comunidad seleccionando valores predefinidos de la lista desplegable o ingresando manualmente valores de texto o valores en el formato <número de 0 a 65535>:<número de 0 a 65535>. Puede combinar valores ingresados manualmente y valores predefinidos.

        Los siguientes valores predefinidos están disponibles:

        - `local-AS`
        - `no-advertise`
        - `no-export`
        - `internet`
        - `graceful-shutdown`
        - `accept-own-nexthop`
        - `accept-own`
        - `route-filter-translated-v4`
        - `route-filter-v4`

- `route-filter-translated-v6`
- `route-filter-v6`
- `llgr-stale`
- `no-llgr`
- `agujero negro`
- `no-peer`

- Para listas de comunidades extendidas, en el campo de la columna **Expresión regular**, ingrese una expresión regular BGP para especificar los límites de los números AS. La sintaxis de expresiones regulares BGP es un subconjunto de la sintaxis de expresiones regulares POSIX y utiliza el carácter de guion bajo "_" para representar espacios, comas, delimitadores de conjuntos AS { }, delimitadores de confederaciones AS ( ) y el inicio y el final de una línea.

Se crea la regla. Puede crear varias reglas o eliminarlas. Para eliminar una regla, haga clic en el ícono de eliminar junto a él.

6. Haga clic en **Crear**.

   La lista de comunidades se crea y se muestra en la tabla.

   Puede utilizar la lista de comunidades generada en los mapas de ruta para vincular por prefijo o para cambiar los atributos del prefijo.

7. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar una lista de comunidades

Puede editar una lista de comunidades en una plantilla de CPE o en un dispositivo CPE. Las listas de comunidades editadas en la plantilla de CPE se modifican automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una lista de comunidades, siga estos pasos:*

1. Edite una lista de comunidades de una de las siguientes maneras:

   - Si desea editar una lista de comunidades en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.
   - Si desea editar una lista de comunidades en un dispositivo CPE, vaya a la sección del menú **SD-WAN**, haga clic en el dispositivo CPE, seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.

   Se muestra una tabla de listas de comunidades.

2. Haga clic en el nombre de la lista de comunidades que desea editar o selecciónela en la tabla y haga clic en el botón **Editar**.

3. En la ventana que se abre, si es necesario, edite la configuración de la lista de comunidades. Para obtener una descripción de la configuración, consulte las instrucciones para crear una lista de comunidades.

4. Haga clic en **Guardar**.

   La lista de comunidades se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una lista de comunidades

Puede eliminar listas de comunidades en una plantilla de CPE o en un dispositivo CPE. Las listas de comunidades eliminadas en la plantilla de CPE se eliminan automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE.

Las listas de comunidades eliminadas no se pueden restaurar.

*Para eliminar una lista de comunidades:*

1. Elimine una lista de comunidades de una de las siguientes maneras:

   - Si desea eliminar una lista de comunidades en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.

   - Si desea eliminar una lista de comunidades en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Enrutamiento** → **Filtros de enrutamiento** → **Listas de comunidad**.

   Se muestra una tabla de listas de comunidades.

2. En la tabla, seleccione la lista de comunidades que desea eliminar y haga clic en el botón **Eliminar**.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La lista de comunidades se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar mapas de rutas

Puede ver la tabla de mapas de ruta en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de mapas de ruta en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento** → **Mapas de ruta**.
- Para ver la tabla de mapas de ruta en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Filtros de enrutamiento** → **Mapas de ruta**.

La información sobre los mapas de ruta se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del mapa de ruta.
- **Heredado** indica si el mapa de ruta se hereda de la plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Secuencia** es el número de secuencia de la regla en el mapa de ruta. La regla con el número de secuencia más bajo es la primera en ser aplicada al prefijo IPv4 por el mapa de ruta.
- **Acción** es la acción que realiza la regla en el prefijo IPv4:
  - **Permitir** permite el prefijo IPv4.
  - **Denegar** bloquea el prefijo IPv4.
- **Tipo de coincidencia** es el criterio que hace que el mapa de ruta aplique la regla al prefijo IPv4:
  - **Ninguna** aplica la regla a todos los prefijos IPv4.
  - **Prefix-List** aplica la regla a los prefijos IPv4 permitidos por la lista de prefijos especificada.
  - **Lista de comunidades** aplica la regla a los prefijos IPv4 permitidos por la lista de comunidades especificada.
- **Valor** es un prefijo IPv4 que la lista de prefijos debe permitir para que el mapa de ruta aplique la regla al prefijo IPv4. Esta columna muestra un valor solo si la columna **Tipo de coincidencia** muestra **Prefix-List**.
- **Cambiar atributo** es el atributo cuyo valor cambia la regla.
- **Nuevo valor** es el valor que establece la regla para el atributo.
- **Administración** contiene las acciones que se pueden realizar con el mapa de ruta.

# Crear un mapa de ruta

Puede crear un mapa de ruta en una plantilla de CPE o en un dispositivo CPE. Un mapa de ruta creado en la plantilla CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla CPE.

*Para crear un mapa de ruta:*

1. Cree un mapa de ruta de una de las siguientes maneras:

   - Si desea crear un mapa de ruta en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Filtros de enrutamiento → Mapas de ruta**.

   - Si desea crear un mapa de ruta en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento→ Mapas de ruta** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de mapas de ruta.

2. Haga clic en **+ Mapa de ruta**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del mapa de ruta. La longitud máxima del nombre es de 50 caracteres. No utilice espacios en este campo.

4. Cree una regla en el mapa de ruta:

   a. haga clic en **+ Regla**.

   b. En el campo **Secuencia**, escriba el número de secuencia de la regla. La regla con el número de secuencia más bajo es la primera en ser aplicada al prefijo IPv4 por el mapa de ruta. Rango de valores: 1 a 4 294 967 295.

   c. En la lista desplegable **Acción**, seleccione la acción que realiza la regla en el prefijo IPv4:

      - **Permitir** permite el prefijo IPv4. Esta es la configuración predeterminada.

      - **Denegar** bloquea el prefijo IPv4.

   d. En la lista desplegable **Tipo de coincidencia**, seleccione el criterio que hace que el mapa de ruta aplique la regla al prefijo IPv4:

      - **Ninguna** aplica la regla a todos los prefijos IPv4. Esta es la configuración predeterminada.

      - **Prefix-List** aplica la regla a los prefijos IPv4 permitidos por la lista de prefijos especificada. Si selecciona este valor, en la lista desplegable **Lista de prefijos**, seleccione una lista de prefijos creada.

      - **Lista de comunidades** aplica la regla a los prefijos IPv4 permitidos por la lista de prefijos especificada. Si selecciona este valor, en la lista desplegable **Lista de comunidad**, seleccione una lista de comunidades creada.

e. Si en la lista desplegable **Tipo de coincidencia** seleccionó **Lista de prefijos** o **Lista de comunidades**, en la lista desplegable **Cambiar atributo**, seleccione el atributo que modifica la regla:// TODO

- **Ninguna**— No cambie los valores de los atributos. Esta es la configuración predeterminada.
- **IP next-hop** si desea cambiar el valor del atributo "próximo salto" a la dirección IPv4 especificada. Si selecciona este valor, ingrese una dirección IPv4 en el campo **Nuevo valor**.
- **Local Preference** si desea cambiar el valor del atributo "preferencia local" al valor especificado. Si selecciona este valor, en el campo **Nuevo valor**, ingrese un valor para el atributo "preferencia local". Rango de valores: 0 a 4,294,967,295.
- **Metric** si desea cambiar el valor del atributo MED al valor especificado. Si selecciona este valor, en el campo **Nuevo valor**, ingrese un valor para el atributo MED. Rango de valores: 0 a 4,294,967,295.
- **AS Path Prepend**: agregue el número del sistema autónomo al atributo "ruta de as". Si selecciona este valor, ingrese el número del sistema autónomo en el campo **Nuevo valor**. Puede ingresar varios números separados por espacios. Rango de valores: 0 a 4,294,967,295.

Se crea la regla. Puede crear varias reglas o eliminarlas. Para eliminar una regla, haga clic en el ícono de eliminar ✕ junto a él.

5. Haga clic en **Crear**.

   El mapa de ruta se crea y se muestra en la tabla.

6. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla CPE o el dispositivo CPE, o programar un guardado diferido de la configuración del dispositivo CPE haciendo clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionando la opción **Guardado programado**.

## Editar un mapa de ruta

Puede editar un mapa de ruta en una plantilla de CPE o en un dispositivo CPE. Un mapa de ruta editado en la plantilla de CPE se edita automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

> Si desea que los cambios que realiza en un mapa de ruta se apliquen inmediatamente a los pares de BGP o grupos de pares de BGP que utilizan ese mapa de ruta, seleccione la casilla de verificación **BFD** o **Soft-reconfiguration inbound** cuando se cree o edite el par de BGP o el grupo de pares de BGP.

*Para editar un mapa de ruta, haga lo siguiente:*

1. Edite un mapa de ruta de una de las siguientes maneras:

   - Si desea editar un mapa de ruta en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y, en el área de configuración que se muestra, seleccione la pestaña **Filtros de enrutamiento → Mapas de ruta**.
   - Si desea editar un mapa de ruta en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en el área de configuración que se muestra, seleccione la pestaña **Filtros de enrutamiento → Mapas de ruta** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de mapas de ruta.

2. Haga clic en **Editar** junto al mapa de ruta que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración del mapa de ruta. Para obtener una descripción de la configuración, consulte las instrucciones para crear un mapa de ruta.

4. Haga clic en **Guardar**.

   El mapa de ruta se modificará y se actualizará en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un mapa de ruta

Puede eliminar un mapa de ruta en una plantilla de CPE o en un dispositivo CPE. Un mapa de ruta eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

Los mapas de ruta eliminados no se pueden restaurar.

*Para eliminar un mapa de ruta, siga esos pasos:*

1. Elimine un mapa de ruta de una de las siguientes maneras:

   - Si desea eliminar un mapa de ruta en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Filtros de enrutamiento → Mapas de ruta**.

   - Si desea eliminar un mapa de ruta en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Filtros de enrutamiento→ Mapas de ruta** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de mapas de ruta.

2. Haga clic en **Eliminar** junto al mapa de ruta que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El mapa de ruta se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Enrutamiento basado en directivas (PBR)

Además del enrutamiento basado en propiedades del paquete estándar, como la dirección IP de destino, Kaspersky SD-WAN es compatible con el enrutamiento basado en directivas (PBR). Este tipo de enrutamiento se basa en el uso de directivas, es decir, conjuntos de reglas de enrutamiento o reglas de IP, creadas por el usuario (administrador o administrador de inquilinos) y almacenadas en el dispositivo. Los siguientes son algunos ejemplos de casos de uso para el enrutamiento PBR:

- Redirigir el tráfico para redes especificadas por el usuario para omitir el firewall en caso de que surjan problemas con él
- Redirigir el tráfico vinculado a Internet para redes especificadas por el usuario a través de SD-WAN hacia una puerta de enlace que actúa como un punto único de acceso a Internet para todos los dispositivos CPE

Puede crear y ver reglas de enrutamiento tanto en la línea de comandos del dispositivo CPE mediante los comandos del kit de herramientas iproute2 como desde la interfaz gráfica del orquestador. En esta sección se describe la administración de las reglas de enrutamiento en la interfaz gráfica del orquestador.

## Administrar reglas de enrutamiento IP

Puede ver la tabla de reglas de IP en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de reglas de IP en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral, seleccione la sección **PBR**.
- Para ver la tabla de reglas de IP en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y, en la barra lateral, seleccione la sección **PBR**.

La información sobre las reglas de IP se muestra en las siguientes columnas de la tabla:

- **Prioridad** es la prioridad de la regla. Las reglas con un valor de prioridad más bajo se aplican antes.
- **Estado** es el estado de la regla. Valores posibles:
  - **Sí** significa que la regla está activa.
  - **No** significa que la regla está inactiva.
- **Protocolo de IP** es el protocolo IP. Los siguientes valores son posibles:
  - TCP
  - UDP
  - ICMP
  - SCTP
  - AH

- ESP
- GRE
- IPIP

- **Interfaz de red de origen** es la interfaz de entrada con la que se debe coincidir. Si la interfaz es una interfaz de bucle invertido, la regla solo coincide con los paquetes que se originan en este host.
- **Puerto de origen** es el puerto de origen.
- **Host o red de origen** es el host o la red de origen.
- **Interfaz de red de destino** es la interfaz de salida con la que se debe coincidir. La interfaz de salida está disponible solo para paquetes que se originan en sockets locales vinculados al dispositivo.
- **Puerto de destino** es el puerto de destino.
- **Host o red de destino** es el host o la red de destino.
- **VRF** es el VRF en el que se realiza la búsqueda de rutas.
- **Acciones** enumera las acciones que se pueden realizar con la regla de IP (habilitar, deshabilitar, editar, eliminar).

## Crear una regla de IP

Puede crear una regla de IP en una plantilla de CPE o en un dispositivo CPE. Las reglas de IP creadas en la plantilla de CPE se crean automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una regla de IP, haga lo siguiente:*

1. Cree una regla de IP de una de las siguientes maneras:
   - Si desea crear una regla de IP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral, seleccione la sección **PBR**.
   - Si desea crear una regla de IP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en la barra lateral, seleccione la sección **PBR**.

   Se muestra una tabla de reglas de IP.
2. Haga clic en **+ Regla de dirección IP**.
3. En la ventana que se abre, en el campo **Prioridad**, ingrese la prioridad de la regla. Las reglas con un valor de prioridad más bajo se aplican antes. Este valor debe ser único.
4. En la lista desplegable **Protocolo de IP**, seleccione el protocolo de IP. Los siguientes valores son posibles:
   - TCP
   - UDP
   - ICMP

- SCTP
- AH
- ESP
- GRE
- IPIP

5. En **Origen** y **Destino**, especifique la configuración de origen y de destino para la regla de IP según sea necesario:

   - Seleccione el origen o destino **Tipo**: host o red.
   - Dependiendo del **Tipo** seleccionado, en el campo a continuación, especifique lo siguiente:
     - Dirección IP de origen o de destino si seleccionó el tipo **Host** (el título del campo es entonces **Dirección IP**).
     - Dirección IP de origen o de destino y máscara si seleccionó el tipo **Red** (el título del campo es entonces **Máscara/dirección IP**).
   - En el campo **Puerto**, especifique el puerto de origen o de destino.

     Puede ingresar un solo valor o un rango de valores de 1 a 65 535 con un guion, por ejemplo: `443`, `1024-65535`.
   - En la lista desplegable **Alias de la interfaz de red**, seleccione la interfaz de origen (entrante) o la interfaz de destino (saliente).

     Si la interfaz de entrada es una interfaz de bucle invertido, la regla solo coincide con los paquetes que se originan en este host. La interfaz de salida está disponible solo para paquetes que se originan en sockets locales vinculados al dispositivo.

6. En la lista desplegable **VRF de búsqueda**, seleccione el VRF para buscar rutas.

   Si selecciona principal/254, entonces en **Destino**, debe especificar una dirección IP de origen distinta a 0.0.0.0/0; de lo contrario, la regla no se podrá guardar.

7. Haga clic en **Crear**.

   La regla de IP se creará y se mostrará en la tabla.

8. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE o dispositivo CPE.

## Editar una regla de IP

Puede crear reglas de IP en una plantilla de CPE o en un dispositivo CPE. Las reglas de IP editadas en la plantilla de CPE se modifican automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una regla de IP, siga estos pasos:*

1. Edite una regla de IP de una de las siguientes maneras:

   - Si desea editar una regla de IP en una plantilla de CPE, siga estos pasos:

     - En el menú, vaya a la sección del menú **SD-WAN→Plantillas de CPE**, haga clic en la plantilla CPE y, en la barra lateral, seleccione la sección **PBR**.

     - En la tabla de reglas de IP que se muestra, en la columna **Acciones**, haga clic en el botón **Editar** correspondiente a la regla que desee editar.

   - Si desea editar una regla de IP en un dispositivo CPE:

     - En el menú, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en la barra lateral, seleccione la sección **PBR**.

     - En la tabla de reglas de IP que se muestra, en la columna **Acciones**, haga clic en el botón **Editar** correspondiente a la regla que desee editar. Si la regla de IP se heredó de una plantilla, primero seleccione la casilla **Anular** para que la regla muestre el botón **Editar**.

2. En la ventana que se abre, edite la configuración de la regla de IP que desea cambiar. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla de IP.

3. Haga clic en **Guardar**.

   La regla de IP se modifica y se actualiza en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una regla de IP

Puede eliminar reglas de IP en una plantilla de CPE o en un dispositivo CPE. Las reglas de IP eliminadas en la plantilla de CPE se eliminan automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. En un dispositivo CPE, puede eliminar solo las reglas de IP que se agregaron directamente en el dispositivo, pero no puede eliminar las reglas de IP heredadas de la plantilla.

Las reglas de IP eliminadas no se pueden restaurar.

*Para eliminar una regla de IP, siga estos pasos:*

1. Elimine una regla de IP de una de las siguientes maneras:

   - Si desea eliminar una regla de IP en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral, seleccione la sección **PBR**.

   - Si desea eliminar una regla de IP que no se heredó de la plantilla de CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en la barra lateral, seleccione la sección **PBR**.

   Se muestra una tabla de reglas de IP.

2. Haga clic en **Eliminar** junto a la regla de IP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La regla de IP se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

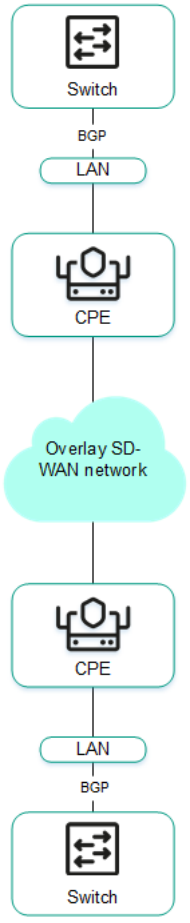
# Intercambio de rutas a través de BGP

Kaspersky SD-WAN admite el protocolo de enrutamiento dinámico BGP (protocolo de puerta de enlace fronteriza) para intercambiar información de enrutamiento entre dispositivos CPE y dispositivos de red externos. Puede establecer sesiones internas de iBGP (BGP interno) y sesiones eBGP externas (BGP externo).

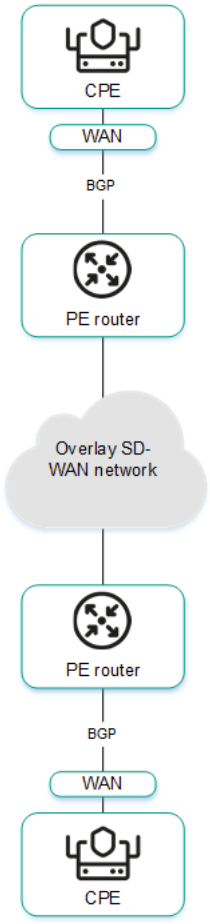
También se admite la creación de pares BGP individuales y grupos de pares BGP. Las sesiones TCP dinámicas se establecen con grupos de pares BGP.

Las figuras siguientes muestran ejemplos del uso de BGP en la solución:

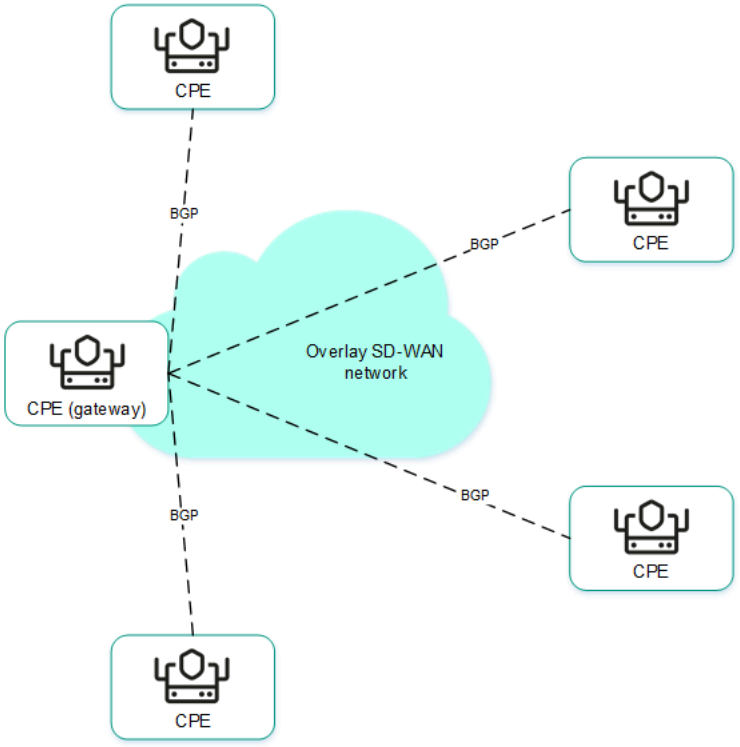
- Conexión de varias ubicaciones de clientes a la red L3 SD-WAN a través de BGP.



- Conexión de dispositivos CPE a la red IP/MPLS del proveedor de servicios a través de BGP.




- Usar BGP para configurar la conexión de los dispositivos CPE dentro del dominio.



# Configuración básica de BGP

Puede especificar la configuración básica de BGP en una plantilla de CPE o en un dispositivo CPE. La configuración de BGP especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para modificar la configuración básica de BGP, siga estos pasos:*

1. Especifique la configuración básica de BGP de una de las siguientes maneras:

   - Si desea editar la configuración básica de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP** en la barra lateral de la ventana mostrada.

   - Si desea administrar la configuración básica de BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en la barra lateral de la ventana que se muestra, seleccione la opción **BGP** y seleccione la casilla **Anular**, que desbloquea el campo **Sistema autónomo**.

2. En el campo **Sistema autónomo**, ingrese el número del sistema autónomo (de 1 a 4 294 967 295). El sistema autónomo especificado se utilizará para todas las instancias de BGP creadas en este dispositivo o en esta plantilla de CPE y se mostrará en el campo **AS**.

   Después de especificar el número del sistema autónomo, el botón **+ BGP** está disponible.

3. En la lista **Instancia de BGP con VRF predeterminada**, seleccione la instancia de BGP que desea utilizar de manera predeterminada. Si aún no se creó una instancia de BGP, cree una instancia de BGP siguiendo los pasos a continuación y luego seleccione la instancia de BGP creada.

4. Cree una o más instancias de BGP. Para hacerlo:

   1. Haga clic en el botón **+ BGP**. Se muestra el espacio de trabajo para agregar una instancia de BGP.

   2. De manera predeterminada, está seleccionada la pestaña **Configuración general**, que muestra la configuración básica de BGP.

   3. En la lista desplegable **BGP**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

   4. En la lista desplegable **VRF**, seleccione un VRF existente al que desee anunciar rutas BGP. La lista solo muestra los VRF que no están asociados con otras instancias de BGP en el dispositivo o en la plantilla de CPE.

   5. En el campo **ID de enrutador**, ingrese la dirección IPv4 que desea asignar al ID del enrutador del dispositivo CPE. Si desea asignar una dirección IPv4 de un rango específico de direcciones IP, siga estos pasos:

   6. Seleccione la casilla **ID del enrutador de la agrupación de IP**. Esta casilla está desactivada por defecto.

   7. En la lista desplegable **Agrupación de direcciones IP**, seleccione un rango creado de direcciones IP.

   8. Si es necesario, en el campo **Cantidad máxima de rutas**, ingrese el número máximo de entradas en la tabla de enrutamiento y reenvío del dispositivo CPE. Rango de valores: 1 a 8.

   9. Si es necesario, seleccione las siguientes casillas:

10. Seleccione la casilla **Siempre comparar MED**. Esta casilla permite al dispositivo CPE comparar el discriminador de salida múltiple (MED) de las rutas anunciadas desde diferentes sistemas autónomos.

    Debe asegurarse de que esta casilla esté seleccionada en todos los dispositivos CPE de su sistema autónomo. De lo contrario, el intercambio de información de enrutamiento puede generar bucles de enrutamiento.

    - Seleccione la casilla **Reinicio ordenado (modo de ayuda)** para habilitar el reinicio ordenado en el dispositivo CPE.

      Estas casillas de verificación están desactivadas de manera predeterminada.

11. Si no desea que el dispositivo CPE intercambie rutas IPv4 con pares de BGP de manera predeterminada, desmarque la casilla **Utilizar rutas unidifusión IPv4 predeterminadas**. Esta casilla está seleccionada por defecto.

12. Si desea configurar los temporizadores BGP, siga estoss pasos:

13. Seleccione la casilla **Temporizadores de BGP**. Esta casilla está desactivada por defecto.

    a. En el campo **Keepalive (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa para enviar paquetes de control a los pares de BGP. Rango de valores: de 0 a 65 535.

    b. En el campo **Tiempo de retención (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa cuando recibe paquetes de control de pares de BGP. Si no se reciben paquetes de control del par de BGP dentro del tiempo especificado, el dispositivo CPE considera que el par no está disponible. Rango de valores: de 0 a 65 535.

14. Si desea configurar la redistribución de rutas en BGP, en **Redistribución de ruta**, haga lo siguiente:

    a. Seleccione las casillas de verificación que se encuentran junto a los tipos de ruta:

       - **Kernel** para redistribuir las rutas del Kernel generadas por el sistema operativo del dispositivo CPE.
       - **Conectados** para redistribuir las rutas conectadas directamente a las interfaces de red del dispositivo CPE.
       - **Estática** para redistribuir rutas estáticas.
       - **OSPF** para redistribuir las rutas OSPF.

       Estas casillas de verificación están desactivadas de manera predeterminada.

    b. En la lista desplegable **Mapa de ruta**, seleccione un mapa de ruta creado para las rutas redistribuidas.

    c. En el campo **Métrica**, ingrese una métrica de rutas redistribuidas. Rango de valores: de 0 a 16 777 214.

15. Si desea que el dispositivo CPE anuncie la subred especificada a los pares de BGP:

    a. En **Redes**, haga clic en **+ Red**.

    b. En el campo **Red**, ingrese el prefijo IPv4 de la subred.

c. En la lista desplegable **Mapa de ruta**, seleccione un mapa de ruta creado para la subred.

La subred se especifica y se muestra en **Redes**. Puede especificar varias subredes o eliminar subredes. Para eliminar una subred, haga clic en el ícono de eliminar ✕ junto a ella.

16. Si es necesario, también administre la configuración de la instancia de BGP en las pestañas **Vecinos**, **Grupos de pares** y **Fuga de rutas**.

17. En la parte inferior del espacio de trabajo para agregar una instancia de BGP, haga clic en **Guardar** para guardar la configuración de la instancia de BGP.

    La instancia de BGP se guarda y se agrega a la tabla de instancias de BGP en el área de configuración.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar pares de BGP

*Para ver o editar la tabla de pares de BGP de una instancia de BGP en una plantilla de CPE o en un dispositivo CPE, haga lo siguiente:*

1. Vaya a la sección **BGP**. Para hacerlo:

   - Para ver o editar la tabla de pares de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral del área de configuración, seleccione **BGP**.

   - Para ver o editar la tabla de pares de BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, y en la barra lateral del área de configuración, haga clic en **BGP**.

2. Abra una instancia de BGP existente haciendo clic en **Editar** en su fila de la tabla o cree una nueva instancia de BGP.

3. En el área de configuración de la instancia de BGP, seleccione la pestaña **Vecinos**.

La información sobre los pares de BGP se muestra en las siguientes columnas de la tabla:

- **IP de vecino** es la dirección IPv4 del par de BGP.
- **Nombre** es el nombre del par de BGP.
- **Descripción** es una breve descripción del par de BGP.
- **Heredado** indica si el par de BGP es heredado de la plantilla de CPE:

  - **Sí**.

  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.

- **AS remoto** es el número de sistema autónomo del par de BGP.

- **Apagar** indica si el par de BGP está deshabilitado y no se establece una sesión TCP con él:
  - **Sí**.
  - **No**.
- **Peso** es el peso de las rutas anunciadas por el par de BGP.
- **Administración** contiene las acciones que se pueden realizar con el par de BGP.

## Crear un par de BGP

Puede crear un par de BGP en una plantilla de CPE o en un dispositivo CPE. Un par de BGP creado en la plantilla CPE se crea automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. El número máximo de pares de BGP dinámicos es 512.

*Para crear un par de BGP, siga estos pasos:*

1. Cree un par de BGP de una de las siguientes maneras:
   - Si desea crear un par de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP → Vecinos**.
   - Si desea crear un par de BGP en un dispositivo CPE, vaya a la sección el menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BGP→ Vecinos**y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BGP.
2. Haga clic en **+ Vecino de BGP**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del par de BGP. La longitud máxima del nombre es de 50 caracteres.
4. Si desea deshabilitar un par de BGP y evitar que se establezca una sesión TCP con él, seleccione la casilla **Deshabilitar par de BGP**. Esta casilla está desactivada por defecto.
5. En el campo **IP de vecino**, ingrese la dirección IPv4 del par de BGP.
6. En el campo **AS remoto**, ingrese el número de sistema autónomo del par de BGP. Rango de valores: 1 a 4 294 967 295.
7. Si es necesario, ingrese una breve descripción del par de BGP en el campo **Descripción**.
8. Si desea que el dispositivo CPE use una contraseña cuando establece una sesión TCP con el par de BGP, en el campo **Contraseña**, ingrese la contraseña. Para que se establezca una sesión TCP entre dos pares de BGP, deben usar la misma contraseña. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar 👁.
9. Si es necesario, en el campo **Origen de actualizaciones**, ingrese la dirección IPv4 de la interfaz de bucle invertido que el dispositivo CPE envía al par de BGP cuando establece una sesión TCP.
10. Si la sesión TCP no se establece directamente entre el dispositivo CPE y el par de BGP, en el campo **Saltos de eBGP**, ingrese el número de saltos entre el dispositivo CPE y el par de BGP. Rango de valores: 1 a 255.

11. Si desea configurar los temporizadores de BGP, siga estos pasos:

    a. Seleccione la casilla **Temporizadores personalizados de BGP**. Esta casilla está desactivada por defecto.

    b. En el campo **Keepalive (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa para enviar paquetes de control al par de BGP. Rango de valores: de 0 a 65 535.

    c. En el campo **Tiempo de retención (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa cuando recibe paquetes de control del par de BGP. Si no se reciben paquetes de control del par de BGP dentro del tiempo especificado, el dispositivo CPE considera que este par de BGP no está disponible. Rango de valores: de 0 a 65 535.

12. Si desea utilizar el protocolo BFD para detectar la pérdida de conexión, seleccione la casilla **BFD**. Esta casilla está desactivada por defecto. Cuando se selecciona la casilla, los cambios que realiza en el mapa de ruta se aplican inmediatamente a un par de BGP si el par de BGP usa este mapa de ruta. Puede seleccionar un mapa de ruta para el par de BGP en el paso 14 de estas instrucciones.

13. Si desea especificar la configuración avanzada para el par de BGP:

    a. Seleccione la pestaña **Configuración avanzada**.

    Se muestra la configuración avanzada del par de BGP.

    b. Si es necesario, seleccione las siguientes casillas:

    - Seleccione la casilla **Soft-reconfiguration inbound** para almacenar las rutas anunciadas por el par de BGP localmente en el dispositivo CPE. El uso de esta función reduce la cantidad de memoria disponible en el dispositivo CPE. Cuando se selecciona la casilla, los cambios que realiza en el mapa de ruta se aplican inmediatamente a un par de BGP si el par de BGP usa este mapa de ruta. Puede seleccionar un mapa de ruta para el par de BGP en el paso 14 de estas instrucciones.
    - Seleccione la casilla **Atribuir ruta de AS no modificada** para no modificar el atributo "AS path" de las rutas que el dispositivo CPE anuncia al par de BGP.
    - Seleccione la casilla **Permitir AS en** para permitir que los pares de BGP anuncien rutas al dispositivo CPE con el atributo "AS path", cuyo valor es el número de sistema autónomo del dispositivo CPE.
    - Seleccione la casilla de verificación **Atribuir next-hop no modificado** para no modificar el atributo "next hop" de las rutas que el dispositivo CPE anuncia al par de BGP.
    - Seleccione la casilla de verificación **Next-hop self** para usar la dirección IPv4 del dispositivo CPE como el valor del atributo "next hop" cuando se anuncian rutas al par de BGP.
    - Seleccione la casilla **Atribuir MED no modificado** para no modificar el atributo "MED" de las rutas que el dispositivo CPE anuncia al par de BGP.
    - Seleccione la casilla **Cliente de reflector de rutas** para asignar la función *Reflector de ruta* al dispositivo CPE y la función *Cliente de reflector de ruta* al par de BGP. Solo puede seleccionar esta casilla para un par de BGP que esté en el mismo sistema autónomo que el dispositivo CPE.

    Estas casillas de verificación están desactivadas de manera predeterminada.

    c. En el campo **AS local**, ingrese el número del sistema autónomo local que el dispositivo CPE envía al par de BGP. Rango de valores: 1 a 4 294 967 295.

    d. En el campo **Peso**, ingrese el peso de las rutas anunciadas por el par de BGP. Cuanto mayor sea el peso de una ruta, mayor será su prioridad. Rango de valores: de 0 a 65 535.

e. En el campo **Cantidad máxima de prefijos**, ingrese el número máximo de rutas que el par de BGP puede anunciar a un dispositivo CPE. Rango de valores: 1 a 4 294 967 295.

f. Si desea que un dispositivo CPE anuncie rutas con el atributo "community" a su par de BGP, seleccione la casilla **Enviar comunidad** y seleccione el tipo de atributo en la lista desplegable:

- **Todos** cubre todos los tipos disponibles del atributo "community".
- **Comunidad estándar y extendida**.
- **Comunidad extendida**.
- **Comunidad grande**.
- **Comunidad estándar**.

Esta casilla está desactivada por defecto.

a. Si desea que el dispositivo CPE anuncie la ruta 0.0.0.0/0 predeterminada al par de BGP, seleccione la casilla **Origen predeterminado**. Esta casilla está desactivada por defecto. Puede seleccionar la casilla **Configurar mapa de ruta** y, en la lista desplegable que se muestra, seleccione el mapa de ruta creado para la ruta predeterminada 0.0.0.0/0.

14. Si desea configurar el filtrado de rutas para el par de BGP:

a. Seleccione la pestaña **Filtrado**.

Se muestra la configuración del filtrado de rutas.

b. En **Mapa de ruta**, seleccione los mapas de ruta creados:

1. En la lista desplegable **Entrante**, seleccione un mapa de ruta para las rutas que el par de BGP anuncia al dispositivo CPE.
2. En la lista desplegable **Saliente**, seleccione un mapa de ruta para las rutas que el dispositivo CPE anuncia al par de BGP.

c. En **Lista de prefijos**, seleccione las listas de prefijos creadas:

1. En la lista desplegable **Entrante**, seleccione una lista de prefijos para las rutas que el par e BGP anuncia al dispositivo CPE.
2. En la lista desplegable **Saliente**, seleccione una lista de prefijos para las rutas que el dispositivo CPE anuncia al par de BGP.

d. En **Lista de control de acceso**, seleccione las listas de control de acceso creadas:

1. En la lista desplegable **Entrante**, seleccione una lista de control de acceso para las rutas que el par de BGP anuncia al dispositivo CPE.
2. En la lista desplegable **Saliente**, seleccione una lista de control de acceso para las rutas que el dispositivo CPE anuncia al par de BGP.

15. Haga clic en **Crear**.

    El par de BGP se crea y se muestra en la tabla.

16. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar un par de BGP

Puede editar un par BGP en una plantilla de CPE o en un dispositivo CPE. Un par BGP editado en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. No puede editar un par BGP que se hereda de una plantilla de CPE en un dispositivo CPE.

*Para editar un par BGP, siga estos pasos:*

1. Edite un par BGP de una de las siguientes maneras:

    - Si desea editar un par BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP → Vecinos**.

    - Si desea editar un par BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BGP→ Vecinos** y marque la casilla de verificación **Anular**.

    Se muestra una tabla de pares BGP.

2. Haga clic en **Editar** junto al par BGP que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de pares BGP. Para obtener una descripción de la configuración, consulte las instrucciones para crear un par BGP.

4. Haga clic en **Guardar**.

    El par de BGP se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un par de BGP

Puede eliminar un par BGP en una plantilla de CPE o en un dispositivo CPE. Un par BGP eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede eliminar un par BGP heredado de una plantilla de CPE en un dispositivo CPE.

Los pares BGP eliminados no se pueden restaurar.

*Para eliminar un par BGP, siga estos pasos:*

1. Elimine un par BGP de una de las siguientes maneras:

   - Si desea eliminar un par BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP → Vecinos**.

   - Si desea eliminar un par BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BGP→ Vecinos** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BGP.

2. Haga clic en **Eliminar** junto al par BGP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El par de BGP se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar grupos de pares de BGP

*Para ver o editar la tabla de grupos de pares BGP de una instancia de BGP en una plantilla de CPE o en un dispositivo CPE, siga estos pasos:*

1. Vaya a la sección **BGP**. Para hacerlo:

   - Para ver o editar la tabla de grupos de pares BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral del área de configuración, seleccione **BGP**.

   - Para ver o editar la tabla de grupos de pares BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en la barra lateral del área de configuración, haga clic en **BGP**.

2. Abra una instancia de BGP existente haciendo clic en **Editar** en su fila de la tabla o cree una nueva instancia de BGP.

3. En el área de configuración de la instancia de BGP, seleccione la pestaña **Grupos de pares**.

La información sobre los grupos de pares BGP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del grupo de pares BGP.

- **Rango de BGP** es el prefijo IPv4 del grupo de pares BGP.

- **Descripción** es una breve descripción del grupo de pares BGP.

- **Heredado** indica si el grupo de pares BGP se hereda de la plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **AS remoto** es el número de sistema autónomo del grupo de pares BGP.
- **Apagar** indica si el grupo de pares BGP está deshabilitado y no se establece una sesión TCP con él.
  - **Sí**.
  - **No**.
- **Peso** es el peso de las rutas anunciadas por el grupo de pares BGP.
- **Administración** contiene las acciones que se pueden realizar con el grupo de pares BGP.

## Crear un grupo de pares de BGP

Puede crear un grupo de pares de BGP en una plantilla de CPE o en un dispositivo CPE. Un grupo de pares de BGP creado en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear un grupo de pares de BGP, siga estos pasos:*

1. Cree un grupo de pares de BGP de una de las siguientes maneras:
   - Si desea crear un grupo de pares de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP**→ **Grupos de pares**.
   - Si desea crear un grupo de pares de BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione **BGP** → **Grupos de pares** y marque la casilla **Anular**.

   Se muestra una tabla de grupos de pares de BGP.
2. Haga clic en **+ Grupo de pares**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del grupo de pares de BGP. La longitud máxima del nombre es de 50 caracteres.
4. Si desea deshabilitar un grupo de pares de BGP y evitar establecer una sesión TCP con él, seleccione la casilla **Deshabilitar grupo de pares de BGP**. Esta casilla está desactivada por defecto.
5. En el campo **Rango de BGP**, ingrese el prefijo IPv4 del grupo de pares de BGP.
6. En el campo **AS remoto**, ingrese el número del sistema autónomo del grupo de pares de BGP. Rango de valores: 1 a 4 294 967 295.
7. Si es necesario, ingrese una breve descripción del grupo de pares de BGP en el campo **Descripción**.

8. Si desea que el dispositivo CPE use una contraseña cuando se establece una sesión TCP con el grupo de pares de BGP, en el campo **Contraseña**, ingrese la contraseña. Para que se establezca una sesión TCP entre dos pares de BGP, deben usar la misma contraseña. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar 👁.

9. En el campo **Origen de actualizaciones**, ingrese la dirección IPv4 de la interfaz de bucle invertido que el dispositivo CPE envía al grupo de pares de BGP cuando se establece una sesión TCP.

10. Si la sesión TCP no se establece directamente entre el dispositivo CPE y el grupo de pares de BGP, en el campo **Saltos de eBGP**, ingrese el número de saltos entre el dispositivo CPE y el grupo de pares de BGP. Rango de valores: 1 a 255.

11. Si desea configurar los temporizadores de BGP, siga estos pasos:

    a. Seleccione la casilla **Temporizadores personalizados de BGP**. Esta casilla está desactivada por defecto.

    b. En el campo **Keepalive (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa para enviar paquetes de control al grupo de pares de BGP. Rango de valores: de 0 a 65 535.

    c. En el campo **Tiempo de retención (s)**, ingrese el intervalo de tiempo en segundos que el dispositivo CPE usa cuando recibe paquetes de control del grupo de pares de BGP. Si no se reciben paquetes de control del par de BGP dentro del tiempo especificado, el dispositivo CPE considera que este par de BGP no está disponible. Rango de valores: de 0 a 65 535.

12. Si desea utilizar el protocolo BFD para detectar la pérdida de conexión, seleccione la casilla **BFD**. Esta casilla está desactivada por defecto. Cuando se selecciona la casilla, los cambios que realiza en el mapa de ruta se aplican inmediatamente a un grupo de pares de BGP si el grupo de pares de BGP usa este mapa de ruta. Puede seleccionar un mapa de ruta para el grupo de pares de BGP en el paso 14 de estas instrucciones.

13. Si desea especificar la configuración avanzada para el grupo de pares de BGP:

    a. Seleccione la pestaña **Configuración avanzada**.

    Se muestra la configuración avanzada del grupo de pares de BGP.

    b. Si es necesario, seleccione las siguientes casillas:

    - Seleccione la casilla **Soft-reconfiguration inbound** para almacenar las rutas anunciadas por el grupo de pares de BGP localmente en el dispositivo CPE. El uso de esta función reduce la cantidad de memoria disponible en el dispositivo CPE. Cuando se selecciona la casilla, los cambios que realiza en el mapa de ruta se aplican inmediatamente a un grupo de pares de BGP si el grupo de pares de BGP usa este mapa de ruta. Puede seleccionar un mapa de ruta para el grupo de pares de BGP en el paso 14 de estas instrucciones.

    - Seleccione la casilla **Atribuir ruta de AS no modificada** para no modificar el atributo "AS path" de las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

    - Seleccione la casilla **Permitir AS en** para permitir que el grupo de pares de BGP anuncie rutas al dispositivo CPE con el atributo "AS path", cuyo valor es el número de sistema autónomo del dispositivo CPE.

    - Seleccione la casilla de verificación **Atribuir next-hop no modificado** para no modificar el atributo "next hop" de las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

    - Seleccione la casilla **Next-hop self** para usar la dirección IPv4 del dispositivo CPE como el valor del atributo "next hop" cuando se anuncian rutas al grupo de pares de BGP.

- Seleccione la casilla **Atribuir MED no modificado** para no modificar el atributo "MED" de las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

- Seleccione la casilla **Cliente de reflector de rutas** para asignar la función *Reflector de ruta* al dispositivo CPE y la función *Cliente de reflector de ruta* al grupo de pares de BGP. Solo puede seleccionar esta casilla para un grupo de pares de BGP que esté en el mismo sistema autónomo que el dispositivo CPE.

Estas casillas de verificación están desactivadas de manera predeterminada.

c. En el campo **AS local**, ingrese el número del sistema autónomo local que el dispositivo CPE envía al grupo de pares de BGP. Rango de valores: 1 a 4 294 967 295.

d. En el campo **Peso**, ingrese el peso de las rutas anunciadas por el grupo de pares de BGP. Cuanto mayor sea el peso de una ruta, mayor será su prioridad. Rango de valores: de 0 a 65 535.

e. En el campo **Cantidad máxima de prefijos**, ingrese el número máximo de rutas que el grupo de pares de BGP puede anunciar a un dispositivo CPE. Rango de valores: 1 a 4 294 967 295.

f. Si desea que un dispositivo CPE anuncie rutas con el atributo "community" al grupo de pares de BGP, seleccione la casilla **Enviar comunidad** y seleccione el tipo de atributo que se enviará en la lista desplegable:

- **Todos** cubre todos los tipos disponibles del atributo "community".
- **Comunidad estándar y extendida**.
- **Comunidad extendida**.
- **Comunidad grande**.
- **Comunidad estándar**.

Esta casilla está desactivada por defecto.

a. Si desea que el dispositivo CPE anuncie la ruta 0.0.0.0/0 predeterminada al grupo de pares de BGP, seleccione la casilla **Origen predeterminado**. Esta casilla está desactivada por defecto. Puede seleccionar la casilla **Configurar mapa de ruta** y, en la lista desplegable que se muestra, seleccione el mapa de ruta creado para la ruta predeterminada 0.0.0.0/0.

14. Si desea configurar el filtrado de rutas para el grupo de pares de BGP:

a. Seleccione la pestaña **Filtrado**.

Se muestra la configuración del filtrado de rutas.

b. En **Mapa de ruta**, seleccione los mapas de ruta creados:

1. En la lista desplegable **Entrante**, seleccione un mapa de ruta para las rutas que el grupo de pares de BGP anuncia al dispositivo CPE.

2. En la lista desplegable **Saliente**, seleccione un mapa de ruta para las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

c. En **Lista de prefijos**, seleccione las listas de prefijos creadas:

1. En la lista desplegable **Entrante**, seleccione una lista de prefijos que el grupo de pares de BGP anuncia al dispositivo CPE .

2. En la lista desplegable **Saliente**, seleccione una lista de prefijos para las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

d. En **Lista de control de acceso**, seleccione las listas de control de acceso creadas:

1. En la lista desplegable **Entrante**, seleccione una lista de control de acceso para las rutas que anuncia el grupo de pares de BGP al dispositivo CPE.

2. En la lista desplegable **Saliente**, seleccione una lista de control de acceso para las rutas que el dispositivo CPE anuncia al grupo de pares de BGP.

15. Haga clic en **Crear**.

    El grupo de pares de BGP se crea y se muestra en la tabla.

16. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar un grupo de pares de BGP

Puede editar un grupo de pares de BGP en una plantilla de CPE o en un dispositivo CPE. Un grupo de pares de BGP editado en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. No puede editar un grupo de pares e BGP heredado de una plantilla d CPE en un dispositivo CPE.

*Para editar un grupo de pares de BGP, siga estos pasos:*

1. Edite un grupo de pares de BGP de una de las siguientes maneras:

   - Si desea editar un grupo de pares de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP** → **Grupos de pares**.

   - Si desea editar un grupo de pares de BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione **BGP** → **Grupos de pares** y marque la casilla **Anular**.

   Se muestra una tabla de grupos de pares de BGP.

2. Haga clic en **Editar** junto al grupo de pares de BGP que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración del grupo de pares de BGP. Para obtener una descripción de la configuración, consulte las instrucciones para crear un grupo de pares de BGP.

4. Haga clic en **Guardar**.

   El grupo de pares de BGP se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un grupo de pares de BGP

Puede eliminar un grupo de pares de BGP en una plantilla de CPE o en un dispositivo CPE. Un grupo de pares de BGP eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilicen esta plantilla de CPE. No puede eliminar un grupo de pares de BGP heredado de una plantilla de CPE en un dispositivo CPE.

Los grupos de pares de BGP eliminados no se pueden restaurar.

*Para eliminar un grupo de pares de BGP, haga lo siguiente:*

1. Elimine un grupo de pares de BGP de una de las siguientes maneras:

   - Si desea eliminar un grupo de pares de BGP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BGP** → **Grupos de pares**.

   - Si desea eliminar un grupo de pares de BGP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BGP** → **Grupos de pares** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de grupos de pares de BGP.

2. Haga clic en **Eliminar** junto al grupo de pares de BGP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El grupo de pares de BGP se eliminará y ya no se mostrará en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Configurar fugas de rutas entre VRF

*Para ver o editar la fuga de rutas entre VRF para una instancia de BGP en una plantilla de CPE o en un dispositivo de CPE, siga estos pasos:*

1. Vaya a la sección **BGP**. Para hacerlo:

   - Para ver o editar la configuración de la fuga de rutas entre VRF en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y, en la barra lateral del área de configuración, seleccione **BGP**.

   - Para ver o editar la configuración de la fugas de rutas entre VRF en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y, en la barra lateral del área de configuración, haga clic en **BGP**.

2. Abra una instancia de BGP existente haciendo clic en **Editar** en su fila de la tabla o cree una nueva instancia de BGP.

3. En el área de configuración de la instancia de BGP, seleccione la pestaña **Fuga de rutas**.

4. Si es necesario, administre la siguiente configuración de la fuga de rutas entre VRF:

   - En el campo **Distinguidor de ruta**, especifique el atributo Distinguidor de ruta (RD) para la fuga de rutas (un ID único para distinguir rutas). Se puede especificar en uno de los dos formatos:

     - Número de sistema autónomo (de 0 a 4294967295):ID (de 0 a 65535). Ejemplo: `100:65000`.

     - Dirección IPv4: ID (de 0 a 65535) Ejemplo: `1.2.3.4:15`.

     Puede hacer que el atributo Distinguidor de ruta se genere automáticamente; para ello, seleccione la casilla **Generación automática** (seleccionada de manera predeterminada).

   - En **Exportación de destino de ruta**, haga clic en **Agregar** para agregar uno o más valores de Destino de ruta (RT) para exportar rutas del VRF de esta instancia de BGP a otros VRF.

   - En **Importación de destino de ruta**, haga clic en **Agregar** para agregar uno o más valores de Destino de ruta (RT) para importar rutas al VRF de esta instancia de BGP desde otros VRF.

     Los valores de entrada del Destino de ruta individual para **Exportación de destino de ruta** y **Importación de destino de ruta** se especifican en uno de dos formatos:

     - Número de sistema autónomo (de 0 a 4294967295):ID (de 0 a 65535). Ejemplo: `100:3000`.

     - Dirección IPv4: ID (de 0 a 65535) Ejemplo: `6.6.6.6:77`.

   - Active el conmutador **Exportar rutas** si necesita exportar rutas desde el VRF de esta instancia de BGP.

   - Active el conmutador **Importar rutas** si necesita importar rutas al VRF de esta instancia de BGP.

   - En las listas **Exportar mapa de ruta** y **Importar mapa de ruta**, seleccione los mapas de ruta creados para las rutas exportadas e importadas.

5. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para descartar los cambios.

# Intercambio de rutas a través de OSPF

Kaspersky SD-WAN es compatible con el protocolo de enrutamiento dinámico OSPF (Open Shortest Path First) para intercambiar información de enrutamiento entre dispositivos CPE y dispositivos de red externos. Cuando configura el protocolo OSPF, puede usar áreas OSPF e interfaces OSPF.

## Configuración básica de OSPF

Puede especificar la configuración básica de OSPF en una plantilla de CPE o en un dispositivo CPE. La configuración básica de OSPF especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para modificar la configuración básica de OSPF, siga estos pasos:*

1. Especifique la configuración básica de OSPF de una de las siguientes maneras:

   - Si desea editar la configuración básica de OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF**.

   - Si desea editar la configuración básica de OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF** y seleccione la casilla de verificación **Anular**.

   De manera predeterminada, está seleccionada la pestaña **Configuración general**, que muestra la configuración de OSPF.

2. En la lista desplegable **OSPF**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

3. En el campo **ID de enrutador**, ingrese la dirección IPv4 que desea asignar al ID del enrutador del dispositivo CPE.

4. En el campo **Cantidad máxima de rutas**, ingrese el número máximo de entradas en la tabla de enrutamiento y reenvío del dispositivo CPE. Rango de valores: 1 a 16.

5. Si desea utilizar el dispositivo CPE como un Enrutador de borde de área (ABR), en la lista desplegable **Tipo de ABR**, seleccione una de las siguientes implementaciones:

   - **IBM** (implementación predeterminada)

   - **CISCO**

   - **SHORTCUT**

   - **STANDARD**

6. En el campo **Ancho de banda de referencia para el cálculo automático del costo**, ingrese el ancho de banda de referencia para calcular el costo de los vínculos en el dispositivo CPE. Rango de valores: de 1 a 4 294 967.

7. Si desea cambiar todas las interfaces OSPF del dispositivo CPE al modo pasivo, seleccione la casilla **Interfaz pasiva predeterminada**. En el modo pasivo, las interfaces OSPF no intercambian paquetes de tráfico. Esta casilla está desactivada por defecto.

8. Si desea mantener un registro OSPF, seleccione la casilla **Registrar cambios de adyacencia**. Puede seleccionar la casilla **Detalle** para mantener un registro OSPF más detallado. Estas casillas de verificación están desactivadas de manera predeterminada.

9. Si desea configurar la redistribución de rutas en OSPF, en **Redistribución de ruta**, haga lo siguiente:

   a. Seleccione las casillas de verificación que se encuentran junto a los tipos de ruta:

      - **BGP** para redistribuir las rutas BGP.

      - **Conectados** para redistribuir las rutas conectadas directamente a las interfaces de red del dispositivo CPE.

      - **Kernel** para redistribuir las rutas del Kernel generadas por el sistema operativo del dispositivo CPE.

      - **Estática** para redistribuir rutas estáticas.

Estas casillas de verificación están desactivadas de manera predeterminada.

b. En la lista desplegable **Mapa de ruta**, seleccione un mapa de ruta creado para las rutas redistribuidas.

c. En el campo **Métrica**, ingrese una métrica de rutas redistribuidas. Rango de valores: de 0 a 16 777 214.

d. En la lista desplegable **Tipo de métrica**, seleccione el tipo de métrica:

- **Tipo 1** (o "métrica interna")
- **Tipo 2** (o "métrica externa")

e. Seleccione la casilla **Filtrado** y, en la lista desplegable **Lista de control de acceso**, seleccione una lista de control de acceso creada para las rutas reasignadas. Esta casilla está desactivada por defecto.

10. En el campo **Métrica predeterminada**, ingrese la métrica predeterminada de las rutas OSPF. Rango de valores: de 0 a 16 777 214.

11. Si desea configurar el dispositivo CPE para anunciar la ruta predeterminada 0.0.0.0/0 a los vecinos OSPF:

a. Seleccione la casilla **Origen predeterminado**. Esta casilla está desactivada por defecto.

b. Seleccione la casilla **Siempre** para anunciar siempre la ruta predeterminada 0.0.0.0/0, incluso si no está presente en la tabla de rutas del dispositivo CPE. Esta casilla está desactivada por defecto.

c. En la lista desplegable **Tipo de métrica**, seleccione el tipo de métrica para la ruta predeterminada 0.0.0.0/0:

- **Tipo 1**
- **Tipo 2**

d. En el campo **Métrica**, ingrese una métrica para la ruta predeterminada 0.0.0.0/0. Rango de valores: de 0 a 16 777 214.

e. En la lista desplegable **Mapa de ruta**, seleccione un mapa de ruta creado para la ruta predeterminada 0.0.0.0/0.

12. En el campo **Distancia**, ingrese la distancia administrativa para todas las rutas OSPF. Cuanto menor sea la distancia administrativa especificada para un protocolo, mayor será la prioridad de su ruta. Por ejemplo, si desea que las rutas OSPF tengan preferencia sobre las rutas BGP, especifique la distancia administrativa de 1 para OSPF y 2 para BGP. Rango de valores: 1 a 255.

13. Si desea configurar distancias administrativas para rutas OSPF individuales:

a. Seleccione la casilla **Distancia de OSPF**. Esta casilla está desactivada por defecto.

b. En el campo **Externo**, ingrese la distancia administrativa para las rutas de dominios OSPF externos o protocolos de enrutamiento. Rango de valores: 1 a 255.

c. En el campo **Entre áreas**, ingrese la distancia administrativa para las rutas de diferentes áreas OSPF del mismo dominio OSPF. Rango de valores: 1 a 255.

d. En el campo **Dentro del área**, ingrese la distancia administrativa para las rutas de la misma área OSPF. Rango de valores: 1 a 255.

14. Si desea habilitar el reinicio ordenado en el dispositivo CPE:

    a. Seleccione la casilla **Reinicio ordenado**. Esta casilla está desactivada por defecto.

    b. En el campo **Período de gracia (s)**, ingrese el tiempo, en segundos, durante el cual el dispositivo CPE anuncia su intención de reiniciarse a los vecinos OSPF. Rango de valores: de 1 a 1800.

15. Si desea configurar temporizadores para los cálculos del algoritmo Shortest Path First (SPF):

    a. Seleccione la casilla **Temporizador para el límite de SPF**. Esta casilla está desactivada por defecto.

    b. En el campo **Demora (ms)**, ingrese la duración en milisegundos del retraso antes de iniciar los cálculos del algoritmo SPF. Rango de valores: de 0 a 600 000.

    c. En el campo **Tiempo de espera inicial (ms)**, ingrese el tiempo de retención mínimo en milisegundos entre dos cálculos del algoritmo SPF. Rango de valores: de 0 a 600 000.

    d. En el campo **Tiempo de espera máximo (ms)**, ingrese el tiempo máximo de retención en milisegundos entre dos cálculos del algoritmo SPF. Rango de valores: de 0 a 600 000.

16. Si desea configurar el Anuncio de estado de vínculo (LSA) a los vecinos OSPF para el dispositivo CPE:

    a. Seleccione la casilla **Administrativo** para que el dispositivo CPE utilice la métrica máxima en los anuncios de estado de vínculo a los vecinos OSPF.

    b. Si desea especificar el tiempo durante el cual el dispositivo CPE debe usar la métrica máxima en el anuncio de estado de vínculo a los vecinos OSPF cuando se inicia o reinicia el protocolo OSPF:

        1. Seleccione la casilla **Durante inicio**. Esta casilla está desactivada por defecto.

        2. En el campo **Temporizador (s)**, ingrese el tiempo en segundos. Rango de valores: 5 a 86 400.

    c. Si desea especificar el tiempo durante el cual el dispositivo CPE debe usar la métrica máxima en el anuncio de estado de vínculo a los vecinos OSPF cuando el protocolo OSPF está deshabilitado:

        1. Seleccione la casilla **Durante el apagado**. Esta casilla está desactivada por defecto.

        2. En el campo **Temporizador (s)**, ingrese el tiempo en segundos. Rango de valores: de 5 a 100.

17. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar áreas de OSPF

Puede ver la tabla de áreas OSPF en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de áreas OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **OSPF → Áreas de OSPF**.

- Para ver la tabla de áreas OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **OSPF→ Áreas de OSPF**.

La información sobre las áreas OSPF se muestra en las siguientes columnas de la tabla:

- **Área de OSPF** es el ID del área OSPF en el formato de dirección IPv4 o un número entero.
- **Tipo de área** es el tipo del área de OSPF auxiliar:
  - **Talón**
  - **Talón NO-SUMMARY**
  - **NSSA**
  - **NSSA NO-SUMMARY**

  Este valor se muestra solo para áreas auxiliares.
- **Rangos de OSPF** especifica los rangos OSPF.
- **Administración** contiene las acciones que se pueden realizar con el área OSPF.

## Crear un área de OSPF

Puede crear un área de OSPF en una plantilla de CPE o en un dispositivo CPE. Cuando se crea un OSPF en la plantilla de CPE, se crea automáticamente en todos los dispositivos CPE a los que se aplica esta plantilla de CPE.

*Para crear un área de OSPF, siga estos pasos:*

1. Cree un área de OSPF de una de las siguientes maneras:
   - Si desea crear un área de OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF → Áreas de OSPF**.
   - Si desea crear un área de OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF→ Áreas de OSPF** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de áreas de OSPF.
2. Haga clic en **+ Área de OSPF**.
3. En la ventana que se abre, en el campo Área de OSPF, ingrese el ID del área de OSPF como una dirección IPv4 o un número entero.
4. Si desea convertir el área de OSPF en un área de código auxiliar:
   a. Seleccione la casilla de verificación **Talón**. Esta casilla está desactivada por defecto.
   b. En la lista desplegable **Tipo de área**, seleccione el tipo de área de OSPF auxiliar:
      - **Talón**
      - **Talón NO-SUMMARY**

- NSSA
- NSSA NO-SUMMARY

c. Si, en la lista desplegable **Tipo de área**, seleccionó**NSSA** o**NSSA NO-SUMMARY** y necesita evitar el anuncio de la ruta predeterminada 0.0.0.0/0 al área NSSA, seleccione la casilla de verificación **NSSA suprimir FA**. Esta casilla está desactivada por defecto.

d. En el campo **Costo predeterminado**, ingrese una métrica para la ruta predeterminada o para las rutas resumidas. Rango de valores: de 0 a 16 777 215.

5. Si desea utilizar el método de acceso directo para los cálculos de SPF, seleccione la casilla de verificación **Atajo**. Esta casilla está desactivada por defecto.

6. En la lista desplegable **Autenticación**, seleccione el método de autenticación de OSPF:

- **Función hash** para usar el algoritmo MD5.
- **Contraseña** para usar una contraseña no cifrada. Este método de autenticación es menos seguro que el algoritmo MD5, sin embargo, puede proporcionar autenticación cuando se utiliza en un entorno de red de confianza.

7. Si desea especificar rangos de OSPF, siga estos pasos:

a. En **Rangos de OSPF**, haga clic en **+ Rango**.

b. En el campo **Rango**, ingrese el prefijo IPv4 de las rutas.

c. En la lista desplegable **Acción**, seleccione la acción que se realizará con las rutas:

- **Anunciar** si desea anunciar rutas a través del protocolo de OSPF. Esta es la configuración predeterminada.
- **No anunciar** si no desea anunciar rutas a través del protocolo de OSPF.
- **Sustituir** para reemplazar el prefijo IPv4 de las rutas con el prefijo IPv4 especificado y luego anunciarlos a través del protocolo de OSPF. Si selecciona este valor, en el campo **Sustituir**, ingrese el prefijo IPv4.

d. Si ,en la lista desplegable **Acción**, seleccionó**Anunciar** o **Sustituir**, en el campo **Costo** ingrese una métrica para las rutas. Rango de valores: de 0 a 16 777 215.

El rango de OSPF se especifica y se muestra en **Rangos de OSPF**. Puede especificar varios rangos de OSPF o eliminar rangos de OSPF. Para eliminar un rango de OSPF, haga clic en el ícono de eliminar ✕ junto a él.

8. Si desea conectar un área de OSPF a otra área de OSPF a través de un área de OSPF de tránsito, especifique el vínculo virtual:

a. En **Vínculos virtuales**, haga clic en **+ Vínculo virtual**.

b. En el campo **Dirección**, ingrese la dirección IPv4 de la interfaz de red del enrutador en el área de tránsito.

El vínculo virtual se especifica y se muestra en **Rangos de OSPF**. Puede especificar varios vínculos virtuales o eliminar vínculos virtuales. Para eliminar un vínculo virtual, haga clic en el ícono de eliminar ✕ junto a él.

9. Si desea configurar el filtrado de rutas para el área de OSPF, en **Filtrado**, haga lo siguiente:

    a. Seleccione las listas de control de acceso creadas:

        1. En la lista desplegable **Exportar lista**, seleccione una lista de control de acceso para las rutas que se anuncian del área de OSPF a otras áreas de OSPF.

        2. En la lista desplegable **Importar lista**, seleccione una lista de control de acceso para las rutas que se anuncian de otra área OSPF al área de OSPF determinada.

    b. Seleccione las listas de acceso creadas:

        1. En la lista desplegable **Lista de filtros de salida**, seleccione una lista de prefijos para las rutas que se anuncian del área de OSPF a otras áreas de OSPF.

        2. En la lista desplegable **Lista de filtros de entrada**, seleccione una lista de prefijos para las rutas que se anuncian de otra área de OSPF al área de OSPF determinada.

10. Haga clic en **Guardar**.

    El área OSPF se crea y se muestra en la tabla.

11. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar un área de OSPF

Puede editar un área de OSPF en una plantilla de CPE o en un dispositivo. Un área de OSPF editada en la plantilla de CPE se edita automáticamente en todos los dispositivos CPE que utilizan esta plantilla.

*Para editar un área de OSPF:*

1. Edite un área de OSPF de una de las siguientes maneras:

    - Si desea editar un área de OSPF en una plantilla CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF → Áreas de OSPF**.

    - Si desea editar un área de OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF→ Áreas de OSPF** y la casilla **Anular**.

    Se muestra una tabla de áreas de OSPF.

2. Haga clic en **Editar** junto al área de OSPF que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración del área de OSPF. Para obtener una descripción de la configuración, consulte las instrucciones para crear un área de OSPF.

4. Haga clic en **Guardar**.

   El área de OSPF se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un área de OSPF

Puede eliminar un área OSPF en una plantilla de CPE o en un dispositivo CPE. Un área OSPF eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE.

Las áreas OSPF eliminadas no se pueden restaurar.

*Para eliminar un área OSPF, siga estos pasos:*

1. Elimine un área OSPF de una de las siguientes maneras:

   - Si desea eliminar un área OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF → Áreas de OSPF**.

   - Si desea eliminar un área OSPF en un dispositivo CPE, vaya a la sección el menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF→ Áreas de OSPF**y marque la casilla de verificación **Anular**.

   Se muestra una tabla de áreas de OSPF.

2. Haga clic en **Eliminar** junto al área OSPF que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El área OSPF se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar interfaces de OSPF

Puede ver la tabla de interfaces OSPF en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de interfaces OSPF en una plantilla de CPE, vaya a sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF → Interfaces de OSPF**.

- Para ver la tabla de interfaces OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **OSPF→ Interfaces de OSPF**.

La información sobre las interfaces OSPF se muestra en las siguientes columnas de la tabla:

- **Interfaz** es la interfaz de red utilizada como interfaz OSPF.
- **Área de OSPF** es el ID del área OSPF a la que pertenece la interfaz OSPF.
- **Autenticación** es el método de autenticación.
- **Tipo de red** es el tipo de red a la que está conectada la interfaz OSPF.
- **Administración** contiene las acciones que se pueden realizar con la interfaz OSPF.

## Crear una interfaz de OSPF

Puede crear una interfaz OSPF en una plantilla de CPE o en un dispositivo CPE. Una interfaz OSPF creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una interfaz OSPF, siga estos pasos:*

1. Cree una interfaz OSPF de una de las siguientes maneras:

   - Si desea crear una interfaz de OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF → Interfaces de OSPF**.
   - Si desea crear una interfaz de OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF → Interfaces de OSPF** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de interfaces de OSPF.

2. Haga clic en **+ Interfaz de OSPF**.
3. En la ventana que se abre, en la lista desplegable **Interfaz**, seleccione la interfaz de red creada que desea usar como interfaz OSPF.
4. En el campo **Área de OSPF**, ingrese el ID del área OSPF a la que pertenece la interfaz OSPF, como una dirección IPv4 o un número entero.
5. Si desea especificar la autenticación OSPF:

   a. En la lista desplegable **Autenticación**, seleccione un método de autenticación:

      - **Función hash** para usar el algoritmo MD5.
      - **Contraseña** para usar una contraseña no cifrada. Este método de autenticación es menos seguro que el algoritmo MD5, sin embargo, puede proporcionar autenticación cuando se utiliza en un entorno de red de confianza. Si selecciona esta opción, ingrese la contraseña de autenticación en el campo **Contraseña**.

   b. Si, en la lista desplegable **Autenticación**, seleccionó **Función hash**, siga estos pasos:

      1. En el campo **ID de clave**, ingrese el hash MD5. Rango de valores: 1 a 255.
      2. En el campo **Clave**, ingrese la clave MD5.

6. En el campo **Costo**, ingrese la métrica de la interfaz OSPF. Rango de valores: de 1 a 65 535.

7. En la lista desplegable **Tipo de red**, seleccione el tipo de red a la que está conectada la interfaz OSPF:

   - **Transmisión**
   - **Sin transmisión**
   - **Punto a multipunto**
   - **Punto a punto**

8. En el campo **Prioridad**, ingrese la prioridad de la interfaz OSPF. Cuanto mayor sea el valor, mayor será la prioridad de la interfaz OSPF.

   La interfaz OSPF de mayor prioridad se convierte en el enrutador designado del segmento de red. La interfaz OSPF con la segunda prioridad más alta se convierte en el enrutador designado de respaldo.

9. Si desea cambiar la interfaz OSPF al modo pasivo, seleccione la casilla **Interfaz pasiva**. En el modo pasivo, las interfaces OSPF no intercambian paquetes de tráfico.

10. Si desea utilizar el protocolo BFD para detectar la pérdida de conexión, seleccione la casilla **BFD**. Esta casilla está desactivada por defecto.

11. Si desea configurar temporizadores OSPF, siga estos pasos:

    a. Seleccione la casilla **Temporizadores de OSPF**. Esta casilla está desactivada por defecto.

    b. En el campo **Hello (s)**, ingrese el intervalo de tiempo en segundos que utiliza la interfaz OSPF para enviar paquetes de control a los vecinos OSPF. Rango de valores: de 1 a 65 535.

    c. En el campo **Apagado (s)** , ingrese el intervalo de tiempo en segundos que utiliza la interfaz OSPF para recibir paquetes de control de los vecinos OSPF. Si no se reciben paquetes de control de un vecino OSPF dentro del tiempo especificado, la interfaz OSPF considera que este vecino OSPF no está disponible. Rango de valores: de 1 a 65 535.

12. En el campo **Intervalo de retransmisión (s)**, ingrese el intervalo de tiempo en segundos para reenviar paquetes de Anuncio de estado de vínculo (LSA) a los vecinos OSPF que están detrás de la interfaz OSPF. Rango de valores: de 1 a 65 535. Para obtener más información, consulte RFC 2328 (el parámetro `RxmtInterval`).

13. En el campo **Demora de transmisión (s)**, ingrese el tiempo estimado en segundos que se requiere para enviar un paquete LSU (Actualización de estado de vínculo) a través de la interfaz OSPF. Rango de valores: de 1 a 65 535. Para obtener más información, consulte RFC 2328 (el parámetro `InfTransDelay`).

14. Haga clic en **Crear**.

    La interfaz OSPF se crea y se muestra en la tabla.

15. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Editar una interfaz de OSPF

Puede editar una interfaz OSPF en una plantilla de CPE o en un dispositivo CPE. Una interfaz OSPF editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una interfaz OSPF, siga estos pasos:*

1. Edite una interfaz OSPF de una de las siguientes maneras:

   - Si desea editar una interfaz OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF** → **Interfaces de OSPF**.

   - Si desea editar una interfaz OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo de CPE, seleccione la pestaña **OSPF**→ **Interfaces de OSPF** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de interfaces de OSPF.

2. Haga clic en **Editar** junto a la interfaz OSPF que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la interfaz OSPF. Para obtener una descripción de la configuración, consulte las instrucciones para crear una interfaz OSPF.

4. Haga clic en **Guardar**.

   La interfaz OSPF se modifica y actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Eliminar una interfaz de OSPF

Puede eliminar una interfaz de OSPF en una plantilla de CPE o en un dispositivo CPE. Una interfaz de OSPF eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

Las interfaces eliminadas no se pueden restaurar.

*Para eliminar una interfaz de OSPF, haga lo siguiente:*

1. Elimine una interfaz de OSPF de una de las siguientes maneras:

   - Si desea eliminar una interfaz de OSPF en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **OSPF** → **Interfaces de OSPF**.

   - Si desea eliminar una interfaz de OSPF en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **OSPF** → **Interfaces de OSPF** y seleccione la casilla de verificación **Anular**.

Se muestra una tabla de interfaces de OSPF.

2. Haga clic en **Eliminar** junto a la interfaz de OSPF que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La interfaz de OSPF se eliminará y ya no se mostrará en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Utilizar BFD para detectar fallas de enrutamiento

Kaspersky SD-WAN es compatible con el protocolo de Detección de reenvío bidireccional (BFD) para la detección rápida (en un segundo) de problemas de conexión de red en los vínculos. Cuando se detecta un problema, BFD transmite información acerca del problema del plano de datos al plano de control.

Entre pares de BFD, se establece una sesión BFD, como parte de la cual intercambian paquetes de control para detectar problemas de conexión de red. Si ocurren problemas con la conexión de la red, la sesión BFD en la interfaz SD-WAN del dispositivo CPE se finaliza, después de lo cual se reconstruyen las tablas de rutas.

Puede ver la tabla de pares de BFD en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de pares de BFD en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BFD**.

- Para ver la tabla de pares de BFD en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **BFD**.

La información sobre los pares de BFD se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del par de BFD.

- **Dirección IP** es la dirección IPv4 del par de BFD.

- **Intervalo de transmisión (ms)** es el intervalo de tiempo en milisegundos para enviar paquetes de control del dispositivo CPE al par de BFD.

- **Intervalo de recepción (ms)** es el intervalo de tiempo en milisegundos para recibir paquetes de control del par de BFD en el dispositivo CPE. Si no se reciben paquetes de control del par de BFD dentro del tiempo especificado, el dispositivo CPE considera que este par de BFD no está disponible.

- **Multiplicador** es el multiplicador del intervalo de tiempo para enviar los paquetes de control especificados en la configuración de pares de BFD. Este multiplicador determina la cantidad de milisegundos durante los cuales el dispositivo CPE espera la recepción de paquetes de control del par de BFD. Si no se reciben paquetes de control del par de BFD dentro de este tiempo, el dispositivo CPE anuncia un problema de conexión de red.

- **Administración** contiene las acciones que se pueden realizar con el par de BFD.

# Habilitar o deshabilitar el protocolo BFD

Puede habilitar o deshabilitar el protocolo BFD en una plantilla de CPE o en un dispositivo CPE. El protocolo BFD habilitado o deshabilitado en la plantilla de CPE se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE.

*Para habilitar o deshabilitar el protocolo BFD, siga estos pasos:*

1. Habilite o deshabilite el protocolo BFD de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar el protocolo BFD en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BFD**.

   - Si desea habilitar o deshabilitar el protocolo BFD en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BFD** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BFD.

2. En la lista desplegable **BFD**, seleccione uno de los valores siguientes:

   - **Habilitado**

   - **Deshabilitado** Esta es la configuración predeterminada.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Crear un par de BFD

Puede crear un par de BFD en una plantilla de CPE o en un dispositivo CPE. Un par de BFD creado en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. Antes de crear un par de BFD, debe habilitar el protocolo de BFD.

*Para crear un par de BFD, siga estos pasos:*

1. Cree un par de BFD de una de las siguientes maneras:

   - Si desea crear un par de BFD en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BFD**.

   - Si desea crear un par de BFD en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BFD** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BFD.

2. Haga clic en **+ Par BFD**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del par de BFD. La longitud máxima del nombre es de 255 caracteres.

4. En el campo **Dirección IP**, ingrese la dirección IPv4 del par de BFD.

5. En el campo **Intervalo de transmisión (ms)**, ingrese el intervalo de tiempo en milisegundos para enviar paquetes de control del dispositivo CPE al par de BFD. Rango de valores: de 60 a 10 000.

6. En el campo **Intervalo de recepción (ms)**, ingrese el intervalo de tiempo en milisegundos para recibir paquetes de control del par de BFD en el dispositivo CPE. Si no se reciben paquetes de control del par de BFD dentro del tiempo especificado, el dispositivo CPE considera que este par de BFD no está disponible. Rango de valores: de 60 a 10 000.

7. En **Multiplicador**, ingrese el multiplicador del intervalo de tiempo para enviar paquetes de control especificados en la configuración de pares de BFD. Este multiplicador determina la cantidad de milisegundos durante los cuales el dispositivo CPE espera la recepción de paquetes de control del par de BFD. Si no se reciben paquetes de control del par de BFD dentro de este tiempo, el dispositivo CPE anuncia un problema de conexión de red. Rango de valores: de 2 a 255.

   Por ejemplo, si el intervalo de tiempo para enviar paquetes de control en la configuración del par de BFD es de 200 milisegundos y especifica un multiplicador de 2, entonces, si después de 400 milisegundos no se reciben paquetes de control de ese par de BFD, el dispositivo CPE anuncia un problema de conexión de red.

8. Haga clic en **Crear**.

   El par de BFD se crea y se muestra en la tabla.

9. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Editar un par de BFD

Puede editar un par de BFD en una plantilla de CPE o en un dispositivo CPE. Un par de BFD editado en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar un par de BFD, siga estos pasos:*

1. Edite un par de BFD de una de las siguientes maneras:

   - Si desea editar un par de BFD en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BFD**.

   - Si desea editar un par de BFD en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BFD** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BFD.

2. Haga clic en **Editar** junto al par de BFD que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de pares de BFD. Para obtener una descripción de la configuración, consulte las instrucciones para crear un par de BFD.

4. Haga clic en **Guardar**.

   El par de BFD se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un par de BFD

Puede eliminar un par de BFD en una plantilla de CPE o en un dispositivo CPE. Un par BFD eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

Los pares BFD eliminados no se pueden restaurar.

*Para eliminar un par BFD:*

1. Elimine un par BFD de una de las siguientes maneras:

   - Si desea eliminar un par BFD en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **BFD**.
   - Si desea eliminar un par BFD en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **BFD** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de pares BFD.

2. Haga clic en **Eliminar** junto al par BFD que desea eliminar.

3. En la ventana que se abre, haga clic en **Eliminar**.

   El par BFD se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Garantizar una alta disponibilidad con VRRP

Kaspersky SD-WAN es compatible con el Protocolo de redundancia de enrutador virtual (VRRP) para combinar interfaces de red de varios dispositivos CPE en enrutadores virtuales. Cuando las interfaces de red se combinan en un enrutador virtual, comparten una dirección IP virtual. Una interfaz de red es la principal y las otras son secundarias. Se asigna una dirección IP virtual a la interfaz de red principal.

Las interfaces de red en un enrutador virtual intercambian paquetes de control para determinar qué interfaces de red fallaron. Si una interfaz de red principal falla, se elige una nueva interfaz de red principal y se le asigna una dirección IP virtual. La nueva interfaz de red principal asume automáticamente el tráfico que se retransmitió a la dirección IP virtual a través de la interfaz de red fallida.

Puede crear instancias de VRRP para combinar interfaces de red en enrutadores virtuales. Cuando crea una instancia de VRRP, debe especificar una interfaz de red, un ID de enrutador virtual (VRID) y una dirección IP virtual. Las interfaces de red se combinan en un enrutador virtual si se especifican el mismo ID de enrutador virtual y la misma dirección IP virtual en las instancias de VRRP creadas para ellas.

Si necesita cambiar sincrónicamente la interfaz de red principal en varios enrutadores virtuales, puede crear grupos de instancias de VRRP. Si la interfaz de red principal cambia en una de las instancias de VRRP, este cambio también ocurre en todas las demás instancias de VRRP en el grupo de instancias de VRRP.

# Habilitar o deshabilitar el protocolo VRRP

Puede habilitar o deshabilitar el protocolo VRRP en una plantilla de CPE o en un dispositivo CPE. El protocolo VRRP habilitado o deshabilitado en la plantilla de CPE se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE.

*Para habilitar o deshabilitar el protocolo VRRP, siga estos pasos:*

1. Habilite o deshabilite el protocolo VRRP de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar el protocolo VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP→ Instancias de VRRP**.

   - Si desea habilitar o deshabilitar el protocolo VRRP en un dispositivo CPE, vaya a la sección el menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP→ Instancias de VRRP** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de instancias de VRPP.

2. En la lista desplegable **VRRP**, seleccione uno de los valores siguientes:

   - **Habilitado**

   - **Deshabilitado** Esta es la configuración predeterminada.

   Cuando habilita VRRP, debe crear al menos una instancia de VRRP.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar instancias de VRRP

Puede ver la tabla de instancias de VRRP en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de instancias de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Instancias de VRRP → VRRP**.

- Para ver la tabla de instancias de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRRP→ Instancias de VRRP**.

La información sobre las instancias de VRRP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la instancia de VRRP.
- **VRID** es el ID del enrutador virtual.
- **Interfaz** es la interfaz de red que se agregó al enrutador virtual.
- **VIP** es la dirección IP virtual asignada a la interfaz de red.
- **Estado** es la función de la interfaz de red:
  - **Respaldo** es la interfaz de red de respaldo.
  - **Principal** es la interfaz de red principal.
- **Prioridad** es la prioridad de la interfaz de red. Cuanto mayor sea el valor, más alta será la prioridad. Cuando la interfaz de red principal falla, se reemplaza por la interfaz de red de respaldo con la prioridad más alta. Si, cuando selecciona la nueva interfaz de red principal, todas las interfaces de red de respaldo tienen la misma prioridad, la nueva interfaz de red principal se selecciona al azar.
- **Intervalo de anuncios (s)** es el intervalo de tiempo en segundos para enviar paquetes de control de una interfaz de red a otras interfaces de red.
- **Nopreempt** especifica si la función de la interfaz de red que se convirtió en la principal debe cambiar si la interfaz de red principal anterior se recupera:
  - **Sí**.
  - **No**.
- **Administración** contiene las acciones que se pueden realizar con la instancia de VRRP.

## Crear una instancia de VRRP

Puede crear una instancia de VRRP en una plantilla de CPE o en un dispositivo CPE. Una instancia de VRRP que ha sido creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una instancia de VRRP, haga lo siguiente:*

1. Cree una instancia de VRRP de una de las siguientes maneras:
   - Si desea crear una instancia de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP → Instancias de VRRP**.
   - Si desea crear una instancia de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP → Instancias de VRRP** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de instancias de VRPP.
2. Haga clic en **+ Instancia de VRRP**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la instancia de VRRP. La longitud máxima del nombre es de 16 caracteres.

4. En el campo **VRID**, ingrese el ID del enrutador virtual. Debe especificar el mismo ID cuando se crean instancias de VRRP para todas las interfaces de red que desea combinar en un enrutador virtual. Rango de valores: 1 a 255.

5. En la lista desplegable **Interfaz**, seleccione la interfaz de red creada que desea agregar al enrutador virtual.

6. En el campo **VIP**, ingrese la dirección IP virtual que desea asignar a esta interfaz de red. Debe asignar la misma dirección IP virtual a todas las interfaces de red que desee combinar en un enrutador virtual.

7. En la lista desplegable **Estado**, seleccione la función de la interfaz de red:

   - **Respaldo** es la interfaz de red de respaldo. Esta es la configuración predeterminada.
   - **Principal** es la interfaz de red principal.

8. En el campo **Prioridad**, ingrese la prioridad de la interfaz de red. Cuanto mayor sea el valor, más alta será la prioridad. Cuando la interfaz de red principal falla, se reemplaza por la interfaz de red de respaldo con la prioridad más alta. Si, cuando selecciona la nueva interfaz de red principal, todas las interfaces de red de respaldo tienen la misma prioridad, la nueva interfaz de red principal se selecciona al azar. Rango de valores: 1 a 255. El valor predeterminado es `100`.

9. En el campo **Intervalo de anuncios (s)**, ingrese el intervalo de tiempo en segundos para el envío de paquetes de control desde una interfaz de red a otras interfaces de red. Rango de valores: 1 a 60. El valor predeterminado es `5`.

10. Si no desea cambiar la función de la interfaz de red de respaldo que se ha convertido en el enrutador principal, incluso si la interfaz de red principal anterior vuelve a funcionar, seleccione la casilla de verificación **Nopreempt**. Esta casilla está desactivada por defecto.

11. Si desea configurar el envío de unidifusión de los paquetes de control a través de la interfaz de red, haga lo siguiente:

    a. Seleccione la casilla de verificación **Unidifusión**. Esta casilla está desactivada por defecto.

    b. En el campo **IP de origen unidifusión**, ingrese la dirección IP de la interfaz de red de origen para el envío de los paquetes de control.

    c. En el campo **IP de par unidifusión**, ingrese la dirección IP de la interfaz de red de destino para el envío de los paquetes de control.

    De manera predeterminada, la interfaz de red utiliza multidifusión para enviar los paquetes de control.

12. Si desea utilizar una contraseña para la autenticación de los paquetes de control en la interfaz de red, haga lo siguiente:

    a. Seleccione la casilla de verificación **Autenticación**. Esta casilla está desactivada por defecto.

    b. Ingrese una contraseña en el campo que se muestra. La longitud máxima de la contraseña es de 16 caracteres. Debe especificar la misma contraseña para todas las interfaces de red que desee combinar en un enrutador virtual. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar.

13. Haga clic en **Crear**.

    Se crea la instancia de VRRP y se muestra en la tabla.

14. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar una instancia de VRRP

Puede editar una instancia de VRRP en una plantilla de CPE o en un dispositivo CPE. Una instancia de VRRP editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE. No puede editar una instancia de VRRP heredada de una plantilla de CPE en un dispositivo CPE.

*Para editar una instancia de VRRP, siga estos pasos:*

1. Edite una instancia de VRRP de una de las siguientes maneras:

   - Si desea editar una instancia de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP** → **Instancias de VRRP**.

   - Si desea editar una instancia de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP**→ **Instancias de VRRP**y marque la casilla de verificación **Anular**.

   Se muestra una tabla de instancias de VRPP.

2. Haga clic en **Editar** junto a la instancia de VRRP que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la instancia de VRRP. Para obtener una descripción de la configuración, consulte las instrucciones para crear una instancia de VRRP.

4. Haga clic en **Guardar**.

   La instancia de VRRP se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una instancia de VRRP

Puede eliminar una instancia de VRRP en una plantilla de CPE o en un dispositivo CPE. Una instancia de VRRP eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede eliminar una instancia de VRRP heredada de una plantilla de CPE en un dispositivo CPE.

Las instancias de VRRP eliminadas no se pueden restaurar.

*Para eliminar una instancia de VRRP, siga estos pasos:*

1. Elimine una instancia de VRRP de una de las siguientes maneras:

   - Si desea eliminar una instancia de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP** → **Instancias de VRRP**.

   - Si desea eliminar una instancia de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP** → **Instancias de VRRP** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de instancias de VRPP.

2. Haga clic en **Eliminar** junto a la instancia de VRRP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La instancia de VRRP se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar grupos de instancias de VRRP

Puede ver la tabla de grupos de instancias de VRRP en una plantilla de CPE y en un dispositivo de CPE:

- Para ver la tabla de grupos de instancias de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN**→ **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP**.

- Para ver la tabla de grupos de instancias de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP**.

La información sobre los grupos de instancias de VRRP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del grupo de instancias de VRRP.

- **Instancias de VRRP** son instancias de VRRP que se agregaron al grupo de instancias de VRRP.

- **Administración** contiene las acciones que se pueden realizar con el grupo de instancias de VRRP.

## Crear un grupo de instancias de VRRP

Puede crear un grupo de instancias de VRRP en una plantilla de CPE o en un dispositivo CPE. Un grupo de instancias de VRRP creado en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que usan esta plantilla.

*Para crear un grupo de instancias de VRRP:*

1. Cree un grupo de instancias de VRRP de una de las siguientes maneras:

   - Si desea crear un grupo de instancias VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP**.

   - Si desea crear un grupo de instancias VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP** y la casilla **Anular**.

   Se muestra una tabla de grupos de instancias de VRRP.

2. Haga clic en **+ Grupo de instancias de VRRP**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del grupo de instancias de VRRP. La longitud máxima del nombre es de 16 caracteres. El valor predeterminado es `1`.

4. En la lista desplegable **Instancias de VRRP**, seleccione la instancia de VRRP creada que desea agregar al grupo de instancias de VRRP.

   La instancia de VRRP se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias instancias de VRRP o eliminarlas. Para eliminar una instancia de VRRP, haga clic en **Eliminar** junto a ella.

5. Haga clic en **Crear**.

   El grupo de instancias de VRRP se crea y se muestra en la tabla.

6. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar un grupo de instancias de VRRP

Puede editar un grupo de instancias de VRRP en una plantilla de CPE o en un dispositivo de CPE. Un grupo de instancias de VRRP editado en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede editar un grupo de instancias de VRRP heredado de una plantilla de CPE en un dispositivo CPE.

*Para editar un grupo de instancias de VRRP, siga estos pasos:*

1. Edite un grupo de instancias de VRRP de una de las siguientes maneras:

   - Si desea editar un grupo de instancias de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP**.

   - Si desea editar un grupo de instancias de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP**→ **Grupos de instancias de VRRP** y la casilla **Anular**.

   Se muestra una tabla de grupos de instancias de VRRP.

2. Haga clic en **Editar** junto al grupo de instancias de VRRP que desea editar.

3. En la ventana que se abre, si es necesario, edite el nombre del grupo de instancias de VRRP y agregue o elimine las instancias de VRRP creadas.

4. Haga clic en **Guardar**.

   El grupo de instancias de VRRP se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar un grupo de instancias de VRRP

Puede eliminar un grupo de instancias de VRRP en una plantilla de CPE o en un dispositivo CPE. Un grupo de instancias de VRRP eliminado en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede eliminar un grupo de instancias de VRRP heredado de una plantilla de CPE en un dispositivo CPE.

Los grupos de instancias de VRRP eliminados no se pueden restaurar.

*Para eliminar un grupo de instancias de VRRP, siga estos pasos:*

1. Elimine un grupo de instancias de VRRP de una de las siguientes maneras:

   - Si desea eliminar un grupo de instancias de VRRP en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRRP→ Grupos de instancias de VRRP**.

   - Si desea eliminar un grupo de instancias de VRRP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **VRRP→ Grupos de instancias de VRRP** y la casilla **Anular**.

   Se muestra una tabla de grupos de instancias de VRRP.

2. Haga clic en **Eliminar** junto al grupo de instancias de VRRP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El grupo de instancias de VRRP se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Transmisión de tráfico multidifusión mediante protocolos PIM e IGMP

Kaspersky SD-WAN admite la transmisión de tráfico de multidifusión entre dispositivos CPE y dispositivos de red externos mediante los protocolos PIM e IGMP. Puede especificar la configuración básica del protocolo PIM en los dispositivos CPE, por ejemplo, los puntos de encuentro que se utilizarán, y luego crear interfaces de multidifusión para la interacción con otros dispositivos CPE. Las interfaces de red creadas se utilizan como interfaces de multidifusión.

Si se establece la conectividad PIM entre los dispositivos CPE y se definen puntos de encuentro para estos dispositivos, las interfaces de multidifusión pueden recibir solicitudes IGMP de los clientes a través de IGMP. Las solicitudes IGMP contienen direcciones IP de orígenes de los cuales los clientes desean recibir paquetes de tráfico de multidifusión. Cuando los orígenes envían paquetes de multidifusión a un punto de encuentro, los clientes reciben estos paquetes de tráfico de multidifusión.

Si es necesario, puede usar el protocolo PIM para conectar dispositivos CPE a enrutadores externos. Para hacerlo, debe habilitar el protocolo PIM en la interfaz de multidifusión a la que está conectado el enrutador externo.

## Configuración básica de PIM

Puede especificar la configuración básica de PIM en una plantilla de CPE o en el dispositivo CPE. La configuración básica de PIM especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para modificar la configuración básica de PIM, siga estos pasos:*

1. Especifique la configuración básica de PIM de una de las siguientes maneras:

   - Si desea editar la configuración básica de PIM en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Multidifusión**.

   - Si desea editar la configuración básica de PIM en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Multidifusión**.

   De manera predeterminada, está seleccionada la pestaña **Configuración general**, que muestra la configuración básica de PIM.

2. En la lista desplegable **Multidifusión**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

3. Especifique el punto de encuentro para los orígenes de paquetes de tráfico de multidifusión y los clientes que están conectados al dispositivo CPE:

   a. En **IP de RP**, haga clic en **+ Agregar** e ingrese la dirección IPv4 del punto de encuentro.

   b. Si desea especificar un grupo de multidifusión asociado con el punto de encuentro, en **Grupo de RP**, ingrese el prefijo IPv4 de su grupo de multidifusión. Cada punto de encuentro se puede asociar con un grupo de multidifusión exclusivo.

El punto de encuentro se especifica y se muestra en las secciones **IP de RP** y **Grupo de RP**. Puede especificar varios puntos de encuentro o eliminarlos. Para eliminar un punto de encuentro, haga clic en el ícono de eliminar ✕ junto a él.

4. En el campo **Temporizador keepalive de RP (s)**, ingrese la duración en segundos de los flujos de tráfico entre el origen y el grupo de multidifusión (S, G). La cuenta regresiva se reinicia si el dispositivo CPE recibe un paquete de registro. Rango de valores: de 31 a 60 000. El valor predeterminado es `185`.

5. Si desea filtrar paquetes de tráfico de multidifusión con las direcciones IPv4 de origen especificadas en el dispositivo CPE, en la lista desplegable **Lista de aceptación del registro de PIM**, seleccione una lista de prefijos creada.

6. Si un dispositivo CPE está en el último salto y desea evitar que este dispositivo CPE cambie del árbol compartido al árbol de ruta más corta (SPT) cuando se transmiten paquetes de tráfico de multidifusión:

   a. Seleccione la casilla **Conmutación de SPT**. Esta casilla está desactivada por defecto.

   b. Si desea denegar o permitir el cambio del árbol de puntos de encuentro (RPT) al árbol de la ruta más corta cuando se transmiten paquetes de tráfico de grupos de multidifusión con prefijos de IPv4 de origen especificados, seleccione una lista de prefijos creada en la lista desplegable **Lista de prefijos de SPT**. Si la conmutación está permitida o denegada se determina de la siguiente manera:

      - Si la lista de prefijos permite el prefijo IPv4, la conmutación no se produce.
      - Si la lista de prefijos niega el prefijo IPv4, se produce la conmutación.

7. Si desea realizar el equilibrio de ECMP en un dispositivo CPE para distribuir flujos de tráfico de multidifusión a través de múltiples rutas:

   a. Seleccione la casilla **ECMP**. Esta casilla está desactivada por defecto. Para el equilibrio de ECMP, deben existir varias rutas. Si el equilibrio de ECMP está deshabilitado, el tráfico se transmite a lo largo de una ruta.

   b. Si desea equilibrar todo el tráfico entre las rutas restantes en caso de que una de las interfaces de multidifusión falle, seleccione la casilla **Reequilibrio de ECMP**. La casilla está desactivada de manera predeterminada y, si una de las interfaces de multidifusión falla, solo se redistribuye el tráfico que se transmitió a través de esa interfaz de multidifusión.

8. En el campo **Intervalo de conexión/eliminación de PIM (s)**, ingrese el intervalo de tiempo en segundos para que las interfaces de multidifusión envíen paquetes de unión/eliminación a los pares PIM. Rango de valores: de 60 a 600. El valor predeterminado es `60`.

9. En el campo **Temporizador keepalive de PIM (s)**, ingrese la duración en segundos de los flujos de tráfico entre el origen y el grupo de multidifusión (S, G). La cuenta regresiva se reinicia si el dispositivo CPE recibe un paquete de unión/eliminación. Rango de valores: de 31 a 60 000. El valor predeterminado es `210`.

10. Si desea que el dispositivo CPE retransmita paquetes de tráfico con prefijos IPv4 de origen especificados de grupos de multidifusión a pedido del cliente (multidifusión específica de origen; SSM), en la lista desplegable **Lista de prefijos de SSM**, seleccione un lista de prefijos creada.

11. En la lista desplegable **Modo de búsqueda de RPF**, seleccione un modo de búsqueda de Reenvío de ruta inversa (RPF) en el dispositivo CPE:

    - **longer-prefix**.
    - **lower-distance**.

- **mrib-only**.
- **mrib-then-urib**. Esta es la configuración predeterminada.
- **urib-only**.

12. Si desea agregar una ruta IPv4 estática a la tabla de enrutamiento de multidifusión del dispositivo CPE:
    a. En **Rutas de multidifusión estáticas**, haga clic en **+ Agregar**.
    b. En el campo **Destino de IP**, ingrese la dirección IPv4 de destino de la ruta estática.
    c. En la lista desplegable **Tipo**, seleccione el tipo de origen de la ruta estática:
        - **Dirección** es una dirección IPv4. Si selecciona este valor, en el campo **Nexthop**, ingrese la dirección IPv4 de origen y el prefijo de la ruta estática.
        - **Interfaz** es la interfaz de red creada. Si selecciona este valor, en la lista desplegable **Nexthop**, seleccione la interfaz de red de origen de la ruta estática.
    d. Si es necesario, en el campo **Distancia**, ingrese la métrica de la ruta estática. Rango de valores: 1 a 255.

    La ruta estática se agrega y se muestra en **Rutas de multidifusión estáticas**. Puede agregar varias rutas estáticas o eliminar rutas estáticas. Para eliminar una ruta estática, haga clic en el ícono de eliminar ✕ junto a ella.

13. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar interfaces de multidifusión

Puede ver la tabla de interfaces de multidifusión en una plantilla de CPE y en un dispositivo CPE:

- Para ver la tabla de interfaces de multidifusión en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Multidifusión→ Interfaces**.
- Para ver la tabla de interfaces de multidifusión en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Multidifusión→ Interfaces**.

La información sobre las interfaces de multidifusión se muestra en las siguientes columnas de la tabla:

- **Interfaz de red** es la interfaz de red utilizada como interfaz de multidifusión.
- **PIM** indica si el intercambio de mensajes con pares a través del protocolo PIM está habilitado en la interfaz de multidifusión:
    - **Habilitado**
    - **Deshabilitado**

- **IGMP** indica si el intercambio de mensajes con pares a través del protocolo IGMP está habilitado en la interfaz de multidifusión:
  - **Habilitado**
  - **Deshabilitado**
- **Prioridad de DR** es la prioridad de la interfaz de multidifusión. La interfaz de multidifusión de mayor prioridad se convierte en el enrutador designado del segmento LAN. Cuanto mayor sea el valor, mayor será la prioridad de la interfaz de multidifusión.
- **Heredado** indica si la interfaz de multidifusión se hereda de la plantilla CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Administración** contiene las acciones que se pueden realizar con la interfaz de multidifusión.

## Crear una interfaz de multidifusión

Puede crear una interfaz de multidifusión en una plantilla de CPE o en un dispositivo individual. Una interfaz de multidifusión creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una interfaz de multidifusión, haga lo siguiente:*

1. Cree una interfaz de multidifusión de una de las siguientes maneras:
   - Si desea crear una interfaz de multidifusión en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Multidifusión** → **Interfaces**.
   - Si desea crear una interfaz de multidifusión en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Multidifusión** → **Interfaces** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de interfaces de multidifusión.
2. Haga clic en **+ interfaz de multidifusión**.
3. En la ventana que se abre, en la lista desplegable **Interfaz de red**, seleccione una interfaz de red creada que desee usar como interfaz de multidifusión.
4. Configure el protocolo PIM en la interfaz de multidifusión:
   a. En la lista desplegable **PIM**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.
   b. Si desea cambiar la interfaz de multidifusión al modo pasivo, seleccione la casilla de verificación **Pasiva**. En el modo pasivo, las interfaces de multidifusión no intercambian paquetes de control. Esta casilla está desactivada por defecto.

c. Si desea prohibir el intercambio de paquetes bootstrap en la interfaz de multidifusión, desmarque la casilla de verificación **BSM**. Esta casilla está seleccionada por defecto.

d. Si desea prohibir el intercambio de paquetes bootstrap de unidifusión en la interfaz de multidifusión, desmarque la casilla de verificación **BSM unidifusión**. Esta casilla está seleccionada por defecto.

e. En el campo **Prioridad de DR**, ingrese la prioridad de la interfaz de multidifusión. La interfaz de multidifusión de mayor prioridad se convierte en el enrutador designado del segmento LAN. Cuanto mayor sea el valor, mayor será la prioridad de la interfaz de multidifusión. Rango de valores: 1 a 4 294 967 295. El valor predeterminado es `1`.

f. En el campo **Hello (s)**, ingrese el intervalo de tiempo en segundos que la interfaz de multidifusión utiliza para enviar los paquetes de control a los vecinos PIM. Rango de valores: 1 a 180. El valor predeterminado es `30`.

g. En el campo **Espera (s)**, ingrese el intervalo de tiempo en segundos que la interfaz de multidifusión utiliza para recibir los paquetes de control de los PIM vecinos. Si no se reciben paquetes de control de un vecino PIM dentro del tiempo especificado, la interfaz de PIM considera que este vecino PIM no está disponible. Rango de valores: 1 a 630. El valor predeterminado es `105`.

h. Si se asignan varias direcciones IP a una interfaz de multidifusión y desea utilizar la dirección IPv4 de origen especificada cuando se envíen los mensajes de PIM, ingrese la dirección IPv4 en el campo **IP de origen**.

5. Configure el protocolo IGMP en la interfaz de multidifusión:

a. En la lista desplegable **IGMP**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

b. En la lista desplegable **Versión**, seleccione la versión del protocolo IGMP en la interfaz de multidifusión:

- **2**.
- **3**. Esta es la configuración predeterminada.

c. En el campo **Intervalo de consulta (s)**, ingrese el intervalo de tiempo en segundos para enviar consultas desde la interfaz de multidifusión a los clientes. Las consultas se utilizan para determinar si es necesario enviar tráfico de multidifusión a los clientes. Rango de valores: 1 a 250. El valor predeterminado es `125`.

d. En el campo **Tiempo de respuesta a consultas (s)**, ingrese el tiempo en segundos que la interfaz de multidifusión debe esperar para recibir respuestas de los clientes. Si no se recibe una respuesta a una consulta del cliente dentro del tiempo especificado, la interfaz de multidifusión no envía los paquetes de tráfico. Rango de valores: 1 a 125. El valor predeterminado es `10`.

e. Si desea especificar grupos de multidifusión, haga lo siguiente:

1. En **Conectarse con el grupo**, haga clic en **+ Agregar** e ingrese la dirección IPv4 del grupo de multidifusión.

2. Si desea conectar la interfaz de multidifusión al origen especificado del grupo de multidifusión, en **Dirección de la fuente**, ingrese la dirección IPv4 del origen.

El grupo de multidifusión se especifica y se muestra en las secciones **Conectarse con el grupo** y **Dirección de la fuente**. Puede especificar varios grupos de multidifusión o eliminar grupos de multidifusión. Para eliminar un grupo de multidifusión, haga clic en el ícono de eliminar ✕ junto a él.

Debe especificar grupos de multidifusión en uno de los siguientes casos:

- El segmento de red tiene clientes permanentes a los que debe enviar paquetes de tráfico desde un grupo de multidifusión de manera rápida y estable.
- El segmento de red no contiene clientes o los hosts en el segmento no pueden enviar mensajes de informes, pero los paquetes de tráfico de un grupo de multidifusión deben enviarse a este segmento.

6. Haga clic en **Crear**.

   La interfaz de multidifusión se creará y se mostrará en la tabla.

7. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Editar una interfaz de multidifusión

Puede editar la configuración de la interfaz de multidifusión en una plantilla de CPE o en un dispositivo CPE. Una interfaz de multidifusión editada en la plantilla de CPE se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para editar una interfaz de multidifusión, siga estos pasos:*

1. Edite una interfaz de multidifusión de una de las siguientes maneras:

   - Si desea editar una interfaz de multidifusión en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Multidifusión** → **Interfaces**.
   - Si desea editar una interfaz de multidifusión en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Multidifusión** → **Interfaces** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de interfaces de multidifusión.

2. Haga clic en **Editar** junto a la interfaz de multidifusión que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la interfaz de multidifusión. Para obtener una descripción de la configuración, consulte las instrucciones para crear una interfaz de multidifusión.

4. Haga clic en **Guardar**.

   La interfaz de multidifusión se modifica y actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Eliminar una interfaz de multidifusión

Puede eliminar una interfaz de multidifusión en una plantilla CPE o en un dispositivo CPE. Una interfaz de multidifusión eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

Las interfaces de multidifusión eliminadas no se pueden restaurar.

*Para eliminar una interfaz de multidifusión, siga estos pasos:*

1. Elimine una interfaz de multidifusión de una de las siguientes maneras:

   - Si desea eliminar una interfaz de multidifusión en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Multidifusión → Interfaces** .
   - Si desea eliminar una interfaz de multidifusión en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Multidifusión→ Interfaces** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de interfaces de multidifusión.

2. Haga clic en **Eliminar** junto a la interfaz de multidifusión que desea eliminar.
3. En la ventana de confirmación, haga clic en **Eliminar**.

   La interfaz de multidifusión se elimina y ya no se muestra en la tabla.
4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Administrar tablas de enrutamiento y reenvío virtuales (VRF)

Kaspersky SD-WAN es compatible con la tecnología de enrutamiento y reenvío virtuales (VRF) para crear tablas de enrutamiento y reenvío virtuales en dispositivos CPE. Puede crear hasta 100 tablas de enrutamiento y reenvío virtuales.

Cuando crea una tabla de enrutamiento y reenvío virtuales, debe seleccionar las interfaces de red que desea agregar. No puede agregar la misma interfaz de red a varias tablas de enrutamiento y reenvío virtuales. Las interfaces de red para conectar el dispositivo CPE al controlador y al orquestador se agregan automáticamente a la tabla de enrutamiento y reenvío virtuales predeterminada y no se pueden agregar a otras tablas de enrutamiento y reenvío virtuales.

Si se agregan interfaces de red a diferentes tablas de enrutamiento y reenvío virtuales, las redes conectadas a estas interfaces de red no tienen conexión entre sí. En esta situación, las interfaces de red pueden tener direcciones IP de subredes idénticas o superpuestas.

Cuando crea una tabla de enrutamiento y reenvío virtuales, se crea automáticamente una interfaz de red del sistema correspondiente a esta tabla de enrutamiento y reenvío virtuales en el dispositivo CPE. Esta interfaz de red del sistema se utiliza para reenviar el tráfico de red entre las interfaces de red en la tabla de enrutamiento y reenvío virtuales. Para que la interfaz de red del sistema funcione, debe crear un registro en la interfaz web del orquestador.

Cuando crea una tabla de enrutamiento y reenvío virtuales, puede crear una ruta de agujero negro para aislar el tráfico. En este caso, la ruta de agujero negro 0.0.0.0/0 se crea automáticamente en el dispositivo y la información al respecto se muestra en la sección **Rutas estáticas**. Sin una ruta de agujero negro, el tráfico puede terminar en otras tablas de enrutamiento y reenvío virtuales.

Si no se asignan zonas de firewall a las interfaces de red en la tabla de enrutamiento y reenvío virtuales, debe asegurarse de que, de manera predeterminada, el firewall del dispositivo CPE acepte paquetes de tráfico reenviados entre las interfaces de red y las subredes. Puede especificar acciones predeterminadas cuando ajusta la configuración básica del firewall.

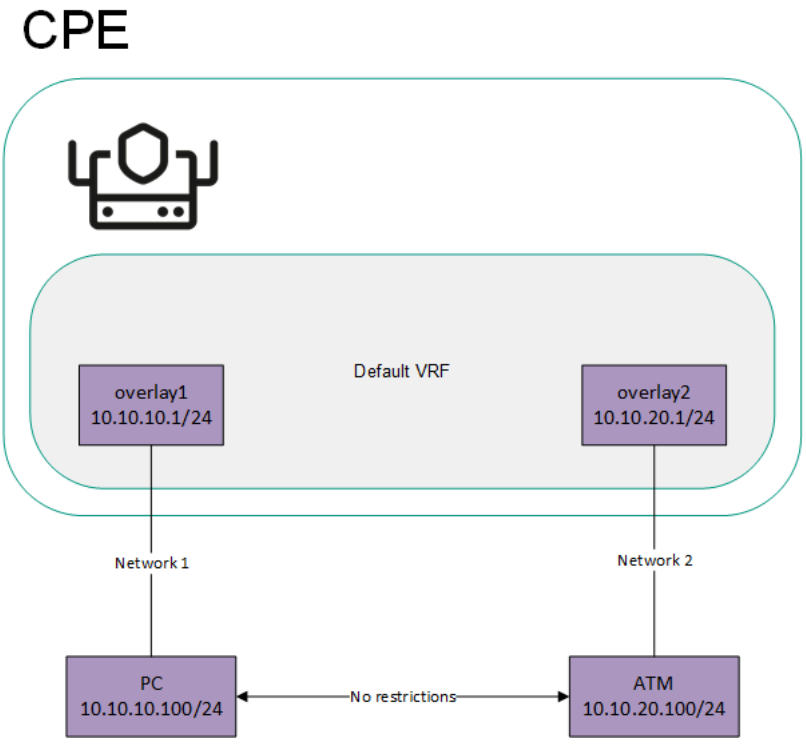
Si las zonas de firewall se asignan a las interfaces de red en la tabla de enrutamiento y reenvío virtuales, y el firewall del dispositivo CPE no acepta, de manera predeterminada, los paquetes de tráfico reenviados entre las interfaces de red y las subredes, debe asignar una zona de firewall a la interfaz de red del sistema. La zona de firewall asignada también debe asignarse a una de las interfaces de red en la tabla de enrutamiento y reenvío virtuales.

Puede agregar rutas de BGP y rutas estáticas a las tablas de enrutamiento y reenvío virtuales de un dispositivo CPE. Para agregar rutas de BGP a una tabla de enrutamiento y reenvío virtuales, especifique esa tabla de enrutamiento y reenvío virtuales cuando edite la configuración básica de BGP. Para agregar una ruta estática a una tabla de enrutamiento y reenvío virtuales, especifique esa tabla de enrutamiento y reenvío virtuales cuando agregue la ruta estática.

Puede usar tablas de enrutamiento y reenvío virtuales en los siguientes escenarios:

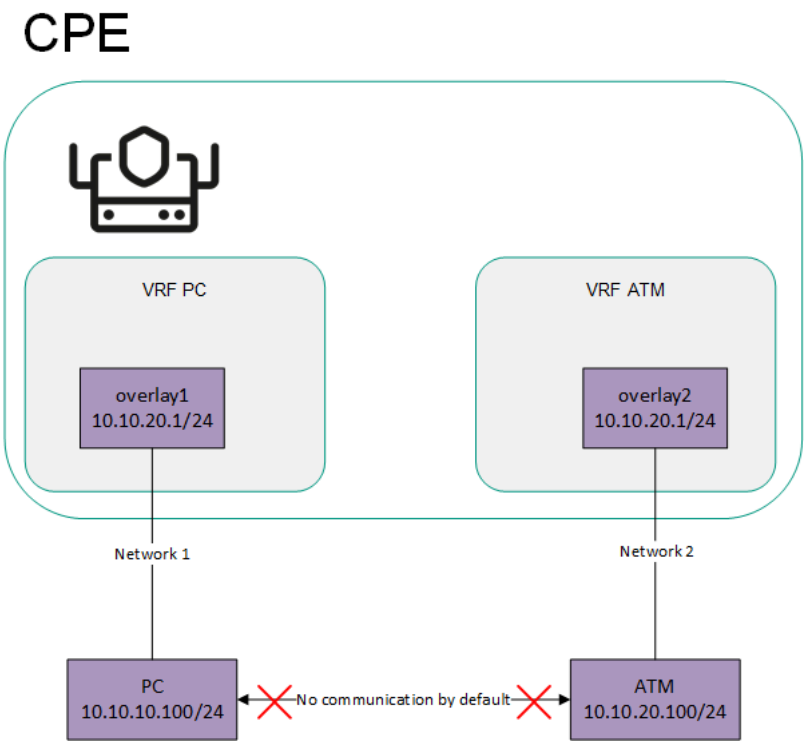
- **Segmentación de la red mediante tablas de enrutamiento y reenvío virtuales**

  Puede crear tablas de enrutamiento y reenvío virtuales para segmentar su red. En la siguiente figura, la red 1 se construye entre la interfaz de red "overlay1" y las PC de usuario, y la red 2 se construye entre la interfaz de red "overlay2" y los cajeros automáticos. Ambas interfaces de red están en la tabla de enrutamiento y reenvío virtuales predeterminada (VRF predeterminada), por lo que las redes tienen acceso entre sí y son inseguras.




Interfaces de red conectadas a diferentes redes en la tabla de enrutamiento y reenvío virtuales predeterminada

Para aislar las redes 1 y 2, las interfaces de red overlay1 y overlay2 deben agregarse a diferentes tablas de enrutamiento y reenvío virtuales (PC VRF y ATM VRF), lo que crea dos segmentos (consulte la figura a continuación).

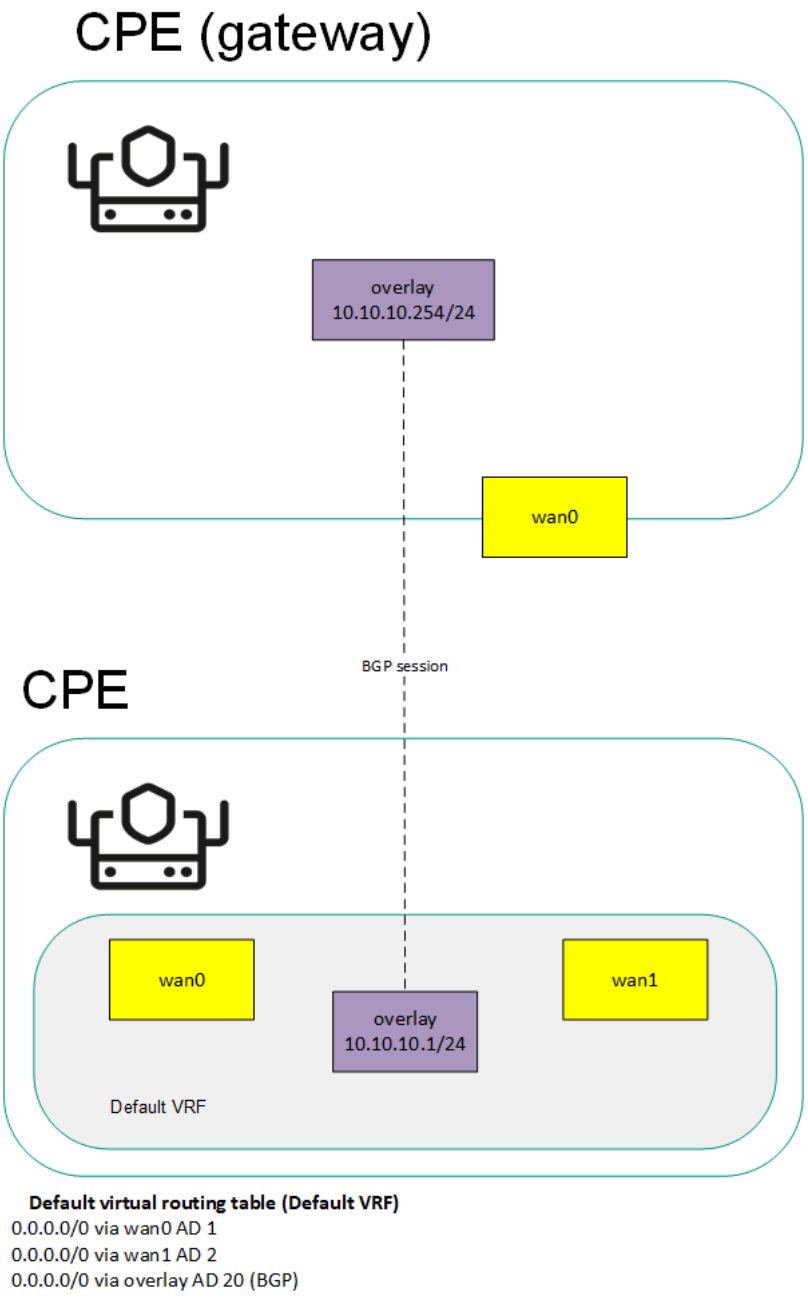



Las interfaces de red conectadas a diferentes redes están en tablas de enrutamiento y reenvío virtuales predeterminadas independientes

- **Envío de 0.0.0.0/0 a través de BGP**.

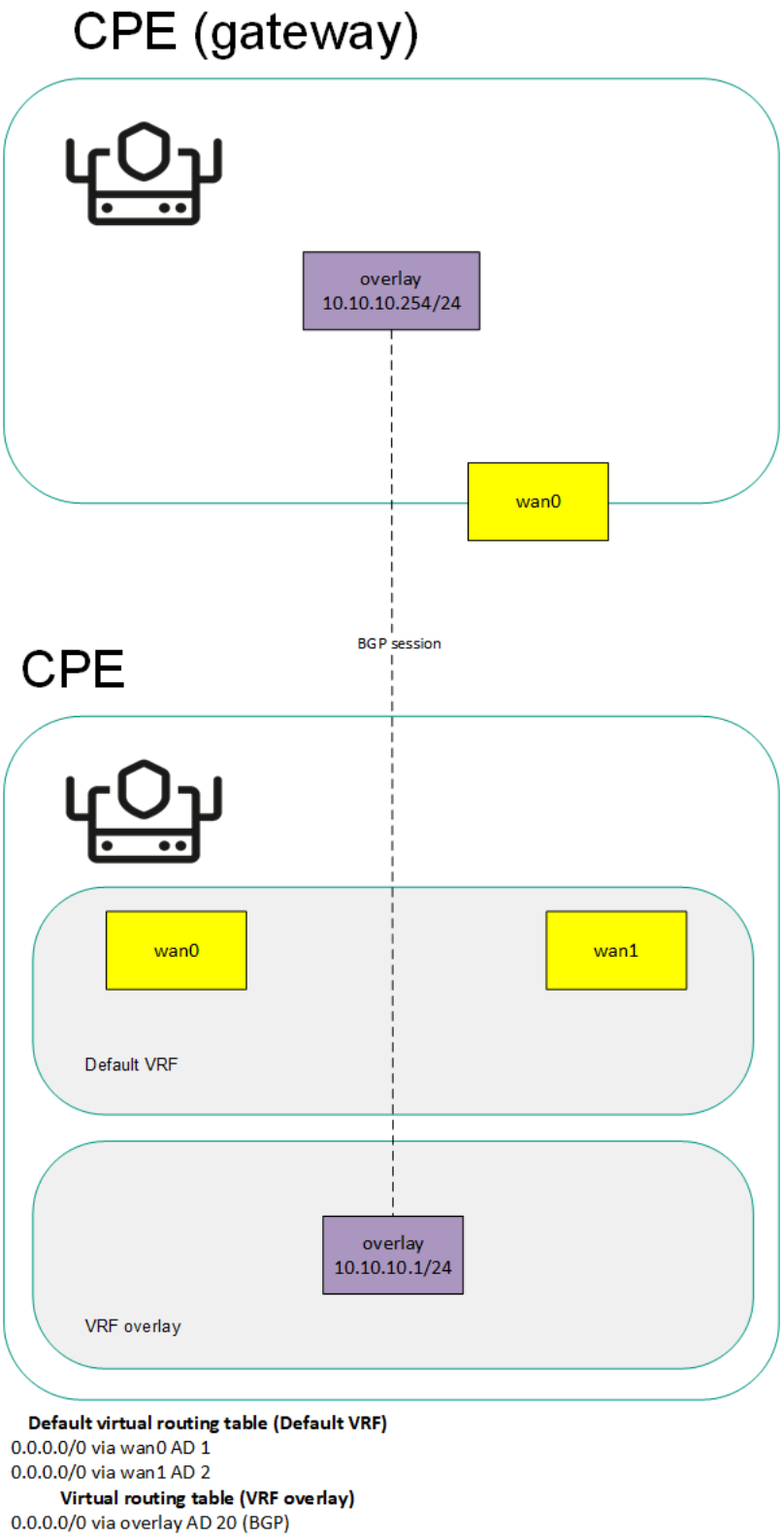
  Puede crear una tabla de enrutamiento y reenvío virtuales independiente para enviar la ruta 0.0.0.0/0 entre dispositivos a través de BGP. La siguiente figura muestra un dispositivo CPE con la función de puerta de enlace SD-WAN y un dispositivo CPE estándar. Todas las interfaces de red del dispositivo CPE se agregan a la tabla de enrutamiento y reenvío virtuales predeterminada (VRF predeterminado).

Si la puerta de enlace SD-WAN envía la ruta BGP 0.0.0.0/0 de la interfaz de red superpuesta 10.10.10.254/24 a la interfaz de red superpuesta 10.10.10.1/24, dicha ruta no se puede utilizar. Esto sucede porque la tabla de enrutamiento y reenvío virtuales predeterminada ya tiene rutas 0.0.0.0/0 con una distancia administrativa más baja para la conexión al controlador y al orquestador.




Enviar la ruta 0.0.0.0/0 a un dispositivo CPE con la tabla de enrutamiento y reenvío virtuales predeterminada

Para enviar la ruta 0.0.0.0/0 a través de BGP mediante la interfaz de red superpuesta 10.10.10.254/24 para superponer 10.10.10.1/24, debe crear una tabla de enrutamiento y reenvío virtuales independiente (superposición de VRF) para la interfaz de red superpuesta 10.10.10.1/24 y agregar las rutas de BGP (consulte la figura a continuación).




Enviar la ruta 0.0.0.0/0 a un dispositivo CPE con una tabla de enrutamiento y reenvío virtuales independiente para las rutas de BGP

Puede ver la tabla de enrutamiento y reenvío virtuales en una plantilla de CPE y en un dispositivo CPE:

- Para ver las tablas de enrutamiento y reenvío virtuales en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRF**.
- Para ver las tablas de enrutamiento y reenvío virtuales en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRF**.

La información sobre las tablas de enrutamiento y reenvío virtuales se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la tabla de enrutamiento y reenvío virtuales.
- **Heredado** indica si la tabla de enrutamiento y reenvío virtuales se hereda de la plantilla de CPE:
  - **Sí**.
  - **No**.

  Esta columna se muestra solo en el dispositivo CPE.
- **Tabla** es el ID de la tabla de enrutamiento y reenvío virtuales.
- **Interfaces** son interfaces de red agregadas a la tabla de enrutamiento y reenvío virtuales.

# Especificar la configuración básica relacionada con el enrutamiento y reenvío virtuales y las tablas de reenvío

Puede especificar la configuración del kernel relacionada con las tablas de enrutamiento y reenvío virtuales en una plantilla de CPE o en un dispositivo CPE. Esto es necesario para el correcto funcionamiento de los servicios de la red en las tablas de enrutamiento y reenvío virtuales creadas por usted. La configuración del kernel especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para especificar la configuración del kernel, siga estos pasos:*

1. Especifique la configuración del kernel de una de las siguientes maneras:
   - Si desea editar la configuración del kernel en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRF → Configuración general**.
   - Si desea editar la configuración del kernel en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña VRF → Ficha **Configuración general** y marque la casilla **Anular**.

   Se muestra la configuración del kernel.

2. Si es necesario, realice una de las siguientes acciones:

   - Si desea utilizar los servicios de red UDP en las tablas de enrutamiento y reenvío virtuales, seleccione la casilla **Servicios de red UDP en todos los VRF**. Esta casilla está desactivada por defecto.

   - Si desea utilizar servicios de red TCP en las tablas de enrutamiento y reenvío virtuales, seleccione la casilla **Servicios de red TCP en todos los VRF**. Esta casilla está desactivada por defecto.

   - Si no desea utilizar sockets RAW en las tablas de enrutamiento y reenvío virtuales, desmarque la casilla **Sockets RAW en todos los VRF**. Esta casilla está seleccionada por defecto.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Crear una tabla de enrutamiento y reenvío virtuales

Puede crear una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE o en un dispositivo CPE. Una tabla de enrutamiento y reenvío virtuales creada en la plantilla de CPE se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para crear una tabla de enrutamiento y reenvío virtuales, siga estos pasos:*

1. Cree una tabla de enrutamiento y reenvío virtuales de una de las siguientes maneras:

   - Si desea crear una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE, vaya a la sección del menú **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRF**.

   - Si desea crear una tabla de enrutamiento y reenvío virtuales en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRF**.

   De manera predeterminada, la pestaña **VRF** está seleccionada y muestra la tabla de enrutamiento y reenvío virtuales.

2. Haga clic en **+ VRF**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la tabla de enrutamiento y reenvío virtuales.

4. En el campo **Tabla**, ingrese el ID de la tabla de enrutamiento y reenvío virtuales. Rango de valores: de 100 a 199.

5. Si desea garantizar un aislamiento de tráfico adicional para la tabla de enrutamiento y reenvío virtuales, seleccione la casilla **Agregar ruta de agujero negro**. Como resultado, una ruta de agujero negro 0.0.0.0/0 se crea automáticamente cuando guarda la tabla de enrutamiento y reenvío virtuales en la sección **Rutas estáticas**.

   Si ya se creó una ruta estática de este tipo, se selecciona la casilla **Agregar ruta de agujero negro** cuando crea una tabla de enrutamiento y reenvío virtuales. Cuando desmarca la casilla, se elimina la ruta estática creada anteriormente.

   Esta casilla está desactivada por defecto. Sin una ruta de agujero negro, el tráfico puede terminar en otras tablas de enrutamiento y reenvío virtuales.

6. En la lista desplegable **Interfaces**, seleccione la interfaz de red creada que desea agregar a la tabla de enrutamiento y reenvío virtuales. No puede agregar la misma interfaz de red a varias tablas de enrutamiento y reenvío virtuales.

   La instancia de red se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias interfaces de red o eliminarlas. Para eliminar una interfaz de red, haga clic en **Eliminar** junto a ella.

   Si agregó una interfaz de red con un nombre en el formato "overlay.<número>" (por ejemplo, "overlay.100") a la tabla de enrutamiento y reenvío virtuales, debe seleccionar las casillas de verificación **Habilitar automáticamente** y **Forzar dirección IP, ruta y gateway** cuando crea o edita la interfaz de red.

7. Haga clic en **Crear**.

   La tabla de enrutamiento y reenvío virtuales se crea y se muestra en la tabla. Se crea una interfaz de red del sistema correspondiente a la tabla de enrutamiento y reenvío virtuales creada en el dispositivo CPE. Si se seleccionó **Agregar ruta de agujero negro**, la ruta del agujero negro 0.0.0.0/0 se crea automáticamente en la sección **Rutas estáticas**.

8. Cree un registro en la interfaz web del orquestador para la interfaz de red del sistema:

   a. Seleccione la pestaña **Red**.

      Se muestra la tabla de interfaces de red.

   b. Haga clic en **+ Interfaz de red**.

   c. En la ventana que se abre, en el campo **Alias**, ingrese el nombre de la tabla de enrutamiento y reenvío virtuales que especificó en el paso 3 de estas instrucciones. La longitud máxima del nombre es de 15 caracteres.

   d. Si las zonas de firewall están asignadas a las interfaces de red en la tabla de enrutamiento y reenvío virtuales, y el firewall del dispositivo CPE no acepta, de manera predeterminada, los paquetes de tráfico reenviados entre las interfaces de red y las subredes, en la lista desplegable **Zona**, seleccione una zona de firewall. La zona de firewall seleccionada también debe asignarse a una de las interfaces de red en la tabla de enrutamiento y reenvío virtuales.

   e. En el campo **Nombre de interfaz**, ingrese el nombre de la tabla de enrutamiento y reenvío virtuales que especificó en el paso 3 de estas instrucciones. La longitud máxima del nombre es de 256 caracteres.

9. Haga clic en **Crear**.

   Se crea un registro para la interfaz de red del sistema y se muestra en la tabla.

10. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Modificar la tabla de enrutamiento y reenvío virtuales

Puede editar una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE o en un dispositivo. Una tabla de enrutamiento y reenvío virtuales editada en la plantilla de CPE se edita automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede editar una tabla de enrutamiento y reenvío virtuales heredada de una plantilla de CPE en un dispositivo CPE.

*Para editar una tabla de enrutamiento y reenvío virtuales:*

1. Edite una tabla de enrutamiento y reenvío virtuales de una de las siguientes maneras:

   - Si desea editar una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRF**.

   - Si desea editar una tabla de enrutamiento y reenvío virtuales en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRF**.

   De manera predeterminada, la pestaña **VRF** está seleccionada y muestra la tabla de enrutamiento y reenvío virtuales.

2. Haga clic en **Editar** junto a la tabla de enrutamiento y reenvío virtuales que desea editar.

3. En la ventana que se abre, administre la configuración de la tabla de enrutamiento y reenvío virtuales.

4. Haga clic en **Guardar**.

   La tabla de enrutamiento y reenvío virtuales se modifica y actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Eliminar una tabla de enrutamiento y reenvío virtuales

Puede eliminar una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE o en un dispositivo CPE. Una tabla de enrutamiento y reenvío virtuales eliminada en la plantilla de CPE se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de CPE. No puede eliminar una tabla de enrutamiento y reenvío virtuales heredada de una plantilla de CPE en un dispositivo CPE.

Las tablas de enrutamiento y reenvío virtuales eliminadas no se pueden restaurar.

*Para eliminar una tabla de enrutamiento y reenvío virtuales, siga estos pasos:*

1. Elimine una tabla de enrutamiento y reenvío virtuales de una de las siguientes maneras:

   - Si desea eliminar una tabla de enrutamiento y reenvío virtuales en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **VRF**.

   - Si desea eliminar una tabla de enrutamiento y reenvío virtuales en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **VRF**.

   De manera predeterminada, la pestaña **VRF** está seleccionada y muestra la tabla de enrutamiento y reenvío virtuales.

2. Haga clic en **Eliminar** junto a la tabla de enrutamiento y reenvío virtuales que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La tabla de enrutamiento y reenvío virtuales se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programar un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

# Supervisar la información de paquetes de tráfico mediante el protocolo NetFlow

Kaspersky SD-WAN es compatible con las versiones 1, 5 y 9 de NetFlow para supervisar la información sobre paquetes de tráfico en un dispositivo CPE.

Las plantillas de NetFlow se utilizan para la configuración centralizada del protocolo de NetFlow en dispositivos CPE. Para evitar configurar cada dispositivo CPE individualmente, puede especificar la configuración básica en la plantilla de NetFlow y luego aplicar la plantilla de NetFlow a los dispositivos CPE cuando los agrega o registra manualmente. Si edita una configuración en una plantilla de NetFlow, la configuración se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de NetFlow. Si edita una configuración en el dispositivo CPE, la configuración se vuelve independiente de la plantilla de NetFlow y, si la configuración se modifica en la plantilla de NetFlow, permanece sin cambios en el dispositivo CPE.

Cuando especifica la configuración básica de NetFlow, puede especificar hasta cuatro recopiladores de NetFlow. Si desea que un dispositivo CPE envíe información sobre paquetes de tráfico a los recopiladores de NetFlow, debe habilitar el protocolo de NetFlow en las interfaces de red. El protocolo de NetFlow se puede habilitar durante la creación o edición de la interfaz de red.

## Administrar plantillas de NetFlow

Para ver la tabla de plantillas de NetFlow, vaya a la sección **SD-WAN → Plantillas de NetFlow**. De manera predeterminada, la **plantilla de NetFlow predeterminada** se crea en el portal del administrador, que actúa como base para todas las demás plantillas de NetFlow que cree. La información sobre las plantillas de NetFlow se muestra en las siguientes columnas de la tabla:

- **Id** es el id. de la plantilla de NetFlow.
- **Nombre** es el nombre de la plantilla de NetFlow.
- **Uso** especifica si los dispositivos CPE utilizan la plantilla de NetFlow:
  - **Sí**.
  - **No**.
- **Actualizado** es la fecha y la hora en que se modificó por última vez la configuración de la plantilla de CPE.
- **Usuario** es el nombre del usuario que creó la plantilla de NetFlow.
- **Propietario** es el inquilino al que pertenece la plantilla de NetFlow.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede seleccionar una plantilla de NetFlow asignada para que esté preseleccionada cuando agrega o registra manualmente un dispositivo CPE. Para los inquilinos, debe crear y seleccionar manualmente una plantilla de NetFlow asignada en el portal de autoservicio.

## Crear una plantilla de NetFlow

*Para crear una plantilla de NetFlow, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.

2. En la parte superior de la página, haga clic en **+ Plantilla de NetFlow**.

3. En la ventana que se abre, ingrese el nombre de la plantilla de NetFlow.

4. Haga clic en **Crear**.

La plantilla de NetFlow se crea y se muestra en la tabla.

Debe configurar la plantilla de NetFlow creada. Para obtener más información sobre la configuración de la plantilla de NetFlow, consulte las instrucciones sobre cómo establecer la configuración básica de NetFlow.

## Seleccionar una plantilla de NetFlow asignada

Puede seleccionar una plantilla de NetFlow asignada para que esté preseleccionada cuando agrega o registra manualmente un dispositivo CPE. Para los inquilinos, debe crear y seleccionar manualmente una plantilla de NetFlow asignada en el portal de autoservicio.

*Para seleccionar una plantilla de NetFlow asignada, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.

2. Haga clic en la plantilla de NetFlow que desee convertir en la plantilla de NetFlow asignada.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Configurar como designado**.

La plantilla de NetFlow se convierte en la plantilla de NetFlow asignada.

# Importar una plantilla de NetFlow

Puede exportar una plantilla de NetFlow y luego importarla a otra plantilla de NetFlow. La configuración de la plantilla de NetFlow se especifica de acuerdo con la configuración de la plantilla de NetFlow importada. Durante la importación, puede seleccionar la configuración que desea dejar sin cambios. La plantilla de NetFlow a la que está importando otra plantilla de NetFlow permanece aplicada a los dispositivos CPE, pero la configuración de esos dispositivos CPE no se modifica.

*Para importar una plantilla de NetFlow, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.

2. Haga clic en la plantilla de NetFlow que desee exportar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar**.

   Se guarda un archivo comprimido en formato TAR.GZ en su dispositivo local. El archivo no contiene información sobre los dispositivos CPE que utilizan la plantilla de NetFlow.

4. Haga clic en la plantilla de NetFlow a la que desea importar otra plantilla de NetFlow.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

5. En la parte superior del área de configuración, en **Acciones**, haga clic en **Importar**.

6. En la ventana que se abre, desactive las casillas de verificación junto a la configuración de la plantilla de NetFlow que desea dejar sin cambios después de la importación.

7. En el campo **Archivo**, especifique la ruta al archivo comprimido TAR.GZ.

8. Haga clic en **Importar**.

La configuración de la plantilla de NetFlow se modifica de acuerdo con la configuración de la plantilla de NetFlow importada.

# Clonar una plantilla de NetFlow

Puede clonar una plantilla de NetFlow para crear una plantilla de NetFlow idéntica con un nombre diferente.

*Para clonar una plantilla de NetFlow, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.

2. Haga clic en la plantilla de NetFlow que desee clonar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Clonar**.
4. En la ventana que se abre, ingrese el nombre de la nueva plantilla de NetFlow.
5. Haga clic en **Clonar**.

Se crea un clon de la plantilla de NetFlow con el nuevo nombre y se muestra en la tabla.

## Verificar el uso de una plantilla de NetFlow

Si es necesario, puede verificar qué dispositivos CPE están usando la plantilla de NetFlow. Por ejemplo, si una plantilla de NetFlow está en uso, no se puede eliminar.

*Para ver si se está utilizando una plantilla de NetFlow, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.
2. Haga clic en la plantilla de NetFlow para la que desea ver la información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃.
3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar uso**.

Esto abre una ventana con una tabla de los dispositivos CPE que están utilizando la plantilla de NetFlow.

## Eliminar una plantilla de NetFlow

No puede eliminar una plantilla de NetFlow si al menos un dispositivo CPE la está utilizando. Para eliminar una plantilla de NetFlow que los dispositivos CPE están utilizando, primero debe cambiar la plantilla de NetFlow de los dispositivos CPE. Puede comprobar qué dispositivos CPE están utilizando la plantilla NetFlow.

Las plantillas de NetFlow eliminadas no se pueden restaurar.

*Para eliminar una plantilla de NetFlow, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de NetFlow**.

   Se muestra una tabla de plantillas de NetFlow.
2. Seleccione la plantilla de NetFlow que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃.
3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.
4. En la ventana de confirmación, haga clic en **Eliminar**.

La plantilla de NetFlow se elimina y ya no se muestra en la tabla.

# Configuración básica de NetFlow

Puede especificar la configuración básica de NetFlow en una plantilla de NetFlow o en un dispositivo CPE. La configuración básica de NetFlow especificada en la plantilla de NetFlow se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de NetFlow.

*Para modificar la configuración básica de NetFlow, siga estos pasos:*

1. Especifique la configuración básica de NetFlow de una de las siguientes maneras:

   - Si desea editar la configuración básica de NetFlow en una plantilla de NetFlow, vaya a la sección del menú **SD-WAN→ Plantillas de NetFlow** y haga clic en la plantilla de NetFlow.

   - Si desea editar la configuración básica de NetFlow en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **NetFlow** y marque la casilla **Anular**.

   Se muestra la configuración básica de NetFlow.

2. En la lista desplegable **NetFlow**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

3. Especifique el recopilador de NetFlow:

   a. En **Recopiladores**, haga clic en **+ Agregar**.

   b. En **Host**, ingrese la dirección IPv4 del recopilador de NetFlow.

   c. En **Puerto**, ingrese el número de puerto del recopilador de NetFlow. Rango de valores: de 1 a 65 535.

   El recopilador de NetFlow se especifica y se muestra en la sección **Recopiladores**. Puede especificar hasta cuatro recopiladores de NetFlow o eliminar un recopilador de NetFlow. Para eliminar un recopilador de NetFlow, haga clic en el ícono de eliminar ✕ junto a él.

4. En la lista desplegable **Exportar versión**, seleccione la versión del protocolo de NetFlow:

   - **1**

   - **5**

   - **9**. Es la configuración predeterminada.

5. En la lista desplegable **Nivel de seguimiento**, seleccione qué información de paquetes de tráfico rastrea el dispositivo CPE:

   - **ETHER** para rastrear la siguiente información:

     - Puertos y direcciones IP de origen y destino

     - Direcciones MAC de origen y destino

     - ID de VLAN exterior

     - Protocolo en uso

- **FULL** para rastrear los puertos y las direcciones IP de origen y destino, así como el protocolo que se está utilizando. Esta es la configuración predeterminada.
- **VLAN** para rastrear la siguiente información:
  - Puertos y direcciones IP de origen y destino
  - ID de VLAN exterior
  - Protocolo en uso
- **PROTO** para rastrear las direcciones IP de origen y destino y el protocolo que se está utilizando.
- **IP** para rastrear las direcciones IP de origen y destino.

6. En el campo **Cantidad máxima de flujos**, ingrese el número máximo de flujos de tráfico que el dispositivo CPE puede rastrear simultáneamente. Rango de valores: de 1 a 65 535. El valor predeterminado es `8192`.

   Cuanto mayor sea el valor, mayor será la carga de la CPU en el dispositivo CPE.

7. En el campo **Frecuencia de muestreo**, especifique con qué frecuencia el dispositivo CPE rastrea la información del paquete de tráfico. Por ejemplo, si ingresa `10`, el dispositivo CPE rastrea información sobre cada décimo paquete de tráfico. Rango de valores: de 1 a 8192. El valor predeterminado es `1024`.

   Cuanto menor sea el valor, más precisa será la información y mayor será la carga de la CPU en el dispositivo CPE.

8. En el campo **Tiempo de espera máximo (s)**, ingrese el tiempo máximo en segundos durante el cual el dispositivo CPE puede rastrear la información del flujo de tráfico. Para deshabilitar esta función, ingrese `0`. Rango de valores: de 1 a 9999. El valor predeterminado es `60`.

9. En el campo **Límite de saltos**, ingrese el número máximo de saltos en los colectores de NetFlow. Rango de valores: 1 a 255. El valor predeterminado es `64`.

10. Si desea que el dispositivo CPE realice un seguimiento del tráfico IPv6, en la lista desplegable **Seguimiento de IPv6**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

11. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de NetFlow o el dispositivo CPE.

Si desea que un dispositivo CPE envíe información sobre paquetes de tráfico a los recopiladores de NetFlow, debe habilitar el protocolo de NetFlow en las interfaces de red. El protocolo de NetFlow se puede habilitar durante la creación o edición de la interfaz de red.

# Cambiar la plantilla de NetFlow de un dispositivo CPE

*Para cambiar la plantilla de NetFlow de un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el que desea cambiar la plantilla de NetFlow.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la lista desplegable **Plantilla de NetFlow**, seleccione una plantilla de NetFlow creada.

4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Diagnosticar un dispositivo CPE

Puede solicitar información de diagnóstico de un dispositivo CPE, como el uso de protocolos BGP, OSPF y PIM. La información de diagnóstico que se devuelve en respuesta a la solicitud se muestra en la interfaz web del orquestador y, si es necesario, se puede descargar como un archivo TXT.

Kaspersky SD-WAN también admite las siguientes utilidades para el diagnóstico de dispositivos CPE:

- Ping es una utilidad para probar el vínculo entre un dispositivo CPE y una dirección IPv4 específica.
- Traceroute es una utilidad para determinar la ruta entre un dispositivo CPE y una dirección IPv4 específica.
- Tcpdump es una utilidad para capturar tráfico en un dispositivo CPE. Capturar significa que se hace una copia del tráfico y el tráfico original se retransmite a su destino.
- Iperf es una utilidad para diagnosticar el rendimiento de la red. Puede utilizar el dispositivo CPE como servidor iperf o como cliente iperf.
- Sweep es una utilidad para realizar las siguientes acciones en un dispositivo CPE:
  - Borrar la caché de ARP
  - Reiniciar el proceso FRR (Free Range Routing)
  - Borrar la tabla de sesiones de NAT
  - Reiniciar módems
- El volcado de OpenFlow es una utilidad para solicitar flujos de volcado y grupos de volcado generados por el interruptor virtual de un dispositivo CPE.

Las utilidades de volcado tcpdump, iperf y OpenFlow generan informes que puede descargar o eliminar.

Ejecutar una utilidad es una tarea que el dispositivo CPE recibe del orquestador; la tarea obedece al período configurado para que el dispositivo CPE envíe solicitudes de API REST al orquestador. Si desea que las utilidades se ejecuten antes, puede habilitar el modo interactivo en el dispositivo CPE.

En el *modo interactivo*, el dispositivo CPE usa un intervalo de tiempo más corto para enviar solicitudes de API REST al orquestador. El modo interactivo finaliza automáticamente cuando transcurre la duración especificada. Puede especificar la siguiente configuración del modo interactivo cuando configura la conexión de un dispositivo CPE al orquestador y al controlador:

- El período de espera hasta que el dispositivo CPE envía otra solicitud de API REST al orquestador en modo interactivo
- El tiempo después del cual se deshabilita el modo interactivo automáticamente

# Solicitar información de diagnóstico

*Para solicitar información de diagnóstico, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea solicitar información de diagnóstico.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Información de diagnóstico**.

   Se muestran los parámetros de solicitud de información de diagnóstico.

4. Haga clic en **Solicitar información de diagnóstico**.

   Espere hasta que se reciba la información de diagnóstico del dispositivo CPE.

5. En la lista desplegable **Nombre**, seleccione el tipo de información de diagnóstico que desea mostrar:

   - **disk usage** para obtener información sobre el uso del disco del dispositivo CPE. Esta es la configuración predeterminada.
   - **ip addresses** para obtener información sobre las direcciones IP asignadas a los puertos físicos o interfaces virtuales del sistema operativo del dispositivo CPE.
   - **vrf data** para obtener información sobre las tablas de enrutamiento y reenvío virtuales.
   - **ip neighbors** para obtener información sobre los vecinos IP del dispositivo CPE, obtenida de la tabla ARP o mediante el Protocolo de detección de vecinos.
   - **ip routes** para obtener información sobre las rutas IPv4 e IPv6.
   - **ip rules** para obtener información sobre las reglas de enrutamiento.
   - **iptables** para obtener información sobre iptables.
   - **cpe log** para ver el registro local del dispositivo CPE.
   - **ovs-ofctl show** para obtener información sobre el conmutador virtual.

- **ovs-vsctl show** para obtener información sobre el vínculo entre el conmutador virtual y los controladores.
- **ovs-vsctl list controller** para obtener información sobre los controladores especificados para el conmutador virtual.
- **show ip ospf** para obtener información sobre el proceso de enrutamiento OSPF.
- **show ip ospf interface** para obtener información sobre las interfaces OSPF.
- **show ip ospf neighbor** para obtener información sobre los vecinos OSPF.
- **show ip ospf database** para ver la base de datos OSPF.
- **bgp show ip route** para obtener información sobre las rutas de BGP.
- **show ip bgp** para obtener información sobre el proceso de enrutamiento de BGP.
- **show ip bgp summary** para obtener información breve sobre el proceso de enrutamiento de BGP.
- **top process** para obtener información sobre los procesos de Linux.
- **uptime** para obtener información sobre el tiempo de actividad del dispositivo CPE.
- **time sync** para obtener información sobre la sincronización de la hora en el dispositivo CPE mediante un servidor NTP.
- **netstat** para obtener información sobre los vínculos de red que estableció el dispositivo CPE.
- **sdwan interfaces** para obtener información sobre las interfaces de SD-WAN.
- **modems** para obtener información sobre los módems.

  La información recibida del dispositivo también se muestra en la sección **Módems** del área de configuración del dispositivo CPE (**SD-WAN** → **CPE**).
- **show bfd peers** para obtener información sobre los pares de BFD.
- **netflow dump-flows** para obtener información sobre los flujos de NetFlow.
- **netflow statistics** para obtener información sobre el uso del protocolo de NetFlow.
- **show bfd peers brief** para obtener información breve sobre los pares de BFD.
- **show ip pim bsr** para obtener información sobre el enrutador de arranque (BSR) actual.
- **show ip pim bsrp-info** para obtener información sobre la asignación de grupo a rp recibida del enrutador de arranque.
- **show ip pim interface** para obtener información sobre las interfaces PIM. Puede configurar el protocolo PIM cuando crea o edita una interfaz múltiple.
- **show ip pim interface traffic** para obtener información sobre el tráfico PIM.
- **show ip pim join** para obtener información sobre los grupos de multidifusión a los que está conectado el dispositivo CPE.

- **show ip pim neighbor** para obtener información sobre los vecinos PIM.
- **show ip pim nexthop** para obtener información sobre los próximos saltos de los grupos de multidifusión.
- **show ip pim rp-info** para obtener información sobre los puntos de encuentro. Puede especificar puntos de encuentro cuando especifica la configuración básica de PIM.
- **show ip pim secondary** para obtener información sobre el enrutador PIM de respaldo.
- **show ip pim state** para obtener información sobre el estado del protocolo PIM.
- **show ip pim statistics** para obtener información sobre el uso del protocolo PIM.
- **show ip pim upstream** para obtener información sobre las fuentes de PIM.
- **show ip igmp groups** para obtener información sobre los grupos IGMP.
- **show ip igmp interface** para obtener información sobre las interfaces IGMP. Puede configurar IGMP cuando crea o edita una interfaz múltiple.
- **show ip igmp interface detail** para obtener información detallada sobre las interfaces IGMP.
- **show ip igmp sources** para obtener información sobre las fuentes de IGMP.
- **igmp statistics** para obtener información sobre el uso de IGMP.
- **show ip multicast** para obtener información sobre el proceso de enrutamiento de multidifusión.
- **show ip mroute** para obtener información sobre las rutas de multidifusión.
- **show ip mroute summary** para obtener información breve sobre las rutas de multidifusión.
- **vswitchd log** para obtener el registro del proceso ovs-vswitchd.
- **firewall config** para obtener información sobre el firewall.
- **sw version** para ver la versión de firmware del dispositivo CPE.
- **vrrp stats** para obtener información breve sobre el uso de VRRP.
- **vrrp data** para obtener información sobre el uso de VRRP.

6. Si desea filtrar la información de diagnóstico que se muestra:

   a. En el campo **Buscar línea por patrón**, ingrese las palabras que se deben encontrar en las líneas de información de diagnóstico que desea que se muestren. Longitud máxima: 64 caracteres. Si desea mostrar solo las líneas que no contienen las palabras que ingresó, seleccione la casilla **Mostrar todo excepto lo encontrado**. Esta casilla está desactivada por defecto.

   b. En el campo **Mostrar líneas antes y después**, ingrese el número de líneas en blanco que desea mostrar antes y después de cada línea de información de diagnóstico.

7. Si desea descargar el archivo con información de diagnóstico, haga clic en **Descargar**.

   Un archivo TXT se guarda en su dispositivo local.

# Utilizar el modo de depuración para protocolos de enrutamiento dinámico en dispositivos CPE

Puede utilizar el modo de depuración para solucionar problemas de los protocolos BGP y OSPF en dispositivos CPE. Cuando habilita el modo de depuración en un dispositivo CPE, el nivel de registro para los registros del proceso FRR se establece en **Depurar**, y los comandos **debug <...>** relevantes del paquete FRR se ejecutan en el dispositivo.

Habilitar el modo de depuración en el CPE puede aumentar considerablemente la carga de la CPU. Recomendamos hacerlo fuera del horario comercial para evitar problemas de rendimiento. Si el dispositivo CPE deja de estar disponible después de habilitar el modo de depuración, deshabilite el modo de depuración en el orquestador y reinicie el dispositivo CPE.

*Para habilitar el modo de depuración, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea habilitar el modo de depuración.

3. Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

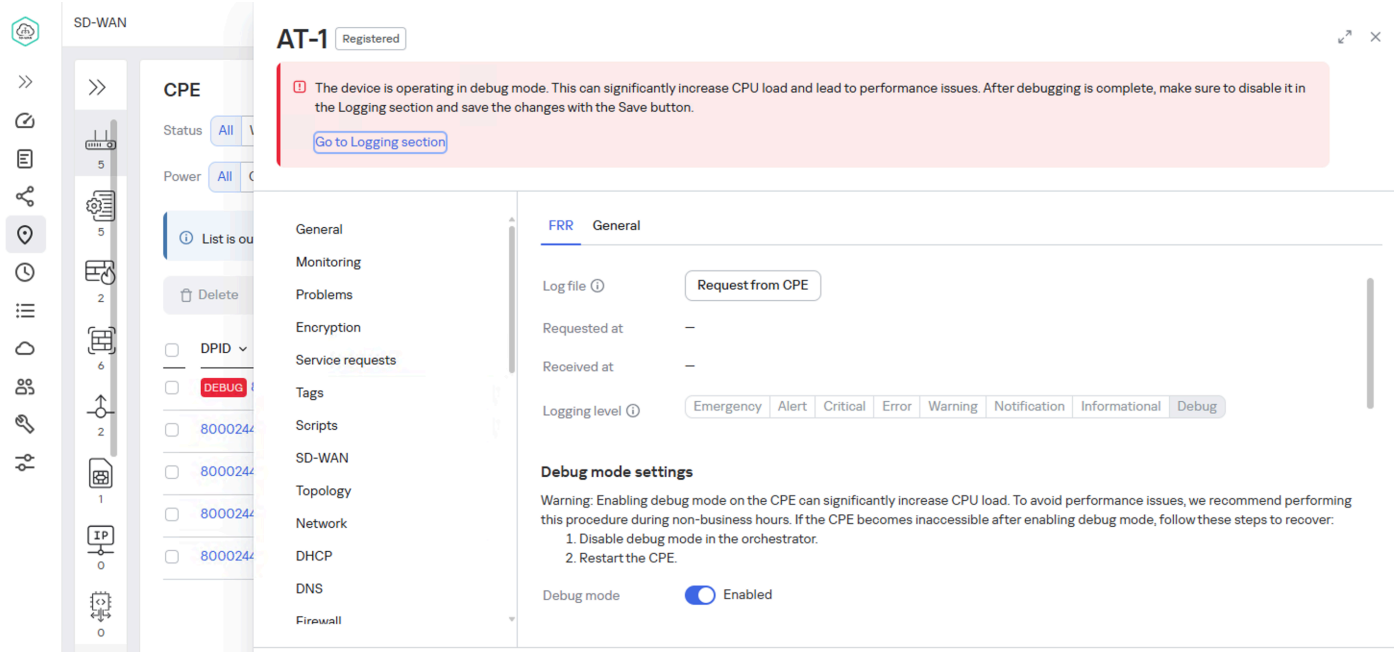
4. En el menú de la izquierda, seleccione la sección **Registros** y luego seleccione la pestaña **FRR**.

5. Active el conmutador **Modo de depuración**.

6. En las pestañas **BGP** y **OSPF** que se muestran, especifique las opciones para los comandos de depuración de FRR según sea necesario. Para habilitar el modo de depuración, debe especificar al menos una opción en cualquiera de las pestañas.

7. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración del dispositivo CPE o programe un guardado diferido por haciendo clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionando la opción **Guardado programado**.

El dispositivo CPE en el que está habilitado el modo de depuración se muestra en la tabla de la sección **SD-WAN → CPE** con el ícono DEBUG junto a su DPID.




El dispositivo CPE está en modo de depuración

Para descargar el archivo de registro de depuración, solicítelo al dispositivo haciendo clic en el botón **Solicitar del CPE** (o **Actualizar del CPE** si ya se solicitó el archivo anteriormente) y, después de que se cargue el archivo en el orquestador, haga clic en el vínculo de descarga. El contenido del archivo se sobrescribe con cada nueva solicitud. Tenga en cuenta que se asigna espacio de almacenamiento limitado para el archivo y, una vez que se alcanza el límite, no se agregan nuevos registros al archivo.

# Especificar servidores NTP en dispositivos CPE

Debe especificar un servidor NTP interno o externo o una agrupación de servidores para los dispositivos CPE con el fin de asegurarse de que se muestre la hora exacta en estos dispositivos CPE. Puede utilizar un dispositivo CPE como un servidor NTP para mostrar la hora exacta en los dispositivos de la red que están conectados al dispositivo CPE.

Puede especificar el servidor NTP en una plantilla de CPE o en el dispositivo CPE. Los servidores NTP especificados en la plantilla de CPE se especifican automáticamente en todos los dispositivos CPE que utilicen esta plantilla de CPE.

*Para especificar el servidor NTP en los dispositivos CPE, haga lo siguiente:*

1. Especifique el servidor NTP de una de las siguientes maneras:

   - Si desea especificar el servidor NTP en una plantilla de CPE, vaya a la sección **SD-WAN → Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **NTP**.

   - Si desea especificar un servidor NTP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **NTP** y seleccione la casilla de verificación **Anular**.

   Se mostrará la configuración de conexión al servidor NTP.

2. Si no desea especificar el servidor NTP para el dispositivo CPE, desactive la casilla de verificación **Conectarse al servidor NTP**. Esta casilla está seleccionada por defecto.

3. Si desea utilizar el dispositivo CPE como un servidor NTP, seleccione la casilla de verificación **Usar CPE como servidor NTP**. Esta casilla está desactivada por defecto.

4. Especifique un servidor NTP o una agrupación de servidores:

   a. En **Servidores NTP**, haga clic en **+ Agregar**.

   b. En el campo que se muestra, ingrese la dirección IP o FQDN del servidor NTP o de la agrupación de servidores. Se admiten los siguientes formatos de dirección IP y FQDN:

      - Para especificar un servidor NTP, ingrese la dirección IP o FQDN en el formato del `servidor <dirección IP o FQDN>`, por ejemplo, `servidor 0.pool.ntp.org`.

      - Para especificar una agrupación de servidores NTP, ingrese la dirección IP o FQDN en el formato de la `agrupación <dirección IP o FQDN>`, por ejemplo, `agrupación pool.ntp.org`.

   Se especificará el servidor NTP y se mostrará en la sección **Servidores NTP**. Puede especificar varios servidores NTP o eliminar servidores NTP. Para eliminar un servidor NTP, haga clic en el ícono de eliminar ✕ junto a él.

5. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

Puede solicitar información sobre el diagnóstico para consultar la configuración de la sincronización de la hora en un dispositivo CPE.

# Habilitar el modo interactivo

Puede especificar la siguiente configuración del modo interactivo cuando configura la conexión de un dispositivo CPE al orquestador y al controlador:

- El período de espera hasta que el dispositivo CPE envía otra solicitud de API REST al orquestador en modo interactivo

- El tiempo después del cual se deshabilita el modo interactivo automáticamente

*Para habilitar el modo interactivo, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea habilitar el modo interactivo.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la parte superior del área de configuración, haga clic en **Modo interactivo**.

El modo interactivo se habilita en el dispositivo CPE.

# Ejecutar la utilidad ping

*Para ejecutar la utilidad ping, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad ping.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades**.

   De manera predeterminada, la pestaña **Ping** está seleccionada, que muestra la configuración de la utilidad ping.

4. En el campo **Dirección IP de destino**, ingrese la dirección IPv4 a la que desea que el dispositivo CPE envíe las solicitudes ICMP.

5. Si desea que el dispositivo CPE envíe las solicitudes ICMP desde una interfaz de red creada, en la lista desplegable **Interfaz de red de origen**, seleccione la interfaz de red.

6. En el campo **Conteo**, ingrese la cantidad de solicitudes ICMP que el dispositivo CPE envía. Rango de valores: 1 a 1 000 000. El valor predeterminado es `5`.

7. En el campo **Tiempo de espera (s)**, ingrese el tiempo en segundos después del cual el dispositivo CPE debe recibir una respuesta de ICMP para considerar la solicitud como correcta. Rango de valores: 1 a 3600. El valor predeterminado es `2`.

8. En el campo **Tamaño**, ingrese el tamaño de la solicitud ICMP en bytes. Rango de valores: de 1 a 65 535. El valor predeterminado es `56`.

9. En el campo **TTL**, ingrese la cantidad máxima de saltos para las solicitudes ICMP. Rango de valores: 1 a 255. El valor predeterminado es `255`.

10. En el campo **Intervalo**, ingrese el intervalo en segundos para utilizar el dispositivo CPE cuando se envíen las solicitudes ICMP a la dirección IPv4 especificada. Rango de valores: 1 a 300. El valor predeterminado es `1`.

11. Haga clic en **Ejecutar**.

La utilidad ping se ejecuta en el dispositivo CPE, y se muestra un informe que contiene el resultado de la utilidad ping en la parte inferior del área de configuración.

# Ejecutar la utilidad traceroute

*Para ejecutar la utilidad traceroute, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad traceroute.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la ficha **Utilidades → Traceroute**.

   Se muestra la configuración de la utilidad traceroute.

4. En el campo **Dirección IP de destino**, ingrese la dirección IPv4 a la que el dispositivo CPE envía la serie de solicitudes ICMP.

5. Si desea que el dispositivo CPE envíe la serie de solicitudes ICMP desde una interfaz de red creada, en la lista desplegable **Interfaz de origen**, seleccione la interfaz de red.

6. Si desea que el dispositivo CPE utilice el servidor DNS para resolver las direcciones IP como nombres de dominio cuando crea el informe con el resultado de la utilidad traceroute, seleccione la casilla **Resolver nombres DNS**. Puede especificar un servidor DNS cuando se crea o edita una interfaz de red. Las direcciones IP que no se pueden resolver como nombres de dominio también se muestran en el informe. Esta casilla está desactivada por defecto.

7. En el campo **Tiempo de espera de exploraciones (s)**, ingrese el tiempo en segundos después del cual el dispositivo CPE debe recibir una serie de respuestas ICMP para considerar la serie de solicitudes ICMP como un éxito. Rango de valores: de 1 a 30. El valor predeterminado es `3`.

8. En el campo **Número máximo de saltos**, ingrese el número máximo de saltos para la serie de solicitudes ICMP. Rango de valores: 1 a 60. El valor predeterminado es `10`.

9. Haga clic en **Ejecutar**.

La utilidad traceroute se ejecuta en el dispositivo CPE y se muestra un informe que contiene el resultado de la utilidad traceroute en la parte inferior del área de configuración.

# Ejecutar la utilidad tcpdump

La utilidad tcpdump genera un informe con el tráfico capturado. Cuando vuelva a ejecutar la utilidad tcpdump, el informe se sobrescribirá. Puede descargar el informe si desea conservarlo.

La utilidad tcpdump coloca una carga adicional en la CPU del dispositivo CPE.

*Para ejecutar la utilidad tcpdump, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad tcpdump.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades** → **Tcpdump**.

   Se muestra la configuración de la utilidad tcpdump.

4. En la lista desplegable **Capturar interfaz de red**, seleccione la interfaz de red creada en la que desea capturar tráfico.

5. En la lista desplegable **Sentido**, selecciona la dirección del tráfico que desea capturar:

   - **Dentro** para capturar el tráfico entrante.
   - **Fuera** para capturar el tráfico saliente.
   - **Dentro/Fuera** para capturar el tráfico entrante y saliente. Esta es la configuración predeterminada.

6. Si desea que el dispositivo CPE utilice el servidor DNS para resolver las direcciones IP como nombres de dominio cuando se cree el informe con el tráfico capturado, seleccione la casilla de verificación **Resolver nombres DNS**. Puede especificar un servidor DNS cuando se crea o edita una interfaz de red. Las direcciones IP que no se pueden resolver como nombres de dominio también se reflejan en el informe. Esta casilla está desactivada por defecto.

7. Si desea utilizar un filtro para capturar el tráfico, en el campo **Filtrar tcpdump**, ingrese la sintaxis del filtro. La longitud máxima del filtro es de 1024 caracteres. Por ejemplo, puede utilizar los siguientes filtros:

   - `icmp` para capturar solo paquetes de tráfico ICMP.
   - `host 1.2.3.4 y (puerto 80 o 443)` para capturar solo paquetes de tráfico con dirección IPv4 1.2.3.4 y puerto TCP de origen o de destino 80 o 443.
   - `tcp[13] & 2 != 0` para capturar solo paquetes de tráfico TCP SYN.

   Se puede obtener información detallada sobre los filtros de tráfico en la documentación oficial de tcpdump.

8. En el campo **Tiempo máximo de captura (s)**, ingrese el tiempo en segundos después del cual la captura de tráfico se detiene. Rango de valores: 10 a 600. El valor predeterminado es `30`.

9. En el campo **Cantidad máxima de paquetes capturados**, ingrese la cantidad de paquetes de tráfico que desea recopilar antes de que se detenga la captura de tráfico. Rango de valores: 1 a 10 000. El valor predeterminado es `1000`.

   La captura de tráfico se detiene cuando pasa el tiempo especificado en el campo **Tiempo máximo de captura (s)** o cuando la cantidad de paquetes de tráfico especificada en el campo **Cantidad máxima de paquetes capturados** se captura.

10. Haga clic en **Ejecutar**.

La utilidad tcpdump se ejecuta en el dispositivo CPE, y se genera un informe con el tráfico capturado.

# Ejecutar la utilidad iperf

La utilidad iperf genera un informe con los resultados del diagnóstico de rendimiento de la red. Cuando vuelva a ejecutar la utilidad iperf, el informe se sobrescribirá. Puede descargar el informe si desea conservarlo.

*Para ejecutar la utilidad iperf, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad iperf.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades → Iperf**.

   Se muestra la configuración de la utilidad iperf.

4. Especifique el modo en el que desea usar la utilidad iperf en el dispositivo CPE seleccionando una de las siguientes opciones:

   - **Servidor** para usar el dispositivo CPE como servidor iperf.
   - **Cliente** para usar el dispositivo CPE como cliente iperf.

5. Si eligió la opción **Servidor**, configure el servidor iperf:

   a. En el campo **Puerto**, ingrese el número de puerto TCP o UDP del servidor iperf. Rango de valores: de 1001 a 65 535. El valor predeterminado es `7777`.

   b. En el campo **Intervalo del informe (s)**, ingrese el intervalo en segundos para escribir líneas en el informe. Rango de valores: de 0 a 60. El valor predeterminado es `3`.

   c. Si no desea crear un informe con los resultados del diagnóstico de rendimiento de la red, seleccione la casilla **Sin informe**. Esta casilla está desactivada por defecto.

d. En **Formato del informe**, seleccione el formato de los resultados del diagnóstico de rendimiento de la red en el informe:

- **Kbit/s**. Esta es la configuración predeterminada.
- **Mbit/s**.
- **Kbyte/s**.
- **Mbyte/s**.

e. En el campo **Ejecutar servidor durante (s)**, ingrese la duración en segundos durante la cual desea que se ejecute el servidor iperf. Rango de valores: de 60 a 3600. El valor predeterminado es `300`.

6. Si eligió la opción **Cliente**, configure el cliente iperf:

a. En el campo **Dirección IP del servidor**, ingrese la dirección IPv4 del servidor iperf al que se conecta el cliente iperf.

b. En el campo **Puerto**, ingrese el número de puerto TCP o UDP del servidor iperf al que se conecta el cliente iperf. Rango de valores: de 1001 a 65 535. El valor predeterminado es `7777`.

c. En el campo **Intervalo del informe (s)**, ingrese el intervalo en segundos para escribir líneas en el informe de diagnóstico de rendimiento. Rango de valores: de 0 a 60. El valor predeterminado es `3`.

d. Si no desea crear un informe con los resultados del diagnóstico de rendimiento de la red, seleccione la casilla **Sin informe**. Esta casilla está desactivada por defecto.

e. En **Formato del informe**, seleccione el formato de los resultados del diagnóstico de rendimiento de la red en el informe:

- **Kbit/s**. Esta es la configuración predeterminada.
- **Mbit/s**.
- **Kbyte/s**.
- **Mbyte/s**.

f. En el campo **Ejecutar cliente durante (s)**, ingrese la duración en segundos durante la cual desea que se ejecute el cliente iperf. Rango de valores: de 60 a 3600. El valor predeterminado es `60`.

g. Especifique el tipo de puerto del servidor iperf; para ello, seleccine una de las siguientes opciones:

- **TCP**. Esta es la configuración predeterminada.
- **UDP**.

h. En el campo **Tasa de bits de cliente**, ingrese la tasa de bits del cliente iperf en uno de los siguientes formatos:

- `<tasa de bits en kbps>k` o `<tasa de bits en kbps>K`

  Por ejemplo, si ingresa `10000K`, la tasa de bits es de 10 000 kbps.

- `<tasa de bits en Mbps>m` o `<tasa de bits en Mbps>M`

  Por ejemplo, si ingresa `10 M`, la tasa de bits es de 10 Mbps.

i. En la lista desplegable **Probar dirección**, seleccione la dirección del tráfico que desea usar para medir el rendimiento de la red:

- **Cliente-Servidor** para usar el tráfico que el cliente iperf envía al servidor iperf. Esta es la configuración predeterminada.
- **Servidor-Cliente** para usar el tráfico que el servidor iperf envía al cliente iperf.
- **Bidireccional** para usar el tráfico que el cliente iperf envía al servidor iperf, así como el tráfico que el servidor iperf envía al cliente iperf.

j. Si es necesario, en el campo **Ventanas TCP (bytes)**, ingrese el tamaño de la ventana TCP en bytes. Si deja este campo en blanco, el tamaño de la ventana de TCP se determina automáticamente.

k. Si es necesario, en el campo **MSS de TCP (bytes)**, ingrese el tamaño máximo del segmento de TCP en bytes.

7. Haga clic en **Ejecutar**.

La utilidad iperf se ejecuta en el dispositivo CPE y se genera un informe con los resultados del diagnóstico de red.

Para administrar informes, haga clic en **Ir a los archivos**.

# Ejecutar la utilidad de barrido

Puede usar la utilidad de barrido para borrar la caché de ARP, reiniciar el proceso de Free Range Routing (FRR), borrar la tabla de sesiones de NAT o reiniciar un módem en un dispositivo CPE.

Reiniciar el proceso de FRR y borrar la tabla de sesiones de NAT puede hacer que la transmisión de tráfico se detenga durante unos segundos.

*Para ejecutar la utilidad de barrido:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad de barrido.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades → Barrido**.

   Se muestra la configuración de la utilidad de barrido.

4. Si desea borrar la caché de ARP:

   a. En **Borrar caché ARP**, seleccione la interfaz de red creada en la que desea borrar la caché de ARP. Si desea borrar la caché de ARP en todas las interfaces de red, seleccione **Todos**.

   b. Haga clic en **Ejecutar**.

   La caché de ARP se borra en el dispositivo CPE.

5. Si desea reiniciar el proceso de FRR, en **Proceso FRR**, haga clic en **Ejecutar**.

   El proceso de FRR se reinicia en el dispositivo CPE.

6. Si desea borrar la tabla de sesiones de NAT, en **Tabla de sesiones de NAT**, haga clic en **Ejecutar**. Puede configurar NAT en un dispositivo CPE utilizando un firewall.

   La tabla de sesiones de NAT se borra en el dispositivo CPE.

7. Si desea reiniciar un módem, en **Módem**, seleccione el módem en la lista **Restablecer módem** y haga clic en el botón **Ejecutar**.

   El módem se reinicia en el dispositivo CPE.

# Ejecutar la utilidad de volcado OpenFlow

La utilidad de volcado de OpenFlow genera un informe con los flujos de volcado y los grupos de volcado solicitados. Cuando vuelva a ejecutar la utilidad de volcado de OpenFlow, el informe se sobrescribirá. Puede descargar el informe si desea conservarlo.

*Para ejecutar la utilidad de volcado de OpenFlow, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar la utilidad de volcado de OpenFlow.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades → Volcado OpenFlow**.

   Se muestran las opciones de la utilidad de volcado de OpenFlow.

4. Haga clic en **Ejecutar**.

   La utilidad de volcado de OpenFlow se ejecuta en el dispositivo CPE y se genera un informe con los flujos de volcado y los grupos de volcado solicitados.

Para administrar informes, haga clic en **Ir a los archivos**.

# Restablecer las sesiones de BGP/OSPF

Puede emitir comandos para restablecer o borrar las sesiones de BGP y OSPF en un dispositivo CPE. Para ejecutar estos comandos, debe crear una solicitud de borrado que conste de uno o más comandos de `borrado`.

*Para crear y ejecutar una solicitud de borrado, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea ejecutar los comandos de borrado.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades** → **Borrar BGP/OSPF**.

   Se muestran las opciones para crear los comandos de borrado.

4. Haga clic en **Crear**.

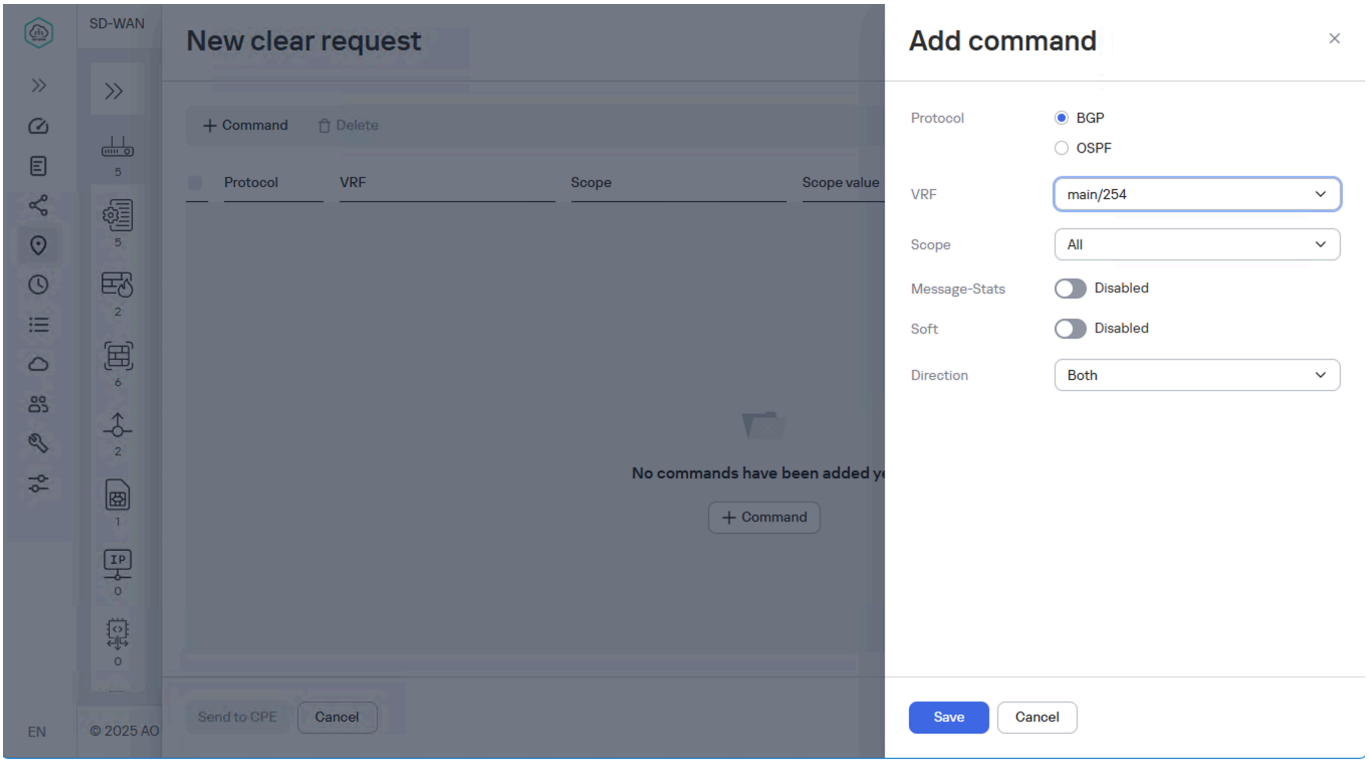
   Esto abre el área de creación de solicitudes de borrado con una tabla que enumera los comandos de borrado que se están creando.

5. Haga clic en el botón **Crear** para agregar uno o más comandos:

   a. En el área de creación de comandos, en el campo **Protocolo**, seleccione un protocolo (**BGP** u **OSPF**).

   b. Especifique las opciones de comandos de borrado para el protocolo seleccionado.

   c. Haga clic en **Guardar** para guardar las opciones de comandos.

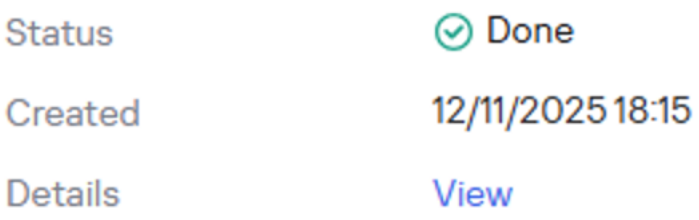



Agregar un comando de borrado

El comando se agrega a la tabla. Si es necesario, puede seleccionar un comando en la tabla y eliminarlo haciendo clic en el botón **Eliminar**.

6. Haga clic en el botón **Enviar al CPE**.

La solicitud de borrado creada con un conjunto de comandos se envía al dispositivo CPE y los comandos se ejecutan uno por uno. Puede ver el estado de ejecución de la última solicitud y sus detalles en **Estado de la última solicitud de borrado**.




Estado de la última solicitud de borrado

# Administrar informes

*Informes* generados por las utilidades tcpdump, iperf y volcado de OpenFlow. Para ver la tabla de informes de un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Utilidades** →**Archivos**. La información sobre los informes se muestra en las siguientes columnas de la tabla:

- **Tipo** es el formato del informe.
- **Creado** es la fecha y hora de creación del informe.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Descargar un informe

*Para descargar un informe, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE desde el que desea descargar el informe.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades** → **Archivos**.

   Se muestra la tabla de informes.

4. Haga clic en **Descargar** junto al informe que desea descargar.

El archivo del informe se guarda en su dispositivo local.

## Eliminar un informe

Los informes eliminados no se pueden restaurar.

*Para generar un informe:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea eliminar un informe.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Utilidades** → **Archivos**.

   Se muestra la tabla de informes.

4. Haga clic en **Eliminar** junto al informe que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El informe se elimina y ya no se muestra en la tabla.

# Ejecutar tareas en dispositivos CPE

Kaspersky SD-WAN admite la ejecución de tareas en dispositivos CPE en un momento específico. Puede usar etiquetas para agrupar los dispositivos CPE en los que desea ejecutar una tarea.

Existen los siguientes tipos de tareas:

- Scripts programados en dispositivos CPE.
- Actualizaciones de firmware programadas en dispositivos CPE seleccionados manualmente y en dispositivos CPE con etiquetas especificadas.
- Actualización programada de la configuración del dispositivo CPE.

Cuando crea una tarea, utiliza la zona horaria de la máquina virtual en la que se implementa el orquestador. Por ejemplo, si programa una secuencia de comandos para que se ejecute en un dispositivo CPE a las 2:00 p.m., la secuencia de comandos se ejecuta a las 2:00 p.m. en la zona horaria del orquestador, incluso si la hora en el dispositivo CPE es 6:00 p.m.

Recomendamos tener en cuenta las siguientes consideraciones especiales al administrar tareas:

- Una imprecisión de 10 segundos se considera aceptable para el momento en que se ejecuta la tarea.
- Si existen varias tareas, estas se ejecutan simultáneamente. Si el orquestador no puede ejecutar todas las tareas simultáneamente, se ejecutan en el orden en que se crearon.
- Al eliminar una plantilla de CPE, se eliminan automáticamente todas las tareas asociadas a ella.
- Al eliminar un dispositivo CPE, se eliminan automáticamente todas las tareas asociadas a él.
- Al eliminar un script asociado con tareas, esta acción requiere una confirmación adicional. Si confirma la acción, el script se elimina y no se puede ejecutar dentro de las tareas creadas.

- Las tareas de actualización de la configuración del dispositivo CPE programadas no están disponibles en la sección del menú **Programador**. Puede programar una actualización solo en el área de configuración de un dispositivo CPE individual.
- Si hay una tarea programada para cambiar la configuración de un dispositivo CPE, la edición de la plantilla CPE asociada con ese dispositivo se bloquea hasta que se complete o cancele la tarea correspondiente.

Las tareas que aún no se han completado se pueden completar manualmente.

Puede ver la tabla de tareas en la sección **Programador**. La información sobre las tareas se muestra en las siguientes columnas de la tabla:

- **Id** es el Id. de la tarea.
- **Nombre** es el nombre de la tarea.
- **Usuario** es el nombre del usuario que creó la tarea.
- **Creado** es la fecha y hora en que se creó la tarea.
- **Estado** es el estado de la tarea:
  - **Realizado**significa que la tarea se ha completado con éxito.
  - **Error**significa que ocurrió un error al ejecutar la tarea.
  - **Pendiente**significa que la tarea se colocó en la base de datos del orquestador y está esperando su ejecución.
  - **En cola**significa que la tarea está en cola para su ejecución.
  - **En ejecución**significa que la tarea se está ejecutando.
- **Programado**es la fecha y hora en que se ejecutará la tarea.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una tarea

*Para crear una tarea, siga estos pasos:*

1. En el menú, vaya a la sección **Programador**.
   Se muestra la tabla de tareas programadas.
2. En la parte superior de la página, haga clic en **+ Tarea**.
3. En la parte superior de la barra lateral que se muestra, en la lista **Tipo**, seleccione un tipo de tarea.
   Se pueden crear tareas de los siguientes tipos en el menú **Programador**:
   - Ejecutar un script
   - Actualizar el firmware

Se crea una tarea del tipo **Configuración de actualización** cuando se realiza un guardado diferido de la configuración haciendo clic en el botón **Guardado programado** en el área de configuración del dispositivo CPE.

4. Especifique la configuración de la tarea. Para obtener una descripción de la configuración de la tarea, consulte las siguientes instrucciones:

   - Scripts programados en dispositivos CPE.
   - Programación de actualizaciones de firmware en dispositivos CPE con etiquetas específicas.

5. Haga clic en **Crear**.

La tarea se crea y se muestra en la tabla.

# Ejecutar una tarea manualmente

*Para ejecutar manualmente una tarea, siga estos pasos:*

1. En el menú, vaya a la sección **Programador**.

   Se muestra la tabla de tareas programadas.

2. Para ejecutar manualmente una tarea individual, siga estos pasos:

   a. Haga clic en la tarea que desea ejecutar manualmente.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

   b. En la parte superior del área de configuración, debajo de**Acciones**, haga clic en **Ejecutar ahora**.

3. Para ejecutar manualmente varias tareas, siga estos pasos:

   a. Marque las casillas situadas junto a las tareas que desea ejecutar manualmente.

   b. En la parte superior de la tabla, haga clic en**Acciones** → **Ejecutar ahora**.

4. En la ventana de confirmación, haga clic en **Ejecutar ahora**.

Las tareas se completan y su estado en la columna **Estado** cambia a**Realizado**.

# Eliminar una tarea

Las tareas eliminadas no se pueden restaurar.

*Para eliminar una tarea:*

1. En el menú, vaya a la sección **Programador**.

   Se muestra la tabla de tareas programadas.

2. Para eliminar una tarea individual:

   a. Seleccione la tarea que desea eliminar.

      Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

   b. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

3. Para eliminar varias tareas:

   a. Marque las casillas situadas junto a las tareas que desea eliminar.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

Las tareas se eliminan y ya no se muestran en la tabla.

# Comprobaciones en dispositivos CPE

Las siguientes funciones se proporcionan en dispositivos CPE para garantizar la integridad y confiabilidad de los componentes críticos del sistema, incluido el firewall:

- La comprobación de integridad ayuda a garantizar que los archivos ejecutables y los archivos de configuración críticos, incluidos los archivos del firewall, coincidan con el firmware publicado y a la detección de cambios no autorizados en el sistema.
- La comprobación automática del firewall verifica su estado.
- El bloqueo del tráfico, en caso de que falle una comprobación, refuerza aún más la seguridad de la red, ya que impide la transmisión de tráfico de tránsito entre dispositivos cuando se detecta algún problema.

Las comprobaciones se pueden ejecutar a pedido o según una programación; puede configurar la programación en una plantilla CPE o directamente en un dispositivo CPE.

## Comprobación de integridad

Esta función permite verificar automática o manualmente la integridad de los archivos de configuración y ejecutables críticos, incluidos los archivos del firewall, comparando estos archivos con sumas de control de referencia. Esta función puede detectar cambios no autorizados y garantizar que los scripts del sistema y los archivos ejecutables coincidan con el firmware publicado.

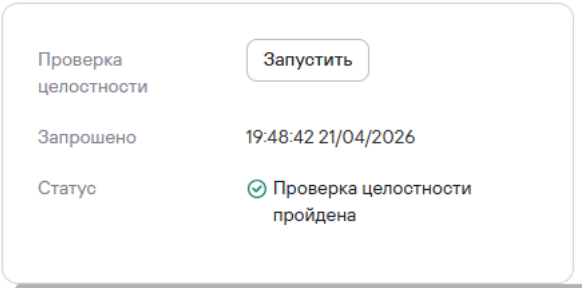
Puede ejecutar una comprobación a pedido o configurar una comprobación programada.

# Ejecutar una comprobación de integridad manual

*Para ejecutar una comprobación de integridad manual, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.
2. Haga clic en el dispositivo CPE en el que desea realizar la comprobación.
3. En el menú, seleccione la sección SD-WAN y la pestaña Comprobaciones de CPE.
4. En Comprobaciones manuales, haga clic en Ejecutar junto al nombre de la comprobación.

Se inicia una herramienta en el dispositivo CPE, que realiza la comprobación y envía la información al registro del sistema del dispositivo CPE. La fecha y la hora en que se inició la comprobación de integridad se muestran en Comprobaciones manuales. Una vez completada la comprobación, el resultado se muestra en el campo **Estado**.




Resultado de la comprobación de integridad en el dispositivo CPE

El estado y el resultado de la comprobación también se muestran en el área de configuración del dispositivo CPE en la sección **General** en **Administración fuera de banda**. Después de iniciar la tarea Comprobación de integridad, el estado será Ejecutando. Luego, en función del resultado que devuelva la herramienta, el CPE envía un estado de éxito o de error al orquestador.

Puede verificar el estado de la tarea en el registro del sistema del dispositivo CPE. Para hacerlo:

1. Abra la configuración del dispositivo CPE y vaya a la sección Información de diagnóstico.
2. Haga clic en el botón Solicitar información de diagnóstico y espere que se complete la solicitud.
3. En la lista desplegable **Tipo**, seleccione `registro de cpe`.

Si el análisis de integridad se realiza correctamente, el registro del sistema del dispositivo CPE incluye una entrada del tipo `sdwan user.info` con el mensaje de `comprobación de integridad realizada con éxito`.

Registro del dispositivo CPE acerca de la finalización satisfactoria de la comprobación de integridad

# Configuración de la comprobación de integridad programada

Puede crear una comprobación de integridad programada en una plantilla de CPE o en un dispositivo CPE.

*Para configurar una comprobación de integridad programada, siga estos pasos:*

1. Configure la comprobación de integridad programada de una de las siguientes maneras:

   - Si desea configurar la comprobación de integridad programada en una plantilla de CPE, vaya a la sección SD-WAN → Plantillas de CPE, haga clic en la plantilla CPE, seleccione la sección SD-WAN en el menú lateral y seleccione la pestaña Comprobaciones de CPE.

   - Si desea configurar la comprobación de integridad programada en un dispositivo CPE, vaya a la sección SD-WAN → CPE, haga clic en el dispositivo CPE, seleccione la sección SD-WAN en el menú lateral, seleccione la pestaña Comprobaciones de CPE y habilite botón de alternancia Anular.

2. En Comprobaciones programadas, habilite el botón de alternancia Comprobación de integridad.

3. Seleccione un intervalo entre comprobaciones de la lista desplegable. Las siguientes opciones están disponibles: 1, 2, 3, 4, 6, 8 y 12 horas. El intervalo predeterminado es 8 horas.

4. Si es necesario, habilite el bloqueo del tráfico de tránsito en el dispositivo CPE en caso de una comprobación fallida mediante el botón de alternancia **Bloquear el reenvío de tráfico si fallan las comprobaciones**.

La herramienta que realiza la comprobación y escribe los resultados en el registro del sistema del dispositivo CPE se iniciará en el CPE en los intervalos especificados.

El estado y el resultado de la comprobación se muestran en el área de configuración del dispositivo CPE en la sección General en Administración fuera de banda. Después de iniciar la tarea Comprobación de integridad, el estado será Ejecutando. Luego, en función del resultado que devuelva la herramienta, el CPE envía un estado de éxito o de error al orquestador.

# Autocomprobación del firewall

Esta función permite verificar el estado del firewall en el CPE.

Puede ejecutar la comprobación manualmente o configurar una comprobación programada.

## Ejecución manual de una comprobación automática del firewall

*Para iniciar una comprobación automática del firewall manualmente, siga estos pasos:*

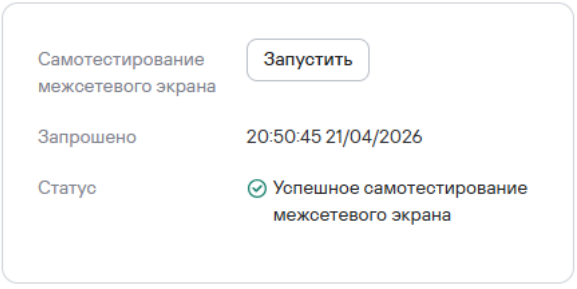
1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

2. Haga clic en el dispositivo CPE en el que desea realizar la comprobación.

3. En el menú, seleccione la sección SD-WAN y la pestaña Comprobaciones de CPE.

4. En Comprobaciones manuales, haga clic en Ejecutar junto al nombre de la comprobación.

Se inicia un script en el dispositivo CPE, que realiza la comprobación automática del firewall y envía la información al registro del sistema del dispositivo CPE. La fecha y la hora en que se inició la comprobación automática del firewall se muestran en Comprobaciones manuales. Una vez completada la comprobación, el resultado se muestra en el campo **Estado**.



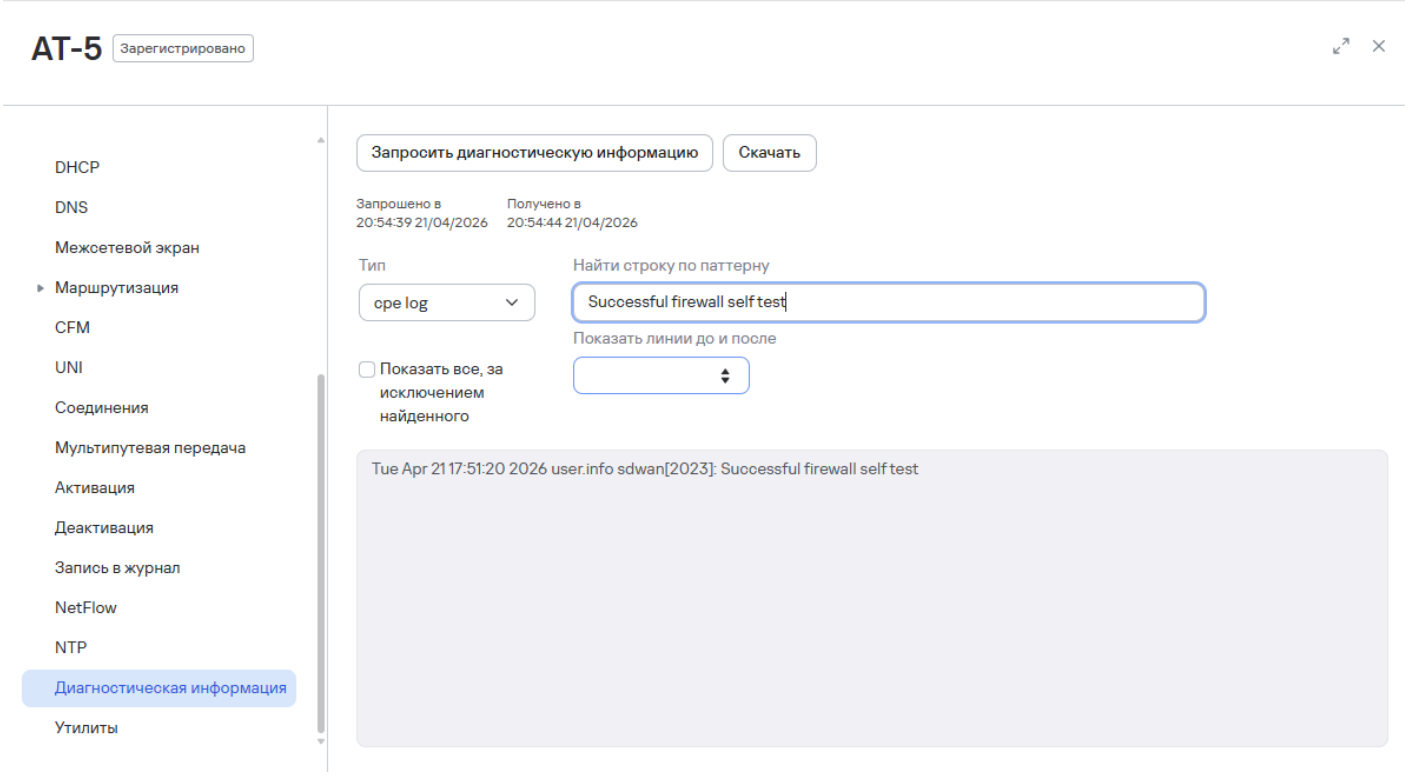

Resultado de una comprobación automática del Firewall en un dispositivo CPE

El estado y el resultado de la comprobación también se muestran en el área de configuración del dispositivo CPE en la sección **General** en **Administración fuera de banda**. Después de iniciar la tarea **Autocomprobación del firewall**, el estado será **Ejecutando**. Luego, en función del resultado que devuelva la herramienta, el CPE envía un estado de éxito o de error al orquestador.

Puede verificar el estado de la tarea en el registro del sistema del dispositivo CPE. Para hacerlo:

1. Abra la configuración del dispositivo CPE y vaya a la sección Información de diagnóstico.
2. Haga clic en el botón Solicitar información de diagnóstico y espere que se complete la solicitud.
3. En la lista desplegable **Tipo**, seleccione `registro de cpe`.

Si la comprobación automática del firewall se realizó correctamente, el registro del sistema del dispositivo CPE contiene un registro del tipo `user.info sdwan` con el mensaje `La comprobación automática de firewall se realizó correctamente`.




Registro del dispositivo CPE acerca de la finalización correcta de la comprobación automática del Firewall

## Configuración de la comprobación automática programada del firewall

Puede configurar una comprobación automática programada del Firewall en una plantilla de CPE o en un dispositivo CPE.

*Para configurar una comprobación automática programada del Firewall:*

1. Configure la comprobación automática programada del firewall de una de las siguientes maneras:

   - Si desea configurar la comprobación automática programada del firewall en una plantilla CPE, vaya a la sección SD-WAN → Plantillas de CPE, haga clic en la plantilla CPE, seleccione la sección SD-WAN en el menú lateral y seleccione la pestaña Comprobaciones de CPE.

   - Si desea configurar la comprobación automática programada del firewall en un dispositivo CPE, vaya a la sección SD-WAN → CPE, haga clic en el dispositivo CPE, seleccione la sección SD-WAN en el menú lateral, seleccione la pestaña Comprobaciones de CPE y habilite botón de alternancia Anular.

2. En Comprobaciones programadas, habilite el botón de alternancia Comprobación de integridad.

3. Seleccione un intervalo entre comprobaciones de la lista desplegable. Las siguientes opciones están disponibles: 1, 2, 3, 4, 6, 8 y 12 horas. El intervalo predeterminado es 8 horas.

4. Si es necesario, habilite el bloqueo del tráfico de tránsito en el dispositivo CPE en caso de una comprobación fallida mediante el botón de alternancia **Bloquear el reenvío de tráfico si fallan las comprobaciones**.

El script que realiza la comprobación y escribe los resultados en el registro del sistema del dispositivo CPE se iniciará en el CPE en los intervalos especificados.

El estado y el resultado de la comprobación se muestran en el área de configuración del dispositivo CPE en la sección General en Administración fuera de banda. Después de iniciar la tarea Autocomprobación del firewall, el estado será Ejecutando. Luego, en función del resultado que devuelva la herramienta, el CPE envía un estado de éxito o de error al orquestador.

Las comprobaciones fallidas también se muestran en la pestaña **Problemas** del menú CPE.

# Bloquear tráfico si falla la comprobación de la integridad o la comprobación automática

Esta función está diseñada para bloquear el tráfico de tránsito (el tráfico entre las interfaces de red de un dispositivo CPE) si la prueba automática y la comprobación de integridad de los archivos críticos del sistema y los scripts en el dispositivo CPE fallan. Complementa las funciones de comprobación de integridad y comprobación automática del Firewall y se configura junto con estas. Puede habilitar el bloqueo del tráfico de tránsito en las comprobaciones programadas de los CPE. Puede habilitar o deshabilitar el bloqueo de tráfico en una plantilla CPE o en un dispositivo CPE. Cuando el bloqueo está habilitado en una plantilla CPE, el tráfico de tránsito se bloquea en caso de errores de comprobación de integridad o de comprobación automática en todos los dispositivos CPE que utilizan esta plantilla.

*Para habilitar el bloqueo del tráfico de tránsito si falla la comprobación automática o la comprobación de integridad, siga estos pasos:*

1. Habilite el bloqueo del tráfico de tránsito de una de las siguientes formas:

   - Si desea habilitar el bloqueo de tráfico de tránsito en una plantilla CPE, vaya a la sección SD-WAN → Plantillas de CPE, haga clic en la plantilla CPE, seleccione la sección SD-WAN en el menú lateral y seleccione la pestaña Comprobaciones de CPE.

   - Si desea habilitar el bloqueo del tráfico de tránsito en un dispositivo CPE, vaya a la sección SD-WAN → CPE, haga clic en el dispositivo CPE, seleccione la sección SD-WAN en el menú lateral, seleccione la pestaña Comprobaciones de CPE y habilite botón de alternancia Anular.

2. Asegúrese de que la verificación de integridad y la comprobación automática del Firewall estén habilitadas y que el intervalo requerido entre las verificaciones esté configurado.

   > Para habilitar el bloqueo de tráfico de tránsito, ambas comprobaciones deben estar habilitadas.

3. Habilite el bloqueo de tráfico habilitando el botón de alternancia Bloquear el reenvío de tráfico si fallan las comprobaciones.

   Si habilitó el bloqueo de tráfico en la plantilla CPE, se muestra una advertencia:

   **Si alguna de las comprobaciones falla, se bloqueará el reenvío del tráfico de tránsito en todos los dispositivos CPE que utilicen esta plantilla. ¿Está seguro de que desea continuar**

   Confirme que desea habilitar el bloqueo haciendo clic enSí, continuar.

4. Guarde los cambios en la plantilla o el dispositivo CPE.

El bloqueo de tráfico de tránsito está habilitado. Si alguna de las comprobaciones falla, el dispositivo CPE comienza a bloquear el tráfico de tránsito y el orquestador muestra una ventana emergente de advertencia para ese dispositivo CPE. Al mismo tiempo, la conexión entre el CPE y el orquestador no se interrumpe, lo que le permite administrar el dispositivo y cambiar su configuración.

Para dejar de bloquear el tráfico de tránsito, siga estos pasos:

1. Determine la causa exacta del bloqueo realizando ambas comprobaciones manuales por separado:

   - Comprobación de la integridad a pedido

   - Ejecutar una comprobación automática del firewall a pedido

2. Elimine la causa:

   - Si el problema se produjo después de una comprobación automática del firewall, reinicie el dispositivo CPE.

   - Si el problema ocurrió después de una verificación de integridad, restaure el firmware del CPE mediante el procedimiento de actualización.

   - Si está seguro de que la funcionalidad del firewall no se ve afectada y la comprobación arrojó un falso positivo, deshabilite el botón de alternancia Bloquear el reenvío de tráfico si fallan las comprobaciones y guarde la configuración del dispositivo CPE. El tráfico se desbloquea, después de lo cual puede volver a habilitar la función de bloqueo.

Cuando se vuelve a permitir el tráfico de tránsito en el dispositivo CPE, desaparece la ventana emergente del orquestador.

Puede consultar el estado de las comprobaciones y los bloqueos de tráfico en el registro del sistema del dispositivo CPE. Para hacerlo:

1. Abra la configuración del dispositivo CPE y vaya a la sección Información de diagnóstico.
2. Haga clic en el botón Solicitar información de diagnóstico y espere que se complete la solicitud.
3. En la lista desplegable **Tipo**, seleccione `registro de cpe`.

   Algunas de las siguientes entradas estarán presentes en el registro del sistema del dispositivo CPE:

   - Tipo `user.crit.fwblock`, mensaje `Error de comprobación automática del Firewall. Reenvío de tráfico bloqueado`.

     Error de comprobación automática del Firewall. El reenvío del tráfico de tránsito está bloqueado.

   - Tipo `user.crit.integrityblock`, mensaje `Error de comprobación de la integridad del Firewall. Reenvío de tráfico bloqueado`.

     Error de comprobación de la integridad. El reenvío del tráfico de tránsito está bloqueado.

   - Tipo `user.info.checksuccess`, mensaje `La comprobación se realizó correctamente`.

     Las comprobaciones se realizaron correctamente. Se permite el tráfico de tránsito.

# Auditoría de eventos de seguridad

Los eventos pueden ocurrir en el orquestador de Kaspersky SD-WAN y en los dispositivos CPE que son relevantes para la seguridad de la información: autorización del usuario, modificación de la plantilla o configuración del dispositivo, interacción con sistemas externos, etc. Estos eventos se denominan *eventos de seguridad* y requieren una atención especial por parte de los administradores de la red. Para el registro centralizado de eventos de seguridad, Kaspersky SD-WAN admite la auditoría de eventos de seguridad. Los eventos de seguridad que ocurren en el orquestador se ingresan en los registros del contenedor de Docker en el que se ejecuta el orquestador. Los eventos de seguridad que ocurren en los dispositivos CPE se ingresan en los registros del sistema de los dispositivos. Una vez ingresados, los eventos de seguridad se envían al servidor syslog especificado en el archivo de configuración durante el despliegue de la solución. Para facilitar el procesamiento de eventos, puede configurar un recopilador SIEM externo como servidor de syslog (por ejemplo, Kaspersky Unified Monitoring and Analysis Platform, en lo sucesivo también denominado KUMA). Para algunos eventos de seguridad, también puede configurar qué eventos desea que se ingresen en el registro de auditoría y el nivel de detalle (registrar solo el hecho del evento o también sus detalles).

En esta sección se proporcionan instrucciones para configurar la auditoría de eventos de seguridad para el orquestador y el dispositivo CPE, y para configurar un recopilador KUMA externo.

# Configurar el registro de eventos de seguridad para la auditoría

Los eventos de seguridad se ingresan y almacenan en los registros del orquestador y los dispositivos CPE. Para aprovechar todo el potencial de los registros de auditoría, debe configurar la exportación de eventos a un servidor de syslog externo. Recomendamos utilizar la solución Kaspersky Unified Monitoring and Analysis Platform (KUMA) como el servidor syslog.

La configuración de syslog para la exportación de registros del orquestador debe especificarse en el archivo de configuración antes de desplegar la solución. Si desea cambiar la configuración, por ejemplo, especificar un certificado CA o una dirección de servidor de syslog diferente, deberá cambiar el archivo de configuración y reinstalar la solución. Si desea usar una conexión cifrada para el servidor de syslog, debe obtener un certificado CA por adelantado

*Para configurar el registro de eventos de seguridad para la auditoría:*

1. Si desea usar un recopilador de KUMA como servidor de syslog:
   a. Implemente y configure el recopilador de KUMA como se describe en las instrucciones Configuración de un recopilador de KUMA para procesar eventos de seguridad.
   b. Guarde el certificado CA del servidor KUMA para usarlo para el cifrado TLS de mensajes de syslog:
      1. Abra la interfaz web de KUMA.
      2. En la esquina inferior izquierda de la ventana, haga clic en el nombre de la cuenta de usuario y, en el menú, haga clic en el botón **Certificado CA de microservicio**.

2. Configure la exportación de los registros del orquestador al servidor de syslog en el archivo de configuración para el despliegue de la solución:

   a. Prepare el archivo de configuración y, en ese archivo, ingrese la configuración básica para el despliegue de la solución.

   b. En la sección `external.orc`, ingrese la siguiente configuración del servidor syslog:

   - `syslog_server_address`

     Especifique la dirección web del servidor syslog al que los contenedores Docker del orquestador enviarán registros. El valor se especifica en el formato `<protocolo>://<dirección del host>:<número de puerto>`. Puede especificar la dirección IP o FQDN del host como la dirección del host.

     Si desea que los mensajes de syslog estén cifrados con TLS, especifique `tcp+ls` como protocolo.

     Ejemplo:

     `tcp+tls://my-syslog-server:1514`

     > Si especificará un servidor syslog externo, por ejemplo, un recopilador de KUMA, deshabilite la opción para desplegar un contenedor independiente para el servidor syslog integrado. Para hacerlo, especifique `disabled` en la configuración `external.syslog.state`.

   - `secure_syslog`

     Especifique `true` para cifrar los registros transmitidos al servidor o `false` para texto sin formato.

     Si se establece en `true`, los mensajes de syslog se envían a través de TCP con cifrado TLS. Para que TLS funcione, también debe especificar la ruta al certificado CA con el que se firma el certificado del servidor syslog en la variable `syslog_server_ca_cert_file_path`.

   - `syslog_server_ca_cert_file_path`

     Especifique la ruta absoluta al archivo del certificado CA que se utilizó para firmar el certificado del servidor syslog. Esta configuración es necesaria si especificó `true` para la configuración `secure_syslog`.

     Si el certificado CA del servidor syslog se emitió para un nombre de dominio, para usar el cifrado TLS debe especificar el FQDN del servidor en la configuración `syslog_server_address`. Este nombre de dominio debe resolverse a través del servidor DNS especificado al configurar el DNS en el dispositivo CPE.

   - `syslog_format`

     Especifique el formato de registro que se utilizará para enviar mensajes de syslog. Valores posibles:

     - `rfc3164` para formato compatible con RFC 3164.
     - `rfc5424` para formato compatible con RFC 5424.
     - `rfc5424micro` para formato compatible con RFC 5424 con marcas de tiempo con precisión de microsegundos.

     Si desea utilizar un recopilador de KUMA como servidor de syslog, especifique `rfc3164`.

3. Despliegue la solución.

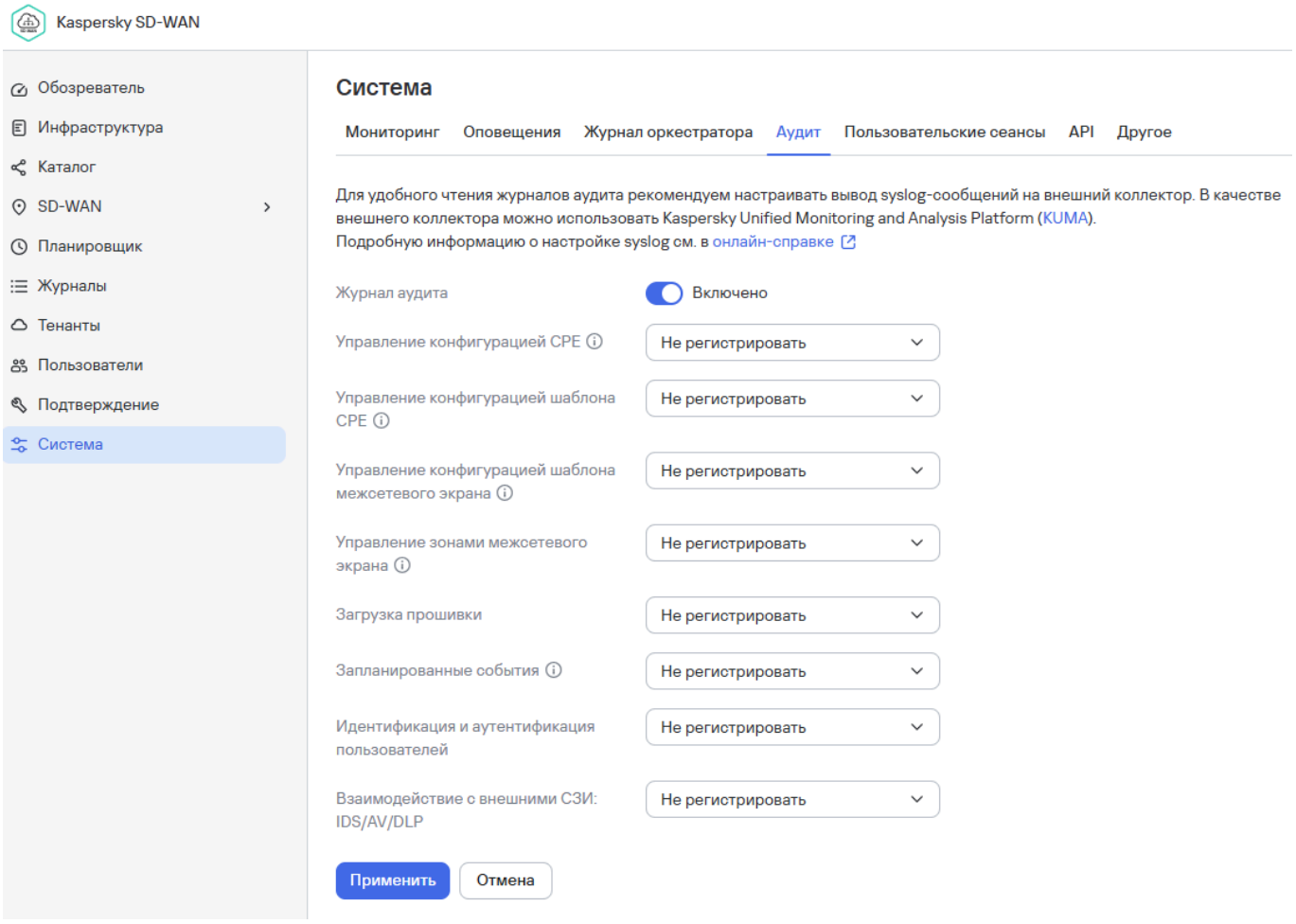
   Los contenedores del orquestador se despliegan con la configuración del servidor syslog especificada en el archivo de configuración.

4. Inicie sesión en la interfaz web del orquestador para administrar más configuraciones de auditoría.

5. Seleccione qué eventos de seguridad del orquestador desea que se ingresen en el registro de auditoría:

a. Vaya a la sección **Sistema** →**Auditoría**.

Se abre una lista de alcances de auditoría para los cuales puede habilitar el registro de eventos de seguridad en el orquestador. Un evento de seguridad ocurre cuando el estado del alcance de la auditoría cambia, por ejemplo, si se cambia la configuración en el dispositivo o en la plantilla de CPE, o si un sistema de seguridad de la información externo realiza una llamada a la API.




Configurar el registro de auditoría para eventos de seguridad del orquestador

a. Habilite el registro de auditoría; para ello, active el botón de alternancia **Registro de auditoría**.

> Cada vez que habilita o deshabilita esta configuración, se ingresa un evento con el código `SYS-AUD` en el registro de auditoría.

b. Para cada categoría de eventos de seguridad que desee registrar, seleccione el modo de registro en la lista desplegable:

- **Estándar** (registro del hecho del evento en el alcance de la auditoría seleccionado)
- **Extendida** (registro de información detallada acerca del evento en el alcance de la auditoría seleccionado, por ejemplo, el valor anterior y el nuevo cuando se cambia una configuración, etc.) No está disponible para todas las áreas de la auditoría).

c. Para guardar los cambios, haga clic en el botón **Aplicar**.

Los eventos de seguridad que ocurren en los alcances de auditoría seleccionados se ingresan en el registro de auditoría y se envían al servidor syslog que especificó en el archivo de configuración durante el despliegue de la solución.

Para obtener una lista detallada de los eventos de seguridad que se pueden registrar en el orquestador, consulte el artículo Lista de eventos de seguridad que se pueden registrar en el orquestador y los dispositivos CPE.

6. Configure el servidor syslog para los registros en dispositivos CPE:

   a. En la interfaz web del orquestador, navegue hasta los dispositivos o las plantillas CPE en los que desea configurar un servidor syslog para que reciba los registros.

   b. Siga las instrucciones de Configurar registros en dispositivos CPE para administrar la configuración del servidor syslog. Si desea utilizar el recopilador de KUMA como servidor de syslog, cargue el certificado CA del servidor guardado anteriormente en los dispositivos.

   Los eventos de seguridad que ocurren en los dispositivos CPE se enviarán al servidor syslog especificado.

   Para obtener una lista detallada de los eventos de seguridad que se pueden registrar en los dispositivos CPE, consulte el artículo Lista de eventos de seguridad que se pueden registrar en el orquestador y los dispositivos CPE.

# Lista de eventos de seguridad que se pueden registrar en el orquestador y los dispositivos CPE

La siguiente es una lista de eventos de seguridad que se pueden ingresar en el registro de auditoría del orquestador.

Lista de eventos de seguridad que se pueden registrar

| Código | Evento | Acción | Gravedad | Gravedad del evento de KUMA | Tiempo de activación | |
|---|---|---|---|---|---|---|
| Registro de auditoría | | | | | | |
| SYS-AUD | Iniciado | Se habilita el subsistema de auditoría | información | baja | Al hacer clic: Guardar | Message: Code Event: Username:$ ...], Extended: [$code ...], OrcVersion<br>SYS-AUD Started: Username:admin SDW-CPET, SDW-FWT, SDW-FWZ SYS-API], Extended: [], OrcVersion:<br>SYS-AUD Started: Username:admin [SDW-CPE, SDW-CPET, SDW-FWT<br>SYS-AUD Started: Username:admin SCH-FMWU, USR-USR, SYS-API], E FWZ], OrcVersion:3.0.0.release.1.cis. |
| SYS-AUD | Detenido | Se deshabilita el subsistema de auditoría | advertencia | media | Al hacer clic: Guardar | Message: Code Event: Username:$ ...], Extended: [$code ...], OrcVersion<br>SYS-AUD Stopped: Username:admi SDW-CPET, SDW-FWT, SDW-FWZ SYS-API], Extended: [], OrcVersion:<br>SYS-AUD Stopped: Username:admi [SDW-CPE, SDW-CPET, SDW-FWT<br>SYS-AUD Stopped: Username:admi SCH-FMWU, USR-USR, USR-PERM FWT, SDW-FWZ], OrcVersion:3.0.0. |

| | | | | | | |
|---|---|---|---|---|---|---|
| SYS-AUD | Error | No se puede iniciar el subsistema de auditoría | advertencia | media | Inmediatamente después de la ocurrencia | Message: Code Event: Standard: [$ OrcVersion:$orcversion, $ErrorMes<br>SYS-AUD Error: Standard: [SDW-C SCH-FMWU, USR-USR, USR-PERM OrcVersion:3.0.0.release.1.cis.amd64<br>SYS-AUD Error: Standard: [], Extend OrcVersion:3.0.0.release.1.cis.amd64<br>SYS-AUD Error: Standard: [SDW-FM Extended: [SDW-CPE, SDW-CPET, OrcVersion:3.0.0.release.1.cis.amd64 |
| **Administración de la configuración de CPE** | | | | | | |
| SDW-CPE | Cualquiera | Cualquier cambio en cualquier sección de CPE que no esté incluido en las secciones especializadas que se describen a continuación. | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-CPE Any: Username:admin(te CTenant:tenant-1, OrcVersion:3.0.0. |
| SDW-CPE | AnyError | Cualquier cambio en cualquier sección de CPE que no esté incluido en las secciones especializadas que se describen a continuación, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE AnyError: CPE:vCPE1, Te |
| SDW-CPE | Crear | Creación de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-CPE Create: Username:admin Template:vCPE1, CTenant:tenant-1. |
| SDW-CPE | CreateError | Creación de CPE con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE CreateError: CPE:vCPE1 |
| SDW-CPE | Registro | Registro de CPE | información | baja | El estado de CPE cambia a: Activar | Standard/Extended: Code Event: C<br>SDW-CPE Registration: CPE:vCPE1 |
| SDW-CPE | RegistrationError | Registro de CPE con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE RegistrationError: CPE: v ErrorMessage |
| SDW-CPE | Eliminar | Eliminación de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-CPE Delete: Username:admin Template:vCPE1, TTenant:tenant-1, |
| SDW-CPE | DeleteError | Eliminación de CPE con error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE DeleteError: CPE:vCPE1, |
| SDW-CPE | Deshabilitar | Deshabilitación de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-CPE Disable: Username:admin Template:vCPE1, TTenant:tenant-1, |
| SDW-CPE | DisableError | Deshabilitación de CPE con error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE DisableError: CPE:vCPE1 |
| SDW-CPE | Habilitar | Habilitación de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-CPE Enable: Username:admin Template:vCPE1, CTenant:tenant-1 |
| SDW-CPE | EnableError | Habilitación de CPE con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE EnableError: CPE:vCPE1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-CPE-GEN | FirewallTemplate | Modificación de las plantillas de instancias de CPE | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$ Template:$name, CTenant:$name, C<br>SDW-CPE-GEN FirewallTemplate: U Template:vCPE1, CTenant:tenant-1,<br>Extended: Code Event: Username:$ Template:$name, CTenant:$name, C<br>SDW-CPE-GEN FirewallTemplate: U Template:vCPE1, CTenant:tenant-1, [Changed:Default firewall template: |
| SDW-CPE-GEN | FirewallTemplateError | Modificación de las plantillas de instancias de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE-GEN FirewallTemplateEr $ErrorMessage |
| SDW-CPE-ENC | Cifrado | Cambio del cifrado de vínculos en una instancia de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen [Changed:$state],<br>SDW-CPE-ENC Encryption: Usern Template:vCPE1, CTenant:tenant-1, [Changed:enabled \|\| disabled] |
| SDW-CPE-ENC | EncryptionError | Cambio del cifrado de vínculos en una instancia de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE-ENC EncryptionError: C $ErrorMessage |
| SDW-CPE-SCR | Scripts | Ejecución de scripts en una instancia de CPE | información | baja | Al hacer clic: Ejecutar | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen $SriptName]<br>SDW-CPE-SCR Scripts: Username Template:vCPE1, CTenant:tenant-1, [Run:custom_config] |
| SDW-CPE-SCR | ScriptsError | Ejecución de scripts en la instancia de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $ErrorMessage<br>SDW-CPE-SCR ScriptsError: CPE: $ErrorMessage |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-CPE-NET | Interfaz | Agregar/Eliminar/Cambiar zona/dirección IP/Dirección MAC/Interfaz QoS en la instancia de CPE | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$ Template:$name, CTenant:$name, C<br>SDW-CPE-NET Interface: Usernam Template:vCPE1, CTenant:tenant-1, [Changed]<br><br>Extended: Code Event: Username:$ Template:$name, CTenant:$name, C Deleted \|\| Changed: GEN \|\| QOS: $D<br>SDW-CPE-NET Interface: Usernam Template:vCPE1, CTenant:tenant-1, [Added: GEN: Zone:lan, Bridge:false IPv4 address:10.1.1.1, IPv4 netmask:25 broadcast:10.1.1.255, Override MAC:( Enable QoS:false, MaxRate:1000, BE<br>SDW-CPE-NET Interface: Usernam Template:vCPE1, CTenant:tenant-1, [Deleted: GEN: Zone:lan, Bridge:fals IPv4 address:10.1.1.1, IPv4 netmask:25 broadcast:10.1.1.255, Override MAC:( Enable QoS:false, MaxRate:1000, BE<br>SDW-CPE-NET Interface: Usernam Template:vCPE1, CTenant:tenant-1, [Changed: GEN: Zone: lan>lan(tenar automatically:true>false, IPv4 input 10.1.1.1>10.2.2.2, IPv4 netmask: 255.0.0 broadcast: 10.1.1.255>10.2.2.255, Over Generate MAC: true>false, Change BE(MaxR):90]<br><br>Mostrar el cambio de/a en Cambio<br>El cambio de/a no se muestra en Ca inmediatamente. |
| SDW-CPE-NET | InterfaceError | Agregar/Eliminar/Cambiar zona/Interfaz de QoS en la instancia de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C $alias, [GEN \|\| QoS], $ErrorMessage<br>SDW-CPE-NET InterfaceError: CPE [GEN], $ErrorMessage<br>SDW-CPE-NET InterfaceError: CPE [QoS], $ErrorMessage |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-CPE-FW | Firewall | Cambiar la configuración del firewall en una instancia de CPE | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$ Template:$name, CTenant:$name, C<br><br>SDW-CPE-FW Firewall: Username:a Template:vCPE1, CTenant:tenant-1,<br><br>Extended: Code Event: Username:$ Template:$name, CTenant:$name, C GEN \|\| RUL \|\| ADVR \|\| NAT \|\| ZF \|\| IPSE<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. protection:Disable, Default INPUT a<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. Action:ACCEPT, IPset:null, IPv:IPv4, DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + ne IPset:null, IPv:IPv4, SrcZ:wan, DstZ: la rule), Changed: RUL: (Name:Allow-P DstZ:null, SrcIP:null, DstIP:null, Proto<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. Name:Test, Ptags:null, Table:FILTER, rules,Start of table, DstIP:1.1.1.1, Make Frag:false, MarkVal:null, MarkMask:n StrAlg:BM, StrRange:1-65535, StrHl RecentProto:SET, RecentSec:null, R new rule), Deleted: ADVR: (Status:C (Status:Off, Name:ICMP ..., + new ru<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZon DestZone:wan(tenant-1), + new rule DestIP:1.1.1.1, SP-SrcZone:lan(tenant- DestZone:wan(tenant-1), + new rule DestIP:1.1.1.1, SP-SrcZone:lan(tenant- DestZone:wan(tenant-1), + new rule<br><br>SDW-CPE-FW Firewall: Username:a template, Owner: admin(tenant-1), C (From:Any zone, To:mgmt,+ new rule Changed: ZF: (From:wan, To:lan,+ ne<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. Direction:Match source, Type:Set o rule), Deleted: IPSET: (Name:test, Di EntryList:10.1.1.[1-254]/24,20.2.2.[1-5] Direction:Match source, Type:Set o rule)]<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0.<br><br>SDW-CPE-FW Firewall: Username:a CTenant:tenant-1, OrcVersion:3.0.0. Input:ACCEPT, Output:ACCEPT, Fo to PMTU:false, Drop logging:false, N ZONE: (Name:RULE2, Input:ACCEPT Masquerading:false, MSS clamp to 22.2.2.2/32, + new rule), Changed: ZC Forwarding:REJECT, Masquerading: Networks:11.1.1.1/32, 33.3.3.3/32, + new<br><br>PKTmark: solo se muestra si habilita<br><br>El cambio de/a no se muestra en Ca inmediatamente. |
| SDW-CPE-FW | FirewallError | Cambiar la configuración del firewall en una instancia de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C RUL \|\| ADVR \|\| NAT, ZF \|\| IPSET \|\| DPI<br><br>SDW-CPE-FW FirewallError: CPE:v \|\| ADVR \|\| NAT, ZF \|\| IPSET \|\| DPI \|\| ZO |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-CPE-STR | StaticRoute | Agregar/Eliminar/Cambiar la configuración de la ruta estática | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U<br>CPE:$name, Template:$name, CTer<br>Deleted \|\| Changed: VRF:$vrf, Desti<br>Gateway:$gateway, Interface:$inter<br>Type:$type]<br>SDW-CPET-STR StaticRoute: User<br>Template:vCPE1, CTenant:tenant-1,<br>VRF:main/254, Destination:10.1.1.1/25<br>MTU:1500, AD:20, Type:unicast]<br>SDW-CPET-STR StaticRoute: User<br>Template:vCPE1, CTenant:tenant-1,<br>VRF:main/254, Destination:10.1.1.1/25<br>MTU:1500, AD:20, Type:unicast]<br>SDW-CPET-STR StaticRoute: User<br>Template:vCPE1, CTenant:tenant-1,<br>VRF:yellow/100, Destination:10.2.2.2<br>Metric:10, MTU:1300, AD:10, Type:bla<br>El cambio de/a no se muestra en Ca<br>inmediatamente. |
| SDW-CPE-STR | StaticRouteError | Agregar/Eliminar/Cambiar la configuración de la ruta estática, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C<br>$ErrorMessage<br>SDW-CPE-STR StaticRoute: CPE:v<br>$ErrorMessage |
| **Administración de la configuración de plantilla de CPE** | | | | | | |
| SDW-CPET | Cualquiera | Cualquier cambio en cualquier sección de la plantilla de CPE que no esté incluido en las secciones especializadas que se describen a continuación. | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U<br>Template:$name, Owner:$owner, Or<br>SDW-CPET Any: Username:admin(t<br>Owner:tenant-1, OrcVersion:3.0.0.re |
| SDW-CPET | AnyError | Cualquier cambio en cualquier sección de la plantilla de CPE que no esté incluido en las secciones especializadas que se describen a continuación, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: T<br>SDW-CPET AnyError: Template:vC |
| SDW-CPET-ENC | Cifrado | Cambio del cifrado de vínculos en la plantilla de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U<br>Template:$name, Owner:$owner, Or<br>SDW-CPET-ENC Encryption: Userr<br>Owner:tenant-1, OrcVersion:3.0.0.re |
| SDW-CPET-ENC | EncryptionError | Cambio de cifrado de vínculos en la plantilla de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: T<br>SDW-CPET-ENC EncryptionError: |
| SDW-CPET-SCR | Scripts | Modificación de scripts en una plantilla de CPE | información | baja | Al hacer clic: Guardar, ejecutar | Standard/Extended: Code Event: U<br>Template:$name, Owner:$owner, Or<br>Changed: $SriptName]<br>SDW-CPET-SCR Scripts: Username<br>Owner:tenant-1, OrcVersion:3.0.0.re<br>custom_config] |
| SDW-CPET-SCR | ScriptsError | Modificación de scripts en una plantilla de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: C<br>$ErrorMessage<br>SDW-CPET-SCR ScriptsError: Tem |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-CPET-NET | Interfaz | Agregar/Eliminar/Cambiar zona/dirección IP/dirección MAC/Interfaz QoS en una plantilla de CPE | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$ Owner:$owner, OrcVersion:$orcver<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re<br>Extended: Code Event: Username:$ Owner:$owner, OrcVersion:$orcver QOS: $Detailed_change]<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re Bridge:false, Enable automatically:t netmask:255.0.0.0, IPv4 gateway:10.1 MAC:01:01:01:01:01:01, Generate MA BE(MinR):10, BE(MaxR):100]<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re Bridge:false, Enable automatically:t netmask:255.0.0.0, IPv4 gateway:10.1 MAC:01:01:01:01:01:01, Generate MA MaxRate:1000, BE(MinR):10, BE(Max<br>SDW-CPET-NET Interface: Usernar Owner:tenant-1, OrcVersion:3.0.0.re lan>lan(tenant-1), Bridge:false>true, Manually>From IP pool, IPv4 addres IPv4 gateway: 10.1.1.254>10.2.2.254, IF 01:01:01:01:01:01>02:02:02:02:02:02, C QoS:true, MaxRate:100, BE(MinR):2(<br>Show change from/to on Change ir<br>Change from/to is not displayed or immediately. |
| SDW-CPET-NET | InterfaceError | Agregar/Eliminar/Cambiar zona/dirección IP/dirección MAC/Interfaz QoS en una plantilla de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: T QoS], $ErrorMessage<br>SDW-CPE-NET InterfaceError: Tem lan, [GEN], $ErrorMessage<br>SDW-CPE-NET InterfaceError: Tem lan, [QoS], $ErrorMessage |
| SDW-CPET-STR | StaticRoute | Agregar/Eliminar/Cambiar la configuración de la ruta estática en una plantilla de CPE | información | baja | Al hacer clic: Guardar | Standard/Extended: Code Event: U Template:$name, Owner:$owner, O VRF:$vrf, Destination:$destination/ Gateway:$gateway, Interface:$inte Type:$type]<br>SDW-CPET-STR StaticRoute: User Template:vCPE1, Owner:tenant-1, O VRF:main/254, Destination:10.1.1.1/25 MTU:1500, AD:20, Type:unicast]<br>SDW-CPET-STR StaticRoute: User Template:vCPE1, Owner:tenant-1, OrcVersion:3.0.0.release.1.cis.amd64 Gateway:10.1.1.254, Interface:lan, Me<br>SDW-CPET-STR StaticRoute: User Template:vCPE1, Owner:tenant-1, O VRF:yellow/100, Destination:10.2.2.2/ Metric:10, MTU:1300, AD:10, Type:bla<br>Change from/to is not displayed or |
| SDW-CPET-STR | StaticRouteError | Cambiar la configuración de la ruta estática en una plantilla de CPE, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: T<br>SDW-CPE-STR StaticRoute: Templ |
| **Administración de la configuración de plantilla de Firewall** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-FWT | Firewall | Crear/Eliminar/Modificar reglas de la plantilla de firewall | información | baja | Al hacer clic: Guardar | Al crear/eliminar una plantilla:<br>Standard/Extended: Code Event: U Name:$name, Owner:$owner, OrcV<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C<br><br>Al modificar:<br>Standard: Code Event: Username:$ Owner:$owner, OrcVersion:$orcver<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C<br><br>Extended: Code Event: Username:$ Owner:$owner, OrcVersion:$orcver \|\| NAT \|\| ZF \|\| IPSET \|\| DPI: $Detailed_<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C Syn-flood protection:Disable, Defa<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C (Name:Test, Action:ACCEPT, IPset:r DstIP:3.3.3.3:4.4.4.4, Proto:icmp, + n IPset:null, IPv:IPv4, SrcZ:wan, DstZ: l rule), Changed: RUL: (Name:Allow-P DstZ:null, SrcIP:null, DstIP:null, Proto<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C (Status:On, Name:Test, Ptags:null, T Placement:Pre-rules,Start of table, Target:ACCEPT, Frag:false, MarkVa StrSrchPatt:null, StrAlg:BM, StrRan RecentName:null, RecentProto:SET applet,WebAsm, ..., + new rule), Dele Changed: ADVR: (Status:Off, Name<br>SDW-FWT Firewall: Username:admi template, Owner: admin(tenant-1), C NAT:DNAT: (Name:Test, Proto:IP, SP SrcIP:11.1.1.1,TP-DstIP:192.1.1.1, TP-Dest (Name:Test, Proto:IP, SP-DestIP:1.1.1.1 DstIP:192.1.1.1, TP-DestZone:wan(tena Proto:IP, SP-DestIP:1.1.1.1, SP-SrcZon DestZone:wan(tenant-1), + new rule<br>SDW-FWT Firewall: Username:admi template, Owner: admin(tenant-1), C (From:Any zone, To:mgmt,+ new rule Changed: ZF: (From:wan, To:lan,+ ne<br>SDW-FWT Firewall: Username:admi template, Owner: admin(tenant-1), C (Name:test, Direction:Match source 254]/24,20.2.2.[1-5], + new rule), Del Type:Set of subnets, EntryList:10.1.1. (Name:test, Direction:Match source 254]/24,20.2.2.[1-5], + new rule)]<br>SDW-FWT Firewall: Username:admi template, Owner:admin(tenant-1), C PKTmark:1,2,3,4]<br><br>PKTmark: only enabled displayed, ot<br>El cambio de/a no se muestra en Ca inmediatamente. |
| SDW-FWT | FirewallError | Crear/Eliminar/Modificar reglas de la plantilla de firewall, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: N NAT, ZF \|\| IPSET \|\| DPI], $ErrorMessa<br>SDW-FWT FirewallError: Name:Defa ADVR \|\| NAT, ZF \|\| IPSET \|\| DPI], $Err |
| **Administración de la configuración de zonas de Firewall** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SDW-FWZ | Zona | Crear/Eliminar/Modificar reglas de zona de la plantilla de firewall | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$ Owner:$owner, OrcVersion:$orcver<br>SDW-FWZ Zone: Username:admin(t Owner:admin(tenant-1), OrcVersion Changed]<br>Extended: Code Event: Username:$ Owner:$owner, OrcVersion:3.0.0.rel $Detailed_change]<br>SDW-FWZ Zone: Username:admin(t Owner:admin(tenant-1), OrcVersion Output:ACCEPT, Forwarding:ACCE Drop logging:false, Networks:11.1.1.1/3<br>SDW-FWZ Zone: Username:admin(t Owner:admin(tenant-1), OrcVersion Output:ACCEPT, Forwarding:ACCE Drop logging:false, Networks:11.1.1.1/3<br>SDW-FWZ Zone: Username:admin(t Owner:admin(tenant-1), OrcVersion Output:ACCEPT, Forwarding:REJE Drop logging:false, Networks:11.1.1.1/3<br>El cambio de/a no se muestra en Ca inmediatamente. |
| SDW-FWZ | ZoneError | Crear/Eliminar/Modificar reglas de zona de la plantilla de firewall, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: N<br>SDW-FWT ZoneError: Name:lan, Ov |
| **Cargar firmware** | | | | | | |
| SDW-FMW | Firmware | Firmware cargado, comprobación de integridad del paquete. | información | información | Al hacer clic: + Firmware | Standard/Extended: Code Event: U [Added \|\| Deleted: $FwName]<br>SDW-FMW Firmware: Username:ad knaas-cpe_2.25.09.release.21.bios.a |
| SDW-FMW | FirmwareError | Firmware cargado, comprobación de integridad del paquete, con un error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: $<br>SDW-FWT FirmwareError: $ErrorM |
| **Eventos programados** | | | | | | |
| SCH-FMWU | FirmwareUpdate | Actualización de firmware en CPE | información | baja | Al recibir la confirmación de que la actualización del CPE se realizó correctamente | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-FMWU FirmwareUpdate: User Template:vCPE1, CTenant:tenant-1, vkesr-m1_en-US_ru-RU.tar>knaas- US_ru-RU.tar] |
| SCH-FMWU | FirmwareUpdateError | Actualización de firmware en CPE | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: U CPE:$name, Template:$name, CTen<br>SDW-FMWU FirmwareUpdate: User Template:vCPE1, CTenant:tenant-1, |
| SCH-UPDS | UpdateSettings | Reconfiguración programada de CPE | información | baja | Cuando llega la hora programada | Standard/Extended: Code Event: U [Scheduled: CPE:$name, Time:$tim<br>SCH-UPDS UpdateSettings: Usern CPE:vCPE1, Time:$time] |
| SCH-UPDS | UpdateSettingsError | Reconfiguración programada de CPE, con error | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: $<br>SCH-UPDS UpdateSettingsError: $ |
| **Identificación y autenticación del usuario** | | | | | | |
| USR-USR | Autenticación | Autenticación correcta en el orquestador | información | baja | Cuando inicia sesión el usuario | Standard/Extended: Code Event: U Role:$role, Account type:$type, Gro Permissions:$permissions, Permissi<br>USR-USR Authentication: Username Account type:LDAP, Group:admin, F d82e-4dfb-b7bc-414cca14abc5, Au |

| | | | | | | |
|---|---|---|---|---|---|---|
| USR-USR | AuthenticationError | Autenticación fallida en el orquestador | advertencia | media | Inmediatamente después de la ocurrencia | Standard/Extended: Code Event: U<br>Role:$role, Account type:$type, Gro<br>PermissionsID:$id, Authentication b<br>USR-USR AuthenticationError: User<br>Account type:LDAP, Group:admin, F<br>d82e-4dfb-b7bc-414cca14abc5, Au<br>Si el usuario no existe:<br>Standard/Extended: Code Event: U<br>by password, $ErrorMessage<br>USR-USR AuthenticationError: User<br>password, $ErrorMessage |
| USR-USR | UserChange | Crear/Eliminar/Modificar roles, permisos, 2FA, contraseña, usuario. | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$<br>\|\| Changed \|\| Blocked \|\| Unblocked \|\|<br>USR-USR UserChange: Username:a<br>USR-USR UserChange: Username:a<br>USR-USR UserChange: Username:a<br>UserTenant1]<br>USR-USR UserChange: Username:a<br>USR-USR UserChange: Username:a<br>UserTenant1]<br>USR-USR UserChange: Username:a<br>UserTenant1]<br>USR-USR UserChange: Username:a<br>UserTenant1]<br>Extended: Code Event: Username:$<br>\|\| Changed \|\| Blocked \|\| Unblocked \|\|<br>$Detailed_change]<br>USR-USR UserChange: Username:a<br>$name, Account type:Local, Login:U<br>2FA:false, Request confirmation is r<br>Email:boris.britva@snatch.com]<br>USR-USR UserChange: Username:a<br>$name, Account type:Local, Login:U<br>2FA:false, Request confirmation is r<br>Email:boris.britva@snatch.com]<br>USR-USR UserChange: Username:a<br>$name, Account type:Local, Login:U<br>2FA:false, Request confirmation is r<br>Email:boris.britva@snatch.com] |
| USR-PERM | UserPermissions | Crear/eliminar/modificar privilegios de acceso. | información | baja | Al hacer clic: Guardar | Standard: Code Event: Username:$<br>\|\| Changed: $PermissionsName]<br>USR-PERM UserPermissions: Usern<br>access]<br>USR-PERM UserPermissions: Usern<br>access]<br>USR-PERM UserPermissions: Usern<br>access]<br>Extended: Code Event: Username:$<br>\|\| Changed: $PermissionsName, $De<br>USR-PERM UserPermissions: Usern<br>All:Editing \|\| Viewing \|\| No access, Int<br>Domain:Editing \|\| Viewing \|\| No acce<br>VIM:Editing \|\| Viewing \|\| No access, C<br>USR-PERM UserPermissions: Usern<br>All:Editing \|\| Viewing \|\| No access, Int<br>Domain:Editing \|\| Viewing \|\| No acce<br>VIM:Editing \|\| Viewing \|\| No access, C<br>USR-PERM UserPermissions: Usern<br>$name, All:Editing \|\| Viewing \|\| No ac<br>Domain:Editing \|\| Viewing \|\| No acce<br>VIM:Editing \|\| Viewing \|\| No access, C |
| | | | | | **Interacción con las herramientas de seguridad de la información externos: IDS/AV/DLP** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| SYS-API | Llamada | Llamada al método API | información | baja | Durante la ejecución | Standard/Extended: Code Event A Username:$username($tenant), src called]<br>SYS-API Call: API-[/api/nfv/sdwan/ 1), UserIp:127.0.0.1, Obj:[ .. ] |
| SYS-API | CallComplete | Llamada al método API completada | información | baja | Durante la ejecución | Standard/Extended: Code Event A Username:$username($tenant), src called], Ret: [return code]<br>SYS-API CallComplete: API-[/api/n [GET]: Username:admin(tenant-1), U |

La siguiente es una lista de eventos de seguridad que se pueden ingresar en el registro de auditoría de un dispositivo CPE.

Tabla 2. Lista de eventos de seguridad que se pueden registrar en dispositivos CPE

| Facility.Severity (Código) | Aplicación | Evento | Acción | Gravedad del evento de KUMA | Tiempo de activación | Mensaje |
|---|---|---|---|---|---|---|
| **Identificación y autenticación del usuario** | | | | | | |
| authpriv.info (10.6) | dropbear | Conexión secundaria desde | Autenticación en el dispositivo | baja | Durante la ejecución | Tue Oct 21 07:43:34 2025 authpriv.info dropbear[16 Child connection from 172.17.9.200:60634<br>Tue Oct 21 07:43:34 2025 authpriv.info dropbear[16 Exit before auth from <172.17.9.200:60634>: Exited normally<br>Tue Oct 21 07:43:42 2025 authpriv.info dropbear[16 Child connection from 172.17.9.200:56364 |
| authpriv.info (10.6) | dropbear | Se alcanzó el número máximo de intentos de autenticación | Autenticación en el dispositivo | alta | Durante la ejecución | Tue Oct 21 07:46:54 2025 authpriv.info dropbear[18 Exit before auth from <172.17.9.200:57270>: (user 'roo fails): Max auth tries reached - user 'root' |
| authpriv.notice (10.5) | dropbear | La autenticación con contraseña se realizó correctamente | Autenticación en el dispositivo | baja | Durante la ejecución | Tue Oct 21 07:43:45 2025 authpriv.notice dropbear[16170]: Password auth succeeded for 'roo from 172.17.9.200:56364 |
| authpriv.warn (10.4) | dropbear | Intento de contraseña incorrecto | Autenticación en el dispositivo | media | Durante la ejecución | Tue Oct 21 07:46:52 2025 authpriv.warn dropbear[18 Bad password attempt for 'root' from 172.17.9.200:57<br>Tue Oct 21 07:46:53 2025 authpriv.warn dropbear[18 Bad password attempt for 'root' from 172.17.9.200:57<br>Tue Oct 21 07:46:54 2025 authpriv.warn dropbear[18 Bad password attempt for 'root' from 172.17.9.200:57 |
| **Administración de la configuración de firewall/CPE** | | | | | | |
| user.info (1.6) | sdwan-oob | Se recibió y ejecutó la tarea de firewall | Reglas de firewall cambiadas | baja | Durante la ejecución | Wed Nov 12 09:01:04 2025 user.info sdwan-oob: Recieved and execute task firewall id abb0629b-757 423a-b71d-2e330ef11b8b executor oob_firewall<br>Wed Nov 12 09:01:05 2025 user.info sdwan-oob: Tas firewall id abb0629b-757e-423a-b71d-2e330ef11b8 executor oob_firewall completed |
| user.crit (1.2) | firewall | Firewall detenido | Servicio de firewall detenido | crítica | Durante la ejecución | Thu Oct 23 13:04:40 2025 user.crit firewall: Firewall stopped |
| user.info (1.6) | firewall | Firewall iniciado | Servicio de firewall iniciado | baja | Durante la ejecución | Thu Oct 23 13:04:44 2025 user.info firewall: Firewall started |
| user.warn (1.4) | firewall | Firewall reiniciado | Servicio de firewall reiniciado | media | Durante la ejecución | Thu Oct 23 13:04:55 2025 user.warn firewall: Firewal restarted |
| user.warn (1.4) | firewall | Firewall recargado | Servicio de firewall recargado | media | Durante la ejecución | Thu Oct 23 13:04:59 2025 user.warn firewall: Firewall reloaded |
| **Registro de filtrado/transmisión de tráfico en el firewall** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| kern.info (0.6) | kernel | FW-AUD | Auditoría de rendimiento de firewall | baja | Durante la ejecución | Sat Nov 1 11:54:41 2025 kern.info kernel: [337220.695<br>FW-AUD= OUT=eth0 SRC=172.17.9.221 DST=172.17.9.2<br>LEN=299 TOS=0x00 PREC=0xC0 TTL=64 ID=3954<br>PROTO=TCP SPT=54280 DPT=6653 WINDOW=321<br>RES=0x00 ACK PSH URGP=0 MARK=0x1f4 |
| **Comprobación de integridad de firewall/CPE** | | | | | | |
| user.info (1.6) | sdwan | Comprobación de integridad realizada correctamente | Integridad no vulnerada | baja | Durante la ejecución | Thu Apr 9 11:45:44 2026 user.info sdwan[31284]: Int<br>check successful |
| user.crit (1.2) | sdwan | La comprobación de integridad falló | Vulneración de la integridad del archivo | crítica | Durante la ejecución | Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Int<br>check failed |
| user.crit (1.2) | sdwan | Incompatibilidad de verificación con el verificador 'Gost2012'. Motivo: archivo <$file> | Vulneración de la integridad del archivo | crítica | Durante la ejecución | Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]:<br>Verification mismatch with 'Gost2012' checker. Reas<br>File "/usr/sbin/sdwan" has unexpected hash<br>Vmd5sJ2GwLK35woBdeivZ1NAtsXlZNDBga2W4LH<br>!= expected<br>ttDJAQ1XW+UmYx4RdVru2YFWR2Al1YzG9BO4Nv |
| user.crit (1.2) | sdwan | Falló la comprobación de integridad. Reenvío de tráfico bloqueado | Tráfico bloqueado | crítica | Durante la ejecución | Thu Apr 9 11:00:03 2026 user.crit sdwan[18383]: Int<br>check failed. Reenvío de tráfico bloqueado |
| user.info (1.6) | sdwan | La comprobación automática de firewall se realizó correctamente | Prueba de firewall exitosa | información | Durante la ejecución | Thu Feb 26 12:15:48 2026 user.info sdwan[7241]:<br>Successful firewall self test |
| user.crit (1.2) | sdwan | La comprobación automática de firewall falló | Prueba de firewall fallida | crítica | Durante la ejecución | Thu Feb 26 13:27:06 2026 user.crit sdwan[30591]: Fi<br>self test failed |
| **Conexión de dispositivos USB** | | | | | | |
| kern.info (0.6) | kernel | usb | Dispositivo USB conectado | media | Durante la ejecución | Tue Feb 10 08:08:34 2026 kern.info kernel: [ 136.326<br>usb 2-2: new SuperSpeed Gen 1 USB device numbe<br>using xhci_hcd<br>Tue Feb 10 08:08:34 2026 kern.info kernel: [ 136.372<br>usb-storage 2-2:1.0: USB Mass Storage device dete<br>Tue Feb 10 08:08:34 2026 kern.info kernel: [ 136.372<br>scsi host2: usb-storage 2 |
| kern.info (0.6) | kernel | montado | Dispositivo USB montado | alta | Durante la ejecución | Tue Feb 10 08:09:30 2026 kern.info kernel: [ 191.8772<br>EXT4-fs (sdb2): mounted filesystem with ordered d<br>mode. Opciones: (nulo) |
| **Cambio de hora** | | | | | | |
| daemon.warn (3.4) | chronyd | salto de tiempo detectado | Cambio de hora | media | Durante la ejecución | Tue Feb 10 08:04:13 2026 daemon.warn chronyd[44<br>Backward time jump detected!<br>Tue Feb 10 08:04:13 2026 daemon.info chronyd[442<br>Can't synchronise: no selectable sources<br>Tue Feb 10 08:07:27 2026 daemon.info chronyd[44<br>Selected source 45.141.102.99 (0.pool.ntp.org)<br>Tue Feb 10 08:07:27 2026 daemon.warn chronyd[44<br>System clock wrong by 77.778277 seconds<br><br>Tue Feb 10 08:56:20 2026 daemon.warn chronyd[83<br>Forward time jump detected!<br>Tue Feb 10 08:56:20 2026 daemon.info chronyd[83<br>Can't synchronise: no selectable sources<br>Tue Feb 10 08:58:33 2026 daemon.info chronyd[83<br>Selected source 89.109.251.24 (0.pool.ntp.org)<br>Tue Feb 10 08:58:33 2026 daemon.warn chronyd[83<br>System clock wrong by -53.343945 seconds |

# Rangos de subredes y direcciones IP para dispositivos CPE

Puede crear rangos de direcciones IP y subredes para asignar direcciones IPv4 de manera centralizada cuando crea o edita interfaces de red de dispositivos CPE. También puede usar rangos de direcciones IP para asignar direcciones IPv4 de manera centralizada a los ID de enrutadores de los dispositivos CPE cuando especifica la configuración básica de BGP.

## Administrar rangos de direcciones IP

Para ver la tabla de rangos de direcciones IP, vaya a la sección **SD-WAN → IPAM**. La pestaña **Agrupaciones de direcciones IP** está seleccionada de manera predeterminada. La información sobre los rangos de direcciones IP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del rango de direcciones IP.
- **CIDR** es el prefijo IPv4 de la subred en la que se encuentra el rango de direcciones IP.
- **Rango de IP** indica los valores inicial y final del rango de direcciones IP.
- **Uso** es la cantidad de direcciones IP en el rango que se asignaron a las interfaces de red o los ID de enrutadores de los dispositivos CPE.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Crear un rango de direcciones IP

*Para crear un rango de direcciones IP, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. En la parte superior de la página, haga clic en **+ Agrupación de direcciones IP**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del rango de direcciones IP. La longitud máxima del nombre es de 32 caracteres.

4. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred en la que se encuentra el rango de direcciones IP.

5. Especifique un rango de direcciones IP. Para hacerlo, en **Rango de IP**, haga clic en **+ Agregar** e ingrese el valor inicial y el valor final del rango de direcciones IP.

   El rango de direcciones IP se especifica y se muestra en la sección **Rango de IP**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en el ícono de eliminar ✕ junto a él.

6. Haga clic en **Crear**.

El rango de direcciones IP se crea y se muestra en la tabla.

# Editar un rango de direcciones IP

*Para cambiar un rango de direcciones IP, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Haga clic en el rango de direcciones IP que desea editar.

3. En la ventana que se abre, edite el nombre y el prefijo IPv4 de la subred que contiene el rango de direcciones IP y especifique o elimine los rangos de direcciones IP.

4. En la parte superior del área de configuración, haga clic en **Guardar**.

El rango de direcciones IP se modifica y actualiza en la tabla.

# Ver el uso de un rango de direcciones IP

Si es necesario, puede verificar qué plantillas CPE y dispositivos CPE están usando un rango de direcciones IP. Por ejemplo, si un rango de direcciones IP está en uso, no se puede eliminar. También puede ver información sobre las direcciones IP que se asignaron desde el rango de direcciones IP.

*Para ver si se está utilizando un rango de direcciones IP, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Haga clic en el intervalo de direcciones IP para el que desea ver la información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra las configuraciones del rango de direcciones IP.

3. Vea el uso del rango de direcciones IP de una de las siguientes maneras:

   - Si desea verificar qué dispositivos CPE están usando un rango de direcciones IP, seleccione la pestaña **Uso → CPE**.

     Se muestra una lista de dispositivos CPE que están usando el rango de direcciones IP.

- Si desea verificar qué plantillas de CPE están usando un rango de direcciones IP, seleccione la pestaña **Uso → Plantilla**.

  Se muestra una lista de plantillas de CPE que están usando el rango de direcciones IP.

4. Si desea ver información sobre las direcciones IP que se asignaron desde el rango de direcciones IP, seleccione la pestaña **Arrendamientos**.

   Se muestra una tabla de direcciones IP asignadas desde el rango de direcciones IP. La información sobre las direcciones IP se muestra en las siguientes columnas de la tabla:

   - **Dirección IP** es la dirección IP que se asignó desde el rango de direcciones IP.
   - **CPE** es el dispositivo CPE al que se asigna la dirección IP.
   - **Tipo** indica si la dirección IP está asignada a una interfaz de red o al ID de enrutador de un dispositivo CPE.
   - **Nombre** es el nombre de la interfaz de red a la que se asigna la dirección IP. Si se asignó una dirección IP al ID del enrutador del dispositivo CPE, no se muestra ningún valor en esta columna.
   - **Inquilino** es el inquilino al que se agregó el dispositivo CPE.

Las acciones que puede realizar con las listas y la tabla se describen en las instrucciones de Administración de las tablas de componentes de la solución.

# Eliminar rangos de direcciones IP

No se puede eliminar un rango de direcciones IP si está siendo utilizado por al menos una plantilla de CPE o dispositivo CPE. Para eliminar un rango de direcciones IP que utilizan las plantillas de CPE o los dispositivos CPE, primero debe eliminar el rango de direcciones IP de la configuración de la interfaz de red y la configuración de BGP. Puede verificar qué plantillas de CPE y dispositivos CPE están usando un rango de direcciones IP.

Los rangos de direcciones IP eliminados no se pueden restaurar.

*Para eliminar rangos de direcciones IP, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Para eliminar un rango de direcciones IP individual, siga estos pasos:

   a. Haga clic en el rango de direcciones IP que desea eliminar.

      El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración** está seleccionada y muestra las configuraciones del rango de direcciones IP.

   b. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

3. Para eliminar varios rangos de direcciones IP:

   a. Marque las casillas situadas junto a los rangos de direcciones IP que desea eliminar.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

Los rangos de direcciones IP se eliminan y ya no se muestran en la tabla.

# Administrar rangos de subredes

Para ver la tabla de rangos de subredes, vaya a la sección **SD-WAN**→ **IPAM** y seleccione la pestaña **Agrupaciones de subredes**. La información sobre los rangos de subredes se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del rango de subred.
- **CIDR** es el prefijo IPv4 del rango de subredes.
- **Uso** es la cantidad de subredes que se asignaron a las interfaces de red.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Crear un rango de subredes

*Para crear un rango de subred, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Seleccione la pestaña **Agrupaciones de subredes**.

   Se muestra una tabla de rangos de subredes.

3. En la parte superior de la página, haga clic en **+ Agrupación de subredes**.

4. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del rango de subred. La longitud máxima del nombre es de 32 caracteres.

5. En el campo **CIDR base**, ingrese el prefijo IPv4 del rango de subred.

6. En el campo **Subprefijo**, ingrese la longitud del prefijo de subred IPv4 en el rango de subred. Rango de valores: de 0 a 32.

7. Haga clic en **Crear**.

El rango de subredes se crea y se muestra en la tabla.

# Editar un rango de subredes

*Para editar un rango de subredes, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Seleccione la pestaña **Agrupaciones de subredes**.

   Se muestra una tabla de rangos de subredes.

3. Haga clic en el rango de subred que desea editar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Configuración**, que muestra la configuración del rango de subredes.

4. En la ventana que se abre, si es necesario, edite la siguiente configuración:

   - Nombre del rango de subredes
   - Prefijo IPv4 del rango de subredes
   - Longitud del prefijo IPv4 de las subredes en el rango de subredes

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del rango de subred.

El rango de la subred se modifica y se actualiza en la tabla.

# Ver el uso de un rango de subredes

Si es necesario, puede verificar qué plantillas de CPE y dispositivos CPE están usando un rango de subredes. Por ejemplo, si un rango de subredes está en uso, no se puede eliminar. También puede ver información sobre las subredes que se asignaron desde el rango de subredes.

*Para ver si se está utilizando un rango de subredes:*

1. En el menú, vaya a la sección **SD-WAN → IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Seleccione la pestaña **Agrupaciones de subredes**.

   Se muestra una tabla de rangos de subredes.

3. Haga clic en el rango de subredes para el que desea ver la información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Configuración**, que muestra la configuración del rango de subredes.

4. Verifique el uso del rango de subredes de una de las siguientes maneras:

   - Si desea ver qué dispositivos CPE están usando un rango de subredes, seleccione la pestaña **Uso** → **CPE**.

     Se muestra una lista de dispositivos CPE que están usando el rango de subredes.

   - Si desea ver qué plantillas de CPE están usando un rango de subredes, seleccione la pestaña **Uso** → **Plantilla**.

     Se muestra una lista de plantillas de CPE que están usando el rango de subredes.

5. Si desea ver información sobre las subredes que se asignaron desde el rango de subredes, seleccione la pestaña **Arrendamientos**.

   Se muestra una tabla de subredes asignadas desde el rango de subredes. La información sobre las subredes se muestra en las siguientes columnas de la tabla:

   - **CIDR** es el prefijo IPv4 de la subred que se asignó desde el rango de subredes.
   - **CPE** es el dispositivo CPE al que se asigna una dirección IPv4 de la subred.
   - **Nombre** es el nombre de la interfaz de red a la que se asigna una dirección IPv4 de la subred.
   - **Inquilino** es el inquilino al que se agregó el dispositivo CPE.

Las acciones que puede realizar con las listas y la tabla se describen en las instrucciones de Administración de las tablas de componentes de la solución.

# Eliminar rangos de subredes

No se puede eliminar una subred si se está utilizando con al menos una plantilla de CPE o un dispositivo CPE. Para quitar un rango de subredes que se está utilizando con plantillas de CPE o dispositivos CPE, primero debe quitar el rango de subredes de la configuración de la interfaz de red y de la configuración de BGP. Puede verificar qué plantillas de CPE y dispositivos CPE están utilizando un rango de subredes.

Los rangos de subredes eliminados no se pueden restaurar.

*Para eliminar los rangos de subredes, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN** → **IPAM**.

   De manera predeterminada, la pestaña **Agrupaciones de direcciones IP** está seleccionada y muestra una tabla de rangos de direcciones IP.

2. Seleccione la pestaña **Agrupaciones de subredes**.

   Se muestra una tabla de rangos de subredes.

3. Para eliminar un rango de subredes individual, haga lo siguiente:

   a. Haga clic en el rango de subredes que desea eliminar:

      El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, está seleccionada la pestaña **Configuración**, que muestra la configuración del rango de subredes.

   b. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. Para eliminar varios rangos de subredes, haga lo siguiente:

   a. Seleccione las casillas de verificación junto a los rangos de subredes que desea eliminar.

   b. En la parte superior de la tabla, haga clic en **Acciones** → **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

Se eliminan los rangos de subredes y ya no se muestran en la tabla.

# Administrar el firewall

Hay dos enfoques principales para filtrar el tráfico:

- El filtro de tráfico de red clásico
- El firewall basado en zonas

El **modelo de filtro de tráfico de red** ofrece un bajo nivel de abstracción: las reglas definen el comportamiento de cada paquete individual. La sintaxis de un filtro de paquetes, como iptables, vincula *reglas* a *cadenas* que forman *tablas*. Cada paquete pasa por varias tablas y, en cada tabla, pasa por una de las cadenas estándar. El hecho de que una regla pertenezca a una tabla (filter, nat, mangle, raw, etc.) generalmente se determina por el tipo de acción a realizar. Las reglas suelen estar vinculadas a interfaces individuales (entrantes o salientes). Para cubrir interfaces adicionales, se debe copiar y modificar una regla.

El **modelo de firewall basado en zonas** ofrece un alto nivel de abstracción: las zonas actúan como contenedores para las interfaces, y una directiva (un conjunto de reglas) define la interacción entre las zonas.

Las zonas son grupos lógicos de interfaces que la directiva de seguridad considera del mismo tipo.

Una directiva (conjunto de reglas) define cómo las zonas interactúan entre sí. Las reglas se escriben solo una vez para un par de zonas (Zona A ↔ Zona B) y se aplican automáticamente a todas las interfaces que pertenecen a estas zonas. El tráfico se clasifica por protocolo y dirección, y se compara con la directiva entre las dos zonas.

Por lo tanto, el concepto de **firewall basado en zonas** corresponde a las tablas y cadenas de un **filtro de paquetes** iptables solo en el nivel de procesamiento de paquetes de bajo nivel. El firewall basado en zonas agrega agrupación lógica y directiva centralizada al filtro de paquetes, lo que hace que la administración sea más escalable, menos propensa a errores y más fácil de reutilizar.

Kaspersky SD-WAN implementa ambos enfoques para filtrar paquetes de tráfico en dispositivos CPE.

El firewall puede aceptar, descartar o rechazar los paquetes de tráfico. Si se rechaza un paquete de tráfico, su remitente recibe un mensaje de `icmp-reject`. El firewall puede aplicar cada acción a los paquetes de tráfico entrante y saliente, así como a los paquetes de tráfico retransmitidos entre las interfaces de red y las subredes de los dispositivos CPE. Cuando se especifica la configuración básica del firewall, debe establecer las acciones predeterminadas que el firewall realiza con los paquetes de tráfico.

Las plantillas de firewall se utilizan para la administración centralizada de la configuración del firewall en dispositivos CPE. Para no tener que administrar la configuración en cada dispositivo CPE individual, puede especificar la configuración de filtrado en una plantilla de firewall y luego aplicar la plantilla de firewall a los dispositivos CPE cuando agrega o registra dispositivos CPE manualmente. Si edita una configuración en una plantilla de firewall, la configuración se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall. Si edita una configuración en el dispositivo CPE, la configuración se vuelve independiente de la plantilla de firewall, y si la configuración se modifica en la plantilla de firewall, permanece sin cambios en el dispositivo CPE.

## Zonas de firewall

Puede agregar interfaces de red y subredes a una zona de firewall (en adelante también denominada 'zona') para recibir, descartar o rechazar paquetes de tráfico transmitidos a través de estas interfaces de red y subredes. Cuando crea o edita una zona de firewall, debe especificar las acciones que se realizarán con los paquetes de tráfico y, si es necesario, agregar subredes. Puede agregar interfaces de red a una zona de firewall cuando se crea o se edita una interfaz de red.

Si desea permitir la transmisión de paquetes de tráfico de una zona de firewall a otra, debe crear un reenvío. Cuando se crea un reenvío, debe especificar las zonas de firewall entrantes y salientes.

Puede crear zonas de firewall comunes que pueden usar varios dispositivos CPE, así como zonas de firewall en un dispositivo CPE individual.

## Reglas de firewall estándar (firewall basado en zonas)

Puede crear reglas de firewall estándar para aceptar, descartar o rechazar los paquetes de tráfico según los criterios especificados. Por ejemplo, puede crear una regla de firewall que rechace los paquetes de tráfico con una zona de firewall de origen específica.

Si desea especificar las mismas direcciones IP o subredes en varias reglas de firewall, puede crear un conjunto de direcciones IP. Cuando crea un conjunto de direcciones IP, debe especificar si las direcciones IP y las subredes pertenecen al origen o al destino. Puede especificar el conjunto de IP creado cuando se crea o se modifica una regla de firewall.

Cuando un paquete de tráfico se reenvía a un dispositivo CPE, la acción especificada en la configuración de una de las reglas de firewall se realiza en el paquete de tráfico. Si no se puede aplicar ninguna de las reglas de firewall, la acción especificada en la configuración de la zona de firewall a la que se reenvió este paquete se aplicará al paquete de tráfico. Si el paquete de tráfico no se reenvió a ninguna de las zonas de firewall, la acción predeterminada que especificó en la configuración básica del firewall se aplica al paquete de tráfico.

## Reglas de firewall avanzadas (filtro de paquetes clásico)

Las reglas de firewall avanzadas permiten un procesamiento de paquetes más flexible y detallado que las reglas estándar mediante el uso de criterios y acciones de coincidencia adicionales que se pueden realizar con los paquetes. Puede usar reglas de firewall avanzadas en situaciones en las que las reglas estándar no son suficientes, por ejemplo, cuando necesita hacer coincidir paquetes con criterios adicionales o realizar una acción no estándar con un paquete. Por ejemplo, si configuró varias reglas de firewall por zona e interfaz en un CPE, pero necesita ocultar la estructura de la red en la que se encuentra el CPE, puede crear una regla avanzada adicional para descartar paquetes con códigos ICMP que pueden utilizarse para el reconocimiento de la topología de la red y colocar esta regla avanzada en una de las primeras etapas del procesamiento de tráfico.

De acuerdo con el modelo de filtro de paquetes clásico, las reglas de firewall avanzadas se pueden agrupar en dos grupos. El primer grupo permite agregar nuevas reglas antes de las reglas existentes (tales reglas avanzadas se denominan reglas previas) o en el segundo grupo que va después de las reglas existentes (tales reglas avanzadas se denominan reglas posteriores). El orden de las reglas determina el orden del procesamiento del tráfico. Tener dos grupos para procesar las reglas en cada cadena de cada tabla permite cambiar de manera flexible la lógica de procesamiento del tráfico de un grupo individual de reglas sin romper la lógica y el orden de procesamiento del tráfico en un grupo de reglas ya configurado.

Las reglas de firewall basadas en zonas se implementan en el filtro de paquetes clásico mediante cadenas personalizadas. Por lo tanto, las reglas estándar creadas de acuerdo con el enfoque basado en zonas y las reglas avanzadas creadas en la sintaxis del filtro de paquetes clásico no se cruzan ni se afectan entre sí.

### Traducción de direcciones de red

El firewall basado en zonas admite los siguientes mecanismos de traducción de direcciones de red (NAT):

- Las reglas DNAT pueden reemplazar los siguientes componentes de los paquetes de tráfico con los valores especificados:
  - Direcciones IP de destino o prefijos
  - Zonas de firewall de destino
  - Puertos de destino (traducción de direcciones de puerto, PAT)
- Las reglas SNAT pueden reemplazar las direcciones IP de origen o los prefijos de paquetes de tráfico con los valores especificados.

Las reglas DNAT y las reglas SNAT se aplican a los paquetes de tráfico según los criterios especificados. Por ejemplo, puede crear una regla DNAT que reemplace la dirección IP de destino de los paquetes de tráfico TCP.

En la sintaxis clásica del filtro de paquetes, la traducción de direcciones de red se describe mediante las acciones correspondientes en la tabla mangle en las reglas avanzadas.

# Administrar zonas de firewall

Puede ver la tabla de zonas de firewall comunes o la tabla de zonas de firewall en el dispositivo CPE:

- Para ver la tabla de zonas de firewall comunes, vaya a la sección del menú **SD-WAN → Zonas de firewall**.
- Para ver la tabla de zonas de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall → Zonas**.

Las siguientes zonas de firewall se crean de manera predeterminada:

- **wan** (zona de firewall de WAN) es la zona de firewall para las interfaces de red que están conectadas a la WAN, por ejemplo, a Internet o a la red del proveedor de servicios. El enmascaramiento está habilitado en la configuración de la zona de WAN del firewall para reemplazar la dirección IP de origen de los paquetes de tráfico saliente de la zona del firewall con la dirección IP asignada a la interfaz de red de salida.
- **lan** (zona de firewall de LAN) es la zona de firewall para las interfaces de red que están conectadas a la LAN.
- **mgmt** (zona de firewall de administración) es la zona de firewall para la interfaz de red que se usa para la supervisión pasiva del dispositivo CPE por parte del sistema de supervisión Zabbix, así como para la conexión SSH del orquestador al dispositivo CPE.

No puede eliminar las zonas de firewall predeterminadas ni crear zonas de firewall con los mismos nombres.

Cuando actualiza Kaspersky SD-WAN de la versión 2.1 a la 2.2, se realizan los siguientes cambios en la configuración de todas las plantillas de CPE:

- Las interfaces de red **sdwan<0–4>** se agregan automáticamente a la zona de WAN del firewall.
- Las interfaces de red **lan**, **br-lan** y **overlay** se agregan automáticamente a la zona LAN del firewall.

La información sobre las zonas comunes del firewall se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la zona de firewall.
- **Uso** indica si la zona de firewall está siendo utilizada por plantillas de firewall, plantillas de CPE y dispositivos CPE:
  - **Sí**.
  - **No**.
- **Autoría** es el nombre del usuario que creó la zona de firewall.
- **Creado** es la fecha y la hora en que se creó la zona de firewall.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

La información sobre las zonas de firewall en el dispositivo CPE se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la zona de firewall.
- **Configuración** contiene las acciones que el firewall aplica a los paquetes de tráfico.
- **Interfaces de red/Redes** son interfaces de red y subredes que se agregaron a la zona de firewall.

# Crear una zona de firewall

Puede crear una zona común de firewall o una zona de firewall en el dispositivo CPE.

*Para crear una zona de firewall, siga estos pasos:*

1. Cree una zona de firewall de una de las siguientes maneras:
   - Si desea crear una zona de firewall común, vaya a la sección **SD-WAN → Zonas de firewall** y en la parte superior de la página, haga clic en **+ Zona de firewall** .
   - Si desea crear una zona de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la ficha **Firewall →Zonas**, marque la casilla **Anular** y haga clic en **+ Zona de firewall**.

   Se muestra una tabla de zonas de firewall.
2. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la zona de firewall. La longitud máxima del nombre es de 255 caracteres.
3. En la lista desplegable **Entrada**, seleccione la acción que el firewall aplicará a los paquetes de tráfico entrante:
   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

4. En la lista desplegable **Salida**, seleccione la acción que el firewall aplicará a los paquetes de tráfico saliente:

   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

5. En la lista desplegable **Reenvío**, seleccione la acción que el firewall aplicará a los paquetes de tráfico reenviados entre las interfaces de red y las subredes:

   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

6. Si desea habilitar el enmascaramiento para reemplazar la dirección IP de origen de los paquetes de tráfico saliente de la zona de firewall con la dirección IP asignada a la interfaz de red de salida:

   a. Seleccione la casilla **Enmascaramiento**. Esta casilla está desactivada por defecto.

   b. Si desea reemplazar la dirección IP de origen solo para los paquetes de tráfico con la subred de origen especificada, en **Subredes de origen de enmascaramiento**, haga clic en **+ Agregar** e ingrese el prefijo IPv4 de la subred de origen.

   La subred se especifica y se muestra en **Subredes de origen de enmascaramiento**. Puede especificar varias subredes o eliminar subredes. Para eliminar una subred, haga clic en el ícono de eliminar ✕ junto a ella.

   c. Si desea reemplazar la dirección IP de destino solo para los paquetes de tráfico con la subred de origen especificada, en **Subredes de destino de enmascaramiento**, haga clic en **+ Agregar** e ingrese el prefijo IPv4 de la subred de destino.

   La subred se especifica y se muestra en **Subredes de destino de enmascaramiento**. Puede especificar varias subredes o eliminar subredes. Para eliminar una subred, haga clic en el ícono de eliminar ✕ junto a ella.

7. Desmarque la casilla **Restricción de MSS para PMTU** si no desea que el firewall limite el Tamaño máximo del segmento (MSS) de los paquetes de tráfico retransmitidos a través de la zona de firewall al valor de la Unidad de transmisión máxima de ruta (PMTU) menos 40. El propósito de restar 40 es excluir el tamaño del encabezado TCP. Esta casilla está seleccionada por defecto.

8. Si desea que el firewall mantenga un registro de los paquetes de tráfico colocados en la zona de firewall, seleccione la casilla **Registro de desconexiones**. Si los registros creados en un dispositivo CPE se envían a un servidor syslog, puede ver los registros en el servidor syslog. Si los registros creados en el dispositivo CPE se almacenan localmente, puede ver los registros solicitando información de diagnóstico. Esta casilla está desactivada por defecto.

9. Si las interfaces de red se conectan a conmutadores o enrutadores L3 y desea retransmitir paquetes de tráfico desde las subredes de estos conmutadores o enrutadores L3, agregue una subred a la zona de firewall. Para hacerlo, en **Redes**, haga clic en **+ Agregar** e ingrese un prefijo de subred IPv4.

   La subred se agrega y se muestra en **Redes**. Puede agregar varias subredes o eliminarlas. Para eliminar una subred, haga clic en el ícono de eliminar ✕ junto a ella.

10. Haga clic en **Crear**.

    La zona de firewall se crea y se muestra en la tabla.

11. Si creó una zona de firewall en un dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

Debe agregar interfaces de red a la zona de firewall creada. Puede hacerlo cuando crea o edita una interfaz de red. Si creó una zona de firewall en un dispositivo CPE, las interfaces de red que agregue a la zona de firewall deben crearse en el mismo dispositivo CPE.

# Clonar una zona común de firewall

Puede clonar la zona común de firewall creada para crear una zona común de firewall idéntica con un nombre diferente. No se admite la clonación de zonas de firewall en un dispositivo CPE.

*Para clonar una zona común de firewall, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN → Zonas de firewall**.

   Se muestra una tabla de zonas comunes de firewall.

2. Haga clic en la zona común de firewall que desea clonar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Clonar**.

4. En la ventana que se abre, ingrese un nombre para la nueva zona común de firewall.

5. Haga clic en **Clonar**.

Se crea un clon de la zona común de firewall con el nuevo nombre y se muestra en la tabla.

# Ver el uso de una zona común de firewall

Si es necesario, puede verificar qué plantillas de firewall, plantillas de CPE y dispositivos CPE están usando la zona común de firewall. Por ejemplo, si una zona común de firewall está en uso, no se puede eliminar.

*Para ver si se está utilizando una zona común de firewall:*

1. En el menú, vaya a la sección **SD-WAN → Zonas de firewall**.

   Se muestra una tabla de zonas comunes de firewall.

2. Haga clic en la zona común de firewall cuyo uso desea ver.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar uso**.

Se abre una ventana con una tabla de plantillas de firewall, plantillas de CPE y dispositivos CPE que utilizan la zona común de firewall.

# Editar una zona de firewall

Puede editar una zona común de firewall o una zona de firewall en el dispositivo CPE.

## Editar una zona común de firewall

Cuando edita una zona común de firewall, la nueva configuración se aplica a todos los dispositivos CPE que utilizan la zona común de firewall. Esto puede sobrecargar el orquestador si la cantidad de dispositivos CPE es grande.

*Para editar una zona común de firewall, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Zonas de firewall**.

   Se muestra una tabla de zonas comunes de firewall.

2. Haga clic en la zona común de firewall que desee editar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. Si es necesario, edite la configuración de la zona común de firewall. Para obtener una descripción de la configuración, consulte las instrucciones para crear una zona de firewall.

4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la zona común de firewall.

   Se abre una ventana de confirmación con la cantidad de dispositivos CPE a los que se aplicará la nueva configuración de la zona común de firewall.

5. Haga clic en **Sí, cambiar**.

La zona común de firewall se modifica y actualiza en la tabla.

## Editar una zona de firewall en un dispositivo CPE

*Para editar una zona de firewall en un dispositivo CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea editar la zona de firewall.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Firewall** → **Zonas**.

   Se muestra una tabla de zonas de firewall.

4. Seleccione la casilla de verificación **Anular**.

5. Haga clic en **Editar** junto a la zona de firewall que desea editar.

6. En la ventana que se abre, si es necesario, edite la configuración de la zona de firewall. Para obtener una descripción de la configuración, consulte las instrucciones para crear una zona de firewall.

7. Haga clic en **Guardar**.

   La zona de firewall se modifica y actualiza en la tabla.

8. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Eliminar una zona de firewall

Puede eliminar una zona común de firewall o una zona de firewall en el dispositivo CPE.

Las zonas de firewall eliminadas no se pueden restaurar.

## Eliminación de una zona común de firewall

No puede eliminar una zona común de firewall si está siendo utilizada por al menos una plantilla de firewall, plantilla de CPE o dispositivo CPE. Para eliminar una zona común de firewall que utilizan las plantillas de firewall, las plantillas de CPE o los dispositivos CPE, primero debe eliminar la zona común de firewall de su configuración. Puede verificar qué plantillas de firewall, plantillas de CPE y dispositivos CPE están utilizando la zona común de firewall.

*Para eliminar una zona común de firewall:*

1. En el menú, vaya a la sección **SD-WAN → Zonas de firewall**.

   Se muestra una tabla de zonas comunes de firewall.

2. Haga clic en la zona común de firewall que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

La zona común de firewall se elimina y ya no se muestra en la tabla.

## Eliminación de una zona de firewall en un dispositivo CPE

*Para eliminar una zona de firewall en un dispositivo CPE:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE en el que desea eliminar la zona de firewall.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. Seleccione la pestaña **Firewall** → **Zonas**.

   Se muestra una tabla de zonas de firewall.

4. Seleccione la casilla de verificación **Anular**.

5. Haga clic en **Eliminar** junto a la zona de firewall que desea eliminar.

6. En la ventana de confirmación, haga clic en **Eliminar**.

   La zona de firewall se elimina y ya no se muestra en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Administrar plantillas de firewall

Puede ver la tabla de plantillas de firewall en la sección **SD-WAN** → **Plantillas de firewall**. De manera predeterminada, se crea la **plantilla de firewall predeterminada**, que forma la base para otras plantillas de firewall que cree. La información sobre las plantillas de firewall se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la plantilla de firewall.
- **Uso** especifica si los dispositivos CPE usan la plantilla de firewall:
  - **Sí**.
  - **No**.
- **Propietario** es el nombre del usuario que creó la plantilla de firewall .
- **Última actualización** es la fecha y hora en que se modificó por última vez la configuración de la plantilla de firewall.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

Puede seleccionar una plantilla de firewall asignada para que esté preseleccionada cuando agrega o registra manualmente un dispositivo CPE.

Puede administrar la configuración de la plantilla de firewall en las siguientes pestañas:

- **Configuración general** contiene la configuración básica del firewall.
- **Reglas** contiene las reglas de firewall.

- **NAT** contiene la configuración de la traducción de direcciones de red. Las siguientes pestañas se muestran en esta pestaña:
  - **DNAT** contiene las reglas DNAT.
  - **SNAT** contiene las reglas SNAT.
- **Reenvío de zona** contiene los reenvíos entre zonas de firewall.
- **Conjuntos de direcciones IP** contiene los conjuntos de IP.

# Crear una plantilla de firewall

*Para crear una plantilla de firewall, haga lo siguiente:*

1. Vaya a la sección **SD-WAN → Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. En la parte superior de la página, haga clic en **+ Plantilla de firewall**.
3. En la ventana que se abre, ingrese el nombre de la plantilla de firewall.
4. Haga clic en **Crear**.

La plantilla de firewall se crea y se muestra en la tabla.

Debe configurar la plantilla de firewall creada. Para obtener más información sobre la administración de las plantillas de firewall, consulte Administrar plantillas de firewall.

# Seleccionar una plantilla de firewall asignada

Puede seleccionar una plantilla de firewall asignada para que esté preseleccionada cuando agrega o registra manualmente un dispositivo CPE.

*Para seleccionar una plantilla de firewall asignada, siga estos pasos:*

1. Vaya a la sección **SD-WAN → Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. Haga clic en la plantilla de firewall que desea convertir en la plantilla de firewall asignada.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Configurar como designado**.

La plantilla de firewall se convierte en la plantilla de firewall asignada.

# Importar una plantilla de firewall

Puede exportar una plantilla de firewall y luego importarla a otra plantilla de firewall. La configuración de la plantilla de firewall se especifica de acuerdo con la configuración de la plantilla de firewall importada. Durante la importación, puede seleccionar las pestañas que desea dejar sin cambios. Una plantilla de firewall en la que se importa otra plantilla de firewall permanece aplicada a los dispositivos CPE, pero la configuración de esos dispositivos CPE no se modifica.

*Para importar una plantilla de firewall, siga estos pasos:*

1. Vaya a la sección **SD-WAN** → **Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. Haga clic en la plantilla de firewall que desea exportar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Exportar**.

   Se guarda un archivo comprimido en formato TAR.GZ en su dispositivo local. El archivo comprimido no contiene información sobre los dispositivos CPE que utilizan la plantilla de firewall.

4. Haga clic en la plantilla de firewall a la que desea importar otra plantilla de firewall.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

5. En la parte superior del área de configuración, en **Acciones**, haga clic en **Importar**.

6. En la ventana que se abre, desmarque las casillas de verificación junto a las pestañas de la plantilla de firewall que desea dejar sin cambios después de la importación.

7. En el campo **Archivo**, especifique la ruta al archivo comprimido TAR.GZ.

8. Haga clic en **Importar**.

La configuración de la plantilla de firewall se modifica de acuerdo con la configuración de la plantilla de firewall importada.

# Clonar una plantilla de firewall

Puede clonar una plantilla de firewall para crear una plantilla de firewall idéntica con un nombre diferente.

*Para clonar una plantilla de firewall, siga estos pasos:*

1. Vaya a la sección **SD-WAN** → **Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. Haga clic en la plantilla de firewall que desea clonar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Clonar**.

4. En la ventana que se abre, ingrese el nombre de la nueva plantilla de firewall.

5. Haga clic en **Clonar**.

Se crea un clon de la plantilla de firewall con el nuevo nombre y se muestra en la tabla.

# Ver el uso de una plantilla de firewall

Si es necesario, puede verificar qué dispositivos CPE están usando la plantilla de firewall. Por ejemplo, si una plantilla de firewall está en uso, no se puede eliminar.

*Para ver si se está utilizando una plantilla de firewall, haga lo siguiente:*

1. Vaya a la sección **SD-WAN → Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. Haga clic en la plantilla de firewall para la que desea ver la información de uso.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Mostrar CPE asociados**.

Esto abre una ventana con una tabla de dispositivos CPE que están usando la plantilla de firewall.

# Eliminar una plantilla de firewall

No puede eliminar una plantilla de firewall si al menos un dispositivo CPE la está utilizando. Para eliminar una plantilla de firewall que los dispositivos están utilizando, primero debe cambiar la plantilla de firewall de los dispositivos CPE. Puede comprobar qué dispositivos CPE están usando la plantilla de firewall.

Las plantillas de firewall eliminadas no se pueden restaurar.

*Para eliminar una plantilla de firewall, siga estos pasos:*

1. Vaya a la sección **SD-WAN → Plantillas de firewall**.

   Se muestra una tabla de plantillas de firewall.

2. Seleccione la plantilla de firewall que desea eliminar.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, la pestaña **Configuración general** está seleccionada, que muestra la configuración principal de la plantilla de firewall.

3. En la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar**.

4. En la ventana de confirmación, haga clic en **Eliminar**.

La plantilla de firewall se elimina y ya no se muestra en la tabla.

# Configuración básica del firewall

Puede ajustar la configuración básica del firewall en una plantilla de firewall o en un dispositivo CPE. La configuración básica del firewall especificada en la plantilla de firewall se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de firewall.

El firewall aplica las acciones especificadas en su configuración básica al tráfico de paquetes. Los paquetes de tráfico se ven afectados por esto si no se les aplicaron reglas de firewall y no se reenviaron a ninguna de las zonas de firewall.

*Para especificar la configuración básica del firewall, siga estos pasos:*

1. Especifique la configuración básica del firewall de una de las siguientes maneras:

   - Si desea editar la configuración básica del firewall en una plantilla de firewall, vaya a la sección el menú **SD-WAN→ Plantillas de firewall** y haga clic en la plantilla de firewall.

   - Si desea editar la configuración básica del firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** y marque la casilla **Anular**.

   De manera predeterminada, está seleccionada la pestaña **Configuración general**, que muestra la configuración principal del firewall.

2. Si desea deshabilitar la protección contra inundaciones de SYN, desmarque la casilla **Protección de inundación de SYN**. Esta casilla está seleccionada por defecto. Cuando la protección contra inundaciones SYN está habilitada, se puede enviar un máximo de 25 paquetes de tráfico por segundo con los indicadores SYN, ACK, RST y FIN a un dispositivo CPE.

3. Si desea que el firewall descarte los paquetes de tráfico marcados como no válidos por la función conntrack, seleccione la casilla **Desconectar paquetes no válidos**. Esta casilla está desactivada por defecto.

4. Si desea deshabilitar la tecnología DPI (Inspección profunda de paquete), desmarque la casilla **Habilitar DPI**. Esta casilla está seleccionada por defecto. La tecnología DPI le permite crear reglas de firewall que se aplican solo a los paquetes de tráfico de la aplicación especificada.

   Cuando la tecnología DPI está deshabilitada, no puede configurar el marcado DPI y las reglas de firewall que usan la tecnología DPI se deshabilitan automáticamente.

5. En la lista desplegable **Acción de ENTRADA predeterminada**, seleccione la acción que el firewall aplicará a los paquetes de tráfico entrante:

   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.

   - **DROP** para descartar paquetes de tráfico.

   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

6. En la lista desplegable **Acción de SALIDA predeterminada**, seleccione la acción que el firewall aplicará a los paquetes de tráfico saliente:

   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

7. En la lista desplegable **Acción de REENVÍO predeterminada**, seleccione la acción que el firewall aplicará a los paquetes de tráfico reenviados entre las interfaces de red y las subredes:

   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.

8. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Configurar el marcado de DPI

Kaspersky SD-WAN admite la creación de reglas de firewall que se aplican solo a los paquetes de tráfico de la aplicación especificada. Puede especificar las marcas de DPI que determinan los paquetes de tráfico a los que se aplica la regla. No puede configurar el marcado DPI si deshabilitó la tecnología de marcado DPI en la configuración básica del firewall.

Puede configurar el marcado DPI en una plantilla de firewall o en un dispositivo CPE. La configuración de marcado DPI especificada en la plantilla de firewall se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para configurar el marcado DPI, siga estos pasos:*

1. Configure el marcado DPI para el firewall de una de las siguientes maneras:

   - Si desea configurar el marcado DPI en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Marcado de DPI**.
   - Si desea configurar el marcado de DPI en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall →Marcado de DPI** y marque la casilla **Anular**.

   Se muestra la configuración de marcado de DPI.

2. Seleccione las casillas de verificación junto a las marcas de DPI que desee que rijan las reglas de firewall que se aplican a los paquetes de tráfico.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Administrar reglas de firewall

Puede ver la tabla de reglas de firewall en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de reglas de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN**→ **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas**.
- Para ver la tabla de reglas de firewall en un dispositivo CPE, vaya a la sección de menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall** → **Reglas**.

Las siguientes reglas de firewall se crean de manera predeterminada:

- **Allow-GENEVE** permite que el dispositivo CPE reciba paquetes GENEVE de la zona de firewall de la WAN. Los paquetes GENEVE son tráfico de Kaspersky SD-WAN encapsulado.
- **Allow-DHCP-Renew** permite que el dispositivo CPE reciba paquetes BOOTP de la zona de firewall de la WAN, lo cual es necesario para que DHCP funcione.
- **Allow-IGMP** permite que el dispositivo CPE reciba paquetes IGMP de la zona de firewall de la WAN, que es necesaria para que VRRP y multidifusión funcionen.
- Las siguientes reglas de firewall están deshabilitadas temporalmente hasta que Kaspersky SD-WAN sea totalmente compatible con IPv6:
  - **Allow-DHCPv6** permite que el dispositivo CPE reciba paquetes DHCPv6 de la zona de firewall de la WAN, lo cual es necesario para que IPv6 funcione.
  - **Allow-MLD** permite que el dispositivo CPE reciba paquetes MLD de la zona de firewall de la WAN, que es necesario para que IPv6 funcione.
  - **Allow-ICMPv6-Input** permite que el dispositivo CPE reciba paquetes ICMPv6 de la zona de firewall de la WAN, lo cual es necesario para que IPv6 funcione.
  - **Allow-ICMPv6-Forward-From-Wan** permite que el dispositivo CPE reciba paquetes ICMPv6 de la zona de firewall de la WAN, los cuales se reenvían a la zona de firewall de la LAN, que es necesario para que IPv6 funcione.
  - **Allow-ICMPv6-Forward-From-Lan** permite que el dispositivo CPE reciba paquetes ICMPv6 de la zona de firewall de la LAN, los cuales se reenvían a la zona del firewall de la WAN, que es necesario para que IPv6 funcione.
- **Explicit-deny-http-on-wan** impide que el dispositivo CPE reciba paquetes de tráfico TCP con el puerto de destino 80 para evitar el acceso desde la zona de firewall de la WAN al servidor web del dispositivo CPE.
- **Explicit-deny-https-on-wan** impide que el dispositivo CPE reciba paquetes de tráfico TCP con el puerto de destino 443 para evitar el acceso desde la zona de firewall de la WAN al servidor web del dispositivo CPE.

Para que las reglas de firewall predeterminadas funcionen correctamente, debe agregar interfaces de red **sd-wan<0–4>** a la zona de firewall de la WAN. Puede agregar interfaces de red a una zona de firewall cuando crea o edita una interfaz de red.

La información sobre las reglas de firewall se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la regla de firewall.
- **Detalles** contiene los criterios según los cuales el firewall aplica la regla a los paquetes de tráfico.
- **Acción** es la acción que la regla de firewall aplica a los paquetes de tráfico.

# Crear una regla de firewall

Puede crear una regla de firewall en una plantilla de firewall o en un dispositivo CPE. Una regla de firewall creada en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para crear una regla de firewall, siga estos pasos:*

1. Cree una regla de firewall de una de las siguientes maneras:
   - Si desea crear una regla de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla del firewall y seleccione la pestaña **Reglas**.
   - Si desea crear una regla de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** →**Reglas** y marque la casilla **Anular**.

   Se muestra una tabla de reglas de firewall.
2. haga clic en **+ Regla**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la regla de firewall. La longitud máxima del nombre es de 255 caracteres.
4. En la lista desplegable **Acción**, seleccione la acción que la regla de firewall aplicará a los paquetes de tráfico:
   - **ACCEPT** para aceptar paquetes de tráfico. Esta es la configuración predeterminada.
   - **DROP** para descartar paquetes de tráfico.
   - **REJECT** para rechazar paquetes de tráfico con un mensaje `icmp-reject`.
   - **ADJ-MSS** para cambiar el valor en el campo MSS del encabezado TCP de los paquetes de tráfico al valor de MSS especificado. Si selecciona este valor, en el campo **Valor de MSS**, ingrese el valor de MSS. Rango de valores: 68 a 10 000.
5. Especifique los criterios según los cuales el firewall debe aplicar la regla de firewall a los paquetes de tráfico:
   a. Si desea aplicar la regla de firewall solo a paquetes de tráfico con las direcciones IP o subredes de origen o destino especificadas, en la lista desplegable **Dirección IP configurada**, seleccione un conjunto de IP creado. Si selecciona un valor de esta lista desplegable, los bloques **IP de origen** y **IP de destino** dejarán de estar disponibles.
   b. Si desea aplicar la regla de firewall solo a los paquetes de tráfico con la versión de direcciones IPv4 o subredes de origen o destino, en la lista desplegable **Versión de IP**, seleccione **IPv4**: si no selecciona un valor, la regla de firewall se aplica a los paquetes de tráfico con cualquier versión de las direcciones IP o subredes de origen o destino.

c. Si desea aplicar la regla de firewall solo a los paquetes de tráfico con la zona de firewall de origen especificada, en la lista desplegable **Zona de origen**, seleccione la zona de firewall creada.

d. Si desea aplicar la regla de firewall solo a los paquetes de tráfico con la zona de firewall de destino especificada, en la lista desplegable **Zona de destino**, seleccione una zona de firewall creada.

e. Si desea aplicar la regla de firewall solo a los paquetes de tráfico con la dirección IPv4 o el prefijo de origen especificados, en **IP de origen**, haga clic en **+ Agregar** e ingrese la dirección IPv4 o el prefijo de origen.

La dirección IPv4 o el prefijo se especifica y se muestra en **IP de origen**. Puede especificar varias direcciones IPv4 o prefijos o eliminar direcciones IPv4 o prefijos. Para eliminar una dirección IPv4 o un prefijo, haga clic en el ícono de eliminar ✕ junto a él.

f. Si desea aplicar la regla de firewall solo a los paquetes de tráfico con la dirección IPv4 o el prefijo de destino especificados, en **IP de destino**, haga clic en **+ Agregar** e ingrese la dirección IPv4 o el prefijo de destino.

La dirección IPv4 o el prefijo se especifica y se muestra en **IP de destino**. Puede especificar varias direcciones IPv4 o prefijos o eliminar direcciones IPv4 o prefijos. Para eliminar una dirección IPv4 o un prefijo, haga clic en el ícono de eliminar ✕ junto a él.

g. Si desea aplicar la regla de firewall solo a los paquetes de tráfico del protocolo especificado, seleccione un protocolo en la lista desplegable **Protocolo**. Cuando selecciona una opción en esta lista desplegable, la lista desplegable **Protocolo de DPI** deja de estar disponible.

Con **TCP** o **UDP** seleccionado, si desea aplicar la regla de firewall solo a los paquetes de tráfico con los puertos de origen o destino especificados, siga estos pasos:

1. En el campo **Puerto de origen**, ingrese un número de puerto de origen o un rango de números de puertos de origen.

2. En el campo **Puerto de destino**, ingrese un número de puerto de destino o un rango de números de puertos de destino.

Rango de valores: de 0 a 65 535. El formato del rango de números de puerto es `<primer valor>-<último valor>`. Por ejemplo, puede ingresar `10` o `10-15`.

h. Si desea aplicar la regla de firewall solo a los paquetes de tráfico de la aplicación especificada, seleccione una aplicación en la lista desplegable **Protocolo de DPI**.

El tráfico se atribuye a las aplicaciones que utilizan la tecnología DPI, que coloca una carga adicional en la CPU del dispositivo CPE.

Puede especificar las marcas de DPI que determinan los paquetes de tráfico a los que se aplica la regla. Si deshabilitó la tecnología DPI cuando especificó la configuración básica del firewall, la regla de firewall se deshabilita automáticamente.

6. Haga clic en **Crear**.

La regla de firewall se crea y se muestra en la tabla.

7. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

De manera predeterminada, esta tecnología está deshabilitada. Debe habilitar la regla de firewall para que se aplique a los paquetes de tráfico.

# Configurar el orden de las reglas del firewall

Las reglas del firewall se aplican a los paquetes de tráfico en orden descendente, comenzando con la primera regla de firewall en la parte superior de la tabla. De manera predeterminada, las reglas de firewall se muestran en la tabla en el orden de creación. Cuanto antes se haya creado una regla de firewall, más arriba se mostrará en la tabla.

Puede configurar el orden en que se aplican las reglas de firewall en una plantilla de firewall o en un dispositivo CPE. El orden en el que se aplican las reglas de firewall, que se especifica en la plantilla de firewall, se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para configurar el orden en el que se aplican las reglas de firewall, siga estos pasos:*

1. Edite el orden en el que se aplican las reglas de firewall de una de las siguientes maneras:

   - Si desea configurar el orden en el que se aplican las reglas de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas**.

   - Si desea configurar el orden en el que se aplican las reglas de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall→Reglas** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de reglas de firewall.

2. Configure el orden en que se aplican las reglas del firewall; para ello, haga clic en los botones **Arriba** y **Abajo** junto a ellos.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Habilitar o deshabilitar una regla de firewall

De manera predeterminada, las reglas de firewall se crean en un estado deshabilitado. Debe habilitar la regla de firewall para que se aplique a los paquetes de tráfico.

Puede habilitar o deshabilitar una regla de firewall en una plantilla de firewall o en un dispositivo CPE. Una regla de firewall habilitada o deshabilitada en una plantilla de firewall se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para habilitar o deshabilitar una regla de firewall, haga lo siguiente:*

1. Habilite o deshabilite una regla de firewall de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar una regla de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas**.

   - Si desea habilitar o deshabilitar una regla de firewall en un dispositivo CPE, vaya la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → Reglas** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de reglas de firewall.

2. Haga clic en **Habilitar** o **Deshabilitar** junto a la regla de firewall que desea habilitar o deshabilitar.

   La regla de firewall se habilita o deshabilita.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Editar una regla de firewall

Puede editar una regla de firewall en una plantilla de firewall o en un dispositivo CPE. Una regla de firewall modificada en una plantilla de firewall se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para editar una regla de firewall, siga estos pasos:*

1. Edite una regla de firewall de una de las siguientes maneras:

   - Si desea editar una regla de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas**.

   - Si desea editar una regla de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** →**Reglas** y marque la casilla **Anular**.

   Se muestra una tabla de reglas de firewall.

2. Haga clic en **Editar** junto a la regla de firewall que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la regla de firewall. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla de firewall.

4. Haga clic en **Guardar**.

   La regla de firewall se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Eliminar una regla de firewall

Puede eliminar una regla de firewall en una plantilla de firewall o en un dispositivo CPE. Una regla de firewall eliminada en una plantilla de firewall se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

Las reglas de firewall eliminadas no se pueden restaurar.

*Para eliminar una regla de firewall, haga lo siguiente:*

1. Elimine una regla de firewall de una de las siguientes maneras:

   - Si desea eliminar una regla de firewall en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas**.

   - Si desea eliminar una regla de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** → **Reglas** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de reglas de firewall.

2. Haga clic en **Eliminar** junto a la regla de firewall que desea eliminar.

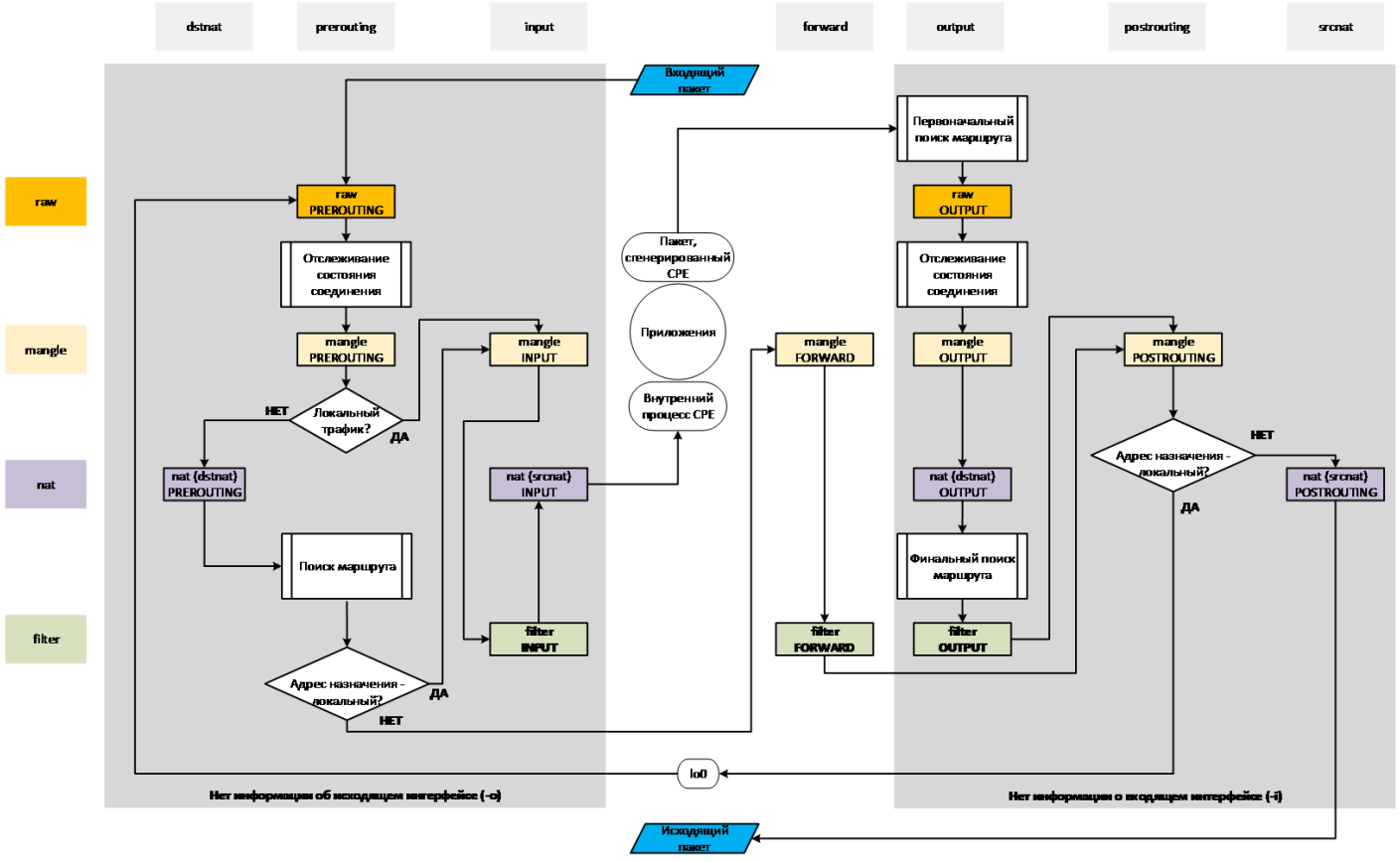
3. En la ventana de confirmación, haga clic en **Eliminar**.

   La regla de firewall se eliminará y ya no se mostrará en la tabla.

4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Administrar reglas de firewall avanzadas

Las reglas avanzadas implementan el modelo clásico de filtro de paquetes al estilo de iptables. La siguiente figura muestra el diagrama de procesamiento de paquetes con reglas avanzadas:




Esquema de procesamiento de paquetes con reglas avanzadas siguiendo el modelo de filtro de paquetes clásico estilo iptables

Puede ver la tabla de reglas de firewall avanzadas en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de reglas de firewall avanzadas en una plantilla de firewall, vaya a la sección del menú **SD-WAN→ Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas avanzadas**.
- Para ver la tabla de reglas de firewall avanzadas en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall → Reglas avanzadas**.

# Criterios de coincidencia adicionales para reglas avanzadas

En las reglas de firewall avanzadas, puede usar criterios de coincidencia adicionales para seleccionar paquetes. En esta sección se describen estos criterios y sus parámetros.

## Paquete fragmentado

Este criterio coincide cuando se detectan fragmentos de paquetes IP en el tráfico, pero no para el primer fragmento. Dichos paquetes se marcan provisionalmente con una marca especial, por lo que este criterio no puede utilizarse al mismo tiempo que el criterio **Coincidencia por marca**. Al habilitar la configuración **Paquete fragmentado**, se deshabilita automáticamente la configuración **Coincidencia por marca**, si estaba habilitada, y se bloquea.

## Coincidencia por marca

Este criterio coincide cuando se detecta un campo con una marca que se estableció previamente mediante la acción `MARK`.

Parámetros:

**Valor**

Marque el valor en formato hexadecimal (`0x0–0xFFFFFFFF`) o decimal (`0–4294967295`).

Ejemplos: `0x1`; `1`

**Máscara**

Valor de máscara de bits opcional en formato hexadecimal (`0x0–0xFFFFFFFF`) o decimal (`0–4294967295`). Si se especifica, se aplica con un AND a nivel de bits a la marca para especificar los bits individuales que deben coincidir.

Ejemplo: `0xFF`

## TOS

Este criterio coincide cuando el valor especificado del campo `TOS (Tipo de servicio)` se detecta en el encabezado IPv4 de un paquete.

Parámetros:

**Valor**

Valor del TOS en formato hexadecimal (`0x0–0xFF`) o decimal (`0-255`).

**Máscara**

Valor de máscara de bits opcional en formato hexadecimal (`0x0–0xFF`) o decimal (`0–255`). Si se especifica, se aplica con un AND a nivel de bits al `TOS` para especificar los bits individuales que deben coincidir.

## Coincidencia por cadena

El criterio coincide cuando los caracteres especificados se encuentran en el paquete en texto o notación hexadecimal.

Parámetros:

**Patrón de búsqueda**

Un patrón de búsqueda en texto o notación hexadecimal. La longitud máxima es de 255 caracteres. Se admiten los siguientes caracteres:

- Letras mayúsculas (A–Z)
- Letras minúsculas (a–z)
- Números (0-9)
- Caracteres especiales (_ - . , : ; / + = @ ( ) ! ?)
- El carácter de espacio

**Algoritmo**

Algoritmo de comparación de cadenas para la búsqueda:

- BM (Boyer–Moore)
- KMP (Knuth-Morris-Pratt).

**Rango de posiciones**

Rango de bytes en el paquete en el que se buscan cadenas coincidentes. Los índices de bytes están basados en cero. Si no se especifica, se utiliza el tamaño del paquete.

**Cadena HEX**

Si está habilitado, el valor en el campo **Patrón de búsqueda** se trata como una cadena hexadecimal.

**Ignorar mayúsculas y minúsculas**

Si está habilitado, se ignoran las mayúsculas y minúsculas.

## Coincidencia por reciente

Este criterio se aplica en función de la actividad anterior de los vínculos. Si está habilitado, le permite crear dinámicamente una lista de direcciones IP y luego buscar paquetes en esta lista.

Parámetros:

**Nombre de la lista**

Nombre de la lista para la búsqueda.

**Acción**

Acción a realizar con la lista:

- `set` (agregar una dirección IP a la lista)
- `rcheck` (buscar una dirección IP en la lista sin actualizar la hora)
- `update` (buscar una dirección IP y actualizar la hora)
- `update` (buscar una IP dirección en la lista y actualizar la hora)
- `remove` (eliminar una dirección IP de la lista)

## Marcas TCP no válidas

Este criterio coincide cuando se detecta una combinación no válida de indicadores TCP (comúnmente utilizados en técnicas de análisis de subredes) en un paquete.

Cuando se habilita esta configuración, el valor del campo **Protocolo** en la sección **General** se establece automáticamente en `TCP`.

Configuración:

**Combinaciones de marcas**

Permite seleccionar combinaciones de indicadores correspondientes a técnicas de análisis generalizadas:

- Todas las marcas (análisis TCP ALL)
- Indicadores vacíos (análisis TCP NULL)
- Marcas FIN+ACK (análisis Maimon)
- Indicador ACK en una sesión no establecida (análisis TCP ACK)
- Marcas FIN+PSH+URG (análisis Xmas)

## Tasa límite

Este criterio coincide si el valor de paquetes por segundo no excede el límite configurado según el algoritmo "token bucket".

Parámetros:

**Límite, paquetes/s**

Especifica la velocidad máxima permitida en paquetes por segundo. Una regla con el límite especificado se activa solo en el tráfico cuya velocidad no excede el límite, teniendo en cuenta la ráfaga (ver debajo). Los paquetes cuya velocidad excede el límite no son procesados por esta regla.

**Ráfaga, paquetes**

El número máximo de paquetes que se envían una vez que se supera el límite definido. Cuando se agota, se repone a una tasa constante igual al valor en el campo **Límite, paquetes/s**.

**Activar en SYN de TCP**

Criterios adicionales para hacer coincidir los paquetes TCP que contienen el indicador `SYN`. Cuando se habilita esta configuración, el valor del campo **Protocolo** en la sección **General** se establece automáticamente en `TCP`.

## Código móvil

Este criterio coincide cuando se detecta un código móvil en el tráfico HTTP no cifrado. Requiere DPI habilitado para detectar tráfico HTTP, incluso en puertos no estándar.

Al habilitar esta opción, se deshabilitan automáticamente todas las demás opciones de coincidencia avanzadas (configuración de **Protocolo** y **DPI** en la sección **Principal** y todos los demás criterios avanzados en la sección **Coincidencias adicionales**.

Parámetros:

**Tipos de códigos móviles**

Permite seleccionar uno o más tipos de código móvil que desea que activen el criterio.

- Applets de Java
- Ensamblados WebAsm
- Scripts de JavaScript/ECMAScript
- JavaScript en el cuerpo de la página
- Controles ActiveX
- Scripts/documentos PDF
- Scripts/documentos PostScript

- Animaciones/scripts de Adobe Flash
- Scripts VB/VBA

## Emparejamiento por comandos del protocolo de la capa de aplicación

El criterio se activa cuando los comandos especificados de ciertos protocolos de la capa de la aplicación se detectan en el tráfico no cifrado. Para utilizar este criterio, debe habilitar la función DPI en la configuración básica del firewall.

Puede especificar los siguientes protocolos de la capa de la aplicación y sus comandos:

| Protocolo | Comando |
|---|---|
| HTTP | GET<br>POST<br>PUT<br>DELETE<br>HEAD<br>OPTIONS<br>CONNECT |
| SMTP | HELO<br>MAIL<br>RCPT<br>DATA<br>QUIT<br>RSET<br>VRFY<br>NOOP |
| SIP | INVITE<br>ACK<br>BYE<br>REGISTER<br>OPTIONS |
| IMAP | STARTTLS<br>AUTHENTICATE<br>LOGIN<br>SELECT<br>EXAMINE<br>CREATE<br>DELETE<br>RENAME<br>SUBSCRIBE<br>UNSUBSCRIBE<br>LIST<br>LSUB<br>STATUS<br>APPEND<br>CHECK<br>EXPUNGE<br>SEARCH<br>FETCH<br>COPY |

| | |
|---|---|
| POP3 | USER<br>PASS<br>STAT<br>LIST<br>RETR<br>DELE<br>NOOP<br>RSET<br>TOP<br>UIDL |
| FTP control | USER<br>PASS<br>QUIT<br>LIST<br>RETR<br>STOR<br>DELE<br>RMD<br>REMOVE DIRECTORY<br>MKD<br>MAKE DIRECTORY<br>PASV<br>EPSV |

Puede utilizar este criterio al crear o editar reglas de firewall avanzadas. Para hacerlo, en la sección **General** del área de configuración avanzada de reglas, habilite el botón de alternancia **DPI**, seleccione un protocolo de capa de aplicación en la lista desplegable **Protocolo específico** y seleccione un comando en la lista desplegable **Comando**. Si selecciona "Cualquiera", el criterio se activará mediante cualquiera de los comandos enumerados en el protocolo seleccionado.

# Crear una regla avanzada

Puede crear una regla avanzada en una plantilla de firewall o en un dispositivo CPE. Una regla avanzada creada en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla.

*Para crear una regla avanzada, haga lo siguiente:*

1. Cree una regla avanzada de una de las siguientes maneras:

   - Si desea crear una regla avanzada en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas avanzadas**.

   - Si desea crear una regla de firewall en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** →**Reglas avanzadas** y active el botón de alternancia **Anular**.

   Se muestra la tabla de reglas de firewall avanzadas.

2. Clic en **+ Agregar**.

   Se abre la ventana de creación de reglas avanzadas.

3. Especifique la configuración básica en la sección **General**.

   a. Ingrese el nombre de la regla avanzada en el campo **Nombre**. La longitud máxima del nombre es de 255 caracteres. Caracteres válidos: A-Z, a-z, 0-9, _ - . , : ; / + = @ ( ) ! ? y espacios

   b. Si es necesario, ingrese una descripción de la regla avanzada en el campo **Descripción**.

   c. Si es necesario, especifique una o más etiquetas de directiva seleccionándolas en la lista desplegable **Etiquetas de directiva**. Una regla etiquetada se vuelve inactiva de manera predeterminada. Puede activarla más tarde.

      Si usa etiquetas de directiva, puede habilitar o deshabilitar simultáneamente un conjunto de reglas que sirven para un propósito determinado. También puede integrar un sistema de protección de datos externo y habilitar o deshabilitar etiquetas de directiva a través de la API.

   d. Especifique la tabla de firewall a la que desea agregar la regla avanzada; para ello, selecciónela en la lista desplegable **Tabla**. Las siguientes tablas están disponibles:

      - FILTRO
      - MANGLE
      - NAT
      - RAW

   e. Para la tabla seleccionada, especifique la cadena a la que desea agregar la regla avanzada; para ello, selecciónela en la lista desplegable **Cadena**. El conjunto de cadenas disponibles depende de la tabla que seleccionó en el paso anterior:

      - FILTRO
        - ENTRADA
        - REENVÍO
        - SALIDA
      - MANGLE
        - ENTRADA
        - REENVÍO
        - SALIDA
        - PREENRUTADO
        - POSTENRUTADO
      - NAT
        - PREENRUTADO
        - POSTENRUTADO

- ENTRADA
- SALIDA

- RAW
  - SALIDA
  - PREENRUTADO

f. Si es necesario, especifique el protocolo al que desea aplicar la regla avanzada; para ello, selecciónelo en la lista desplegable **Protocolo**:

- TCP
- UDP
- ICMP
- Todos (la regla se aplica a todos los protocolos anteriores)

Si seleccionó el protocolo ICMP, especifique el tipo y el código de paquete ICMP en el que desea que se active la regla. Para hacerlo, en los campos **Tipo** y **Código**, ingrese un valor de `0` a `255`.

g. Configure la coincidencia de DPI según sea necesario:

1. Active el botón de alternancia **DPI**.
2. Especifique el protocolo de la aplicación o el ID del servicio o la aplicación en el que desea que se active la regla; para ello, selecciónelo en la lista **Protocolo específico**.
3. Si es necesario, configure la coincidencia según los comandos de los protocolos de la capa de aplicación si seleccionó uno de los siguientes protocolos como criterio de coincidencia de DPI: `HTTP`, `SMTP`, `SIP`, `IMAP`, `POP3`, `control de FTP`.

> No puede usar la coincidencia de **DPI** al mismo tiempo que la coincidencia de **protocolo** del paso anterior. Cuando se usa la coincidencia de **DPI**, la configuración del **protocolo** se bloquea y los valores especificados para ella se ignoran.

h. En **Ubicación de la regla**, configure el orden en el que se agregará la regla avanzada a la lista de reglas avanzadas:

1. Especifique el tipo de ubicación de la regla avanzada:
   - Las reglas previas se insertan antes que otras reglas.
   - Las reglas posteriores se agregan al final de la tabla después de otras reglas.

2. Especifique la ubicación de la regla avanzada en la tabla:

   - Inicio de la tabla
   - Fin de la tabla
   - Después de la regla avanzada especificada

i. Si es necesario, especifique la dirección IP de origen y la dirección IP de destino en la que desea que se active la regla.

   Si desea que la regla se active en todas las direcciones IP de origen o de destino, excepto las direcciones especificadas, seleccione la casilla **Hacer una excepción** para el campo correspondiente.

j. Si es necesario, especifique las interfaces de origen o destino mediante los campos de **Interfaces**.

k. Especifique la acción de destino que desea que la regla avanzada aplique al paquete cuando se active. Para hacerlo, seleccione un valor en la lista desplegable **Destino**:

   - ACEPTAR
   - DESCONECTAR
   - TTL
   - RECHAZAR
   - MARCAR
   - TOS
   - REGISTRO
   - VOLVER
   - DNAT
   - CLASIFICAR

   La elección de acciones depende de la tabla seleccionada. Al seleccionar las acciones TTL, MARK, TOS, DNAT, CLASSIFY, también debe especificar valores adicionales que se deben agregar al paquete.

4. Configure criterios de coincidencia adicionales para la regla avanzada en la sección **Coincidencias adicionales**. Para obtener una descripción detallada de la configuración de los criterios, consulte la sección de ayuda Criterios de coincidencia adicionales para reglas avanzadas.

5. Si es necesario, haga clic en **Ver comando** en la parte superior del área de configuración para ver el comando iptables resultante que se ejecutará en el dispositivo CPE.

6. Haga clic en **Crear**.

   La regla avanzada se crea y se muestra en la tabla.

7. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Habilitar y deshabilitar reglas avanzadas

Puede habilitar o deshabilitar una regla de firewall avanzada en una plantilla de firewall o en un dispositivo CPE. Una regla de firewall avanzada habilitada o deshabilitada en una plantilla de firewall se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para habilitar o deshabilitar una regla avanzada:*

1. Habilite o deshabilite la regla avanzada de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar una regla avanzada en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas avanzadas**.

   - Si desea habilitar o deshabilitar una regla avanzada en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Reglas avanzadas** y active el botón de alternancia **Anular**.

   Se muestra la tabla de reglas avanzadas.

2. Establezca el botón de alternancia en **Deshabilitado** o **Habilitado** para deshabilitar o habilitar las reglas avanzadas según sea necesario.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Editar una regla avanzada

Puede editar una regla avanzada en una plantilla de firewall o en un dispositivo CPE. Una regla avanzada modificada en una plantilla de firewall se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para editar una regla avanzada, siga estos pasos:*

1. Edite una regla avanzada de una de las siguientes maneras:

   - Si desea editar una regla avanzada en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas avanzadas**.

   - Si desea editar una regla avanzada en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall →Reglas avanzadas** y active el botón de alternancia **Anular**.

   Se muestra la tabla de reglas avanzadas.

2. Seleccione la regla avanzada que desea editar en la tabla y haga clic en el botón **Editar**.

3. En la ventana que se abre, edite la configuración de la regla avanzada según sea necesario. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla avanzada.

4. Haga clic en **Guardar**.

   La regla avanzada se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Eliminar una regla avanzada

Puede eliminar una regla avanzada en una plantilla de firewall o en un dispositivo CPE. Una regla avanzada eliminada en una plantilla de firewall se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

Las reglas avanzadas eliminadas no se pueden restaurar.

*Para eliminar una regla avanzada, siga estos pasos:*

1. Elimine una regla avanzada de una de las siguientes maneras:

   - Si desea eliminar una regla avanzada en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reglas avanzadas**.
   - Si desea eliminar una regla avanzada en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** →**Reglas avanzadas** y active el botón de alternancia **Anular**.

   Se muestra la tabla de reglas avanzadas.

2. Seleccione una o más reglas avanzadas que desee eliminar en la tabla y haga clic en el botón **Eliminar**.

3. Para confirmar la eliminación, haga clic en el botón **Eliminar** en la ventana que se muestra.

   Las reglas avanzadas se eliminan y ya no se muestran en la tabla.

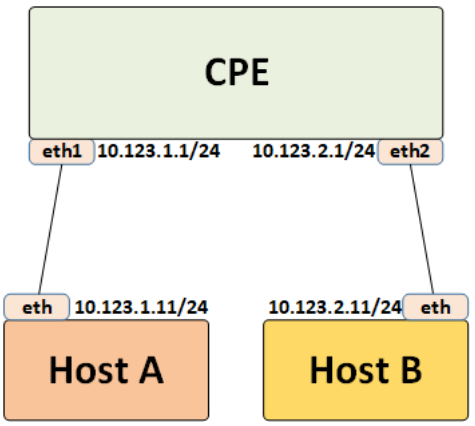
4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Escenario: ocultar un dispositivo CPE en la ruta de tráfico mediante reglas de firewall

Cuando despliegan un dispositivo CPE en una ubicación remota, los administradores a menudo carecen de control completo sobre las acciones de los usuarios en la red interna en la que se encuentra el dispositivo CPE. En tal situación, es posible que deba excluir la posibilidad de que se pueda detectar el dispositivo CPE como un nodo activo en la red cuando se realiza el análisis desde el interior de la red interna. Puede ocultar el dispositivo CPE en la topología de la red mediante reglas de firewall avanzadas.

Este escenario describe los pasos para crear reglas avanzadas a fin de ocultar el dispositivo CPE de la detección por parte de las herramientas de análisis de red estándar.

## Estado inicial




Topología de la red

El estado inicial de los componentes de la red es el siguiente:

- Hay dos hosts, A y B, conectados al dispositivo CPE.
- Las interfaces `eth1` y `eth2` en el CPE están en la misma zona.
- Los firewalls de los hosts A y B están configurados para permitir el tráfico ICMP.
- El host A realiza el seguimiento de la ruta al host B mediante `traceroute`:

  ```
  tracert -d 10.123.2.11
  ```

  Resultado:

  ```
  1 10.123.1.1
  2 10.123.2.11
  ```

  Interpretación del resultado:

  El seguimiento revela un nodo intermedio entre los hosts, que es el dispositivo CPE.

- El análisis del tráfico de red en el dispositivo CPE para el protocolo ICMP entre los hosts A y B mediante el comando `tcpdump -i any net 10.123.0.0/16` muestra lo siguiente:

```
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 102, length 72
eth1 Out ARP, Request who-has 10.123.1.11 tell 10.123.1.1, length 28
eth1 In ARP, Reply 10.123.1.11 is-at bc:24:11:0a:91:06 (oui Unknown), length 28
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 103, length 72
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 104, length 72
eth1 Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit, length 100
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 105, length 72
eth2 Out ARP, Request who-has 10.123.2.11 tell 10.123.2.1, length 28
eth2 In ARP, Reply 10.123.2.11 is-at bc:24:11:59:58:b7 (oui Unknown), length 28
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 105, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 105, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 105, length 72
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 106, length 72
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 106, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 106, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 106, length 72
eth1 In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 107, length 72
eth2 Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 107, length 72
eth2 In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 107, length 72
eth1 Out IP 10.123.2.11 > 10.123.1.11: ICMP echo reply, id 1, seq 107, length 72
```

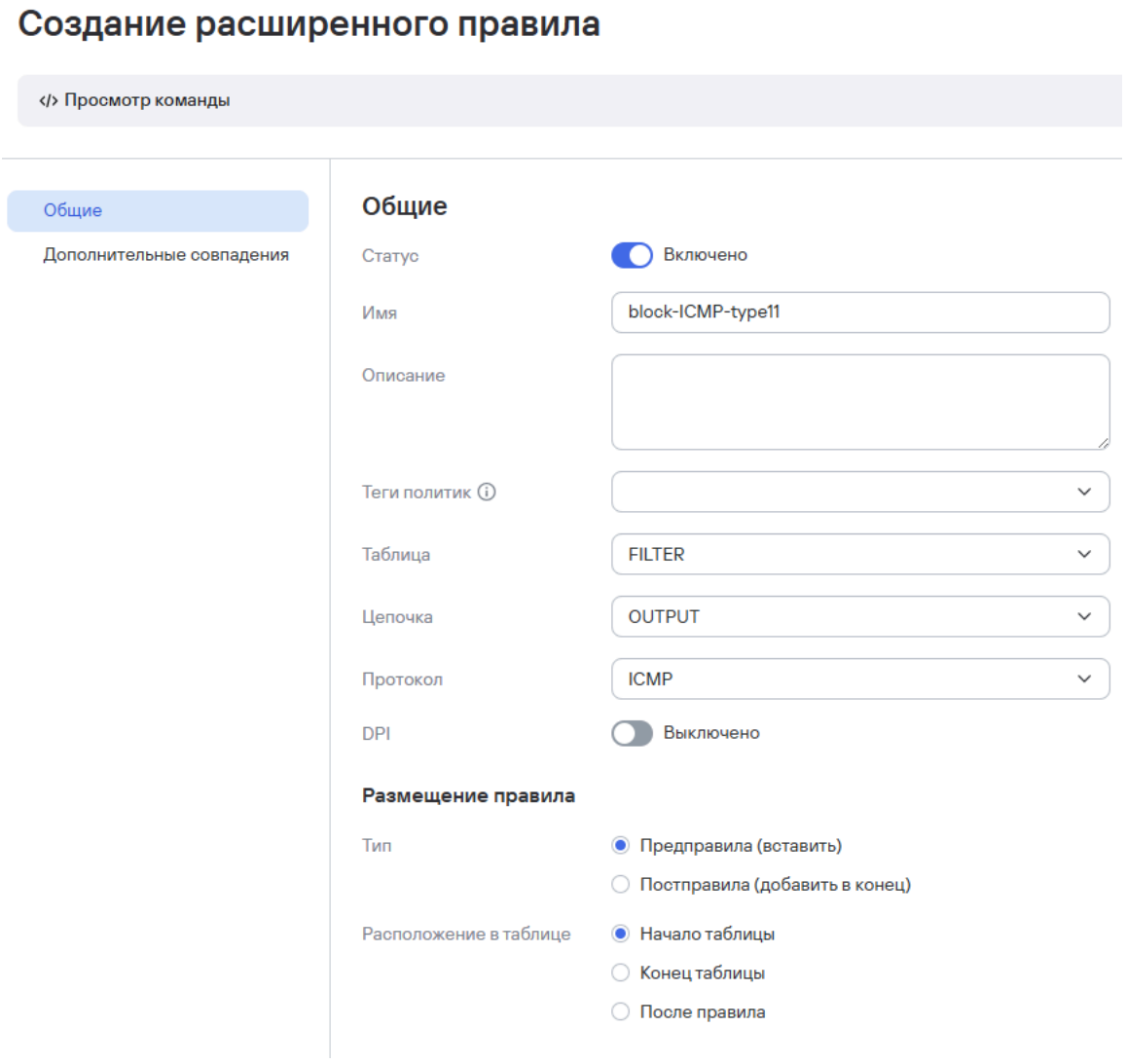
Interpretación:

| Qué hace traceroute | Cómo se ve en tcpdump | Qué sucede en el CPE |
|---|---|---|
| Envía una solicitud de eco ICMP (o un paquete UDP) con TTL = 1 a la IP de destino 10.123.2.11 (host B). | In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, id 1, seq 102... | El enrutador recibe el paquete, reduce el TTL a 0, descarta el paquete y genera un mensaje de Tiempo superado de ICMP al origen. |
| Recibe un mensaje de Tiempo superado de ICMP del enrutador (origen = enrutador 10.123.1.1). | Out IP 10.123.1.1 > 10.123.1.11: ICMP time exceeded in-transit... | Este es el primer salto en el resultado de traceroute, la dirección del enrutador. |
| Incrementa el TTL a 2 y envía una nueva solicitud. | In IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 103... | TTL = 2 permite que el paquete pase a través del enrutador (TTL-1 = 1), pero el enrutador aún no conoce la dirección MAC del host de destino, por lo que realiza una solicitud ARP a 10.123.2.11. |
| Solicitud ARP del enrutador (10.123.2.1) ⟶ 10.123.2.11. | Out ARP, Request who-has 10.123.2.11 tell 10.123.2.1 | El enrutador intenta resolver la dirección MAC del host B en la segunda subred del enrutador. |
| Respuesta ARP de 10.123.2.11. | In ARP, Reply 10.123.2.11 is-at bc:24:11:59:58:b7 | Después de obtener la dirección MAC del host B, el enrutador envía el paquete. |
| Un paquete con TTL = 2 ya llegó al host de destino (TTL-1 = 1), por lo que el enrutador no genera un mensaje de Tiempo superado, sino que simplemente reenvía el paquete. | Out IP 10.123.1.11 > 10.123.2.11: ICMP echo request, seq 105... | El host B recibe la solicitud y envía una respuesta de eco ICMP. |
| Respuesta de eco ICMP de 10.123.2.11 ⟶ 10.123.1.11. | In IP 10.123.2.11 > 10.123.1.11: ICMP echo reply... | traceroute recibe la respuesta y genera el segundo salto, la dirección del host B. |

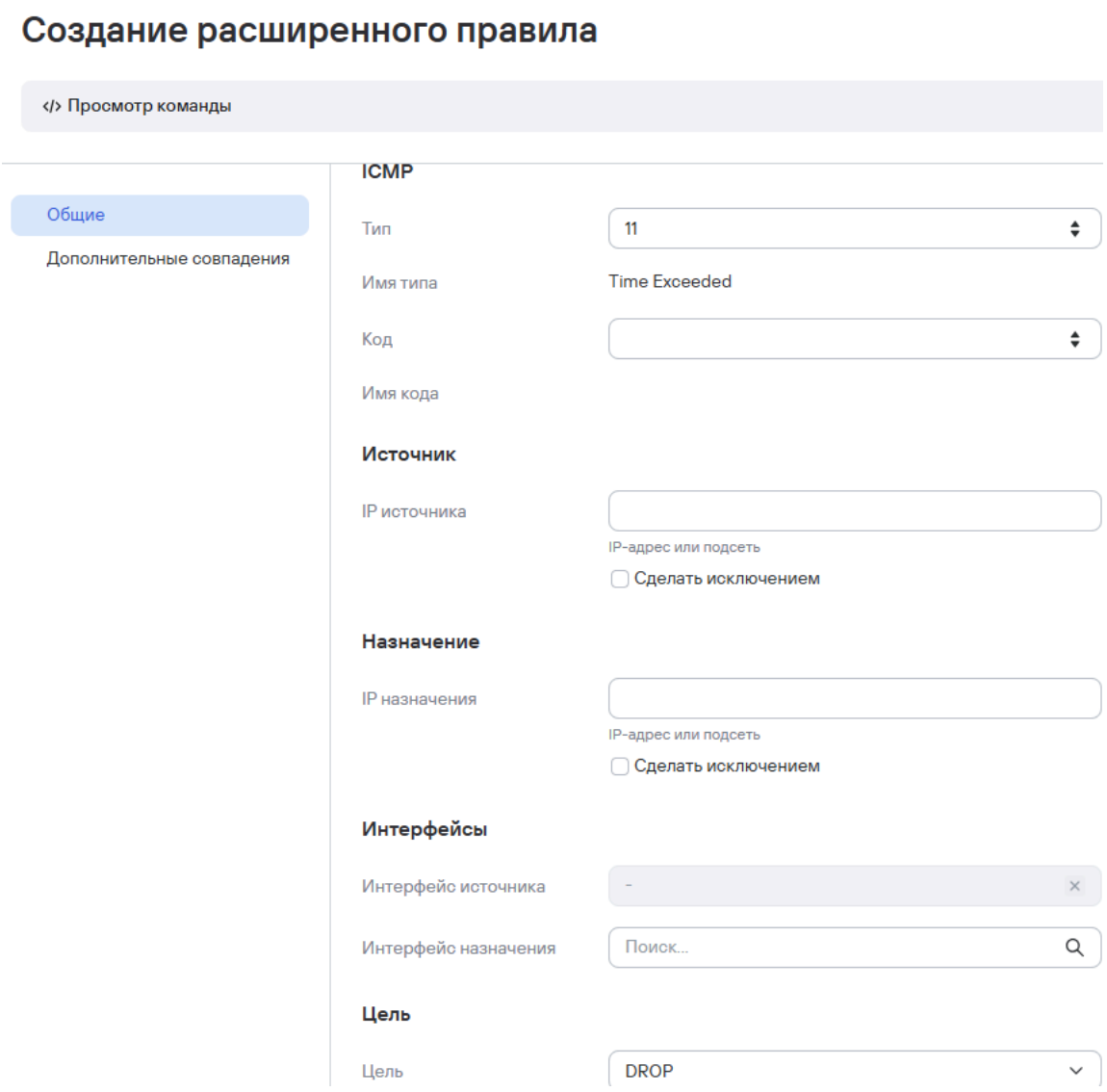
Por lo tanto, el escenario para ocultar el dispositivo CPE de la detección en la red implica los siguientes pasos:

1. **Ocultar el CPE del resultado de traceroute**

   a. **Cree una regla avanzada en el dispositivo CPE para bloquear los mensajes de `Tiempo superado de ICMP` salientes generados en el CPE cuando recibe un paquete de IP con `TTL=1`:**




Crear una regla avanzada para bloquear mensajes de Tiempo superado de ICMP 1




Crear una regla avanzada para bloquear mensajes de Tiempo superado de ICMP 2

La regla avanzada creada corresponde al siguiente comando en formato iptables:

```
iptables -t filter -I OUTPUT -p icmp --icmp-type 11 -j DROP -m comment --comment "#ADV Name: block-ICMP-type11"
```

Una regla similar en el formato iptables en el resultado de `iptables -L` luce así:

```
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
DROP icmp -- 0.0.0.0/0 0.0.0.0/0 icmptype 11 /* #ADV Name: block-ICMP-type11 */
```

a. Verifique el seguimiento de la ruta del host A al host B:

En el host A, realice el seguimiento de la ruta al host B:

```
tracert -d 10.123.2.11
```

Resultado:

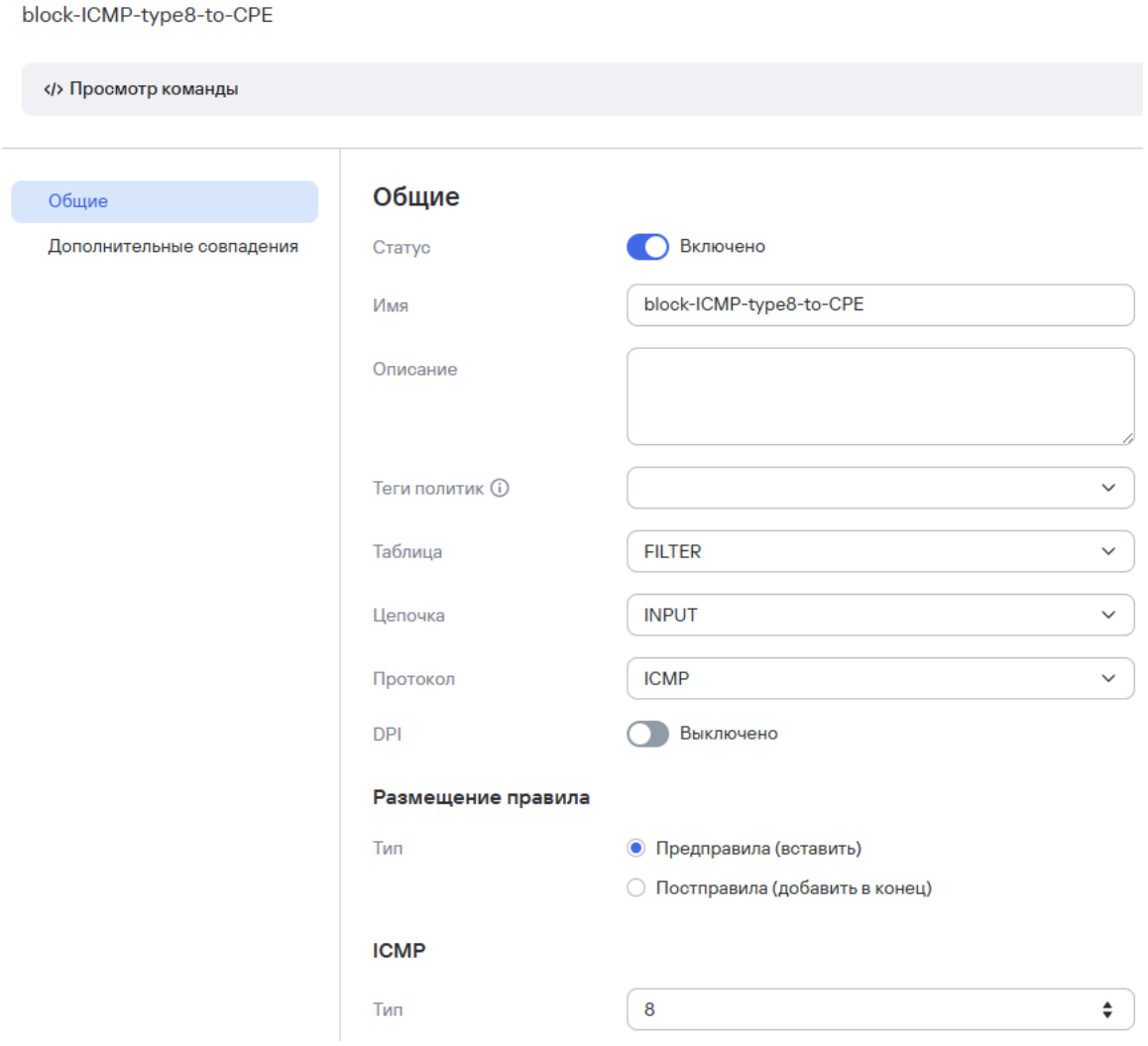
```
1 Request timed out
2 10.123.2.11
```

Interpretación del resultado:

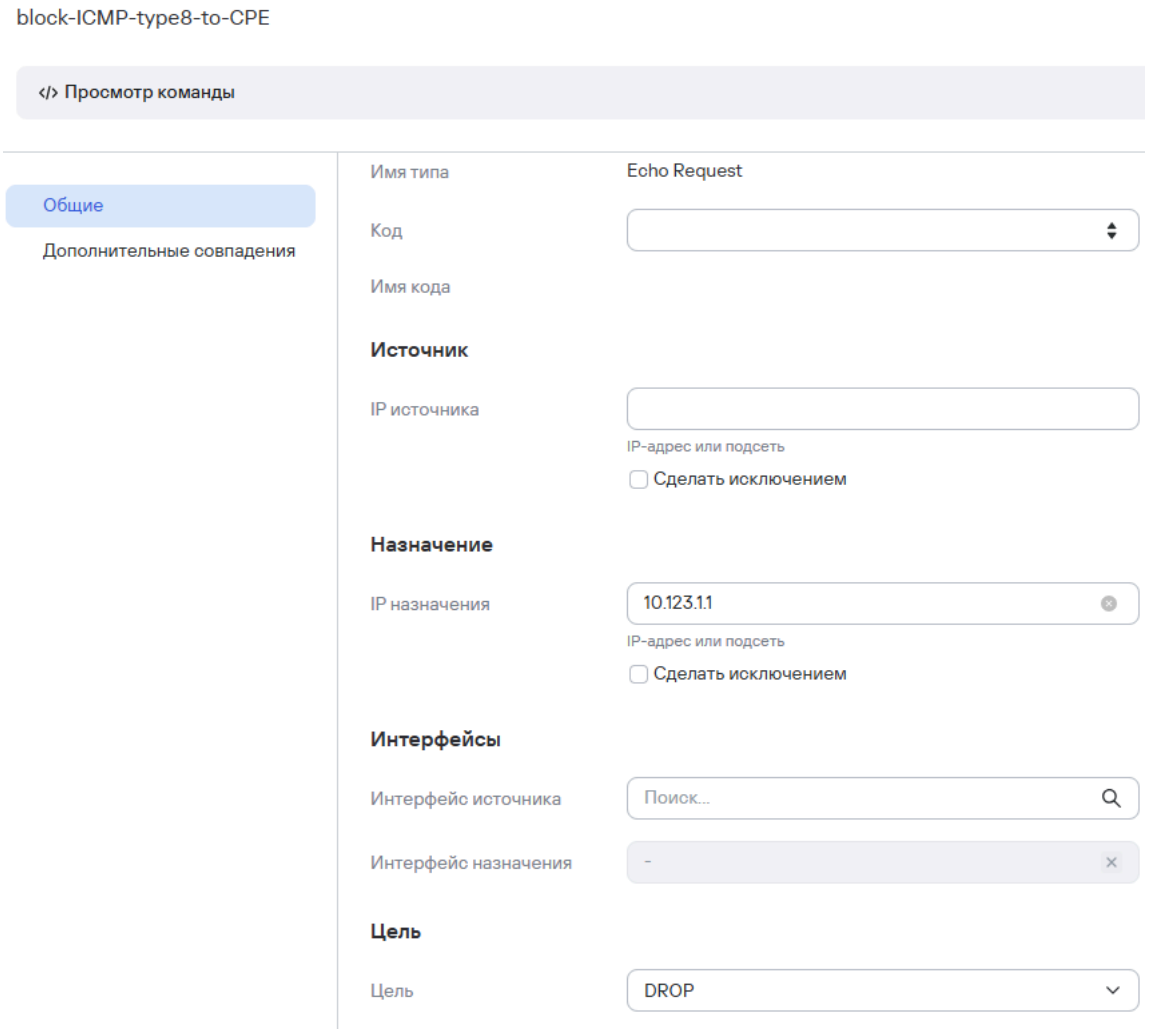
Traceroute envía solicitudes de eco ICMP con mayor TTL. El enrutador genera el mensaje `ICMP type 11 (Time-Exceeded)`, pero la regla de firewall avanzada lo bloquea y, por lo tanto, no aparece en el seguimiento. Después de que el host A incremente el valor de TTL suficientes veces, la solicitud llega al host B en `10.123.2.11`, que responde con una `respuesta de eco` regular. Este es el único mensaje que finalmente se puede ver en el volcado.

2. Bloquear respuestas de CPE a solicitudes ICMP

a. Cree una regla extendida en el dispositivo CPE que descarte los paquetes ICMP destinados al dispositivo CPE:




Crear una regla avanzada para descartar paquetes ICMP en el CPE (1)




Crear una regla avanzada para descartar paquetes ICMP en el CPE (2)

La regla avanzada creada corresponde al siguiente comando en formato iptables:

```
iptables -t filter -I INPUT -p icmp -d 10.123.1.1 --icmp-type 8 -j DROP -m comment --comment "#ADV Name: block-ICMP-type8-to-CPE"
```

Una regla similar en el formato iptables en el resultado de iptables -L luce así:

a. Verifique que la regla funcione: en el host A, `envíe ping` a la dirección del CPE en `eth1`:

```
ping 10.123.1.1
```

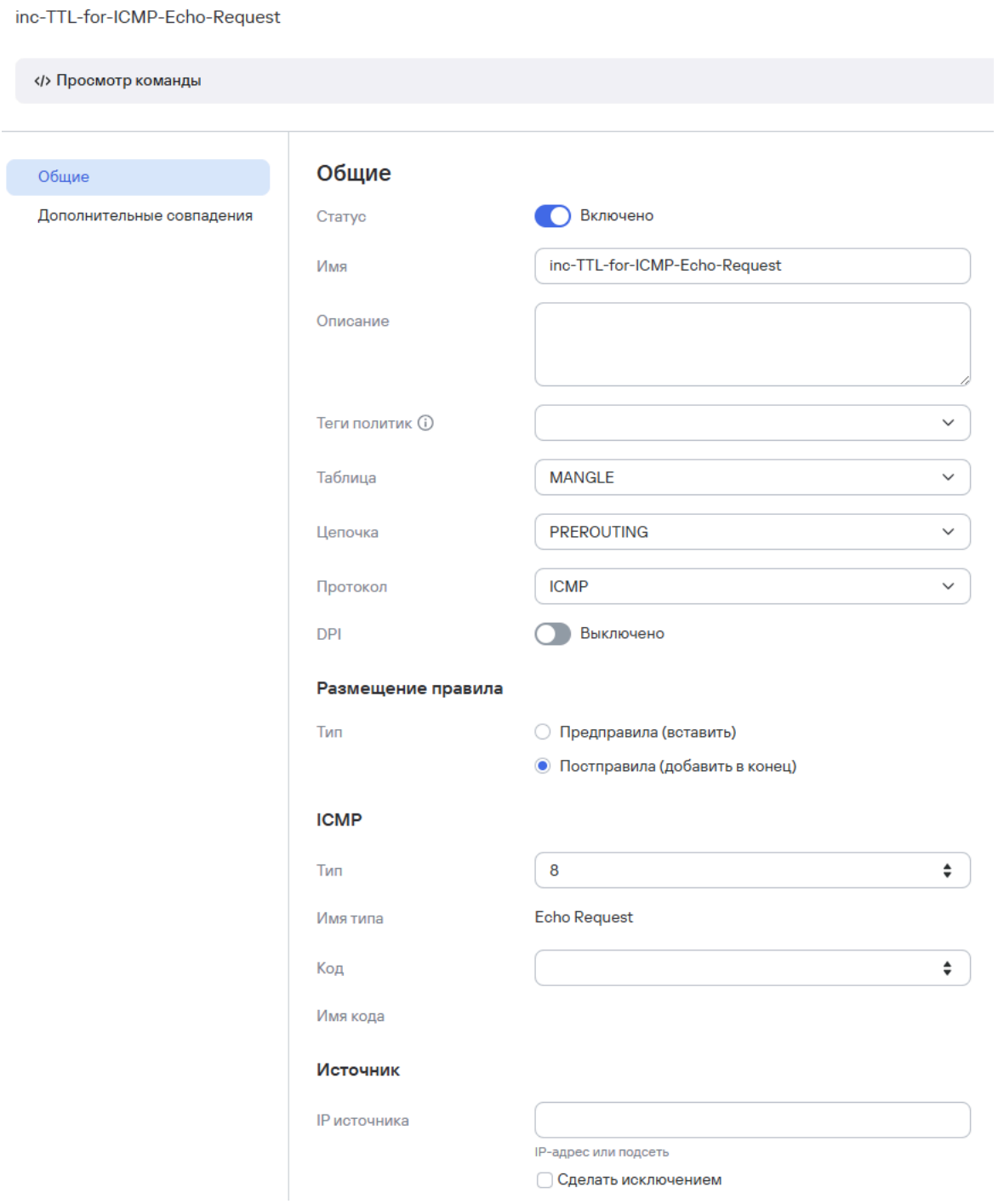
Resultado:

```
Se agotó el tiempo de espera de la solicitud
```

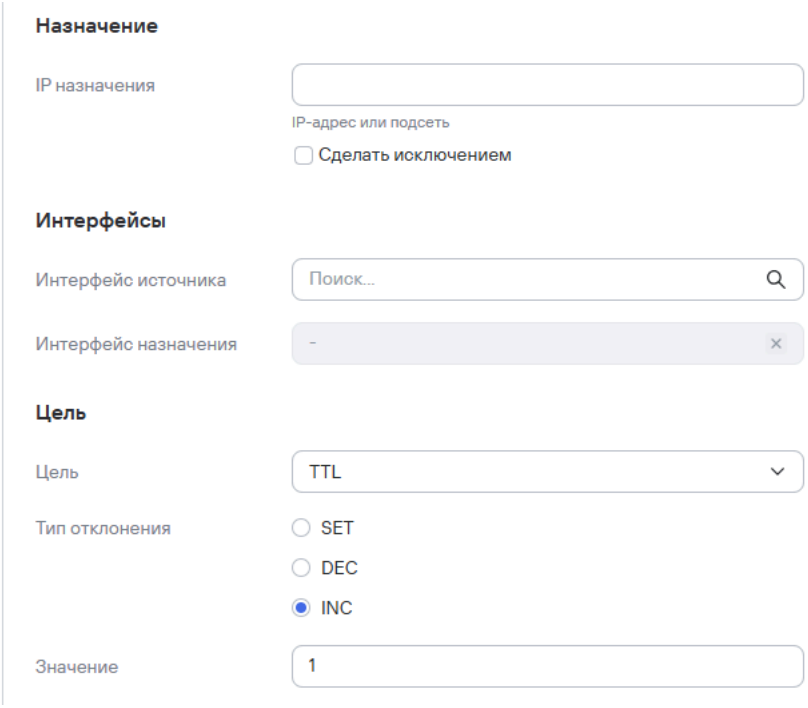
3. Ocultar el CPE de la ruta de tráfico mediante la manipulación TTL

Debe crear una regla avanzada que incremente el TTL de los mensajes `ICMP Tipo 8 (Solicitud de eco)` en 1 antes de que el enrutador disminuya este valor en 1. Para hacerlo, agregue la regla a la cadena PREROUTING de la tabla MANGLE.

a. Cree una regla avanzada en el dispositivo CPE que incremente el TTL en 1:




Crear una regla avanzada para incrementar TTL (1)




Crear una regla avanzada para incrementar TTL (2)

La regla avanzada creada corresponde al siguiente comando en formato iptables:

```
iptables -t mangle -A PREROUTING -p icmp --icmp-type 8 -j TTL --ttl-inc 1 -m comment --comment "#ADV Name: inc-TTL-for-ICMP-Echo-Request"
```

a. En el host A, realice un seguimiento de la ruta al Host B.

```
tracert -d 10.123.2.11
```

Resultado:

```
1 10.123.2.11
```

Cómo se refleja esta regla en los seguimientos de rutas entre los dos hosts conectados al CPE:

| Paso | Qué sucede sin la regla | Qué sucede con la regla |
|---|---|---|
| 1. El host A envía un paquete con TTL = 1 (primer salto) | El CPE recibe el paquete, reduce el TTL a 0, descarta el paquete y genera un Tiempo superad de ICMP (tipo 11) que regresa a A. El host A ve el CPE como el primer salto. | En la cadena PREROUTING, TTL se incrementa a 2. El CPE luego lo reduce a 1. El paquete no se descarta y el CPE lo envía. Por lo tanto, no se genera un mensaje de Tiempo superado de ICMP y el primer salto (CPE) no aparece en el resultado. |
| 2. El paquete llega al host de destino (host B) | | El paquete llega al host B con TTL = 1. Aquí, el TTL se reduce a 0 y el Host B genera un mensaje de Tiempo superado de ICMP. Traceroute muestra al Host B como el primer salto. |
| 3. Próximos pasos de traceroute | En este paso, TTL se incrementa a 2, CPE lo reduce a 1. El Host B reduce TTL a 0, descarta el paquete y genera un mensaje de Tiempo superado de ICMP. Traceroute muestra al Host B como el segundo salto. | |

La regla creada afecta solo a los paquetes `ICMP tipo 8 (solicitud de eco)`. Si traceroute o un rastreador de rutas similar usa paquetes UDP, el primer salto seguirá siendo visible. Para ocultar el enrutador del seguimiento de rutas mediante paquetes UDP, debe crear una regla similar para UDP.

4. **Ocultar información acerca del proveedor del dispositivo CPE mediante la asignación de direcciones MAC del rango LAA a las interfaces LAN del dispositivo CPE.**

   **Para evitar que los usuarios de la red local conozcan el fabricante del dispositivo CPE al ver las direcciones MAC predeterminadas de sus interfaces LAN, debe reasignar las direcciones MAC del rango LAA (Dirección administrada localmente) a las interfaces. Una dirección MAC se considera administrada localmente si el segundo bit menos significativo en su primer octeto es 1. Ejemplo:**

```
06:1A:2B:3C:4D:5E
06 → 0000 0110
```

   **Para ocultar información acerca del proveedor de un dispositivo CPE:**

   **a. Verifique que la dirección MAC predeterminada del dispositivo CPE contiene información del proveedor:**

   1. Desde el host B, envíe `ping` a la dirección de la puerta de enlace (interfaz `eth2` en el CPE con la dirección IP `10.123.2.1`).

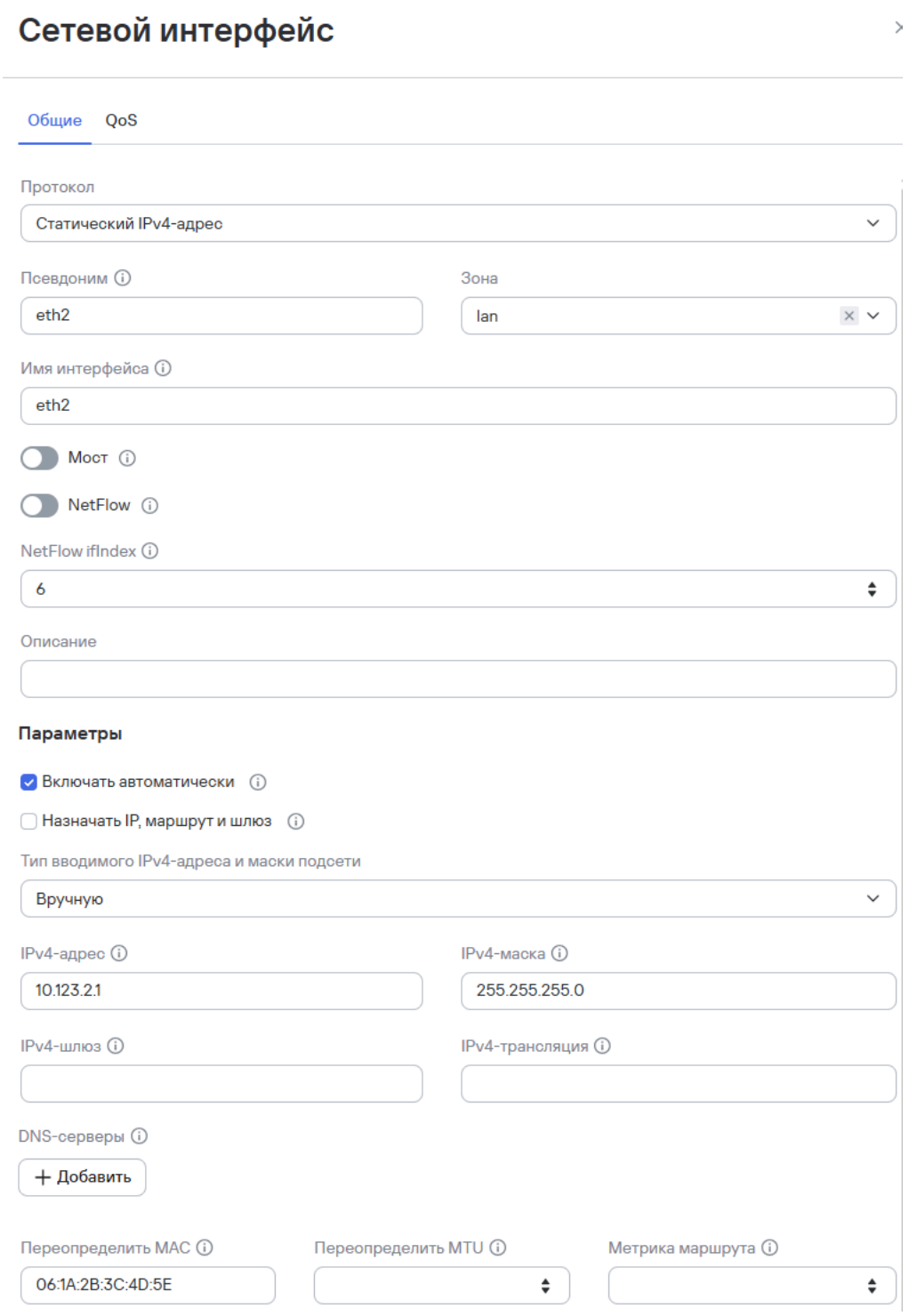
   2. Utilice WireShark para analizar el tráfico ICMP enviado al CPE:

```
> Frame 4534: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interf
v Ethernet II, Src: ProxmoxServe_59:58:b7 (bc:24:11:59:58:b7), Dst: ProxmoxServe_57:11:dc
  v Destination: ProxmoxServe_57:11:dc (bc:24:11:57:11:dc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: ProxmoxServe_59:58:b7 (bc:24:11:59:58:b7)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Internet Protocol Version 4, Src: 10.123.2.11, Dst: 10.123.2.1
v Internet Control Message Protocol
    Type: Echo (ping) request (8)
    Code: 0
    Checksum: 0x4c0d [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence Number (BE): 334 (0x014e)
    Sequence Number (LE): 19969 (0x4e01)
    [Response frame: 4535]
  > Data (32 bytes)
```

   Análisis de tráfico en Wireshark: se muestra la información del proveedor de CPE para la dirección MAC de destino.

En el campo `Destino`, la dirección MAC de la interfaz `eth2` del dispositivo CPE se muestra con el prefijo de proveedor `ProxmoxServe_`. Este prefijo corresponde a las direcciones MAC predeterminadas asignadas a las máquinas virtuales en un entorno de virtualización Proxmox. Esto le permite a uno saber que el dispositivo CPE se está ejecutando como una máquina virtual en Proxmox. Por lo tanto, la aplicación WireShark pudo determinar el prefijo del proveedor a partir de la dirección MAC predeterminada.

a. Asigne una dirección MAC del rango LLA a la interfaz LAN del dispositivo CPE hacia el host B (`eth2`):

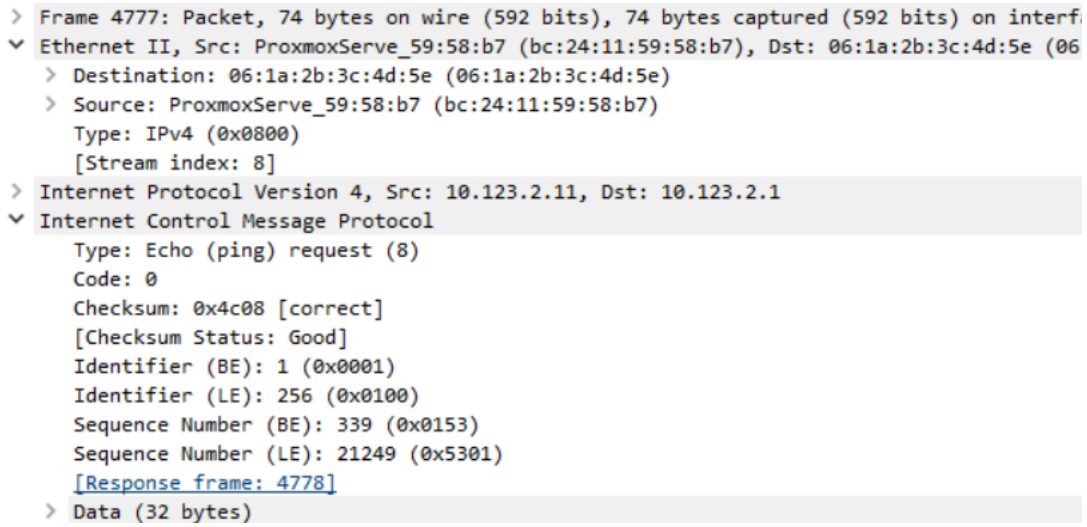



Asignar una dirección MAC del rango LLA a la interfaz LAN del dispositivo

a. Verifique que la dirección MAC predeterminada del dispositivo CPE no contiene información del proveedor:

1. Desde el host B, vuelva a enviar `ping` a la dirección de la puerta de enlace (interfaz `eth2` en el CPE con la dirección IP `10.123.2.1`).

2. Utilice WireShark para analizar el tráfico ICMP enviado al CPE:




Análisis de tráfico en Wireshark: no se muestra la información del proveedor del dispositivo CPE.

**Ahora, en el campo Destino, la dirección MAC de la interfaz `eth2` del dispositivo CPE se muestra en su forma original y no indica el entorno de virtualización ni el proveedor del equipo de red.**

# Administrar conjuntos de IP

Puede ver la tabla de conjuntos de IP en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de conjuntos de IP en una plantilla de firewall, vaya a la sección del menú **SD-WAN→ Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Conjuntos de direcciones IP**.
- Para ver la tabla de conjuntos de IP en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall → Conjuntos de direcciones IP**.

La información sobre los conjuntos de IP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del conjunto de IP.
- **Coincidencia** indica si el conjunto de IP está asociado con el origen o el destino de los paquetes de tráfico, y si el conjunto contiene direcciones IP o subredes.
- **Entradas** son direcciones IP o subredes que se agregaron al conjunto de IP.

# Crear un conjunto de IP

Puede crear un conjunto de direcciones IP en una plantilla de firewall o en un dispositivo CPE. Un conjunto de IP creado en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para crear un conjunto de IP, haga lo siguiente:*

1. Cree un conjunto de IP de una de las siguientes maneras:

   - Si desea crear un conjunto de IP en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Conjuntos de direcciones IP**.

   - Si desea crear un conjunto de IP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → Conjuntos de direcciones IP** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de conjuntos de IP.

2. Haga clic en **+ Dirección IP configurada**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del conjunto de IP. La longitud máxima del nombre es de 255 caracteres.

4. En la lista desplegable **Sentido**, seleccione si el conjunto de IP está asociado con el origen o el destino de los paquetes de tráfico:

   - **Destino de origen** si el conjunto de IP contiene direcciones IP o subredes de origen.

   - **Destino de coincidencia** si el conjunto de IP contiene direcciones IP o subredes de destino.

5. En la lista desplegable **Tipo**, seleccione si el conjunto contiene direcciones IP o subredes.

   - **Conjunto de subredes** si el conjunto de direcciones IP contiene subredes.

   - **Conjunto de IP** si el conjunto de IP contiene direcciones IP.

6. Si en la lista desplegable **Tipo** seleccionó **Conjunto de subredes**, especifique una subred. Para hacerlo, en **Lista de entradas**, haga clic en **+ Agregar** e ingrese el prefijo IPv4 de la subred. Puede especificar rangos de octetos del prefijo IPv4 utilizando corchetes, por ejemplo, 192.[165-168].2.0/24.

   La subred se especifica y se muestra en **Lista de entradas**. Puede especificar varias subredes o eliminar subredes. Para eliminar una subred, haga clic en el ícono de eliminar ✕ junto a ella.

7. Si en la lista desplegable **Tipo** seleccionó **Conjunto de IP**, especifique una dirección IP. Para hacerlo, en **Lista de entradas**, haga clic en **+ Agregar** e ingrese una dirección IPv4. Puede especificar rangos de octetos de la dirección IPv4 utilizando corchetes, por ejemplo, 192.[165-168].2.0.

   La dirección IP se especifica y se muestra en la sección **Lista de entradas**. Puede especificar varias direcciones IP o eliminar direcciones IP. Para eliminar una dirección IP, haga clic en el ícono de eliminar ✕ junto a ella.

8. Haga clic en **Crear**.

   El conjunto de IP se crea y se muestra en la tabla.

9. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Deshabilitar o habilitar un conjunto de IP

Puede deshabilitar o habilitar un conjunto de IP en una plantilla de firewall o en un dispositivo CPE. Un conjunto de IP habilitado o deshabilitado en una plantilla de firewall se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para deshabilitar o habilitar un conjunto de IP, siga estos pasos:*

1. Deshabilite o habilite un conjunto de IP de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar un conjunto de IP en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Conjuntos de direcciones IP**.

   - Si desea habilitar o deshabilitar un conjunto de IP en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall→Conjuntos de direcciones IP** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de conjuntos de IP.

2. Haga clic en **Deshabilitar** o **Habilitar** junto al conjunto de IP que desea deshabilitar o habilitar.

   El conjunto de IP se deshabilita o habilita.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Editar un conjunto de IP

Puede editar un conjunto de direcciones IP en una plantilla de firewall o en un dispositivo CPE. Un conjunto de IP modificado en una plantilla de firewall se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para editar un conjunto de IP, haga lo siguiente:*

1. Edite un conjunto de IP de una de las siguientes maneras:

   - Si desea editar un conjunto de IP en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Conjuntos de direcciones IP**.

   - Si desea editar un conjunto de IP en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → Conjuntos de direcciones IP** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de conjuntos de IP.

2. Haga clic en **Editar** junto al conjunto de IP que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración del conjunto de IP. Para obtener una descripción de la configuración, consulte las instrucciones para crear un conjunto de IP.

4. Haga clic en **Guardar**.

   El conjunto de IP se modificará y actualizará en la tabla.

5. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

## Eliminar un conjunto de direcciones IP

Puede eliminar un conjunto de direcciones IP en una plantilla de firewall o en un dispositivo CPE. Los conjuntos de direcciones IP eliminados en una plantilla de firewall se eliminan automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

Los conjuntos de direcciones IP eliminados no se pueden restaurar.

*Para eliminar un conjunto de direcciones IP:*

1. Elimine un conjunto de direcciones IP de una de las siguientes maneras:

   - Si desea eliminar un conjunto de direcciones IP en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla del firewall y seleccione la pestaña **Conjuntos de direcciones IP**.

   - Si desea eliminar un conjunto de direcciones IP en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → Conjuntos de direcciones IP** y la casilla **Anular**.

   Se muestra una tabla de conjuntos de IP.

2. Haga clic en **Eliminar** junto al conjunto de direcciones IP que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El conjunto de direcciones IP se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Administrar reglas DNAT

Puede ver la tabla de reglas DNAT en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de reglas DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN→ Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT→ DNAT**.

- Para ver la tabla de reglas DNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall → NAT → DNAT**.

La información sobre las reglas DNAT se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la regla DNAT.
- **Entrante** contiene los criterios según los cuales el firewall aplica la regla DNAT a los paquetes de tráfico:
- **Redirección** es la dirección IP de destino y el puerto de los paquetes de tráfico después de que se aplica la regla DNAT.

# Crear una regla DNAT

Puede crear una regla DNAT en una plantilla de firewall o en un dispositivo CPE. Una regla DNAT creada en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para crear una regla DNAT, siga estos pasos:*

1. Cree una regla DNAT de una de las siguientes maneras:
   - Si desea crear una regla DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → DNAT**.
   - Si desea crear una regla DNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → DNAT** y seleccione la casilla **Anular**.

   Se muestra una tabla de reglas DNAT.
2. Haga clic en **+ DNAT**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la regla DNAT. La longitud máxima del nombre es de 255 caracteres.
4. Especifique los criterios según los cuales el firewall debe aplicar la regla DNAT a los paquetes de tráfico:
   a. En la lista desplegable **Protocolo**, seleccione el protocolo de paquetes de tráfico al que el firewall aplicará la regla DNAT:
      - **Dirección IP**.
      - **TCP**.
      - **UDP**.
      - **#** para un protocolo personalizado o no estándar. Si selecciona este valor, en el campo **Número de protocolo** que se muestra, ingrese el número de protocolo de acuerdo con el estándar IANA.
   b. En el campo **IP de destino**, ingrese el prefijo o la dirección IPv4 de destino de los paquetes de tráfico a los que el firewall aplica la regla DNAT.
   c. Si desea aplicar la regla DNAT solo al tráfico de paquetes con la zona de firewall de origen especificada, en la lista desplegable **Zona de origen**, seleccione una zona de firewall creada del origen.

d. Si en la lista desplegable **Protocolo**, seleccionó **TCP** o **UDP** y desea aplicar la regla DNAT solo a los paquetes de tráfico con el puerto de destino especificado, ingrese el número de puerto de destino en el campo **Puerto de destino**. Rango de valores: de 1 a 65 535.

e. Si desea aplicar la regla DNAT solo al tráfico de paquetes con el prefijo o la dirección IPv4 de origen especificado, en el campo **IP de origen**, ingrese la dirección IPv4 de origen o el prefijo.

5. Especifique cómo la regla DNAT modifica los paquetes de tráfico:

   a. En el campo **IP de destino**, ingrese un nuevo prefijo o dirección IPv4 de destino.

   b. En la lista desplegable **Zona de destino**, seleccione la nueva zona de firewall de destino.

   c. Si en la lista desplegable **Protocolo**, seleccionó **TCP** o **UDP** y desea cambiar el número de puerto de destino de los paquetes de tráfico, ingrese un nuevo número de puerto de destino en el campo **Puerto de destino**. Rango de valores: de 1 a 65 535.

6. Haga clic en **Crear**.

   La regla DNAT se crea y se muestra en la tabla.

7. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Configurar el orden de las reglas DNAT

Las reglas DNAT se aplican a los paquetes de tráfico en orden descendente, comenzando con la primera regla DNAT en la parte superior de la tabla. De manera predeterminada, las reglas DNAT se muestran en la tabla en el orden de creación. Cuanto antes se creó una regla DNAT, más arriba se muestra en la tabla.

Puede configurar el orden en el que se aplican las reglas DNAT en una plantilla de firewall o en un dispositivo CPE. El orden en el que se aplican las reglas DNAT, que se especifica en la plantilla de firewall, se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para configurar el orden en el que se aplican las reglas DNAT:*

1. Edite el orden en el que se aplican las reglas DNAT de una de las siguientes maneras:

   - Si desea configurar el orden en el que se aplican las reglas DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT**→ **DNAT**.

   - Si desea configurar el orden en el que se aplican las reglas DNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall**→ **NAT**→ **DNAT** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de reglas DNAT.

2. Configure el orden en que se aplican las reglas DNAT haciendo clic en los botones **Arriba** y **Abajo**.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Deshabilitar o habilitar una regla DNAT

Puede deshabilitar o habilitar una regla DNAT en una plantilla de firewall o en un dispositivo CPE. Una regla DNAT habilitada o deshabilitada en una plantilla de firewall se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para deshabilitar o habilitar una regla DNAT, siga estos pasos:*

1. Deshabilite o habilite una regla DNAT de una de las siguientes maneras:

   - Si desea deshabilitar o habilitar una regla DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y, en el área de configuración que se muestra, seleccione la pestaña **NAT→ DNAT**.

   - Si desea deshabilitar o habilitar una regla DNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y, en el área de configuración que se muestra, seleccione la pestaña **Firewall→ NAT→ DNAT** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de reglas DNAT.

2. Haga clic en **Deshabilitar** o **Habilitar** junto a la regla DNAT que desea deshabilitar o habilitar.

   La regla DNAT se habilita o deshabilita.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Editar una regla DNAT

Puede editar una regla DNAT en una plantilla de firewall o en un dispositivo CPE. Las reglas DNAT modificadas en una plantilla de firewall se modifican automáticamente en todos los dispositivos CPE que utilizan esta plantilla.

*Para editar una regla DNAT:*

1. Edite una regla DNAT de una de las siguientes maneras:

   - Si desea editar una regla DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla del firewall y seleccione la pestaña **NAT → DNAT**.

   - Si desea editar una regla DNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → DNAT** y la casilla **Anular**.

   Se muestra una tabla de reglas DNAT.

2. Haga clic en **Editar** junto a la regla DNAT que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración de la regla DNAT. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla DNAT.

4. Haga clic en **Guardar**.

   La regla DNAT se modifica y se actualiza en la tabla.

5. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

## Eliminar una regla DNAT

Puede eliminar una regla DNAT en una plantilla de firewall o en un dispositivo CPE. Una regla DNAT eliminada en una plantilla de firewall se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

Las reglas DNAT eliminadas no se pueden restaurar.

*Para eliminar una regla DNAT:*

1. Elimine una regla DNAT de una de las siguientes maneras:

   - Si desea eliminar una regla DNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → DNAT**.
   - Si desea eliminar una regla DNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → DNAT** y seleccione la casilla **Anular**.

   Se muestra una tabla de reglas DNAT.

2. Haga clic en **Eliminar** junto a la regla DNAT que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La regla DNAT se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Administrar reglas de SNAT

Puede ver la tabla de reglas SNAT en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de reglas SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → SNAT**.
- Para ver la tabla de grupos de reglas SNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo, seleccione la pestaña **Firewall → NAT → SNAT** y seleccione la casilla **Anular**.

La información sobre las reglas SNAT se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la regla SNAT.
- **Saliente** son criterios según los cuales el firewall aplica la regla SNAT a los paquetes de tráfico.
- **Acción** es la acción que la regla SNAT aplica a los paquetes de tráfico.

# Crear una regla SNAT

Puede crear una regla SNAT en una plantilla de firewall o en un dispositivo CPE. Una regla SNAT creada en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para crear una regla SNAT:*

1. Cree una regla SNAT de una de las siguientes maneras:
   - Si desea crear una regla SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → SNAT**.
   - Si desea crear una regla SNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → SNAT** y seleccione la casilla **Anular**.

   Se muestra una tabla de reglas SNAT.
2. Haga clic en **+ SNAT**.
3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la regla SNAT. La longitud máxima del nombre es de 255 caracteres.
4. Especifique los criterios según los cuales el firewall debe aplicar la regla SNAT a los paquetes de tráfico:
   a. En la lista desplegable **Protocolo**, seleccione el protocolo de paquetes de tráfico al que el firewall aplicará la regla SNAT:
      - **TCP**.
      - **UDP**.
      - **IP**.
   b. En la lista desplegable **Zona de destino**, seleccione la zona de firewall de destino creada de los paquetes de tráfico a los que el firewall aplica la regla SNAT.
   c. Si desea aplicar la regla SNAT solo al tráfico de paquetes con la dirección IPv4 o el prefijo de origen especificados, en el campo **IP de origen**, ingrese la dirección IPv4 o el prefijo de origen.
   d. Si desea aplicar la regla SNAT solo al tráfico de paquetes con la dirección IPv4 de destino o el prefijo especificado, en el campo **IP de destino**, ingrese la dirección IPv4 o el prefijo de destino.
5. En la lista desplegable **Acción**, seleccione **SNAT**.
6. En el campo **IP de SNAT**, ingrese una nueva dirección IP de origen o un prefijo que la regla SNAT especifica para los paquetes de tráfico.

7. Haga clic en **Crear**.

   La regla SNAT se crea y se muestra en la tabla.

8. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Configurar el orden de las reglas SNAT

Las reglas SNAT se aplican a los paquetes de tráfico en orden descendente, comenzando con la primera regla SNAT en la parte superior de la tabla. De manera predeterminada, las reglas SNAT se muestran en la tabla en el orden de creación. Cuanto antes se haya creado una regla SNAT, más arriba se mostrará en la tabla.

Puede configurar el orden en el que se aplican las reglas SNAT en una plantilla de firewall o en un dispositivo CPE. El orden en el que se aplican las reglas SNAT, que se especifica en la plantilla de firewall, se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para configurar el orden en el que se aplican las reglas SNAT, siga estos pasos:*

1. Edite el orden en el que se aplican las reglas SNAT de una de las siguientes maneras:

   - Si desea configurar el orden en el que se aplican las reglas SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT→ SNAT**.

   - Si desea configurar el orden en el que se aplican las reglas SNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall→ NAT→ SNAT** y marque la casilla de verificación **Anular**.

   Se muestra una tabla de reglas SNAT.

2. Configure el orden en el que se aplican las reglas SNAT haciendo clic en los botones **Arriba** y **Abajo**.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Deshabilitar o habilitar una regla SNAT

Puede deshabilitar o habilitar una regla SNAT en una plantilla de firewall o en un dispositivo CPE. Una regla SNAT habilitada o deshabilitada en una plantilla de firewall se habilita o deshabilita automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para deshabilitar o habilitar una regla SNAT, siga estos pasos:*

1. Deshabilite o habilite una regla SNAT de una de las siguientes maneras:

   - Si desea habilitar o deshabilitar una regla SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT→ SNAT**.

   - Si desea habilitar o deshabilitar una regla SNAT en un dispositivo CPE, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall→ NAT→ SNAT** y marque la casilla de verificación **Anular**.

Se muestra una tabla de reglas SNAT.

2. Haga clic en **Deshabilitar** o **Habilitar** junto a la regla SNAT que desea deshabilitar o habilitar.

   La regla SNAT se deshabilita o habilita.

3. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Editar una regla SNAT

Puede editar una regla SNAT en una plantilla de firewall o en un dispositivo CPE. Una regla SNAT modificada en una plantilla de firewall se modifica automáticamente en todos los dispositivos CPE que utilizan esta plantilla de firewall.

*Para editar una regla SNAT, siga estos pasos:*

1. Edite una regla SNAT de una de las siguientes maneras:

   - Si desea editar una regla SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → SNAT**.

   - Si desea editar una regla SNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → SNAT** y seleccione la casilla **Anular**.

   Se muestra una tabla de reglas SNAT.

2. Haga clic en **Editar** junto a la regla SNAT que desea editar.

3. En la ventana; que se abre, si es necesario, edite la configuración de la regla SNAT. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla SNAT.

4. Haga clic en **Guardar**.

   La regla SNAT se modifica y se muestra en la tabla.

5. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Eliminar una regla SNAT

Puede eliminar una regla SNAT en una plantilla de firewall o en un dispositivo CPE. Una regla SNAT eliminada en una plantilla de firewall se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

Las reglas SNAT eliminadas no se pueden restaurar.

*Para eliminar una regla SNAT, siga estos pasos:*

1. Elimine una regla SNAT de una de las siguientes maneras:

   - Si desea eliminar una regla SNAT en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **NAT → SNAT**.

   - Si desea eliminar una regla SNAT en un dispositivo CPE, vaya a la sección de menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall → NAT → SNAT** y seleccione la casilla **Anular**.

   Se muestra una tabla de reglas SNAT.

2. Haga clic en **Eliminar** junto a la regla SNAT que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La regla SNAT se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Administrar un reenvío

Puede ver la tabla de reenvíos en una plantilla de firewall o en un dispositivo CPE:

- Para ver la tabla de reenvíos en una plantilla de firewall, vaya a la sección del menú **SD-WAN → Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reenvío de zona**.

- Para ver la tabla de reenvíos en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Firewall → Reenvío de zona**.

La información sobre los reenvíos se muestra en las siguientes columnas de la tabla:

- **Remitente** es la zona de firewall de salida.

- **Destinatario** es la zona de firewall de entrada.

# Crear un reenvío

Puede crear un reenvío en una plantilla de firewall o en un dispositivo CPE. Un reenvío creado en una plantilla de firewall se crea automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

*Para crear un reenvío, haga lo siguiente:*

1. Cree un reenvío de una de las siguientes maneras:

   - Si desea crear un reenvío en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reenvío de zona**.

   - Si desea crear un reenvío en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** → **Reenvío de zona** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de reenvíos.

2. Haga clic en **+ Reenvío**.

3. En la ventana que se abre, en la lista desplegable **Remitente**, seleccione una zona de firewall creada.

4. En la lista desplegable **Destinatario**, seleccione una zona de firewall entrante creada.

5. Haga clic en **Crear**.

   El reenvío se creará y se mostrará en la tabla.

6. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Eliminar un reenvío

Puede eliminar un reenvío en una plantilla de firewall o en un dispositivo CPE. Un reenvío eliminado en una plantilla de firewall se elimina automáticamente en todos los dispositivos CPE que usan esta plantilla de firewall.

Los reenvíos eliminados no se pueden restaurar.

*Para eliminar un reenvío, siga estos pasos:*

1. Elimine un reenvío de una de las siguientes maneras:

   - Si desea eliminar un reenvío en una plantilla de firewall, vaya a la sección del menú **SD-WAN** → **Plantillas de firewall**, haga clic en la plantilla de firewall y seleccione la pestaña **Reenvío de zona**.

   - Si desea eliminar un reenvío en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Firewall** → **Reenvío de zona** y seleccione la casilla de verificación **Anular**.

   Se muestra una tabla de reenvíos.

2. Haga clic en **Eliminar** junto al reenvío que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El reenvío se elimina y ya no se muestra en la tabla.

4. En la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de firewall o dispositivo CPE.

# Cambiar la plantilla de firewall de un dispositivo CPE

Editar una plantilla de firewall de un dispositivo CPE puede provocar la pérdida de comunicación con otros dispositivos CPE, así como la pérdida de los paquetes de tráfico retransmitidos.

*Para cambiar la plantilla de firewall de un dispositivo CPE, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → CPE**.

   Se muestra una tabla de dispositivos CPE.

2. Haga clic en el dispositivo CPE para el que desea cambiar la plantilla de firewall.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, en el menú de la izquierda, se selecciona la sección **Configuración**, que muestra información general sobre el dispositivo CPE. En esta sección también se muestra la tabla de tareas **Administración fuera de banda** que está realizando el orquestador.

3. En la lista desplegable **Plantilla de firewall**, seleccione una plantilla de firewall creada.

4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del dispositivo CPE.

# Integración con herramientas de seguridad de la información externas

Puede integrar una herramienta de seguridad de la información externa con Kaspersky SD-WAN para la administración externa de reglas de firewall avanzadas mediante la API del orquestador. Para integrar herramientas de seguridad de la información externas, cree un usuario local con el rol especial **Restricted-API-extern-ISU**, cuyos permisos se limitan a llamar a operaciones de API diseñadas específicamente para administrar reglas de firewall avanzadas. Un mecanismo de etiquetas de directiva permite habilitar o deshabilitar las reglas de firewall avanzadas como grupos. Al crear reglas de firewall avanzadas, puede asignarles etiquetas de directiva y luego habilitar o deshabilitar todas las reglas que tienen una etiqueta determinada al mismo tiempo.

Ejemplo del uso de etiquetas:
Un usuario crea las siguientes reglas avanzadas en una plantilla de firewall:

1. Denegar el acceso de la subred del usuario a la subred del servidor de producción con la etiqueta `"user-subnet-compromised"`.

2. Permitir el acceso desde la subred del usuario a todas las subredes del servidor.
   La regla 1 tiene una etiqueta, y la etiqueta aún no se implementó; por lo tanto, la regla 1 está deshabilitada y los usuarios pueden acceder a todas las subredes con servidores, incluidos los servidores de producción.
   Luego, cada vez que se detectan indicadores de vulneración para cualquier estación de trabajo en la subred del usuario, una herramienta de análisis externa (por ejemplo, FortiNet NDR o Kaspersky XDR) llama a la API del orquestador para activar las etiquetas que tienen la etiqueta `"user-subnet-compromised"`.
   El orquestador habilita la regla 1 en la directiva, y todos los dispositivos CPE a los que se aplica esta directiva tienen habilitada esta regla. Como resultado, se bloquea el acceso de los usuarios a la subred del servidor de producción.

## Descripción de la API

Las llamadas a la API deben contar con autenticación y autorización.

La autenticación se realiza en tres pasos:

1. Realice una solicitud `GET` a `/api/core/users/current`, reciba una respuesta vacía con el estado `200/OK` con un encabezado que incluya el archivo cookie `CSRF-TOKEN`.

2. Para una autenticación posterior, realice una solicitud `POST` a `/api/authentication`, pasando los campos `j_username` (nombre de usuario) y `j_password` (contraseña de usuario) en el cuerpo de la solicitud, y pasando el token obtenido en el paso anterior en el encabezado `X-CSRF-TOKEN`.

3. Para llamadas de API posteriores, el token CSRF debe actualizarse al crear una solicitud `GET` a `/api/core/settings/defpage` y recibir una respuesta `200/OK` con el nuevo valor del archivo cookie `CSRF-TOKEN`.

La autorización se realiza en función del rol de la cuenta de usuario **Restricted-API-extern-ISU**. Los usuarios con este rol solo tienen acceso a las operaciones de la API para herramientas de seguridad de la información externas. Los usuarios con otros roles no tienen acceso a estas operaciones de la API.

La API para herramientas de seguridad de la información externa incluye las siguientes operaciones:

| Método | Endpoint | Descripción |
|---|---|---|
| `GET` | `/api/nfv/sdwan/externalTools/rules` | Obtener la configuración de las reglas de firewall para una plantilla de firewall o dispositivo CPE |
| `POST` | `/api/nfv/sdwan/externalTools/rules` | Crear una regla de firewall de una herramienta de seguridad de la información externa |
| `DELETE` | `/api/nfv/sdwan/externalTools/rules` | Eliminar una regla de firewall de una herramienta de seguridad de la información externa por nombre de regla |
| `GET` | `/api/nfv/sdwan/externalTools/policyTags` | Obtener todas las etiquetas de directiva para el inquilino actual |
| `PUT` | `/api/nfv/sdwan/externalTools/policyTags` | Actualizar estado de la etiqueta de la directiva |
| `POST` | `/api/nfv/sdwan/externalTools/policyTags` | Crear etiqueta de directiva |
| `DELETE` | `/api/nfv/sdwan/externalTools/policyTags` | Eliminar etiqueta de directiva |

Para obtener más información acerca de los métodos, consulte la descripción de la API del orquestador.

# Administrar servicios de red y virtualización de funciones de la red

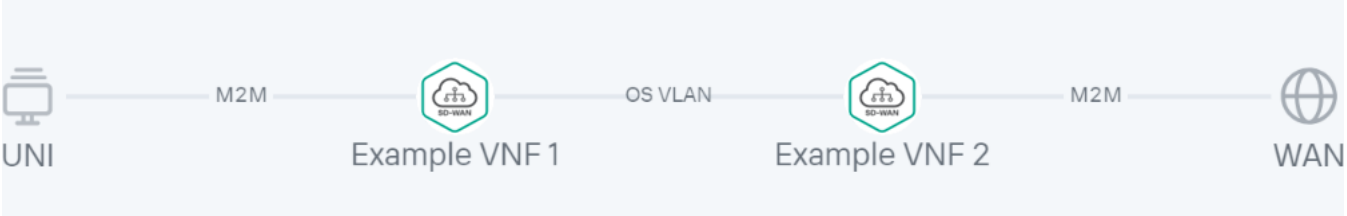
## Servicios de red

Los *servicios de red* retransmiten el tráfico a través de la red y aplican funciones de red al tráfico, como la optimización, el modelado y la protección de tráfico de WAN. Cada servicio de red tiene una topología que se crea con una herramienta de diseño gráfico. Puede agregar componentes de servicio de red a la topología y establecer una conexión entre ellos.

Puede crear una topología en una plantilla de servicio de red y luego asignar esa plantilla de servicio de red a un inquilino. Los componentes del servicio de red agregados a la topología de la plantilla se asignan automáticamente al inquilino junto con la plantilla del servicio de red. Un inquilino puede crear e implementar servicios de red, si es necesario, utilizando plantillas de servicio de red asignadas y editar servicios de red.

Puede utilizar los servicios de red para implementar instancias SD-WAN. El servicio de red para implementar instancias SD-WAN se denomina servicio de red SD-WAN (servicio SD-WAN).

En la siguiente figura se muestra un ejemplo de una topología de servicio de red.




Topología de servicio de red

## Virtualización de funciones de red

La virtualización de funciones *de red* (NFV) le permite usar almacenamiento virtualizado, recursos informáticos y redes para proporcionar funciones de red y combinarlas en servicios de red.

Puede implementar funciones de red virtual (VNF) y funciones de red física (PNF) en servicios de red. La diferencia entre las funciones de red física y virtual es que el orquestador no administra el ciclo de vida de las funciones de red física. Se admiten funciones de red de terceros.

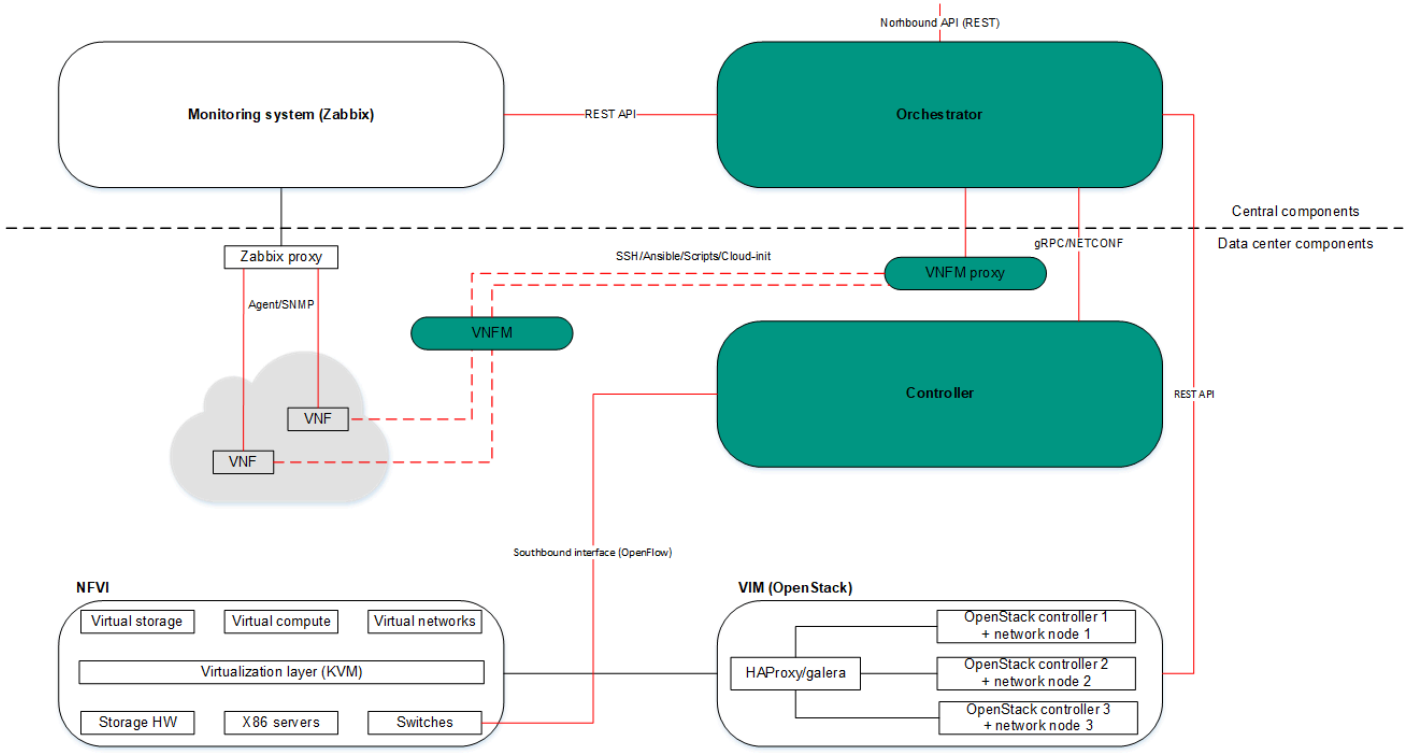
Kaspersky SD-WAN cumple con la arquitectura especificada en la especificación ETSI NFV MANO (Administración y orquestación de la virtualización de funciones de la red), que define los siguientes componentes funcionales principales:

- Orchestrator.
- Administradores de funciones de red virtual (VNFM).
- Administrador de infraestructura virtual.
- El sistema de supervisión Zabbix supervisa el estado de las funciones de la red virtual y las funciones de la red física y notifica al orquestador cuando una función de red necesita ser restaurada o escalada.

- La infraestructura de NFV abarca recursos físicos, como almacenamiento de hardware, servidores y dispositivos de red.

- Controlador.

La siguiente figura muestra las relaciones entre los componentes de la solución y la infraestructura de NFV. Los componentes de las soluciones externas están marcados en blanco, los componentes de Kaspersky SD-WAN están marcados en verde y las líneas rojas son conexiones entre componentes.




Infraestructura NFV

# Administrar plantillas de servicios de red

Puede ver la lista de plantillas de servicios de red en el portal del administrador en la sección **Catálogo**, en el panel **Catálogo**. Para ver información sobre los componentes del servicio de red disponibles, haga clic en el ícono de implementación ». Se muestran las siguientes subsecciones:

- La pestaña **Plantillas** contiene plantillas de servicios de red. La información sobre las plantillas de servicios de red se muestra en las siguientes columnas de la tabla:

  - **Nombre** es el nombre de la plantilla de servicios de red.

  - **Autoría** es el nombre del usuario que creó la plantilla de servicio de red.

  - **Fecha de creación** es la fecha y la hora en que se creó la plantilla de servicio de red.

  - **Descripción** es una breve descripción de la plantilla de servicio de red.

- **Servicios de red compartidos** es una lista de servicios de red compartidos.

- **Funciones de red virtual** es una tabla de funciones de la red virtual. La información sobre las funciones de la red virtual se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la función de la red virtual.
  - **Proveedor** es el proveedor de la función de la red virtual. Puede especificar el proveedor de la función de la red virtual mediante el parámetro `provider` en el descriptor de VNF.
  - **Versión** es la versión de la función de la red virtual. Puede especificar la versión de la función de la red virtual mediante el parámetro `version` en el descriptor de VNF.
  - **Descripción** es la descripción breve de la función de la red virtual. Puede especificar una descripción de la función de la red virtual mediante el parámetro `description` en el descriptor VNF.
- **Funciones de red física** es la tabla de funciones de la red física. La información sobre las funciones de la red física se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la función de la red física.
  - **Proveedor** es el proveedor de la función de la red física. Puede especificar el proveedor de la función de la red física mediante el parámetro `provider` en el descriptor PNF.
  - **Versión** es la versión de la función de la red física. Puede especificar la versión de la función de la red física mediante el parámetro `version` en el descriptor PNF.
  - **Descripción** es la descripción breve de la función de la red física. Puede especificar una descripción de la función de la red física mediante el parámetro `description` en el descriptor PNF.

# Crear una plantilla de servicio de red

*Para crear una plantilla de servicio de red, haga lo siguiente:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En la parte superior de la página, haga clic en **+ Plantilla**.

   Se muestra la herramienta de diseño gráfico para crear la topología.

3. Agregue los componentes del servicio de red a la topología:

   a. Arrastre los componentes del servidor de la red desde el panel **Catálogo** hacia la herramienta de diseño gráfico. En el panel, se muestran los siguientes componentes del servicio de red:

      - Plantillas del servicio de red: cuando se agrega una plantilla del servicio de red a una topología, la topología se construye de acuerdo con la plantilla del servicio de red. Puede agregar varias plantillas del servicio de red a la topología.
      - Servicios de red compartidos: debe agregar un servicio de red compartido a la topología de los servicios de red que desea conectar al servicio de red compartido. Puede especificar una breve descripción del servicio de red compartido.
      - Funciones de la red virtual y física. Las acciones que puede realizar en las funciones de la red virtual y física se describen en las secciones Administrar las funciones de la red virtual y Administrar las funciones de la red física.

   b. Arrastre y suelte los vínculos desde la pestaña **Enlaces** hacia la herramienta de diseño gráfico. En esta pestaña, se muestran los siguientes vínculos:

      - **P2P** es un servicio de transporte de punto a punto (servicio P2P). Puede configurar un servicio P2P.
      - **P2M** es un servicio de transporte de punto a multipunto (servicio P2M). Puede configurar un servicio P2M.
      - **M2M** es un servicio de transporte de multipunto a multipunto (servicio M2M). Puede configurar un servicio M2M.

      Los vínculos restantes son pertinentes para la comunicación de red a nivel del VIM y se establecen entre las VNF alojadas en la plataforma de nube OpenStack:

      - **SO compartido** es la red compartida a través de la cual el servicio de red compartido se conecta a los servicios de red. Puede configurar una red compartida.
      - **Enrutador virtual del SO** es el enrutador virtual L3. Puede configurar un enrutador virtual.
      - **VLAN del SO** es la VLAN para la transmisión del tráfico L2 etiquetado del estándar 802.1Q. Puede configurar una VLAN.
      - **VXLAN del SO** es una VXLAN para la tunelización. Puede configurar una VXLAN.
      - **Red plana del SO** es la red plana para la transmisión del tráfico L2 sin etiquetar. Puede configurar una red plana.

   c. Seleccione la pestaña **UNI** y arrastre las UNI del dispositivo CPE a la herramienta de diseño gráfico. En la pestaña, se muestran dos componentes: **UNI** y **WAN**. Ambos componentes designan UNI abstractas que el inquilino debe reemplazar con las UNI reales cuando cree o edite un servicio de red. El componente **WAN** se refiere a las UNI que se conectan a la WAN.

      Puede configurar una UNI en la topología.

Los componentes del servicio de red se agregan a la topología y se muestran en la herramienta de diseño gráfico.

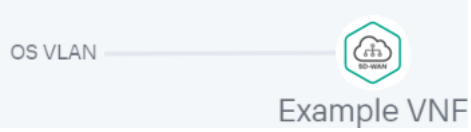
4. Conecte los componentes del servicio de red agregados a la topología entre sí:

   a. Haga clic en el vínculo al que desea conectar un componente del servicio de red.

   b. Haga clic en **Agregar hoja** para conectar un componente del servicio de red con el rol de hoja al vínculo. Si hizo clic en un servicio P2M, puede hacer clic en **Agregar raíz** para conectar el componente del servicio de red con el rol raíz al vínculo.

   c. Haga clic en el componente del servicio de red que desea conectar al vínculo. Si hizo clic en una función de red o en un servicio de red compartido, seleccione el puerto al que hay que conectar el vínculo en la ventana que se muestra.

   El componente del servicio de red está conectado al vínculo, y se muestra una línea entre ellos en la topología. Por ejemplo, en la siguiente imagen, se muestra la VLAN a la que está conectada una función de la red virtual.




5. Si desea asignar UNI de respaldo, haga lo siguiente:

   > Una UNI de respaldo solo se puede asignar para las UNI que están conectadas como mínimo a un vínculo.

   a. Haga clic en la UNI para la que desea asignar una UNI de respaldo.

   b. Haga clic en **Reservar**.

   c. Haga clic en la UNI que desea usar como respaldo.

   La UNI se designa como la UNI de respaldo, y se muestra una línea de puntos entre la UNI, la UNI de respaldo y el vínculo al que está conectada la UNI. Por ejemplo, en la siguiente imagen, la WAN es la interfaz de respaldo para la UNI.

6. Si desea quitar un componente del servicio de red de la topología, haga clic en el componente y, luego, haga clic en **Eliminar**.

   El componente del servicio de red se quita de la topología y ya no se muestra en la herramienta de diseño gráfico.

7. Si desea alinear la topología horizontalmente, haga clic en **Organizar**.

8. Si no desea ocultar las descripciones de los componentes del servicio de red agregados en la topología, desmarque la casilla de verificación **Descripción**. Esta casilla está seleccionada por defecto.

9. En el campo **Nombre**, ingrese el nombre del servicio de red.
10. En la parte superior de la herramienta de diseño gráfico, haga clic en **Guardar**.

Se crea la plantilla del servicio de red y se muestra en el panel **Catálogo**, en la pestaña **Plantillas**.

# Editar una plantilla de servicio de red

Cuando edita una plantilla de servicio de red, los cambios no se aplican a los servicios de red que ya se crearon e implementaron con la plantilla de servicio de red.

*Para editar una plantilla de servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.
2. En el panel **Catálogo**, seleccione la pestaña **Plantillas**.

   Se muestra una lista de plantillas de servicio de red.
3. Haga clic en la plantilla de servicio de red que desea editar.

   Se muestra la herramienta de diseño gráfico para crear la topología.
4. Si es necesario, edite la configuración de la plantilla de servicio de red. Para obtener una descripción de la configuración, consulte las instrucciones para crear una plantilla de servicio de red.
5. En la parte superior de la herramienta de diseño gráfico, haga clic en **Guardar**.

La plantilla de servicio de red se modifica y actualiza en el panel **Catálogo**, en la pestaña **Plantillas**.

# Eliminar una plantilla de servicio de red

Las plantillas de servicio de red eliminadas no se pueden restaurar.

*Para eliminar una plantilla de servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.
2. En el panel **Catálogo**, seleccione la pestaña **Plantillas**.

   Se muestra una lista de plantillas de servicio de red.
3. Haga clic en el ícono de eliminar ✕ junto a la plantilla de servicio de red que desea eliminar.
4. En la ventana de confirmación, haga clic en **Eliminar**.

La plantilla de servicio de red se elimina y ya no se muestra en el panel **Catálogo** de la pestaña **Plantillas**.

# Administrar servicios de red

Antes de administrar los servicios de red, debe iniciar sesión en el portal de autoservicio del inquilino. Puede ver la lista de servicios de red en la sección **Catálogo**, en el panel **Servicios de red**. Para ver información sobre los componentes agregados a la topología del servicio de red, haga clic en el servicio de red y, a continuación, en el panel **Objetos**, haga clic en el ícono de expandir ». Se muestran las siguientes subsecciones:

- **VNF** es una tabla de las funciones de la red virtual. La información sobre las funciones de la red virtual se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la función de la red virtual.
  - **Proveedor** es el proveedor de la función de la red virtual. Puede especificar el proveedor de la función de la red virtual mediante el parámetro `provider` en el descriptor de VNF.
  - **Versión** es la versión de la función de la red virtual. Puede especificar la versión de la función de la red virtual mediante el parámetro `version` en el descriptor de VNF.
  - **Descripción** es la descripción breve de la función de la red virtual. Puede especificar una descripción de la función de la red virtual mediante el parámetro `description` en el descriptor VNF.
  - **Estado** es el estado de la función de la red virtual:
    - **PENDING** significa que se está cambiando el estado de la función de la red virtual.
    - **UNDEPLOYED** significa que la función de la red virtual se agrega a la topología del servicio de red, pero el servicio de red no se implementa.
    - **SCHEDULED** significa que la función de la red virtual se agregó a la topología del servicio de red. Se planifica la implementación de una función de la red virtual en el dispositivo uCPE, pero no hay conexión entre el orquestador y el dispositivo uCPE. El servicio de red se implementará cuando se restablezca la comunicación.
    - **TERMINATING** significa que se está eliminando la función de la red virtual.
    - **RUNNING** significa que la función de la red virtual está funcionando normalmente.
    - **ERROR** significa que ocurrió un error al implementar un servicio de red que tiene la función de la red virtual en su topología.
    - **SCALING** significa que se está cambiando el tipo de función de la red virtual.
    - **HEALING** significa que la función de la red virtual está en curso.
    - **DELETED** significa que la función de la red virtual se eliminó correctamente.
    - **UPDATING** significa que se está modificando el servicio de red que tiene la función de red virtual en su topología.
    - **REPARING** significa que se produjo un error durante la modificación del servicio de red y se están restaurando las configuraciones anteriores del servicio de red.

- **CHECKING** significa que se está realizando una comprobación de consistencia para el servicio de red al que se agrega la función de la red virtual.
- **DEGRADED** significa que la comprobación de consistencia del servicio de red al que se agrega la función de la red virtual reveló la inconsistencia de la función de la red virtual.
- **RECOVERING** significa que la función de la red virtual se está reasignando.

- **Corrección automática** contiene información sobre si la configuración de reparación automática de VDU se especifica en la sección de `reparación automática` del paquete VNF:
  - **Sí**.
  - **No**.
- **Escalado automático** contiene información sobre si la configuración de escalado de la función de la red virtual se especifica en la sección de `escalado` del paquete VNF:
  - **Sí**.
  - **No**.

- **Funciones de red física** es la tabla de funciones de la red física. La información sobre las funciones de la red física se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la función de la red física.
  - **Proveedor** es el proveedor de la función de la red física. Puede especificar el proveedor de la función de la red física mediante el parámetro `provider` en el descriptor PNF.
  - **Versión** es la versión de la función de la red física. Puede especificar la versión de la función de la red física mediante el parámetro `version` en el descriptor PNF.
  - **Descripción** es la descripción breve de la función de la red física. Puede especificar una descripción de la función de la red física mediante el parámetro `description` en el descriptor PNF.
  - **Estado** es el estado de la función de la red física:
    - **PENDING** significa que se está cambiando el estado de la función de la red física.
    - **UNDEPLOYED** significa que la función de la red física se agrega a la topología del servicio de red, pero el servicio de red no se implementa.
    - **TERMINATING** significa que se está eliminando la función de la red física.
    - **RUNNING** significa que la función de la red física está funcionando normalmente.
    - **ERROR** significa que se produjo un error durante la implementación de un servicio de red que tiene la función de la red física en su topología.
    - **SCALING** significa que se está cambiando el tipo de función de la red física.
    - **HEALING** significa que la función de la red física está en curso.
    - **DELETED** significa que la función de la red física se eliminó correctamente.

- **UPDATING** significa que se está modificando el servicio de red que tiene la función de la red física en su topología.
- **REPARING** significa que se produjo un error durante la modificación del servicio de red y se están restaurando las configuraciones anteriores del servicio de red.
- **CHECKING** significa que se está realizando una comprobación de consistencia para el servicio de red al que se agrega la función de la red física.
- **DEGRADED** significa que la comprobación de consistencia del servicio de red al que se agrega la función de la red física reveló la inconsistencia de la función de la red física.
- **RECOVERING** significa que se está reasignando la función de la red física.

- **Corrección automática** contiene información sobre si la configuración de reparación automática se especifica en la sección de `reparación automática` del paquete PNF:
  - **Sí**.
  - **No**.
- **Escalado automático** contiene información sobre si la configuración de escalado de la función de la red física se especifica en la sección de `escalado` del paquete PNF:
  - **Sí**.
  - **No**.

- **Servicio de red compartido** es una lista de servicios de red compartidos.
- **Enlaces** es una tabla de vínculos. La información sobre los vínculos se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre del vínculo.
  - **Tipo** es el tipo de vínculo.
  - **Estado** es el estado del vínculo:
    - **NONE** significa que una comprobación de consistencia del servicio de red al que se agregó el vínculo reveló que el vínculo no existe.
    - **OK** significa que una comprobación de consistencia del servicio de red al que se agregó el vínculo reveló que el vínculo existe.
  - **Compartido** indica si la conexión se está utilizando para crear un servicio de red compartido:
    - **Sí**.
    - **No**.
- **UNI** es una tabla de UNI. La información sobre las UNI se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la UNI.
  - **Alias** es el nombre de la UNI en el momento de agregarse a la topología del servicio de red.

- **Estado** es el estado de la UNI:
  - **NONE** significa que una comprobación de consistencia del servicio de red al que se agregó la UNI reveló que la UNI no existe.
  - **OK** significa que una comprobación de consistencia del servicio de red al que se agregó la UNI revela que la UNI existe.

# Crear un servicio de red

*Para crear un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En la parte superior del panel **Servicios de red**, haga clic en **+ Servicio de red**.

   Se muestra la herramienta de diseño gráfico para crear la topología.

3. Agregue los componentes del servicio de red a la topología:

   a. Arrastre los componentes del servidor de la red desde el panel **Catálogo** hacia la herramienta de diseño gráfico. En el panel, se muestran los siguientes componentes del servicio de red:

   - Plantillas del servicio de red: cuando se agrega una plantilla del servicio de red a una topología, la topología se construye de acuerdo con la plantilla del servicio de red. Puede agregar varias plantillas del servicio de red a la topología.
   - Servicios de red compartidos: debe agregar un servicio de red compartido a la topología de los servicios de red que desea conectar al servicio de red compartido. Puede especificar una breve descripción del servicio de red compartido.
   - Funciones de la red virtual y física. Las acciones que puede realizar en las funciones de la red virtual y física se describen en las secciones Administrar las funciones de la red virtual y Administrar las funciones de la red física.

   b. Arrastre y suelte los vínculos desde la pestaña **Enlaces** hacia la herramienta de diseño gráfico. En esta pestaña, se muestran los siguientes vínculos:

   - **P2P** es un servicio de transporte de punto a punto (servicio P2P). Puede configurar un servicio P2P.
   - **P2M** es un servicio de transporte de punto a multipunto (servicio P2M). Puede configurar un servicio P2M.
   - **M2M** es un servicio de transporte de multipunto a multipunto (servicio M2M). Puede configurar un servicio M2M.

Los vínculos restantes son pertinentes para la comunicación de red a nivel del VIM y se establecen entre las VNF alojadas en la plataforma de nube OpenStack:

- **SO compartido** es la red compartida a través de la cual el servicio de red compartido se conecta a los servicios de red. Puede configurar una red compartida.
- **Enrutador virtual del SO** es el enrutador virtual L3. Puede configurar un enrutador virtual.
- **VLAN del SO** es la VLAN para la transmisión del tráfico L2 etiquetado del estándar 802.1Q. Puede configurar una VLAN.
- **VXLAN del SO** es una VXLAN para la tunelización. Puede configurar una VXLAN.
- **Red plana del SO** es la red plana para la transmisión del tráfico L2 sin etiquetar. Puede configurar una red plana.

c. Seleccione la pestaña **UNI** y arrastre las UNI del dispositivo CPE a la herramienta de diseño gráfico. Si está utilizando una plantilla de servicio de red, debe reemplazar las UNI abstractas en la topología con UNI reales. Las UNI abstractas se pueden designar mediante dos componentes: **UNI** y **WAN**. El componente **WAN** se refiere a las UNI que se conectan a la WAN.

Puede configurar una UNI.

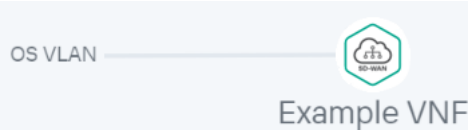
4. Conecte los componentes del servicio de red agregados a la topología entre sí:

a. Haga clic en el vínculo al que desea conectar un componente del servicio de red.

b. Haga clic en **Agregar hoja** para conectar un componente del servicio de red con el rol de hoja al vínculo. Si hizo clic en un servicio P2M, puede hacer clic en **Agregar raíz** para conectar el componente del servicio de red con el rol raíz al vínculo.

c. Haga clic en el componente del servicio de red que desea conectar al vínculo. Si hizo clic en una función de red o en un servicio de red compartido, seleccione el puerto al que hay que conectar el vínculo en la ventana que se muestra.

El componente del servicio de red está conectado al vínculo, y se muestra una línea entre ellos en la topología. Por ejemplo, en la siguiente imagen, se muestra la VLAN a la que está conectada una función de la red virtual.




5. Si desea asignar UNI de respaldo, haga lo siguiente:

Una UNI de respaldo solo se puede asignar para las UNI que están conectadas como mínimo a un vínculo.

a. Haga clic en la UNI para la que desea asignar una UNI de respaldo.

b. Haga clic en **Reservar**.

c. Haga clic en la UNI que desea usar como respaldo.

La UNI se designa como la UNI de respaldo, y se muestra una línea de puntos entre la UNI, la UNI de respaldo y el vínculo al que está conectada la UNI. Por ejemplo, en la siguiente imagen, la WAN es la interfaz de respaldo para la UNI.

6. Si desea quitar un componente del servicio de red de la topología, haga clic en el componente y, luego, haga clic en **Eliminar**.

   El componente del servicio de red se quita de la topología y ya no se muestra en la herramienta de diseño gráfico.

7. Si desea alinear la topología horizontalmente, haga clic en **Organizar**.

8. Si no desea ocultar las descripciones de los componentes del servicio de red agregados en la topología, desmarque la casilla de verificación **Descripción**. Esta casilla está seleccionada por defecto.

9. En el campo **Nombre**, ingrese el nombre del servicio de red.

10. Termine de crear el servicio de red de una de las siguientes maneras:

    - Para guardar el servicio de red, haga clic en **Guardar**.
    - Para guardar e implementar el servicio de red, haga clic en **Implementar**.

El servicio de red se crea y se muestra en el panel **Servicios de red**. Si hizo clic en **Implementar**, comienza la implementación del servicio de red, que puede tardar varios minutos. Puede interrumpir la implementación haciendo clic en **Cancelar implementación**.

# Editar un servicio de red

*Para editar un servicio de red:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, seleccione el servicio de red que desea editar.

   Se muestra la herramienta de diseño gráfico para crear la topología.

3. En la parte superior de la herramienta de diseño gráfico, haga clic en **Editar**.

4. Si es necesario, edite la configuración del servicio de red. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio de red.

5. Termine de editar el servicio de red de una de las siguientes maneras:

   - Si está editando un servicio de red que no está implementado, realice una de las siguientes acciones:

     - Para guardar el servicio de red, haga clic en **Guardar**.

     - Para guardar e implementar el servicio de red, haga clic en **Implementar**.

   - Si está editando un servicio de red implementado, haga clic en **Implementar cambios** para implementar el servicio de red modificado.

   El servicio de red se modifica y actualiza en el panel **Servicios de red**. Si hizo clic en **Implementar** o **Implementar cambios**, comenzará la implementación, que puede tardar varios minutos. Puede interrumpir la implementación haciendo clic en **Cancelar implementación**.

# Implementar servicio de red

Si una función de la red virtual implementada en un dispositivo uCPE se agrega a la topología del servicio de red y hay conexión entre el orquestador y el dispositivo uCPE, el servicio de red se implementa cuando se restaura la conexión.

*Para implementar un servicio de red, haga lo siguiente:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, seleccione el servicio de red que desea implementar.

   Se muestra la herramienta de diseño gráfico para crear la topología.

3. En la parte superior de la herramienta de diseño gráfico, haga clic en **Editar**.

4. Haga clic en **Implementar**.

   Esto inicia la implementación del servicio de red, que puede demorar varios minutos. Puede interrumpir la implementación haciendo clic en **Cancelar implementación**.

# Comprobar la integridad de un servicio de red

La *comprobación de integridad* permite verificar que los componentes que se agregan a la topología del servicio de red realmente existen.

*Para comprobar la integridad de un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el ícono de configuración → **Comprobar consistencia** junto al servicio de red cuya integridad desea verificar.

3. En la ventana de confirmación, haga clic en **Confirmar**.

Esto inicia la comprobación de consistencia del servicio de red.

# Volver a implementar un servicio de red

La redistribución de un servicio de red puede provocar interrupciones a corto plazo o inoperabilidad temporal. Cuando planifica las actividades para volver a implementar el servicio, recomendamos tener en cuenta las circunstancias de su organización para minimizar las interrupciones.

*Para volver a implementar un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el ícono de configuración → **Volver a implementar** junto al servicio de red que desea volver a implementar.

3. En la ventana de confirmación, haga clic en **Confirmar**.

   Se vuelve a implementar el servicio de red, que puede tardar varios minutos. Puede interrumpir la implementación haciendo clic en **Cancelar implementación**.

# Deshabilitar o habilitar la reparación automática para un servicio de red

El servidor Zabbix supervisa los componentes del servicio de red y envía una solicitud de API REST al orquestador cada vez que se detecta un problema. Si la funcionalidad de reparación automática está habilitada para el servicio de red, el orquestador inicia la reparación automática para los componentes del servicio de red que tienen problemas. De manera predeterminada, la función está habilitada.

*Para deshabilitar o habilitar la reparación automática para un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el ícono de configuración → **Deshabilitar corrección automática** o **Habilitar corrección automática** junto al servicio de red para el que desea deshabilitar o habilitar la reparación automática.

La reparación automática se deshabilita o habilita para el servicio de red.

Puede realizar la reparación automática de las funciones de la red virtual o sus VDU incluso si la reparación automática está deshabilitada para el servicio de red.

## Ver el registro de servicios de red

*Para ver el registro de un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el ícono de configuración → **Abrir registro** junto al servicio de red cuyo registro desea ver.

Se muestra la página con el registro del servicio de red.

## Eliminar un servicio de red

Los servicios de red eliminados no se pueden restaurar.

*Para eliminar un servicio de red, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el ícono de configuración → **Eliminar** junto al servicio de red que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

El servicio de red se elimina y ya no se muestra en el panel **Servicios de red**.

# Escenario: implementación de una función de la red virtual

Puede implementar una función de la red virtual para un inquilino en un servicio de red. Un orquestador administra el ciclo de vida de las funciones de la red virtual. Para implementar funciones de la red virtual, necesita la plataforma en la nube de OpenStack.

Por ejemplo, puede implementar una función de la red virtual en la oficina central de su organización para proteger el tráfico de usuarios que se transmite entre dispositivos CPE.

La implementación de la función de la red virtual implica los siguientes pasos:

1. **Preparar un paquete VNF**

   Prepare el paquete VNF que desea implementar y luego cargue el paquete VNF en la interfaz web del orquestador. Si es necesario, puede habilitar la protección de paquetes VNF y PNF contra la sustitución antes de cargar el paquete VNF a la interfaz web del orquestador.

2. **Garantizar la conectividad de la red entre el orquestador y la plataforma en la nube de OpenStack**

   Garantice la conexión de red entre la máquina virtual o el servidor físico donde se implementa el orquestador y la plataforma en la nube de OpenStack.

3. **Asignar la función de la red virtual a un inquilino**

   Utilice uno de los siguientes métodos para asignar la función de la red virtual al inquilino para el que desea implementarla:

   - Si desea implementar una función de la red virtual mediante una plantilla de servicio de red:

     1. Agregue la función de la red virtual a la topología cuando cree o edite una plantilla de servicio de red.
     2. Si es necesario, configure la topología y la función de la red virtual. Para obtener una descripción de lo que puede hacer con las funciones de la red virtual, consulte la sección Administrar funciones de la red virtual.
     3. Asigne la plantilla de servicio de red a un inquilino.

   - Si desea implementar una función de la red virtual sin una plantilla de servicio de red, asigne la función de la red virtual al inquilino.

4. **Iniciar sesión en el portal de autoservicio de inquilinos**

   Inicie sesión en el portal de autoservicio de inquilinos

5. **Implementar la función de la red virtual**

   Haga lo siguiente:

   1. Agregue la función de la red virtual a la topología cuando cree o edite un servicio de red de una de las siguientes maneras:

      - Si desea implementar una función de la red virtual mediante una plantilla de servicio de red, agregue la plantilla de servicio de red a la topología.
      - Si desea implementar una función de la red virtual sin una plantilla de servicio de red, agregue la función de red virtual a la topología.

   2. Si es necesario, configure la topología y la función de la red virtual. Para obtener una descripción de lo que puede hacer con las funciones de la red virtual, consulte la sección Administrar funciones de la red virtual.
   3. Implemente la función de la red virtual mediante uno de los siguientes métodos:

      - Si agregó la función de la red virtual a la topología cuando creó el servicio de red, implemente el servicio de red.
      - Si agregó la función de la red virtual a la topología cuando editó un servicio de red, implemente el servicio de red modificado.

Se implementa la función de la red virtual.

# Escenario: implementación de una función de la red física

Puede implementar una función de la red física para un inquilino en un servicio de red. Como funciones de red física, puede utilizar hardware dedicado, así como entidades virtuales creadas mediante entornos de virtualización de terceros. El orquestador no administra el ciclo de vida de las funciones de red física.

Por ejemplo, puede implementar una función de red física en la oficina central de su organización para proteger el tráfico de usuarios que se transmite entre dispositivos CPE.

La implementación de la función de red física implica los siguientes pasos:

1. **Preparación del paquete PNF**

   Prepare el paquete PNF que desea implementar y luego cargue el paquete PNF en la interfaz web del orquestador. Si es necesario, puede habilitar la protección de paquetes VNF y PNF contra la sustitución antes de cargar el paquete PNF en la interfaz web del orquestador.

2. **Asegurar la conexión de red entre el orquestador y la función de red física**

   Garantizar la conexión de red entre la máquina virtual o el servidor físico en el que se implementa el orquestador y el hardware dedicado o la entidad virtual en el que desea implementar la función de red física.

3. **Asignación de la función de red física a un inquilino**

   Utilice uno de los siguientes métodos para asignar la función de red física al inquilino para el que desea implementarla:

   - Si desea implementar una función de red física mediante una plantilla de servicio de red:

     1. Agregue la función de red física a la topología al crear o editar una plantilla de servicio de red.
     2. Si es necesario, configure la topología y la función de red física. Para obtener una descripción de lo que puede hacer con las funciones de red física, consulte la sección Administración de funciones de red física.
     3. Asigne la plantilla de servicio de red a un inquilino.

   - Si desea implementar una función de red física sin una plantilla de servicio de red, asigne la función de red física al inquilino.

4. **Iniciar sesión en el portal de autoservicio de inquilinos**

   Inicie sesión en el portal de autoservicio de inquilinos

5. **Implementación de una función de red física**

   Haga lo siguiente:

   1. Agregue la función de red física a la topología al crear o editar un servicio de red de una de las siguientes maneras:

      - Si desea implementar una función de red física utilizando una plantilla de servicio de red, agregue la plantilla de servicio de red a la topología.
      - Si desea implementar una función de red física sin una plantilla de servicio de red, agregue la función de red física a la topología.

   2. Si es necesario, configure la topología y la función de red física. Para obtener una descripción de lo que puede hacer con las funciones de red física, consulte la sección Administración de funciones de red física.
   3. Implemente la función de red física mediante uno de los siguientes métodos:

      - Si agregó la función de red física a la topología al crear el servicio de red, implemente el servicio de red.
      - Si agregó la función de red física a la topología mientras editaba un servicio de red, implemente el servicio de red modificado.

Se despliega la función de red física.

# Administrar paquetes VNF y PNF

Un paquete *VNF* o *PNF* es un archivo ZIP en el que debe colocar los siguientes componentes para implementar una función de red y administrar su ciclo de vida:

- El descriptor VNF/PNF, un archivo con parámetros de la función de la red.
- El directorio /image, que contiene imágenes de máquinas virtuales en formato QCOW para implementar la función de la red virtual. Este directorio no está incluido en el paquete PNF.
- El directorio /scripts, que contiene scripts para implementar y administrar la función de la red.
- logo.png, el ícono de la función de la red. Esta información es opcional.
- description-file.pdf, documentación técnica o especificación de la función de la red. Esta información es opcional.

Debe cargar un paquete VNF o PNF a la interfaz web del orquestador para implementar una función de la red virtual o una función de la red física.

# Configurar el descriptor VNF

Especifique la configuración de la función de la red virtual en un descriptor VNF en formato YAML o XML, luego agregue el descriptor VNF al directorio raíz del paquete VNF. Un descriptor VNF tiene la siguiente estructura:

| Sección/configuración | Descripción |
|---|---|
| `name` | Nombre de la función de la red virtual. |
| `description` | Breve descripción de la función de la red virtual. |
| `description_file` | Nombre del archivo PDF con la documentación técnica o especificación de la función de la red virtual. Este archivo debe colocarse en el directorio raíz del paquete VNF. Los usuarios pueden ver y descargar el archivo en la interfaz web del orquestador.<br>Configuración opcional. |
| `provider` | Proveedor de la función de la red virtual. |
| `version` | Versión de la función de la red virtual. |
| `external_connections` | Puntos de conexión externos de la función de la red virtual. Puede configurar los puntos de conexión externos especificados de la función de la red virtual en la interfaz web del orquestador. |
| `internal_connections` | Puntos de conexión internos de las VDU que forman parte de la función de la red virtual.<br>Esta sección es opcional. |
| `virtual_links` | Vínculos virtuales para conectar puntos de conexión internos.<br>Esta sección debe especificarse si especificó la sección `internal_connections`. |
| `images` | Imágenes del disco de VDU. Puede implementar varias VDU con la misma imagen del disco de VDU. |
| `configurations` | Scripts para realizar acciones en varias etapas del ciclo de vida de la función de la red virtual, por ejemplo, durante el despliegue de la función de la red virtual. |
| `flavours` | Tipos de la función de la red virtual. Puede seleccionar uno de los tipos especificados de la función de la red virtual en la interfaz web del orquestador. |

| Sección/configuración | Descripción |
|---|---|
| `scaling` | Parámetros de escalado de la función de la red virtual.<br>Esta sección es opcional. |
| `user_configurations` | Las entradas de la interfaz web del orquestador que se agregan al área de configuración de la función de la red virtual.<br>Esta sección es opcional. |
| `backups` | Tareas de respaldo de la función de la red virtual.<br>Esta sección es opcional. |

### Ejemplo de descriptor de VNF

```
name: OpenWrt18
description: OpenWrt 18.06.1
description_file: openwrt-presentation.pdf
provider: Kaspersky
version: 1.0.1
external_connections:
 - name: LAN
 description: eth1
 ip: AUTO
 mask: AUTO
 group: eth1-group
 - name: WAN
 description: eth2
 ip: AUTO
 mask: AUTO
 group: eth2-group
images:
 - name: openwrt
 container_format: BARE
 disk_format: QCOW2
 type: OPENSTACK
 filename: openwrt-18.06.1-x86-64.qcow2
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 - name: config2
 filename: 3VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
 - name: config3
 filename: 2VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
flavours:
 - name: 2VDU
 description: 1 vCPU, 512MB memory
 position: 1
 affinity:
 groups:
 - name: aff
 vdu_name:
 - OpenWrt
```

```
- OpenWrt2
management:
vnc:
- vdu_name: OpenWrt
ssh:
- vdu_name: OpenWrt
def_user: root
authentication: key
web:
- vdu_name: OpenWrt
vdus:
- name: OpenWrt
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
```

```
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: VDU
description: 1 vCPU, 512MB memory
position: 2
affinity:
groups:
- name: aff
vdu_name:
- OpenWrt
- OpenWrt2
- OpenWrt3
management:
```

```
vnc:
- vdu_name: OpenWrt
ssh:
- vdu_name: OpenWrt
def_user: root
authentication: key
web:
- vdu_name: OpenWrt
vdus:
- name: OpenWrt
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
check_connection_mode: none
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssword
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: OpenWrt2
```

```
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssw0rd
password_authentication: yes
disks:
- name: default
order: 1
type: default
image: openwrt
storage_gb: 1
cpu:
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
- name: OpenWrt3
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
```

```
 - config
 - config2
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 disks:
 - name: default
 order: 1
 type: default
 image: openwrt
 storage_gb: 1
 cpu:
 smt: prefer
 cpu_pinning: dedicated
 num_vpu: 1
 memory:
 total_memory_mb: 512
 network_interfaces:
 - name: Management
 type: management
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
 - type: reprovision
scaling:
 scale_in_status: permit
 scale_out_status: "permit"
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
 - value: out
```

```
 update_configuration_name:
 - update_var
 - change
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
 configuration_name_ref: restore
```

## external_connections

La sección `external_connections` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del punto de conexión externo. |
| | `description` | Breve descripción del punto de conexión externo. |
| | `ip` | Dirección IP del punto de conexión externo. Ingrese un valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126` |
| | `mask` | Máscara de subred del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`255.255.255.0`<br>La máscara de subred se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la máscara de subred no se puede cambiar.<br>• `AUTO`: la máscara de subred se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>• `MANUAL`: la máscara de subred debe especificarse manualmente en la interfaz web del orquestador al configurar los puntos de conexión externos de la función de la red virtual. |
| | `gw` | Dirección IP de la puerta de enlace del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>• `MANUAL`: la dirección IP debe especificarse manualmente en la interfaz web del orquestador al configurar los puntos de conexión externos de la función de la red virtual.<br>Configuración opcional. |
| | `dns` | Dirección IP del servidor DNS del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>• `MANUAL`: la dirección IP debe especificarse manualmente en la interfaz web del orquestador al configurar los puntos de conexión externos de la función de la red virtual.<br>Configuración opcional. |
| | `group` | El grupo al que pertenece el punto de conexión externo.<br>Esta configuración es necesaria si varias VDU dentro de la función de la red virtual usan el mismo punto de conexión externo. |

### Ejemplo de esta sección

```
external_connections:
- name: LAN
 description: eth1
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
```

## `internal_connections`

La sección `internal_connections` tiene la siguiente estructura:

| Sección/configuración | Descripción |
|---|---|
| `- name` | Nombre del punto de conexión interno. |

| | | |
|---|---|---|
| | `description` | Breve descripción del punto de conexión interno. |
| | `virtual_link_name` | Nombre del vínculo virtual de la sección `virtual_links` para el punto de conexión interno. |
| | `ip` | Dirección IP del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>• `MANUAL`: la dirección IP debe especificarse manualmente en la interfaz web del orquestador al configurar los puntos de conexión externos de la función de la red virtual. |
| | `mask` | Máscara de subred del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `255.255.255.0`<br>La máscara de subred se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la máscara de subred no se puede cambiar.<br>• `AUTO`: la máscara de subred se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`. |
| | `gw` | Dirección IP de la puerta de enlace del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `dns` | Dirección IP del servidor DNS del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `group` | El grupo al que pertenece el punto de conexión interno.<br>Esta configuración es necesaria si varias VDU dentro de la función de la red virtual usan el mismo punto de conexión interno. |

### Ejemplo de esta sección

```
internal_connections:
- name: LAN
 description: eth3
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
 virtual_link_name: int-link
```

## virtual_links

La sección `virtual_links` tiene lo siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del vínculo virtual. |
| | `cidr` | Prefijo IPv4 del vínculo virtual. Ingrese un valor en el formato XXX.XXX.XXX.XXX/XX, por ejemplo: `192.168.2.0/24` |
| | `ip_version` | Versión de las direcciones IP en la subred. Valores posibles:<br>• `v4`<br>• `v6` |

**Ejemplo de esta sección**

```
virtual_links:
- name: int_link
 cidr: 203.0.113.0/24
 ip_version: v4
```

## images

La sección `images` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre de la imagen del disco de VDU. |
| | `container_format` | Formato de contenedor de la imagen del disco de VDU. |
| | `disk_format` | Formato de la imagen del disco de VDU. |
| | `type` | Tipo de VIM. |
| | `file_name` | Nombre de archivo de la imagen del disco de VDU. Debe colocar la imagen del disco de VDU en el directorio /image del paquete VNF. |

**Ejemplo de esta sección**

```
images:
- name: VDU_img
 container_format: BARE
 disk_format: QCOW2
 type: OPENSTACK
 filename: VDU_img.qcow2
```

## configurations

La sección `configurations` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del script. |
| | `filename` | El nombre del archivo de script, el manual Ansible o el atributo de datos de usuario para Cloud-init. Debe colocar el script en el directorio /scripts del paquete VNF. |
| | `stage` | La etapa de operación de la función de la red virtual en la que se ejecuta el script. Valores posibles:<br>• `initialization` para ejecutar el script en el despliegue de la función de la red virtual.<br>• `termination` para ejecutar el script cuando se elimina la función de la red virtual.<br>• `none` para ejecutar el script cuando un valor cambia en la sección `user_configurations` en el área de configuración de la función de la red virtual en la interfaz web del orquestador. |
| | `executor` | Intérprete de scripts. Valores posibles:<br>• `ansible`<br>• `expect`<br>• `/bin/sh`<br>• `bin/bash`<br>• `cloud-init`<br>• `< ruta al intérprete de scripts personalizados >`, por ejemplo `/usr/bin/php` |
| | `authentication` | Método para autenticar el VNFM en la función de la red virtual para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de la red virtual utilizando una clave que se genera cuando se implementa la función de la red virtual. Necesita usar un script para obtener la clave, por lo que recomendamos no especificar este valor para el primer script.<br>• `password` significa que el VNFM está autenticado en la función de la red virtual con un nombre de usuario y una contraseña de la sección `flavours` → `vdus`. |
| | `files_path` | Ruta a los archivos para ejecutar scripts mediante el uso de SSH. Debe crear un directorio en el directorio /scripts del paquete VNF y colocar los archivos en ese directorio. Los archivos se copian en la VDU.<br>Configuración opcional. |
| | `config_drive` | Uso de config-drive. Valores posibles:<br>• `true`<br>• `false`<br>Este parámetro debe especificarse si, como `executor`, especificó `cloud_init`. |
| | `timeout` | El tiempo de espera a que finalice el script, en segundos. Si el script no finaliza dentro del tiempo especificado, la ejecución se detiene. El tiempo de espera se inicia en el momento en que se ejecuta el script.<br>Puede especificar este parámetro si especificó una ruta a un ejecutor de script personalizado para el parámetro `executor`. |

### Ejemplo de esta sección

```
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 files_path: SSH_scripts
 config_drive: true
 timeout: 15
```

## flavours

La sección `flavours` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `- name` | | | Nombre del tipo. |
| | `description` | | Breve descripción del tipo. |
| | `position` | | Número secuencial del tipo. El tipo con la posición más baja tiene el rendimiento más bajo. |
| | `affinity` | | Grupos de VDU alojados en el mismo host de OpenStack. Recomendamos alojar las VDU que requieran minimizar los retrasos en la comunicación entre sí en el mismo host de OpenStack. |
| | `anti-affinity` | | Grupos de VDU alojadas en diferentes hosts de OpenStack. Recomendamos implementar las VDU que pueden requerir escalado vertical o alta disponibilidad en distintos hosts de OpenStack. |
| | `management` | | Parámetros de las consolas de administración de VDU. |
| | `vdus` | | Configuración de la VDU. |

Las secciones `affinity` y `anti-affinity` tienen la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `groups` | | | Grupos de VDU. |
| | `- name` | | Nombre del grupo de VDU. |
| | | `vdu_name` | Nombres de las VDU. Especifique una lista de valores, por ejemplo:<br>`vdu_name:`<br>`- VDU_1`<br>`- VDU_2` |

La sección `management` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `vnc` | | | Configuración para administrar las VDU mediante la consola VNC. |
| | `- vdu_name` | | Nombre de la VDU. |
| `ssh` | | | Configuración para administrar las VDU mediante la consola SSH. |
| | `- vdu_name` | | Nombre de la VDU. |
| | | `def_user` | Nombre de usuario para establecer la sesión SSH. |
| | | `authentication` | Método para autenticar el VNFM en la función de la red virtual para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de la red virtual utilizando una clave que se genera cuando se implementa la función de la red virtual. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de la red virtual con un nombre de usuario y una contraseña de la sección `vdus`. |
| `web` | | | Configuración para administrar las VDU mediante la consola web. |
| | `- vdu_name` | | Nombre de la VDU. |
| | | `protocol` | Protocolo de conexión a la consola web. Valores posibles:<br>• `http`.<br>• `https`. |
| | | `port` | Puerto para la conexión a la consola web. Ingrese un valor en el rango de 1 a 65 536. De manera predeterminada, se especifica el número de puerto 80. |
| | | `path` | Ruta a la consola web. |
| | | `def_user` | Nombre de usuario para autenticarse en la consola web. |
| | | `def_password` | Contraseña de autenticación en la consola web. |

La sección `vdus` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `- name` | | | Nombre de la VDU. |
| | `password_rules` | | Requisitos de contraseña de la VDU. Esta sección es opcional. |
| | | `length` | Longitud mínima de la contraseña. |
| | | `use_upper_case` | Los usuarios deben usar caracteres en mayúscula en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `use_lower_case` | Los usuarios deben usar caracteres en minúscula en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `use_digits` | Los usuarios deben usar números en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `specific_symbols` | Si los usuarios deben usar caracteres especiales en la contraseña, como:<br>`@"!` |
| | | `specific_symbols_min_usage` | Número mínimo de caracteres especiales que deben estar presentes en la contraseña. |
| | `check_connection_mode` | | Tipo de prueba de disponibilidad de la VDU realizada durante la implementación. De manera predeterminada, se realiza una prueba de SSH. Valores posibles:<br>• `ssh`<br>• `none`<br>Configuración opcional. |
| | `zabbix_template` | | Nombre de la plantilla Zabbix para la VDU. |
| | `monitoring_type` | | Tipo de supervisión de la función de la red virtual. Valores posibles:<br>• `agent` significa supervisar usando un agente Zabbix.<br>• `snmp` significa supervisar usando el protocolo SNMP. |
| | `ssh_port` | | Número de puerto para establecer una sesión SSH.<br>Configuración opcional. |
| | `ssh_host_key_algorithm` | | El algoritmo de clave de host utilizado. Valores posibles:<br>• `ssh-rsa`.<br>• `ssh-ed25519`. Recomendamos usar este algoritmo de clave de host porque es criptográficamente fuerte.<br>Si no especifica esta configuración, el algoritmo ssh-rsa se utiliza de manera predeterminada para la compatibilidad con versiones anteriores. |
| | `configurations` | | Nombres de los scripts de la sección `configurations` que se ejecutarán en la VDU. Especifique una lista de valores, por ejemplo:<br>`vdu_name:`<br>`- config_1`<br>`- config_2` |
| | `backups` | | Nombres de las tareas de respaldo de los `respaldos` que se usarán en la VDU. Especifique una lista de valores, por ejemplo:<br>`vdu_name:`<br>`- backup_1`<br>`- backup_2`<br>Esta sección es opcional. |
| | `def_user` | | Nombre de usuario para autenticar el VNFM en la función de la red virtual.<br>Configuración opcional. |
| | `def_password` | | Contraseña para autenticar el VNFM en la función de la red virtual.<br>Configuración opcional. |

| Sección/configuración | Descripción |
| --- | --- |
| password_authentication | Autenticación de contraseña del VNFM en la función de la red virtual. Valores posibles:<br>• sí<br>• no<br>Configuración opcional. |
| disks | Parámetros de los discos virtuales de la VDU. |
| - name | Nombre del disco virtual de la VDU. |
| order | Orden de montaje del disco virtual de la VDU. |
| type | Tipo de disco OpenStack efímero. |
| image | Nombre de la imagen del disco virtual de la VDU de la sección images.<br>Parámetro opcional si creará un disco de VDU en blanco. |
| storage_db | Tamaño del disco virtual de la VDU en gigabytes. |
| cpu | Parámetros de CPU de la VDU. |
| smt | Requisitos de subprocesos múltiples simultáneos para la implementación de la VDU. Valores posibles:<br>• prefer para utilizar subprocesos múltiples simultáneos si está habilitado en el host de la VDU.<br>• isolate para no utilizar subprocesos múltiples simultáneos.<br>• requiere para utilizar subprocesos múltiples simultáneos. |
| cpu_pinning | Uso de la asignación de la CPU. Valores posibles:<br>• shared si no desea asignar núcleos de CPU a la VDU.<br>• dedicated si desea asignar núcleos de CPU a la VDU. |
| num_vpu | Número de núcleos de CPU anclados a la VDU. |
| memory | Configuración de RAM de la VDU. |
| total_memory_mb | Cantidad de RAM de la VDU en megabytes. |
| page_size | Tamaño de las páginas de memoria cuando se implementa la VDU. Valores posibles:<br>• small para 4 KB<br>• large para 2 MB o 1 GB<br>• any para cualquier tamaño<br>• 4KB<br>• 2MB<br>• 2048<br>• 1 GB |
| network_interfaces | Configuración de la interfaz de red |
| - name | Nombre de la interfaz de red. |
| type | Tipo de interfaz de red. Valores posibles:<br>• data es una interfaz de red para la transferencia de datos.<br>• management es una interfaz de red de administración que se asigna a un puerto de red. |
| description | Descripción breve de la interfaz de red. |
| connection_point_ref | Nombre del punto de conexión externo de la sección external_connections para la interfaz de red de administración. |
| port_security | Si se utiliza la seguridad del puerto. Valores posibles:<br>• disabled<br>• enabled<br>Configuración opcional. |
| properties | Configuración avanzada de la interfaz de red. |
| vnic_type | Tipo vNIC de la interfaz de red. Valores posibles:<br>• virtio<br>• direct<br>• macvtap<br>• vhost |

| Sección/configuración | | | Descripción |
|---|---|---|---|
| | `auto_healing` | | Parámetros de reparación automática de la VDU. |
| | | `triggers_set` | Desencadenantes externos que inician la reparación automática de la VDU. Valores posibles:<br>• `any` para que cualquier desencadenante externo inicie la reparación automática de la VDU.<br>• `all` para iniciar la reparación automática de la VDU si se activan todos los desencadenantes externos especificados.<br>• `< nombre del desencadenante >` para iniciar la reparación automática de la VDU cuando se activa el desencadenante externo especificado. |
| | | `triggers` | Desencadenantes externos. |
| | | `- name` | Nombre del desencadenante externo. Valores posibles:<br>• `unreachable`<br>• `scale_up`<br>• `scale_down` |
| | | `action_set` | Acción a realizar cuando se activa un desencadenante externo. |
| | | `- type` | Tipo de acción. Valores posibles:<br>• `reprovision` para reaprovisionar la VDU.<br>• `reboot` para reiniciar la VDU.<br>• `script` para ejecutar el script especificado. |
| | | `configuration_name_ref` | Nombre del script de la sección `configuration` que se ejecuta cuando se activa un desencadenante externo.<br>Este parámetro debe especificarse si, como `- type`, seleccionó `script`. |
| | `bootstrap_timeout` | | Tiempo de espera de disponibilidad SSH durante la implementación de la VDU, en segundos. Si la VDU no está disponible a través de SSH después de que caduca el tiempo de espera especificado, la implementación se revierte.<br>Configuración opcional. |

### Ejemplo de esta sección

```
vdus:
 - name: vgw
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 check_connection_mode: none
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config_1
 - config_2
 backups:
 - backup_config
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 disks:
 - name: "default"
 order: 1
 type: default
 image: openwrt
 storage_gb: 1
 cpu:
```

```
smt: prefer
cpu_pinning: dedicated
num_vpu: 1
memory:
total_memory_mb: 512
page_size: small
network_interfaces:
- name: eth
type: data
description: eth0
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
```

## scaling

La sección `scaling` tiene la siguiente estructura:

| Configuración | Descripción |
|---|---|
| `scale_in_status` | Escalado horizontal a un tipo con un número secuencial más bajo. Valores posibles:<br>• `permit`<br>• `deny` |
| `scale_out_status` | Escalado horizontal a un tipo con un número secuencial más alto. Valores posibles:<br>• `permit`<br>• `deny` |
| `scale_up_status` | Escalado vertical a un tipo con un número secuencial más bajo. Valores posibles:<br>• `permit`<br>• `deny` |
| `scale_down_status` | Escalado vertical a un tipo con un número secuencial más alto. Valores posibles:<br>• `permit`<br>• `deny` |

**Ejemplo de esta sección**

```
scaling:
 scale_in_status: permit
 scale_out_status: permit
 scale_up_status: permit
 scale_down_status: permit
```

## user_configurations

La sección `user_configurations` tiene la siguiente estructura:

| Sección/configuración | Descripción |
|---|---|
| `tab` | Pestañas que se agregan al área de configuración de la función de la red virtual. |
| `- name` | Nombre de la pestaña. |

| Sección/configuración | | | Descripción |
|---|---|---|---|
| | `variables` | | Entradas de la interfaz web del orquestado que se muestran en la pestaña. |
| | `- name` | | Nombre de la entrada de la interfaz web del orquestador. |
| | | `description` | Breve descripción de la entrada de la interfaz web del orquestador. |
| | | `input_type` | Tipo de entrada de la interfaz web del orquestador. Valores posibles:<br>• `input` para agregar un campo.<br>• `dropdown` para agregar una lista desplegable. |
| | | `default_value` | Valor predeterminado del campo.<br>Puede especificar este parámetro si, como `input_type`, especificó `input`. |
| | | `values` | Las opciones que se muestran en la lista desplegable.<br>Esta configuración se puede especificar si, como `input_type`, especificó `dropdown`. |
| | | `- value` | El nombre del valor. |
| | | `is_default` | Valor predeterminado. Valores posibles:<br>• `true`<br>• `false`<br>Configuración opcional. |
| | | `required` | Entrada de la interfaz web del orquestador requerida. Valores posibles:<br>• `true`<br>• `false`<br>Configuración opcional. |
| | | `type` | El tipo de valor que se puede especificar en la entrada de la interfaz web del orquestador.<br>Configuración opcional. |
| | | `example` | Información sobre herramientas que se muestra cuando cambia el valor de la entrada de la interfaz web del orquestador.<br>Configuración opcional. |
| | | `update_configuration_name` | Nombres de los scripts de la sección `configurations` que se ejecutan cuando cambia el valor de la entrada de la interfaz web del orquestador. Especifique una lista de valores, por ejemplo:<br>`update_configuration_name:`<br>`- config_1`<br>`- config_2` |

### Ejemplo de esta sección

```
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
 - value: out
 update_configuration_name:
```

```
- update_var
- change
```

## backups

La sección `backups` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `- name` | | | Nombre de la tarea de respaldo. |
| | `description` | | Breve descripción de la tarea de respaldo. |
| | `backup` | | Parámetros del respaldo. |
| | | `path` | Ruta al directorio de funciones de la red virtual donde se encuentran los archivos que desea respaldar. |
| | | `interval` | Intervalo de tiempo en segundos para el respaldo. |
| | | `store_config` | Número de copias de respaldo que se conservarán. |
| | | `backup_type` | Tipo de respaldo. |
| | | `authentication` | Método para autenticar el VNFM en la función de la red virtual para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de la red virtual utilizando una clave que se genera cuando se implementa la función de la red virtual. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de la red virtual con un nombre de usuario y una contraseña de la sección `flavours` → `vdus`. |
| | | `configuration_name_ref` | Nombre del script de la sección `configurations` que se ejecutará antes del respaldo. |
| | `restore` | | Parámetros de restauración del respaldo. |
| | | `path` | Ruta al directorio de funciones de la red virtual donde se colocan los archivos restaurados. |
| | | `backup_type` | Tipo de respaldo. |
| | | `authentication` | Método para autenticar el VNFM en la función de la red virtual para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de la red virtual utilizando una clave que se genera cuando se implementa la función de la red virtual. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de la red virtual con un nombre de usuario y una contraseña de la sección `flavours` → `vdus`. |
| | | `configuration_name_ref` | Nombre del script de la sección `configurations` que se ejecutará después de que comience la restauración del respaldo. |

### Ejemplo de esta sección

```
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
```

```
configuration_name_ref: restore
```

# Configurar descriptor PNF

Especifique la configuración de la función de red física en un descriptor PNF en formato YAML o XML, luego agregue el descriptor PNF al directorio raíz del paquete PNF. Un descriptor de PNF tiene la siguiente estructura:

| Sección/configuración | Descripción |
|---|---|
| `name` | Nombre de la función de red física. |
| `description` | Breve descripción de la función de la red física. |
| `description_file` | Nombre del archivo PDF con la documentación técnica o especificación de la función de red física. Este archivo debe colocarse en el directorio raíz del paquete PNF. Los usuarios pueden ver y descargar el archivo en la interfaz web del orquestador.<br>Configuración opcional. |
| `provider` | Proveedor de la función de red física. |
| `version` | Versión de la función de red física. |
| `external_connections` | Puntos de conexión externos de la función de red física. |
| `internal_connections` | Puntos de conexión internos de las VDU que forman parte de la función de red física.<br>Esta sección es opcional. |
| `configurations` | Scripts para realizar acciones en varias etapas del ciclo de vida de la función de red física, por ejemplo, durante la implementación de la función de red física. |
| `flavours` | Tipos de la función de red física. Puede seleccionar uno de los tipos especificados de la función de red física en la interfaz web del orquestador. |
| `scaling` | Parámetros de escalado de la función de red física.<br>Esta sección es opcional. |
| `user_configurations` | Entradas de la interfaz web del orquestador que se agregan al área de configuración de la función de red física.<br>Esta sección es opcional. |
| `backups` | Tareas de respaldo de la función de red física.<br>Esta sección es opcional. |

### Ejemplo de descriptor de PNF

```
name: OpenWrt18
description: OpenWrt 18.06.1
description_file: openwrt-presentation.pdf
provider: Kaspersky
version: 1.0.1
external_connections:
 - name: LAN
 description: eth1
 ip: AUTO
 mask: AUTO
 group: eth1-group
 - name: WAN
 description: eth2
 ip: AUTO
 mask: AUTO
 group: eth2-group
configurations:
 - name: config
 filename: config.yml
 stage: initialization
```

```
 executor: ansible
 authentication: password
 - name: config2
 filename: 3VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
 - name: config3
 filename: 2VDU.sh
 stage: initialization
 executor: /bin/sh
 authentication: key
flavours:
 - name: 2VDU
 description: 1 vCPU, 512MB memory
 position: 1
 management:
 ssh:
 - vdu_name: OpenWrt
 def_user: root
 authentication: key
 web:
 - vdu_name: OpenWrt
 vdus:
 - name: OpenWrt
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config
 - config3
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 network_interfaces:
 - name: Management
 type: management
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
```

```
- type: reboot
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config3
def_user: root
def_password: p@ssw0rd
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- tipo: reiniciar
- name: VDU
description: 1 vCPU, 512MB memory
position: 2
management:
ssh:
- vdu_name: OpenWrt
def_user: root
authentication: key
web:
- vdu_name: OpenWrt
vdus:
- name: OpenWrt
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
check_connection_mode: none
zabbix_template: Template OS Linux
monitoring_type: agent
```

```
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssword
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reboot
- name: OpenWrt2
password_rules:
length: 12
use_upper_case: true
use_lower_case: true
use_digits: true
specific_symbols: .?$#@![]-{}
specific_symbols_min_usage: 2
zabbix_template: Template OS Linux
monitoring_type: agent
ssh_port: 22
configurations:
- config
- config2
def_user: root
def_password: p@ssw0rd
password_authentication: yes
network_interfaces:
- name: Management
type: management
description: eth0
- name: eth1
type: data
description: eth1
connection_point_ref: LAN
- name: eth2
type: data
description: eth2
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
```

```
 action_set:
 - type: reboot
 - name: OpenWrt3
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config
 - config2
 def_user: root
 def_password: p@ssw0rd
 password_authentication: yes
 network_interfaces:
 - name: Management
 type: management
 description: eth0
 - name: eth1
 type: data
 description: eth1
 connection_point_ref: LAN
 - name: eth2
 type: data
 description: eth2
 connection_point_ref: WAN
 auto_healing:
 triggers_set: any
 triggers:
 - name: unreachable
 action_set:
 - type: reboot
scaling:
 scale_in_status: permit
 scale_out_status: "permit"
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
```

```
 is_default: true
 - value: out
 update_configuration_name:
 - update_var
 - change
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
 configuration_name_ref: restore
```

## external_connections

La sección `external_connections` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del punto de conexión externo. |
| | `description` | Breve descripción del punto de conexión externo. |
| | `ip` | Dirección IP del punto de conexión externo. Ingrese un valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126` |
| | `mask` | Máscara de subred del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`255.255.255.0`<br>La máscara de subred se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la máscara de subred no se puede cambiar.<br>• `AUTO`: la máscara de subred se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`. |
| | `gw` | Dirección IP de la puerta de enlace del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `dns` | Dirección IP del servidor DNS del punto de conexión externo. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo:<br>`192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `group` | El grupo al que pertenece el punto de conexión externo.<br>Esta configuración es necesaria si varias VDU dentro de la función de red física utilizan el mismo punto de conexión externo. |

### Ejemplo de esta sección

```
external_connections:
- name: LAN
 description: eth1
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
 group: lan-group
```

## internal_connections

La sección `internal_connections` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del punto de conexión interno. |
| | `description` | Breve descripción del punto de conexión interno. |
| | `ip` | Dirección IP del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`. |
| | `mask` | Máscara de subred del punto de conexión interno. Valores posibles:<br>• Valor en el formato XXX.XXX.XXX.XXX, por ejemplo: `255.255.255.0`<br>La máscara de subred se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la máscara de subred no se puede cambiar.<br>• AUTO: la máscara de subred se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`. |
| | `gw` | Dirección IP de la puerta de enlace del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `dns` | Dirección IP del servidor DNS del punto de conexión interno. Valores posibles:<br>• Valor en el formato `XXX.XXX.XXX.XXX`, por ejemplo: `192.168.110.126`<br>La dirección IP se asigna mediante DHCP a través de la reserva basada en MAC de un puerto OpenStack. En este caso, la dirección IP no se puede cambiar.<br>• `AUTO`: la dirección IP se asigna automáticamente mediante un servidor DHCP externo o un script de la sección `configurations`.<br>Configuración opcional. |
| | `group` | El grupo al que pertenece el punto de conexión interno.<br>Esta configuración es necesaria si varias VDU dentro de la función de red física utilizan el mismo punto de conexión interno. |

### Ejemplo de esta sección

```
internal_connections:
- name: LAN
 description: eth3
 ip: 192.168.2.0
 mask: 255.255.255.0
 gw: 192.168.0.1
 dns: 192.168.0.10
```

```
group: lan-group
```

## configurations

La sección `configurations` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del script. |
| | `filename` | Nombre de archivo del script o del manual Ansible. Debe colocar el script en el directorio /scripts del paquete PNF. |
| | `stage` | La etapa de operación de la función de red física en la que se ejecuta el script. Valores posibles:<br>• `initialization` para ejecutar el script en la implementación de la función de red física.<br>• `termination` para ejecutar el script al eliminar la función de red física.<br>• `none` para ejecutar el script cuando un valor cambia en la sección `user_configurations` en el área de configuración de la función de red física en la interfaz web del orquestador. |
| | `executor` | Intérprete de scripts. Valores posibles:<br>• `ansible`<br>• `expect`<br>• `/bin/sh`<br>• `bin/bash`<br>• < `ruta al intérprete de scripts personalizados` >, por ejemplo `/usr/bin/php` |
| | `authentication` | Método para autenticar el VNFM en la función de red física para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de red física utilizando una clave que se genera cuando se implementa esa función de red física. Necesita usar un script para obtener la clave, por lo que recomendamos no especificar este valor para el primer script.<br>• `password` significa que el VNFM está autenticado en la función de red física con un nombre de usuario y contraseña de la sección `flavours` → `vdus`. |
| | `files_path` | Ruta a los archivos para ejecutar scripts mediante el uso de SSH. Debe crear un directorio en el directorio /scripts del paquete PNF y colocar los archivos en ese directorio. Los archivos se copian en la VDU.<br>Configuración opcional. |
| | `timeout` | El tiempo de espera a que finalice el script, en segundos. Si el script no finaliza dentro del tiempo especificado, la ejecución se detiene. El tiempo de espera se inicia en el momento en que se ejecuta el script.<br>Puede especificar este parámetro si especificó una ruta a un ejecutor de script personalizado para el parámetro `executor`. |

### Ejemplo de esta sección

```
configurations:
 - name: config
 filename: config.yml
 stage: initialization
 executor: ansible
 authentication: password
 files_path: SSH_scripts
 config_drive: true
 timeout: 15
```

## flavours

La sección `flavours` tiene la siguiente estructura:

| Sección/configuración | | Descripción |
|---|---|---|
| `- name` | | Nombre del tipo. |
| | `description` | Breve descripción del tipo. |
| | `position` | Número secuencial del tipo. El tipo con la posición más baja tiene el rendimiento más bajo. |
| | `management` | Parámetros de las consolas de administración de VDU. |
| | `vdus` | Configuración de la VDU. |

La sección `management` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `ssh` | | | Configuración para administrar las VDU mediante la consola SSH. |
| | `- vdu_name` | | Nombre de la VDU. |
| | | `def_user` | Nombre de usuario para establecer la sesión SSH. |
| | | `authentication` | Método para autenticar el VNFM en la función de red física para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de red física utilizando una clave que se genera cuando se implementa esa función de red física. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de red física con un nombre de usuario y una contraseña de la sección `vdus`. |
| `web` | | | Configuración para administrar las VDU mediante la consola web. |
| | `- vdu_name` | | Nombre de la VDU. |
| | | `protocol` | Protocolo de conexión a la consola web. Valores posibles:<br>• `http`.<br>• `https`. |
| | | `port` | Puerto para la conexión a la consola web. Ingrese un valor en el rango de 1 a 65 536. De manera predeterminada, se especifica el número de puerto 80. |
| | | `path` | Ruta a la consola web. |
| | | `def_user` | Nombre de usuario para autenticarse en la consola web. |
| | | `def_password` | Contraseña de autenticación en la consola web. |

La sección `vdus` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `- name` | | | Nombre de la VDU. |
| | `password_rules` | | Requisitos de contraseña de la VDU. Esta sección es opcional. |
| | | `length` | Longitud mínima de la contraseña. |
| | | `use_upper_case` | Los usuarios deben usar caracteres en mayúscula en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `use_lower_case` | Los usuarios deben usar caracteres en minúscula en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `use_digits` | Los usuarios deben usar números en la contraseña. Valores posibles:<br>• `true`<br>• `false` |
| | | `specific_symbols` | Si los usuarios deben usar caracteres especiales en la contraseña, como:<br>`@"!` |
| | | `specific_symbols_min_usage` | Número mínimo de caracteres especiales que deben estar presentes en la contraseña. |
| | `check_connection_mode` | | Tipo de prueba de disponibilidad de la VDU realizada durante la implementación. De manera predeterminada, se realiza una prueba de SSH. Valores posibles:<br>• `ssh`<br>• `none`<br>Configuración opcional. |
| | `zabbix_template` | | Nombre de la plantilla Zabbix para la VDU. |
| | `monitoring_type` | | Tipo de supervisión de la función de red física. Valores posibles:<br>• `agent` significa supervisar usando un agente Zabbix.<br>• `snmp` significa supervisar usando el protocolo SNMP. |
| | `ssh_port` | | Número de puerto para establecer una sesión SSH.<br>Configuración opcional. |
| | `ssh_host_key_algorithm` | | El algoritmo de clave de host utilizado. Valores posibles:<br>• `ssh-rsa`.<br>• `ssh-ed25519`. Recomendamos usar este algoritmo de clave de host porque es criptográficamente fuerte.<br>Si no especifica esta configuración, el algoritmo ssh-rsa se utiliza de manera predeterminada para la compatibilidad con versiones anteriores. |
| | `configurations` | | Nombres de los scripts de la sección `configurations` que se ejecutarán en la VDU. Especifique una lista de valores, por ejemplo:<br>`vdu_name:`<br>`- config_1`<br>`- config_2` |
| | `backups` | | Nombres de las tareas de respaldo de los `respaldos` que se usarán en la VDU. Especifique una lista de valores, por ejemplo:<br>`vdu_name:`<br>`- backup_1`<br>`- backup_2`<br>Esta sección es opcional. |
| | `def_user` | | Nombre de usuario para autenticar el VNFM en la función de red física.<br>Configuración opcional. |
| | `def_password` | | Contraseña para autenticar el VNFM en la función de red física.<br>Configuración opcional. |

| Sección/configuración | | | Descripción |
|---|---|---|---|
| | password_authentication | | Autenticación de contraseña del VNFM en la función de red física. Valores posibles:<br>• sí<br>• no<br>Configuración opcional. |
| | network_interfaces | | Configuración de la interfaz de red |
| | - name | | Nombre de la interfaz de red. |
| | | type | Tipo de interfaz de red. Valores posibles:<br>• data es una interfaz de red para la transferencia de datos.<br>• management es una interfaz de red de administración que se asigna a un puerto de red. |
| | | description | Descripción breve de la interfaz de red. |
| | | connection_point_ref | Nombre del punto de conexión externo de la sección external_configurations para la interfaz de red de administración. |
| | auto_healing | | Parámetros de reparación automática de la VDU. |
| | triggers_set | | Desencadenantes externos que inician la reparación automática de la VDU. Valores posibles:<br>• any para que cualquier desencadenante externo inicie la reparación automática de la VDU.<br>• all para iniciar la reparación automática de la VDU si se activan todos los desencadenantes externos especificados.<br>• < nombre del desencadenante > para iniciar la reparación automática de la VDU cuando se activa el desencadenante externo especificado. |
| | triggers | | Desencadenantes externos. |
| | | - name | Nombre del desencadenante externo. Valores posibles:<br>• unreachable<br>• scale_up<br>• scale_down |
| | action_set | | Acción a realizar cuando se activa un desencadenante externo. |
| | | - type | Tipo de acción. Valores posibles:<br>• reboot para reiniciar la VDU.<br>• script para ejecutar el script especificado. |
| | | configuration_name_ref | Nombre del script de la sección configuration que se ejecuta cuando se activa un desencadenante externo.<br>Este parámetro debe especificarse si, como - type, seleccionó script. |

### Ejemplo de esta sección

```
vdus:
 - name: vgw
 password_rules:
 length: 12
 use_upper_case: true
 use_lower_case: true
 use_digits: true
 specific_symbols: .?$#@![]-{}
 specific_symbols_min_usage: 2
 check_connection_mode: none
 zabbix_template: Template OS Linux
 monitoring_type: agent
 ssh_port: 22
 configurations:
 - config_1
 - config_2
 backups:
 - backup_config
```

```
def_user: root
def_password: p@ssw0rd
password_authentication: yes
network_interfaces:
- name: eth
type: data
description: eth0
connection_point_ref: WAN
auto_healing:
triggers_set: any
triggers:
- name: unreachable
action_set:
- type: reprovision
```

## scaling

La sección `scaling` tiene la siguiente estructura:

| Configuración | Descripción |
|---|---|
| `scale_up_status` | Escalado vertical a un tipo con un número secuencial más bajo. Valores posibles:<br>• `permit`<br>• `deny` |
| `scale_down_status` | Escalado vertical a un tipo con un número secuencial más alto. Valores posibles:<br>• `permit`<br>• `deny` |

**Ejemplo de esta sección**

```
scaling:
 scale_in_status: permit
 scale_out_status: permit
```

## user_configurations

La sección `user_configurations` tiene la siguiente estructura:

| Sección/configuración | Descripción |
|---|---|
| `tab` | Fichas que se agregan al área de configuración de la función de red física. |
| `- name` | Nombre de la pestaña. |

| Sección/configuración | | | Descripción |
|---|---|---|---|
| | `variables` | | Entradas de la interfaz web del orquestado que se muestran en la pestaña. |
| | `- name` | | Nombre de la entrada de la interfaz web del orquestador. |
| | | `description` | Breve descripción de la entrada de la interfaz web del orquestador. |
| | | `input_type` | Tipo de entrada de la interfaz web del orquestador. Valores posibles:<br>• `input` para agregar un campo.<br>• `dropdown` para agregar una lista desplegable. |
| | | `default_value` | Valor predeterminado del campo.<br>Puede especificar este parámetro si, como `input_type`, especificó `input`. |
| | | `values` | Las opciones que se muestran en la lista desplegable.<br>Esta configuración se puede especificar si, como `input_type`, especificó `dropdown`. |
| | | `- value` | El nombre del valor. |
| | | `is_default` | Valor predeterminado. Valores posibles:<br>• `true`<br>• `false`<br>Configuración opcional. |
| | | `required` | Entrada de la interfaz web del orquestador requerida. Valores posibles:<br>• `true`<br>• `false`<br>Configuración opcional. |
| | | `type` | El tipo de valor que se puede especificar en la entrada de la interfaz web del orquestador.<br>Configuración opcional. |
| | | `example` | Información sobre herramientas que se muestra cuando cambia el valor de la entrada de la interfaz web del orquestador.<br>Configuración opcional. |
| | | `update_configuration_name` | Nombres de los scripts de la sección `configurations` que se ejecutan cuando cambia el valor de la entrada de la interfaz web del orquestador. Especifique una lista de valores, por ejemplo:<br>`update_configuration_name:`<br>`- config_1`<br>`- config_2` |

### Ejemplo de esta sección

```
user_configurations:
 tab:
 - name: GW
 variables:
 - name: "gw_ip"
 description: IP
 input_type: input
 required: true
 type: string
 default_value: 192.168.0.1
 example: 192.168.0.1
 - name: direction
 description: traffic direction
 input_type: dropdown
 required: true
 type: string
 values:
 - value: in
 is_default: true
 - value: out
 update_configuration_name:
```

```
- update_var
- change
```

## backups

La sección `backups` tiene la siguiente estructura:

| Sección/configuración | | | Descripción |
|---|---|---|---|
| `- name` | | | Nombre de la tarea de respaldo. |
| | `description` | | Breve descripción de la tarea de respaldo. |
| | `backup` | | Parámetros del respaldo. |
| | | `path` | Ruta al directorio de funciones de red física donde se encuentran los archivos que desea respaldar. |
| | | `interval` | Intervalo de tiempo en segundos para el respaldo. |
| | | `store_config` | Número de copias de respaldo que se conservarán. |
| | | `backup_type` | Tipo de respaldo. |
| | | `authentication` | Método para autenticar el VNFM en la función de red física para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de red física utilizando una clave que se genera cuando se implementa esa función de red física. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de red física con un nombre de usuario y contraseña de la sección `flavours` → `vdus`. |
| | | `configuration_name_ref` | Nombre del script de la sección `configurations` que se ejecutará antes del respaldo. |
| | `restore` | | Parámetros de restauración del respaldo. |
| | | `path` | Ruta al directorio de funciones de red física donde se colocan los archivos restaurados. |
| | | `backup_type` | Tipo de respaldo. |
| | | `authentication` | Método para autenticar el VNFM en la función de red física para ejecutar scripts. Valores posibles:<br>• `key` significa que el VNFM se autentica en la función de red física utilizando una clave que se genera cuando se implementa esa función de red física. Debe obtener la clave mediante un script de la sección `configurations`.<br>• `password` significa que el VNFM está autenticado en la función de red física con un nombre de usuario y contraseña de la sección `flavours` → `vdus`. |
| | | `configuration_name_ref` | Nombre del script de la sección `configurations` que se ejecutará después de que comience la restauración del respaldo. |

### Ejemplo de esta sección

```
backups:
 - name: backup_config
 description: backup/etc/config
 backup:
 path: /root/config.thz
 interval: 600
 store_configs: 10
 backup_type: vnfm_scp
 authentication: key
 configuration_name_ref: backup
 restore:
 path: /tmp/config.tgz
 backup_type: vnfm_scp
 authentication: password
```

```
configuration_name_ref: restore
```

# Protección de paquetes VNF y PNF contra la sustitución y la modificación

Algunos archivos de paquetes VNF y PNF se encuentran en el directorio local del contenedor Docker del orquestador, y usted puede protegerlos contra la sustitución y la modificación. Cuando los paquetes VNF y PNF están protegidos, el orquestador computa automáticamente su hash SHA256 cuando se cargan a la interfaz web del orquestador. Cuando se accede a los archivos en el directorio local del contenedor Docker, el orquestador compara su hash SHA256 actual con el hash que se guardó anteriormente. Si los hashes SHA256 no coinciden, el orquestador evita que los usuarios realicen acciones con la función de la red, como agregarla a la topología de un servicio de red.

*Para proteger los paquetes VNF y PNF contra la sustitución y la modificación, haga lo siguiente:*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **Otra** y seleccione la casilla de verificación **Calcular suma de comprobación SHA256 para los archivos VNF/PNF en el almacenamiento**. Esta casilla está seleccionada por defecto.

Los paquetes VNF y PNF estarán protegidos contra la sustitución y la modificación.

# Cargar un paquete VNF o PNF a la interfaz web del orquestador

*Para cargar un paquete VNF o PNF a la interfaz web del orquestador, siga estos pasos:*

1. En el menú, vaya a la sección **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En la parte superior de la página, haga clic en **+ VNF** o **+ PNF**.

3. En la ventana que se abre, seleccione el paquete VNF o PNF.

4. Si desea comprobar la integridad del paquete VNF o PNF, ingrese su hash SHA256 en el campo **Suma de comprobación SHA256**. La longitud máxima del hash es de 64 caracteres.

5. Haga clic en **Guardar**.

El paquete VNF o PNF se carga en la interfaz web del orquestador. El VNF o PNF se muestra en el panel **Catálogo**. Si ingresó un hash SHA256 de un paquete VNF o PNF, el orquestador compara el hash que ingresó con el hash SHA256 real. Si los hashes SHA256 no coinciden, el paquete VNF o PNF no se carga.

# Especificar una breve descripción de un servicio de red compartido

*Puede especificar una breve descripción del servicio de red compartido.*

1. Navegue a la topología de una de las siguientes maneras:
   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.
2. En la herramienta de diseño gráfico, haga clic en el servicio de red compartido para el que desea especificar una breve descripción.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Configuración** está seleccionada, que muestra una breve descripción del servicio de red compartido.
3. En el campo **Descripción**, ingrese una breve descripción del servicio de red compartido.
4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del servicio de red compartido.

# Administrar funciones de red virtual

Para administrar una función de la red virtual, realice una de las siguientes acciones:

- En el portal del administrador, vaya a la sección **Catálogo** y, en el panel **Catálogo**, haga clic en la función de red virtual.
- Al crear o editar una plantilla de servicio de red en la topología, haga clic en la función de red virtual.
- Al crear o editar un servicio de red en la topología, haga clic en la función de red virtual.

Puede administrar la configuración de la función de red virtual en las siguientes pestañas:

- **Variantes** contiene variantes de la función de red virtual.
- **Puntos de conexión** contiene puntos de conexión externos de la función de red virtual.
- **Configuración de VNF** contiene la configuración básica de la función de red virtual.
- **Ubicación** contiene la configuración de ubicación de la función de red virtual. Puede colocar una función de red virtual en un centro de datos o en un dispositivo uCPE. Esta pestaña se muestra si hizo clic en la función de red virtual al crear o editar un servicio de red.

Las siguientes pestañas se muestran si hizo clic en la función de red virtual en la topología de un servicio de red implementado:

- **Administración de VDU** es una tabla de VDU que forman parte de la función de red virtual. La información sobre las VDU se muestra en las siguientes columnas de la tabla:
  - **Nombre** es el nombre de la VDU.
  - **Nombre de la instancia** es el Id. de la instancia de VDU.
  - **IP de admin** es la dirección IP que la subred de administración ha asignado a la VDU.
  - **vCPU** es el número de núcleos de CPU virtuales asignados a la VDU.
  - **RAM** es la cantidad de RAM en megabytes asignada a la VDU.
  - **Disco** es la cantidad de espacio en disco en gigabytes asignada a la VDU.
  - **Estado** es el estado de la VDU:
    - **ACTIVE** significa que la VDU está funcionando normalmente.
    - **ERROR** significa que la VDU encontró un error.
    - **HARD_REBOOT** significa que hay un reinicio completo de la VDU.
    - **PAUSED** significa que la VDU está en pausa.
    - **REBOOT** significa que se está realizando un reinicio suave de la VDU.
    - **SHUTOFF** significa que la VDU está detenida.
    - **SUSPENDED** significa que la VDU está suspendida.
- **Supervisión** contiene los resultados de la supervisión de la función de red virtual.
- **Problemas** contiene los problemas que ocurrieron durante el funcionamiento de la función de red virtual. En caso de que haya ocurrido un problema, se muestra un signo de exclamación rojo junto a la pestaña.

Además, es posible que se muestren las pestañas que especificó en la sección `user_configurations` del descriptor VNF.

# Seleccionar el tipo de función de la red virtual

Puede especificar los tipos de función en la sección `tipos de función` del descriptor de VNF.

*Para seleccionar un tipo de función de la red virtual, haga lo siguiente:*

1. Navegue a la topología de una de las siguientes maneras:
   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en la función de la red virtual para la que desea seleccionar un tipo de función.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

3. Seleccione un tipo de función para la función de la red virtual.

4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de red virtual.

# Configurar puntos de conexión externos de una función de la red virtual

Puede especificar puntos de conexión externos de una función de la red virtual en la sección `external_connections` del descriptor VNF.

*Para configurar puntos de conexión externos de la función de la red virtual, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en la función de la red virtual para la que desea configurar puntos de conexión externos.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

3. Seleccione la pestaña **Puntos de conexión**.

   Se muestran los puntos de conexión externos de la función de la red virtual.

4. En la lista desplegable **Tipo**, seleccione cómo desea asignar un prefijo IPv4 al punto de conexión externo:

   - **Reserva de DHCP** para usar DHCP a fin de asignar un prefijo IPv4 al punto de montaje externo. Si selecciona esta opción, haga lo siguiente:

     a. En el campo **Dirección IP**, ingrese la dirección IPv4 que DHCP asigna al punto de conexión externo.

     b. En el campo **Máscara**, ingrese la máscara de subred que DHCP asigna al punto de conexión externo.

   - **AUTO** para asignar automáticamente un prefijo IPv4 al punto de conexión externo. Esta es la configuración predeterminada.

5. En el campo **Descripción**, ingrese una breve descripción del punto de conexión externo.

6. Si desea designar el punto de conexión como puerto troncal, seleccione la casilla **Troncal**. Esta casilla está desactivada por defecto.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de red virtual.

# Configuración básica de una función de red virtual

*Para editar la configuración básica de la función de la red virtual, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en la función de red virtual para la que desea establecer la configuración básica.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir . De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

3. Seleccione la pestaña **Configuración de VNF**.

   Se muestra la configuración básica de la función de red virtual.

4. En el campo **Nombre**, ingrese el nombre de la función de red virtual.

5. En el campo **Descripción**, ingrese una breve descripción de la función de red virtual.

6. En el campo **Orden**, ingrese el número de secuencia para implementar la función de red virtual en la plataforma de la nube OpenStack. Cuando implementa un servicio de red, la función de red virtual con el número más bajo es la primera en implementarse. Si ninguna de las funciones de red virtual agregadas a la topología del servicio de red tiene un número de secuencia especificado, todas las funciones de red virtual se implementan simultáneamente.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de red virtual.

# Alojar la función de la red virtual en un centro de datos y en un dispositivo uCPE

*Para colocar una función de la red virtual en un centro de datos o en un dispositivo uCPE, siga estos pasos:*

1. Navegue a la topología; para ello, comience a crear o editar un servicio de red.

2. Haga clic en la función de la red virtual que desea colocar en un centro de datos o en un dispositivo uCPE.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir . De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

3. Seleccione la pestaña **Ubicación**.

   Se muestra la configuración de ubicación de la función de la red virtual.

4. En la lista **Seleccionar tipo de ubicación**, seleccione uno de estos valores:

   - **Centro de datos** para colocar la función de la red virtual en el centro de datos especificado. Si selecciona esta opción, haga lo siguiente:

     a. En el campo **Centro de datos**, ingrese el nombre del centro de datos creado. A medida que escribe el nombre, se le solicita que seleccione un centro de datos de una lista desplegable.

     b. En el campo **VIM**, ingrese el nombre del VIM implementado para la función de la red virtual. A medida que escribe el nombre, se le solicita que seleccione un VIM de una lista desplegable.

   - **uCPE** para colocar la función de la red virtual en el dispositivo uCPE especificado. Si selecciona esta opción, en el campo **uCPE**, ingrese el nombre del dispositivo uCPE. A medida que escribe el nombre, se le solicita que seleccione un dispositivo uCPE de una lista desplegable.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de red virtual.

# Detener o iniciar una función de la red virtual o una VDU que forma parte de ella

Puede detener una función de la red virtual o una VDU que forma parte de ella para liberar los recursos informáticos de la plataforma en la nube de OpenStack .

Cuando inicia una función de la red virtual o VDU, comienza a consumir recursos informáticos nuevamente. Esto reinicia los procesos que se ejecutan en la función de la red virtual o VDU.

*Para detener o iniciar una función de la red virtual o una VDU que forma parte de ella:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir . De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Si desea detener o iniciar la función de la red virtual, en la parte superior del área de configuración, haga clic en el ícono **Administración**→ **Potencia**→ **Detener VNF** o **Iniciar VNF**.

5. Si desea detener o iniciar una VDU que forma parte de la función de la red virtual:

   a. Seleccione la pestaña **Administración de VDU**.

      Se muestra una tabla de las VDU.

   b. Haga clic en **Administración** → **Potencia** → **Detener VDU** o **Iniciar VDU** junto a la VDU que quiere detener o iniciar.

6. En la ventana de confirmación, haga clic en **Aplicar**.

La función de la red virtual o su VDU se detiene o inicia.

# Pausar o reanudar una función de la red virtual o una VDU que forma parte de ella

Puede pausar una función de la red virtual o una VDU que forma parte de ella para pausar los procesos que se ejecutan en ella. Sin embargo, la función de la red virtual o VDU sigue consumiendo los recursos informáticos de la plataforma en la nube de OpenStack. Cuando se reanuda una función de la red virtual o VDU, los procesos que se ejecutan en ella se reanudan.

*Para pausar o reanudar una función de la red virtual o una VDU que forma parte de ella, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Pause o reanude la función de la red virtual o una VDU que forma parte de ella:

   - Si desea pausar o reanudar una función de la red virtual, en la parte superior del área de configuración, haga clic en **Administración**→ **Potencia**→ **Pausar VNF** o **Reanudar VNF**.

   - Si desea pausar o reanudar una VDU que forma parte de la función de la red virtual:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de las VDU.

     2. Haga clic en **Administración** → **Potencia** → **Pausar VDU** o **Reanudar VDU**.

5. En la ventana de confirmación, haga clic en **Aplicar**.

La función de la red virtual o su VDU se pausa o se reanuda.

# Suspender o anular la suspensión de una función de la red virtual o una VDU que forma parte de ella

Puede suspender una función de red virtual o una VDU que forma parte de ella para liberar el cálculo recursos de la plataforma en la nube de OpenStack. Esto guarda el estado de la función de red virtual o VDU en el disco de la plataforma en la nube de OpenStack. Cuando anula la suspensión de la función de red virtual o VDU, comienza a consumir recursos computacionales nuevamente. Los procesos que se ejecutan en una función de red virtual o VDU se reanudan desde el punto en el que se guardó su estado.

*Para suspender o anular la suspensión de una función de red virtual o su VDU:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Suspender o anular la suspensión de una función de red virtual o su VDU:

   - Si desea suspender o anular la suspensión de una función de red virtual, en la parte superior del área de configuración, haga clic en **Administración** → **Potencia** → **Suspender VNF** o **Reanudar VNF suspendida**.

   - Si desea suspender o anular la suspensión de una VDU que forma parte de la función de red virtual:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de las VDU.

     2. Haga clic en **Administración** → **Potencia** → **Suspender VDU** o **Reanudar VDU suspendida** junto a la VDU que desea suspender o anular la suspensión.

5. En la ventana de confirmación, haga clic en **Aplicar**.

La función de red virtual o su VDU está suspendida o se anuló la suspensión.

# Reinicio suave de una función de la red virtual o una VDU que forma parte de ella

Cuando una función de la red virtual se somete a un reinicio suave, se reinician todas las VDU activas en ella. Para realizar un reinicio suave de una función de la red virtual, no se debe suspender al menos una VDU.

*Para realizar un reinicio suave de una función de la red virtual o una VDU que forma parte de ella, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Realice un reinicio suave de una función de la red virtual o su VDU:

   - Si desea realizar un reinicio suave de una función de la red virtual, en la parte superior del área de configuración, haga clic en **Administración**→ **Potencia**→ **Reinicio suave de VNF**.

   - Si desea realizar un reinicio suave de una VDU que forma parte de la función de la red virtual:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de las VDU.

     2. Haga clic en **Administración** → **Potencia** → **Reinicio suave de VDU** junto a la VDU en la que desea realizar un reinicio suave.

5. En la ventana de confirmación, haga clic en **Aplicar**.

Se realiza un reinicio suave de la función de la red virtual o su VDU.

# Reinicio forzado de una función de la red virtual o una VDU que forma parte de ella

Un reinicio forzado imita el encendido y el apagado. Recomendamos que realice un reinicio forzado solo si el reinicio suave no se realiza correctamente.

*Para realizar un reinicio forzado de una función de la red virtual o una VDU que forma parte de ella, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Para realizar un reinicio forzado de una función de la red virtual o su VDU, siga estos pasos:

   - Si desea realizar un reinicio forzado de la función de la red virtual, en la parte superior del área de configuración, haga clic en **Administración**→ **Potencia**→ **Reinicio forzado de VNF**.
   - Si desea reiniciar una VDU que forma parte de la función de la red virtual:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de las VDU.

     2. Haga clic en **Administración** → **Potencia** → **Reinicio forzado de VDU** junto a la VDU que desea reiniciar.

5. En la ventana de confirmación, haga clic en **Aplicar**.

Se realiza un reinicio forzado de la VNF o su VDU.

# Volver a implementar una función de la red virtual o una VDU que forma parte de ella

El proceso para volver a implementar una función de red virtual o una VDU que forma parte de ella puede provocar interrupciones a corto plazo o la pérdida temporal de la función. Al planificar y coordinar estas actividades, recomendamos tener en cuenta las circunstancias de su organización para minimizar las interrupciones.

*Para volver a implementar una función de red virtual o una VDU que forma parte de ella:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Para volver a implementar una función de red virtual o su VDU:

   - Si desea volver a implementar la función de red virtual, en la parte superior del área de configuración, haga clic en **Administración** → **Volver a implementar VNF**.

   - Si desea volver a implementar una VDU que es parte de la función de red virtual:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de VDU.

     2. Haga clic en **Administración** → **Volver a implementar VDU** junto a la VDU que desea volver a implementar.

5. En la ventana de confirmación, haga clic en **Confirmar**.

Comienza el proceso de volver a implementar la función de red virtual o su VDU, lo que puede tardar varios minutos. Puede interrumpir la implementación haciendo clic en **Cancelar implementación**.

# Reparar automáticamente una función de la red virtual o una VDU que forma parte de ella

Puede reparar automáticamente una función de la red virtual o una VDU que forma parte de ella, incluso si deshabilitó la reparación automática del servicio de red a cuya topología se agregó esta función de la red virtual.

*Para reparar automáticamente una función de la red virtual o una VDU que forma parte de ella, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de red virtual.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Realice la reparación automática de la función de la red virtual o su VDU.

   - Si desea reparar automáticamente la función de la red virtual, en la parte superior del área de configuración, haga clic en **Administración** → **Corrección de VNF**.
   - Si desea reparar automáticamente una VDU que forma parte de la función de la red virtual, siga estos pasos:

     1. Seleccione la pestaña **Administración de VDU**.

        Se muestra una tabla de las VDU.

     2. Haga clic en **Administración** → **Corrección de VDU** junto a la VDU que desea reparar automáticamente.

5. En la ventana de confirmación, haga clic en **Aplicar**.

Comienza la reparación automática de la función de la red virtual o de una VDU que forma parte de ella.

# Administrar instantáneas de la VDU

Para ver la tabla de las instantáneas de la VDU, haga clic en la función de la red virtual en la topología del servicio de red implementado, seleccione la pestaña **Administración de VDU** y haga clic en **Administración** → **Instantánea** junto a la VDU.

La información sobre las instantáneas de la VDU se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la instantánea de la VDU.
- **Creada a las** es la fecha y la hora en que se creó la instantánea de la VDU.
- **Tamaño** es el tamaño de la instantánea de la VDU en bytes.
- **Descripción** es una breve descripción de la instantánea de la VDU.
- **Administración** contiene acciones que se pueden realizar en la instantánea de la VDU.

## Crear una instantánea de la VDU

No recomendamos almacenar instantáneas durante mucho tiempo, ya que su existencia reduce el rendimiento de la VDU.

*Para tomar una instantánea de la VDU, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de la red virtual que incluye la VDU.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Seleccione la pestaña **Administración de VDU**.

   Se muestra una tabla de las VDU.

5. Haga clic en **Potencia** → **Instantánea** junto a la VDU para la que desea crear una instantánea.

   Esto abre una ventana con la tabla de instantáneas de la VDU.

6. En el campo **Nombre**, escriba un nombre para la instantánea de la VDU.

7. En el campo **Descripción**, ingrese una descripción breve de la instantánea de la VDU.

8. Haga clic en **Crear**.

Se crea una instantánea de la VDU y se muestra en la tabla.

## Restaurar la configuración de la VDU mediante una instantánea

*Para restaurar la configuración de la VDU mediante una instantánea, haga lo siguiente:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de la red virtual que incluye la VDU.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Seleccione la pestaña **Administración de VDU**.

   Se muestra una tabla de las VDU.

5. Haga clic en **Potencia** → **Instantánea** junto a la VDU cuya configuración desea restaurar mediante la instantánea.

   Esto abre una ventana con la tabla de instantáneas de la VDU.

6. Haga clic en **Administración** → **Revertir** junto a la instantánea que desea utilizar para restaurar la configuración de la VDU.

7. En la ventana de confirmación, haga clic en **Revertir**.

La configuración de la VDU se restaurará de acuerdo con la instantánea.

## Editar una instantánea de la VDU

*Para editar una instantánea de la VDU, siga estos pasos:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de la red virtual que incluye la VDU.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir . De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Seleccione la pestaña **Administración de VDU**.

   Se muestra una tabla de las VDU.

5. Haga clic en **Potencia** → **Instantánea** junto a la VDU cuya instantánea desea editar.

   Esto abre una ventana con la tabla de instantáneas de la VDU.

6. Haga clic en **Administración** → **Editar** junto a la instantánea de la VDU que desea editar.

7. En la ventana que se abre, si es necesario, edite el nombre o la descripción de la instantánea de la VDU.

8. Haga clic en **Guardar**.

La instantánea de VDU se modifica y se actualiza en la tabla.

## Eliminar una instantánea de la VDU

Las instantáneas de la VDU eliminadas no se pueden restaurar.

*Para eliminar una instantánea de la VDU, haga lo siguiente:*

1. En el portal de autoservicio, vaya a la sección del menú **Catálogo**.

   Se muestra la página de administración de servicios de red.

2. En el panel **Servicios de red**, haga clic en el servicio de red implementado a cuya topología se agregó la función de red virtual.

   Se muestra la topología.

3. Haga clic en la función de la red virtual que incluye la VDU.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir . De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.

4. Seleccione la pestaña **Administración de VDU**.

   Se muestra una tabla de las VDU.

5. Haga clic en **Potencia** → **Instantánea** junto a la VDU cuya instantánea desea editar.

   Esto abre una ventana con la tabla de instantáneas de la VDU.

6. Haga clic en **Administración** → **Eliminar** junto a la instantánea de la VDU que desea eliminar.

7. En la ventana de confirmación, haga clic en **Eliminar**.

La instantánea de la VDU se eliminará y ya no se mostrará en la tabla.

# Administrar funciones de la red física

Para administrar una función de la red física, realice una de las siguientes acciones:

- En el portal del administrador, vaya a la sección **Catálogo** y, en el panel **Catálogo**, haga clic en la función de la red física.
- Cuando crea o edita una plantilla de servicio de red en la topología, haga clic en la función de la red física.
- Cuando crea o edita un servicio de red en la topología, haga clic en la función de red física.

Puede administrar la configuración de la función de la red física en las siguientes pestañas:

- **Variantes** contiene variantes de la función de la red física.
- **Configuración de VNF** contiene la configuración básica de la función de la red física.

Las siguientes pestañas se muestran si hizo clic en la función de la red física en la topología de un servicio de red implementado:

- **Supervisión** contiene los resultados de la supervisión de la función de la red física .
- **Problemas** contiene problemas que ocurrieron durante el funcionamiento de la función de la red física. En caso de que haya ocurrido un problema, se muestra un signo de exclamación rojo junto a la pestaña.

Además, es posible que se muestren las pestañas que especificó en la sección `user_configurations` del descriptor de PNF.

# Seleccionar el tipo de función de una red física

Puede especificar los tipos en la sección `tipos` del descriptor de PNF.

*Para seleccionar el tipo de función de una red física, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:
   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.
2. Haga clic en la función de la red física para la que desea seleccionar un tipo.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.
3. Seleccione un tipo de función de la red física.
4. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de la red física.

# Configuración básica de una función de la red física

*Para editar la configuración básica de la función de la red física, haga lo siguiente:*

1. Navegue a la topología de una de las siguientes maneras:
   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.
2. Haga clic en la función de la red física para la que desea establecer la configuración básica.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, la pestaña **Variantes** está seleccionada y muestra los tipos.
3. Seleccione la pestaña **Configuración de PNF**.

   Se muestra la configuración básica de la función de la red física.
4. En el campo **Nombre**, ingrese el nombre de la función de la red física.
5. En el campo **Descripción**, ingrese una breve descripción de la función de la red física.
6. En el campo **Orden**, ingrese el número de secuencia para implementar la función de la red física. Cuando implementa un servicio de red, la función de la red física con el número más bajo es la primera en implementarse. Si ninguna de las funciones de la red física agregadas a la topología tiene un número de secuencia especificado, todas las funciones de la red física se implementan simultáneamente.
7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la función de la red física.

# Configurar un servicio P2P

*Para configurar un servicio P2P, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en el servicio P2P que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre del servicio P2P.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del servicio P2P.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del servicio P2P.

# Configurar un servicio P2M

*Para configurar un servicio P2M, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en el servicio P2M que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre del servicio P2M.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del servicio P2M.

5. En el campo **Puntos de conexión**, ingrese el número máximo de puntos de conexión del servicio P2M. Rango de valores: de 2 a 9999. Si no especifica un valor para esta configuración, el número de puntos de conexión es ilimitado.

6. En la lista desplegable **Modo**, seleccione si el servicio P2M utiliza una DFI (Interfaz de reenvío predeterminada), a la que se envía el tráfico de unidifusión desconocido:

   - **Clásico** si no desea utilizar una DFI. Esta es la configuración predeterminada.
   - **DFI con FIB en la raíz y las hojas** si desea utilizar una DFI en la interfaz de servicio con el rol raíz.
   - **DFI con FIB en la hoja** si desea utilizar una DFI en la interfaz de servicio con el rol raíz. Debe crear interfaces de servicio con el rol de hoja en el mismo dispositivo CPE. Las interfaces de servicio de respaldo con el rol de hoja deben crearse en el mismo dispositivo CPE, que debe ser diferente del dispositivo CPE en el que se crean las interfaces de servicio principales.

7. En el campo **Antigüedad de MAC (s)**, ingrese el período de tiempo en segundos en el que las entradas se mantienen en la tabla MAC del controlador. Rango de valores: 10 a 65 535. El valor predeterminado es `300`.

8. En la lista desplegable **Modo de aprendizaje de MAC**, seleccione la acción que desea aplicar a una serie de marcos cuando el primer marco se envíe al controlador para conocer la dirección MAC de origen:

   - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio P2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos. Esta es la configuración predeterminada.
   - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

   Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

9. En el campo **Tamaño de la tabla MAC**, ingrese la cantidad máxima de entradas en la tabla MAC del controlador. Rango de valores: de 0 a 65 535. `0` significa que el número de entradas no está limitado. El valor predeterminado es `100`.

10. En la lista desplegable **Sobrecarga en tabla MAC**, seleccione la directiva para el procesamiento de las nuevas direcciones MAC cuando la tabla MAC del controlador esté completa:

    - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.
    - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

11. Si desea configurar la asignación de direcciones IP a las funciones de la red virtual mediante DHCP:

    a. En la lista desplegable **DHCP de OpenStack**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitar**.

    b. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de OpenStack que asigna direcciones IP a las funciones de red virtual.

    c. Si desea que la subred de OpenStack asigne una puerta de enlace en particular a las funciones de red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

d. Especifique el rango de direcciones IP desde el cual la subred OpenStack asigna direcciones IP a funciones de red virtual: para ello, en**Agrupaciones**, haga clic en **+ Agrupación** e ingrese los valores inicial y final del rango de direcciones IP.

   El rango de direcciones IP se especifica y se muestra en la sección **Agrupaciones**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en **Eliminar** junto a él.

e. Especifique el servidor DNS que la subred de OpenStack asigna a las funciones de red virtual. Para hacerlo, en **DNS**, haga clic en **+ DNS** e ingrese la dirección IPv4 del servidor DNS.

   El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en **Eliminar** junto a él.

12. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del servicio P2M.

# Configurar un servicio M2M

*Para configurar un servicio M2M, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en el servicio M2M que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre del servicio M2M.

4. Si es necesario, en el campo **Descripción**, escriba una breve descripción del servicio M2M.

5. En el campo **Puntos de conexión**, ingrese el número máximo de puntos de conexión del servicio M2M. Rango de valores: de 2 a 9999. Si no especifica un valor para esta configuración, el número de puntos de conexión es ilimitado.

6. En el campo **Antigüedad de MAC (s)**, ingrese el período de tiempo en segundos en el que las entradas se mantienen en la tabla MAC del controlador. Rango de valores: 10 a 65 535. El valor predeterminado es `300`.

7. En la lista desplegable **Modo de aprendizaje de MAC**, seleccione la acción que desea aplicar a una serie de marcos cuando el primer marco se envíe al controlador para conocer la dirección MAC de origen:

   - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio P2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos. Esta es la configuración predeterminada.
   - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

8. En el campo **Tamaño de la tabla MAC**, ingrese la cantidad máxima de entradas en la tabla MAC del controlador. Rango de valores: de 0 a 65 535. `0` significa que el número de entradas no está limitado. El valor predeterminado es `100`.

9. En la lista desplegable **Sobrecarga en tabla MAC**, seleccione la directiva para el procesamiento de las nuevas direcciones MAC cuando la tabla MAC del controlador esté completa:

   - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.

   - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

10. Si desea configurar la asignación de direcciones IP a las funciones de la red virtual mediante DHCP:

    a. En la lista desplegable **DHCP de OpenStack**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitar**.

    b. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de OpenStack que asigna direcciones IP a las funciones de red virtual.

    c. Si desea que la subred de OpenStack asigne una puerta de enlace en particular a las funciones de red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

    d. Especifique el rango de direcciones IP desde el cual la subred OpenStack asigna direcciones IP a funciones de red virtual: para ello, en**Agrupaciones**, haga clic en **+ Agrupación** e ingrese los valores inicial y final del rango de direcciones IP.

    El rango de direcciones IP se especifica y se muestra en la sección **Agrupaciones**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en **Eliminar** junto a él.

    e. Especifique el servidor DNS que la subred de OpenStack asigna a las funciones de red virtual. Para hacerlo, en **DNS**, haga clic en **+ DNS** e ingrese la dirección IPv4 del servidor DNS.

    El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en **Eliminar** junto a él.

11. Si desea utilizar un servicio M2M para crear un servicio de red compartido, seleccione la casilla **Compartir servicio de red**. Esta casilla está desactivada por defecto.

12. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del servicio M2M.

# Configurar una red compartida (OS 2 SHARED)

*Para configurar una red compartida en la topología:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.

   - Comience a crear o editar un servicio de red.

2. Haga clic en la red compartida que desea configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre de la red compartida.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción de la red compartida.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de red compartida.

# Configurar un enrutador virtual (OS vRouter)

*Para configurar un enrutador virtual, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.

   - Comience a crear o editar un servicio de red.

2. Haga clic en el enrutador virtual que desea configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre del enrutador virtual.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del enrutador virtual.

5. Si desea configurar el valor "up" para el estado operativo del enrutador virtual, seleccione la casilla **Estado administrativo**. Esta casilla está desactivada por defecto.

6. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración del enrutador virtual.

# Configurar una VLAN

*Para configurar una VLAN, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.

   - Comience a crear o editar un servicio de red.

2. Haga clic en la VLAN que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre de la VLAN.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción de la VLAN.

5. Si desea configurar la asignación de direcciones IP a las funciones de la red virtual mediante DHCP:

   a. En la lista desplegable **DHCP de OpenStack**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitar**.

   b. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de OpenStack que asigna direcciones IP a las funciones de red virtual.

   c. Si desea que la subred de OpenStack asigne una puerta de enlace en particular a las funciones de red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

   d. Especifique el rango de direcciones IP desde el cual la subred OpenStack asigna direcciones IP a funciones de red virtual: para ello, en**Agrupaciones**, haga clic en **+ Agrupación** e ingrese los valores inicial y final del rango de direcciones IP.

      El rango de direcciones IP se especifica y se muestra en la sección **Agrupaciones**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en **Eliminar** junto a él.

   e. Especifique el servidor DNS que la subred de OpenStack asigna a las funciones de red virtual. Para hacerlo, en **DNS**, haga clic en **+ DNS** e ingrese la dirección IPv4 del servidor DNS.

      El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en **Eliminar** junto a él.

6. Si desea utilizar la VLAN para crear un servicio de red compartido, seleccione la casilla **Compartir red**. Esta casilla está desactivada por defecto.

7. Si desea asignar una etiqueta VLAN a las funciones de red virtual, en el campo **ID de segmentación**, ingrese la etiqueta VLAN.

8. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de VLAN.

# Configurar una VXLAN

*Para configurar una VXLAN, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.

   - Comience a crear o editar un servicio de red.

2. Haga clic en la VXLAN que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre de la VXLAN.

4. Si es necesario, en el campo **Descripción**, ingrese una descripción breve de la VXLAN.

5. Si desea configurar la asignación de direcciones IP a las funciones de la red virtual mediante DHCP:

   a. En la lista desplegable **DHCP de OpenStack**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitar**.

   b. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de OpenStack que asigna direcciones IP a las funciones de red virtual.

   c. Si desea que la subred de OpenStack asigne una puerta de enlace en particular a las funciones de red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

   d. Especifique el rango de direcciones IP desde el cual la subred OpenStack asigna direcciones IP a funciones de red virtual: para ello, en**Agrupaciones**, haga clic en **+ Agrupación** e ingrese los valores inicial y final del rango de direcciones IP.

      El rango de direcciones IP se especifica y se muestra en la sección **Agrupaciones**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en **Eliminar** junto a él.

   e. Especifique el servidor DNS que la subred de OpenStack asigna a las funciones de red virtual. Para hacerlo, en **DNS**, haga clic en **+ DNS** e ingrese la dirección IPv4 del servidor DNS.

      El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en **Eliminar** junto a él.

6. Si desea utilizar la VXLAN para crear un servicio de red compartido, seleccione la casilla **Compartir red**. Esta casilla está desactivada por defecto.

7. Si desea asignar una etiqueta VXLAN a las funciones de la red virtual, en el campo **ID de segmentación**, ingrese la etiqueta VXLAN.

8. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de VXLAN.

# Configurar una red plana

*Para configurar una red plana, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en la red plana que desea configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre de la red plana.

4. Si es necesario, en el campo **Descripción**, ingrese una descripción breve de la red plana.

5. Si desea configurar la asignación de direcciones IP a las funciones de la red virtual mediante DHCP:

   a. En la lista desplegable **DHCP de OpenStack**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitar**.

   b. En el campo **CIDR**, ingrese el prefijo IPv4 de la subred de OpenStack que asigna direcciones IP a las funciones de red virtual.

   c. Si desea que la subred de OpenStack asigne una puerta de enlace en particular a las funciones de red virtual, ingrese la dirección IPv4 de la puerta de enlace en el campo **Gateway**.

   d. Especifique el rango de direcciones IP desde el cual la subred OpenStack asigna direcciones IP a funciones de red virtual: para ello, en**Agrupaciones**, haga clic en **+ Agrupación** e ingrese los valores inicial y final del rango de direcciones IP.

      El rango de direcciones IP se especifica y se muestra en la sección **Agrupaciones**. Puede especificar varios rangos de direcciones IP o eliminar rangos de direcciones IP. Para eliminar un rango de direcciones IP, haga clic en **Eliminar** junto a él.

   e. Especifique el servidor DNS que la subred de OpenStack asigna a las funciones de red virtual. Para hacerlo, en **DNS**, haga clic en **+ DNS** e ingrese la dirección IPv4 del servidor DNS.

      El servidor DNS se especifica y se muestra en la sección **DNS**. Puede especificar varios servidores DNS o eliminar servidores DNS. Para eliminar un servidor DNS, haga clic en **Eliminar** junto a él.

6. Si desea utilizar la red plana para crear un servicio de red compartido, seleccione la casilla **Compartir red**. Esta casilla está desactivada por defecto.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la red plana.

# Configurar una UNI

*Para configurar una UNI, siga estos pasos:*

1. Navegue a la topología de una de las siguientes maneras:

   - Comience a crear o editar una plantilla de servicio de red.
   - Comience a crear o editar un servicio de red.

2. Haga clic en la UNI que desee configurar.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗.

3. En el campo **Nombre**, escriba el nombre de la regla.

4. Si es necesario, en el campo **Descripción**, ingrese una breve descripción de la UNI.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la UNI.

# Supervisar los componentes de una solución

Se utiliza un sistema de supervisión Zabbix externo para supervisar los dispositivos CPE, así como las funciones de la red virtual y las funciones de la red física. Debe implementar un servidor Zabbix en una de sus ubicaciones, o hacer una conexión con un servidor Zabbix existente e implementar servidores proxy de Zabbix.

Los servidores proxy de Zabbix se utilizan para recibir los resultados de la supervisión en ubicaciones individuales y enviar estos resultados de supervisión al servidor Zabbix. El servidor Zabbix procesa los resultados de la supervisión, después de lo cual se muestran en la interfaz web del orquestador.

El orquestador utiliza una API para integrarse con el servidor Zabbix. Cuando registra un dispositivo CPE o implementa una función de la red virtual o una función de la red física en un servicio de red, se crea automáticamente un host correspondiente en el servidor Zabbix. Puede especificar los grupos en el servidor Zabbix en los que se colocarán los hosts. El host del servidor Zabbix se elimina automáticamente si elimina el dispositivo CPE correspondiente, la función de la red virtual o la función de la red física.

Se admiten dos métodos de supervisión:

- La supervisión mediante agentes de Zabbix implica que un componente envíe automáticamente datos de supervisión a un servidor proxy de Zabbix.
- La supervisión a través de SNMP implica que el servidor proxy Zabbix establezca automáticamente una conexión con un componente a través de SNMP y reciba datos de supervisión.

Para obtener detalles sobre la configuración del sistema de supervisión, consulte la documentación oficial de la solución Zabbix.

# Especificar el servidor Zabbix

*Para especificar el servidor Zabbix, haga lo siguiente:*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **Supervisión**.

   Se muestra la configuración para conectarse al servidor Zabbix.

3. En el campo **URL**, ingrese la URL de la API de Zabbix. El orquestador envía solicitudes HTTP a la URL especificada para recibir los resultados de la supervisión y mostrarlos como gráficos.

   La URL consta de la dirección de la interfaz web de Zabbix y el nombre del archivo api_jsonrpc.php, que se utiliza para las llamadas a la API. Por ejemplo, si la interfaz web de Zabbix se encuentra en http://192.168.2.1, ingrese `http://192.168.2.1/api_jsonrpc.php`.

4. En el campo **Nombre de usuario**, ingrese el nombre de usuario para conectar el orquestador a la API de Zabbix. Debe ingresar el nombre de usuario de una cuenta que tenga permisos de lectura y escritura para los grupos en el servidor Zabbix, así como el permiso para crear grupos.

5. En el campo **Contraseña**, ingrese la contraseña para conectarse a la API de Zabbix.

6. En la lista desplegable **Agrupación por Zabbix**, seleccione un método para agrupar los hosts del dispositivo CPE, así como las funciones de la red virtual y las funciones de la red física en el servidor Zabbix:

   - **Por grupos especificados** para colocar los hosts de los dispositivos CPE, las funciones de la red virtual y las funciones de la red física en los grupos especificados. Si selecciona esta opción, haga lo siguiente:

     a. En el campo **Grupo de VNF/PNF**, ingrese un nombre de grupo para los hosts de las funciones de la red virtual y las funciones de la red física.

     b. En el campo **Grupo de CPE**, ingrese un nombre de grupo para los hosts del dispositivo CPE.

   - **Por inquilino** para colocar los hosts de los dispositivos CPE, las funciones de la red virtual y las funciones de la red física en los grupos creados automáticamente. Los grupos corresponden a los inquilinos en los que se agregan los dispositivos CPE, y se asignan las funciones de la red virtual y las funciones de la red física.

7. En el campo **Activar sincronización (s)**, ingrese el intervalo en segundos para recibir las notificaciones sobre los problemas del servidor Zabbix en el orquestador. Rango de valores: 5 a 600. El valor predeterminado es `600`.

8. Debajo del campo **Token**, haga clic en **Generate** para generar el token que deben contener las solicitudes de la API desde el servidor Zabbix al orquestador. Si una solicitud de la API no contiene el token, el orquestador no acepta dicha solicitud. La seguridad también está protegida por certificados TLS.

   Puede ingresar el token manualmente o verlo si hace clic en el ícono de visualizar.

9. Si desea consultar la disponibilidad del servidor Zabbix, haga clic en **Probar conexión**.

10. Haga clic en **Aplicar**.

Se especificará el servidor Zabbix.

# Especificar el servidor proxy Zabbix

*Para especificar un servidor proxy Zabbix, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. En el panel **Recursos**, seleccione el dominio creado, luego seleccione el centro de datos agregado para el cual desea especificar un servidor proxy Zabbix.

3. Seleccione la pestaña **Recursos del sistema**.

   Se muestra la configuración para la conexión al servidor proxy Zabbix y VNFM.

4. En **Proxy de Zabbix**, en el campo **Nombre**, ingrese el nombre del servidor proxy Zabbix. El nombre debe coincidir con el nombre especificado en la configuración del servidor Zabbix.

5. En el campo **Dirección IP**, ingrese la dirección IP del servidor proxy Zabbix. La dirección IP ingresada debe ser accesible para los dispositivos CPE y las funciones de la red virtual y las funciones de la red física que desea supervisar.

6. Haga clic en **Aplicar**.

Se especifica el servidor proxy Zabbix.

Para eliminar la configuración de conexión del servidor proxy Zabbix, haga clic en **Eliminar**.

# Configurar la supervisión de dispositivos CPE

Puede configurar la supervisión en una plantilla de CPE. La configuración de la supervisión especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para configurar la supervisión de dispositivos CPE, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea configurar la supervisión.

   El área de configuración se muestra en la parte inferior de la página. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⌃. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Supervisión**.

   Se muestra la configuración de supervisión de los dispositivos CPE.

4. En la lista desplegable **Tipo de supervisión**, seleccione un método de supervisión para el dispositivo CPE:

   - **SNMP** significa supervisar usando el protocolo SNMP.
   - **Agente** implica la supervisión mediante agentes Zabbix.

5. En el campo **Plantilla de Zabbix**, escriba el nombre de la plantilla Zabbix.

6. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Visualizar los resultados del control

Puede ver los resultados del control de una instancia SD-WAN, un dispositivo CPE, una función de red virtual o una función de red física:

- Para ver los resultados del control de una instancia SD-WAN, vaya a la sección **SD-WAN**→**Instancias SD-WAN**, la instancia SD-WAN y seleccione la pestaña **Supervisión**.
- Para ver los resultados del control de un dispositivo CPE, vaya a la sección **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Supervisión**.
- Para ver los resultados del control de una función de red virtual o una función de red física, inicie sesión en el portal de autoservicio, vaya a la sección del menú **Catálogo**, en el panel **Servicios de red**, haga clic en el servicio de red implementado, haga clic en la función de red virtual o física y seleccione la pestaña **Supervisión**.

En la lista desplegable en la parte superior del área de configuración, puede seleccionar el parámetro para el que se muestran los resultados del control. Para ver los resultados del control durante un período seleccionado, puede utilizar los siguientes filtros de tiempo:

- **Tiempo real**
- **Día**
- **Una semana**
- **Mes**

También puede especificar el período de tiempo manualmente.

# Visualización de problemas

La configuración de control en el servidor Zabbix determina qué problemas requieren notificaciones y cómo se clasifican estos problemas de acuerdo con sus niveles de gravedad. Puede ver la tabla de problemas en el dispositivo CPE y en la configuración de la función de red virtual o física:

- Para ver la tabla de problemas para un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Problemas**.
- Para ver la tabla de problemas de una función de red virtual o física, inicie sesión en el portal de autoservicio, vaya a la sección del menú **Catálogo**, en el panel **Servicios de red**, haga clic en el servicio de red implementado, haga clic en la función de red virtual o en la función de red física y seleccione la pestaña **Problemas**.

La información sobre los problemas se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del problema.
- **Nivel** es el nivel de gravedad del problema:
  - **Promedio**
  - **Desastre**
  - **Alto**
  - **Información**
  - **Sin clasificación**
- **Hora** es el momento en que ocurrió el problema.
- **Duración** es la duración del problema en segundos.

# Ver el estado de la solución y sus componentes

*Para ver el estado de los componentes de la solución, haga lo siguiente:*

1. En el menú, vaya a la sección **Panel**.

   Se muestran los siguientes bloques de información:

   - **Errores de evento** contiene los errores que se produjeron durante los eventos.
   - **Errores de la tarea** contiene los errores que se produjeron cuando se realizaron tareas personalizadas.
   - **Sesiones activas** contiene las sesiones de usuario activas.
   - **Recursos** contiene información sobre el uso de los recursos informáticos por parte de los componentes de la solución.
   - **Solicitudes del servicio** contiene las solicitudes de servicio.
   - **CPE desconectado** contiene los dispositivos CPE a los que se ha perdido acceso.
   - **Errores en el CPE** contiene los errores que encontraron los dispositivos CPE.
   - **Problemas en el CPE** contiene los problemas que encontraron los dispositivos CPE.
   - **Problemas en VNF/PNF** contiene los problemas que encontraron las funciones de la red virtual y las funciones de la red física.

   Si un componente de la solución funciona correctamente, el widget correspondiente muestra el mensaje *Todo funciona sin problemas*. Se muestra el ícono de actualizar en la parte superior de un bloque; cuando se hace clic en este ícono, se actualiza la información que se muestra. Puede arrastrar bloques con el mouse para cambiar el diseño.

2. Si desea configurar qué bloques se muestran de manera predeterminada, en la parte superior de la página, haga clic en el ícono de configuración → **Restablecer al diseño predeterminado**.

3. Si desea establecer un intervalo de tiempo diferente para actualizar la información en los bloques, haga lo siguiente:

   a. En la parte superior de la página, haga clic en el ícono de configuración → **Configurar intervalo de actualizaciones**.

   b. En la ventana que se abre, en el campo **Actualizar panel cada (s)**, ingrese el intervalo en segundos para la actualización de la información en los bloques. Rango de valores: 5 a 86 400. La configuración predeterminada es `60`.

   c. Haga clic en **Aceptar**.

   Se modificará el intervalo de actualización de la información en los bloques.

# Ver registros

Puede ver los registros de los componentes de la solución con fines de soporte técnico. Kaspersky SD-WAN no envía registros fuera del perímetro de la infraestructura de información de su organización.

*Para ver los registros, siga estos pasos:*

1. En el menú, vaya a la sección **Registros**.

   Se muestra la página de administración de registros.

2. En el panel **Centros de datos**, seleccione el centro de datos creado al que pertenecen los componentes de la solución.

3. En el panel **Recursos**, seleccione el componente de la solución cuyo registro desea ver.

   Se muestra el registro. De manera predeterminada, está seleccionada la pestaña **Tareas**, que muestra la tabla de tareas personalizadas. La información sobre las tareas personalizadas se muestra en las siguientes columnas de la tabla:

   - **Acción de tarea** es la acción de la tarea personalizada.
   - **Objeto** es el componente de la solución asociado con la tarea personalizada.
   - **SR** es un vínculo a la solicitud de servicio asociada con la tarea personalizada.
   - **ID del objeto** es el ID del componente de la solución asociado con la tarea personalizada.
   - **Nombre de objeto** es el nombre del componente de la solución asociado con la tarea personalizada.
   - **Iniciador** es el nombre del usuario que ejecutó la tarea personalizada.
   - **IP del iniciador** es la dirección IP del usuario que ejecutó la tarea personalizada.
   - **Hora de inicio** es la fecha y la hora en que se inició la ejecución de la tarea personalizada.
   - **Hora de finalización** es la fecha y la hora en que la tarea personalizada terminó de ejecutarse.

4. Si desea ver información sobre los eventos que ocurrieron durante la operación de un componente de la solución, seleccione la pestaña **Eventos**.

   Se muestra una tabla de eventos. La información sobre los eventos se muestra en las siguientes columnas de la tabla:

   - **Acción de evento** es la acción del evento.
   - **Objeto** es el componente de la solución asociado con el evento.
   - **SR** es un vínculo a la solicitud de servicio asociada con el evento.
   - **Nombre de objeto** es el nombre del componente de la solución asociado con el evento.
   - **ID del objeto** es el ID del componente de la solución asociado con el evento.

- **Iniciador** es el nombre del usuario cuya acción causó el evento.
- **Hora** es la fecha y la hora en que se creó el evento.

5. Si desea ver las solicitudes de servicio de un componente de la solución, seleccione la pestaña **Solicitudes del servicio**.

   Se muestra una tabla de solicitudes de servicio. La información sobre las solicitudes de servicio se muestra en las siguientes columnas de la tabla:

   - **Solicitud de servicio** es el nombre de la solicitud de servicio.
   - **Estado** es el estado de la solicitud de servicio.
   - **Iniciador** es el nombre de usuario cuya acción provocó la solicitud de servicio.
   - **Hora** es la fecha y la hora en que se creó la solicitud de servicio.

Las acciones que puede realizar con las tablas se describen en las instrucciones de Administración de las tablas de componentes de la solución.

# Ver y eliminar solicitudes de servicio

Las *solicitudes de servicio* son tareas que se realizan mientras los componentes de la solución están funcionando y se crean automáticamente como resultado de las acciones del usuario. Por ejemplo, cuando un usuario aplica una plantilla de CPE a un dispositivo CPE, se crea una solicitud de servicio correspondiente. Cada solicitud de servicio consta de varios pasos que se ejecutan en secuencia.

## Ver solicitudes de servicio

Puede ver las solicitudes de servicio de un inquilino, un dispositivo CPE y una instancia SD-WAN:

- Para ver las solicitudes de servicio de un inquilino, vaya a la sección **Inquilinos** y, en **Inquilinos**, seleccione un inquilino.

  La lista de solicitudes de servicio se muestra en **Solicitudes del servicio**.

- Para ver las solicitudes de servicio para una instancia SD-WAN, vaya a la sección **SD-WAN→Instancias SD-WAN**, haga clic en la instancia SD-WAN y seleccione la pestaña **Solicitudes del servicio**.

  Se muestra una tabla de solicitudes de servicio.

- Para ver las solicitudes de servicio para un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Solicitudes del servicio**.

  Se muestra una tabla de solicitudes de servicio.

La lista de solicitudes de servicio de un inquilino muestra el nombre y el ID de la solicitud de servicio, así como su fecha y hora de creación. La información sobre las solicitudes de servicio de una instancia SD-WAN y un dispositivo CPE se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la solicitud de servicio.
- **Creado** es la fecha y la hora en que se creó la solicitud de servicio.

- **ID de tarea** es el ID de la solicitud de servicio.
- **Hora** es la duración de la solicitud de servicio en segundos.
- **Estado** es el estado de la solicitud de servicio:
  - **Ejecutando** significa que la solicitud de servicio se está ejecutando.
  - **No ejecutado** significa que ocurrió un error durante la ejecución de la solicitud de servicio.
  - **Ejecutado** significa que la solicitud de servicio se ejecutó correctamente.
  - **Revirtiendo** significa que se produjo un error durante la ejecución de uno de los pasos de la solicitud de servicio, por lo que los pasos que ya se ejecutaron ahora se revierten.
  - **No revertido** significa que se produjo un error al revertir uno de los pasos ejecutados anteriormente de la solicitud de servicio.
  - **Revertido** significa que los pasos de la solicitud de servicio ejecutados anteriormente se revirtieron con éxito.
  - **Suspendida** significa que se produjo un error durante la ejecución de la solicitud de servicio para registrar el dispositivo CPE y no se completó el registro del dispositivo CPE. Puede reanudar el registro del dispositivo CPE.
- **Acciones** contiene las acciones que se pueden realizar con las solicitudes de servicio.

Puede abrir el registro de la solicitud de servicio:

- Si desea abrir el registro de la solicitud de servicio de un inquilino, haga clic en el nombre de la solicitud de servicio.
- Si desea abrir el registro de una solicitud de servicio para una instancia SD-WAN o un dispositivo CPE, haga clic en el ID de la solicitud de servicio.

Se muestra un registro de la solicitud de servicio.

El registro contiene información sobre los pasos en los que se produjeron los errores. Puede hacer clic en el paso en el que se produjo el error para ver una descripción detallada de ese error.

## Eliminar solicitudes de servicio

Puede eliminar las solicitudes de servicio de una instancia SD-WAN o un dispositivo CPE. Solo se eliminan las solicitudes de servicio que tienen un estado diferente a **Suspendida**. Cuando elimina una solicitud de servicio, se detiene la operación asociada.

Las solicitudes de servicio eliminadas no se pueden restaurar.

Para eliminar una solicitud de servicio, realice una de las siguientes acciones:

- Si desea eliminar una solicitud de servicio individual, haga clic en **Eliminar** junto a ella.
- Si desea eliminar todas las solicitudes de servicio, en la parte superior del área de configuración, en **Acciones**, haga clic en **Eliminar todo**.

Para confirmar la eliminación, haga clic en el botón **Eliminar** en la ventana que se muestra.

Las solicitudes de servicio se eliminan y ya no se muestran en la tabla.

# Enviar notificaciones del dispositivo CPE a los usuarios

Kaspersky SD-WAN admite el envío de notificaciones a las direcciones de correo electrónico de los usuarios con la siguiente información sobre los dispositivos CPE:

- Eventos del registro:
  - Habilitar y deshabilitar un dispositivo CPE
  - Conexión o desconexión de un puerto
  - Conexión o desconexión de un vínculo
- Problemas:
  - Problemas encontrados
  - Problemas resueltos

La información se acumula durante cinco segundos antes de que se envíe la notificación. Por ejemplo, si la desconexión de un puerto provoca la desconexión de cinco vínculos, esta información debe acumularse y enviarse al usuario en la misma notificación.

Especifique el servidor SMTP que utilizarán todos los inquilinos para enviar notificaciones. En el portal del administrador, puede configurar notificaciones sobre eventos y problemas para todos los inquilinos. En el portal de autoservicio, puede configurar notificaciones sobre eventos y problemas para un inquilino individual.

# Especificar el servidor SMTP

*Para especificar un servidor SMTP, siga estos pasos:*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **Notificación → SMTP**.

   Se muestra la configuración de conexión del servidor SMTP.

3. Seleccione la casilla **Habilitar** para usar el servidor SMTP. Esta casilla está desactivada por defecto.

4. En el campo **servidor SMTP**, ingrese la dirección IP o el nombre de dominio del servidor SMTP.

5. En el campo **Puerto del servidor SMTP**, ingrese el número de puerto del servidor SMTP. Rango de valores: de 0 a 65 535. El valor predeterminado es `25`.

6. En el campo **Correo electrónico del remitente**, ingrese la dirección de correo electrónico desde la cual el servidor SMTP envía notificaciones a los usuarios.

7. Si desea configurar el cifrado de la conexión entre Kaspersky SD-WAN y el servidor SMTP, en la lista desplegable **SSL/TLS**, seleccione uno de los siguientes valores:

   - **Ninguna** para dejar la conexión sin cifrar. Esta es la configuración predeterminada.
   - **STARTTLS** para determinar el método de cifrado y luego establecer una conexión cifrada.
   - **SMTPS** para establecer una conexión cifrada de inmediato.

8. Si desea habilitar la autenticación de Kaspersky SD-WAN en el servidor SMTP:

   a. Seleccione la casilla de verificación **Autenticación**. Esta casilla está desactivada por defecto.

   b. En el campo **Nombre de usuario**, ingrese el nombre de usuario que utiliza Kaspersky SD-WAN para autenticarse en el servidor SMTP. La longitud máxima del nombre es de 64 caracteres.

   c. En el campo **Contraseña**, ingrese la contraseña que utiliza Kaspersky SD-WAN para autenticarse en el servidor SMTP. La longitud máxima de la contraseña es de 64 caracteres. Para ver la contraseña ingresada, puede hacer clic en el ícono de mostrar 👁.

9. Si desea enviar un mensaje de prueba mediante el servidor SMTP:

   a. Haga clic en **Prueba**.

   b. En la ventana que se abre, ingrese la dirección de correo electrónico a la que desea que el servidor SMTP envíe un mensaje de prueba.

   c. Haga clic en **Enviar**.

   Se envía un mensaje de prueba a la dirección de correo electrónico especificada con *Prueba de notificación* en el asunto y el cuerpo.

10. Haga clic en **Aplicar**.

Se especifica el servidor SMTP.

# Configurar notificaciones

El administrador de la plataforma debe especificar el servidor SMTP para permitir el envío de notificaciones al usuario.

*Para configurar las notificaciones, siga estos pasos:*

1. En el menú, vaya a la sección **Sistema**.

   De manera predeterminada, la pestaña **Supervisión** está seleccionada, que muestra la configuración de conexión del servidor Zabbix.

2. Seleccione la pestaña **Notificación**→ **Alerta**.

   Se muestra la configuración de las notificaciones.

3. Seleccione la casilla **Habilitar** para enviar notificaciones al usuario. Esta casilla está desactivada por defecto.

4. En el campo **Dirección de correo electrónico del destinatario**, ingrese la dirección de correo electrónico a la que desea enviar las notificaciones.

5. En el campo **Asunto**, ingrese el texto del asunto de los mensajes de correo electrónico de notificación. La longitud máxima del tema es de 64 caracteres.

6. Haga clic en **Aplicar**.

Las notificaciones se enviarán a la dirección de correo electrónico especificada.

# Seleccionar la verbosidad del registro del contenedor Docker

Kaspersky SD-WAN mantiene automáticamente los registros de los contenedores de Docker del controlador y el orquestador. Puede seleccionar el nivel de detalle del registro del contenedor de Docker.

*Para seleccionar el nivel de detalle del registro del contenedor de Docker, siga estos pasos:*

1. Seleccione el nivel de detalle de los registros del contenedor de Docker de una de las siguientes maneras:

   - Si desea seleccionar el nivel de detalle del registro del contenedor de Docker para el controlador, en el menú, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador, y vaya a la sección **Registros**.

   - Si desea seleccionar el nivel de detalle del registro del contenedor de Docker para el orquestador, en el menú, vaya a la sección **Sistema** y seleccione la pestaña **Registro del orquestador**.

   Se abre una página en la que se muestra una tabla de contenedores de Docker. La información sobre los contenedores de Docker se muestra en las siguientes columnas de la tabla:

   - **Nombre del módulo** es el nombre del contenedor de Docker.

   - **Nivel de registro** es el nivel de detalle del registro del contenedor de Docker:

   Para buscar el contenedor de Docker, ingrese su nombre en el campo **Filtro**.

2. Seleccione el nivel de detalle del contenedor de Docker de una de las siguientes maneras:

   - Si desea seleccionar el nivel de detalle de todos los contenedores de Docker, haga clic en el botón correspondiente en la sección **Nivel de registro general**.

   - Si desea seleccionar el nivel de detalle para un contenedor de Docker individual, haga clic en el botón correspondiente junto a él.

Puede seleccionar los siguientes niveles de detalle para los contenedores de Docker:

- **SEGUIMIENTO** para que el registro incluya la información más completa sobre el funcionamiento y el estado del módulo y sus variables. Puede utilizar este nivel de detalle para observar la ejecución del código, así como para el diagnóstico y el análisis detallado de los errores que ocurren durante el desarrollo.

- **DEPURAR** para que el registro incluya la información necesaria para depurar el módulo, como el estado de las operaciones y los valores de las variables. Puede utilizar este nivel de detalle para diagnosticar errores y analizar el comportamiento del módulo.

- **INFORMACIÓN** para que el registro incluya información general necesaria para comprender el funcionamiento del módulo, por ejemplo, confirmaciones de operaciones. Puede utilizar este nivel de detalle para realizar un seguimiento del progreso de la ejecución del módulo. Este nivel de detalle está seleccionado de manera predeterminada para todos los contenedores.

- **ADVERTIR** para que el registro incluya información sobre incidentes que no son errores, pero que pueden poner en riesgo el funcionamiento del contenedor y requerir su intervención, como problemas con la configuración y funciones obsoletas. Puede utilizar este nivel de detalle para evitar posibles errores.

- **ERROR** para que el registro incluya información sobre los errores que ocurren durante la ejecución del código y requieren su intervención. Un mensaje de error puede contener información sobre la parte del contenedor en la que se produjo el error, así como información detallada sobre el error. Puede utilizar este nivel de detalle para resolver los errores que se produzcan.

Se modifica el nivel de detalle del registro del contenedor de Docker.

# Supervisar dispositivos CPE, VNF y PNF mediante el SNMP

Puede utilizar el SNMP para supervisar dispositivos CPE, así como funciones de la red virtual y funciones de la red física. Debe instalar un agente de SNMP en el componente que desea supervisar. El agente de SNMP recopila datos de supervisión y los envía al administrador de SNMP para su procesamiento. En Kaspersky SD-WAN, el servidor proxy Zabbix actúa como administrador de SNMP.

El administrador de SNMP y los agentes de SNMP intercambian solicitudes y notificaciones. De manera predeterminada, los agentes de SNMP reciben solicitudes del administrador de SNMP en el puerto 161. Sin embargo, el administrador de SNMP puede enviar solicitudes a través de cualquier puerto disponible. La respuesta llega al mismo puerto desde el que se envió la solicitud.

De manera predeterminada, el administrador de SNMP recibe notificaciones de los agentes de SNMP en el puerto 162. Sin embargo, los agentes de SNMP pueden enviar notificaciones a través de cualquier puerto disponible. Existen dos tipos de notificaciones:

- Las *capturas* son notificaciones sobre eventos que el agente de SNMP envía sin una solicitud previa del administrador de SNMP. Cuando ocurre un evento específico, como el apagado de un dispositivo CPE o una de sus interfaces de red, el agente de SNMP genera una captura y la envía al administrador de SNMP como un mensaje UPD. Las capturas permiten informar automáticamente al administrador de SNMP sobre los eventos sin esperar una solicitud.

- Las *solicitudes de información* son notificaciones similares a las capturas, con la diferencia de que requieren una confirmación adicional del administrador de SNMP. Cuando el agente de SNMP envía una solicitud de información al administrador de SNMP, el agente de SNMP espera recibir un acuse de recibo. Si el administrador de SNMP recibe y procesa correctamente la solicitud de información, envía un mensaje de confirmación al agente de SNMP. El mecanismo de confirmación le permite garantizar la confiabilidad de la entrega de notificaciones.

Cuando se utiliza el protocolo TLS o DTLS, las capturas llegan al puerto 10162 del administrador de SNMP y las solicitudes de información llegan al puerto 10161.

Todas las unidades de datos de protocolo (PDU) básicas tienen la misma estructura (consulte la siguiente figura). El encabezado IP y el encabezado UDP se utilizan para la encapsulación y, en realidad, no forman parte de la unidad de datos de protocolo.

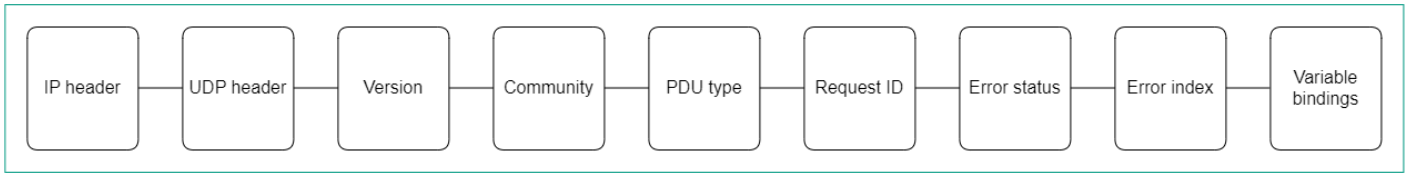



Diagrama de la unidad de datos de protocolo de SNMP

Para ver la tabla de capturas, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador al cual están conectados los componentes que desea supervisar y vaya a la sección **SNMP**. La información sobre las capturas se muestra en las siguientes columnas de la tabla:

- **#** es el número de serie de la captura.

- **IP de administrador** es la dirección IP o el nombre de host del administrador de SNMP.

- **Puerto de administrador** es el número de puerto del administrador de SNMP.

- **Comunidad** es la cadena de comunidad de SNMP.

- **Capturas permitidas** son capturas que los agentes de SNMP deben enviar al administrador de SNMP.

- **Descripción** es una breve descripción de la captura.

# Configurar la conexión del administrador de SNMP a los agentes de SNMP

Debe especificar la configuración para establecer la conexión del administrador SNMP con los agentes SNMP instalados en los dispositivos CPE, así como en las funciones de la red virtual y funciones de la red física. La configuración especificada se utiliza para todos los agentes SNMP.

*Para configurar la conexión del administrador SNMP a los agentes SNMP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. Haga clic en **Administración** → **Configuración de implementación** junto al controlador al que están conectados los componentes que desea supervisar.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **SNMP**.

   Se muestra una tabla de capturas.

4. En la parte superior de la página, en **Administrar parámetros**, haga clic en **Editar**.

5. En la ventana que se abre, en el campo **Dirección**, ingrese la dirección IP o el nombre de host del equipo en el que está instalado el agente SNMP, en el formato `<protocolo de transporte>:<dirección IP o nombre de host>/<número de puerto>`. Por ejemplo, puede ingresar `udp:192.168.2.0/24`.

6. En el campo **Comunidad**, ingrese la cadena de comunidad de SNMP. La cadena de comunidad de SNMP se utiliza como contraseña que el administrador de SNMP utiliza para establecer la conexión con los agentes de SNMP. Valor predeterminado: `público` significa que se otorga acceso de solo lectura. Recomendamos cambiar el valor predeterminado a una cadena de comunidad única para garantizar la seguridad de la comunicación entre el administrador de SNMP y los agentes de SNMP.

   > Debe especificar la misma cadena de comunidad cuando configura la conexión del administrador SNMP a los agentes SNMP y cuando crea o edita capturas.

7. Haga clic en **Guardar**.

Se configura la conexión del administrador SNMP a los agentes.

# Crear una captura

Puede crear una captura que los agentes de SNMP deben enviar al administrador de SNMP.

*Para crear una captura, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. Haga clic en **Administración → Configuración de implementación** junto al controlador al que están conectados los componentes que desea supervisar.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **SNMP**.

   Se muestra una tabla de capturas.

4. En **Parámetros de captura**, haga clic en **Editar**.

5. En la ventana que se abre, haga clic en **+ Agregar** para crear una captura.

6. En el campo **IP de administrador**, ingrese la dirección IP o el nombre de host del administrador de SNMP. Rango de valores: 1 a 255.

7. En el campo **Puerto de administrador**, ingrese el número de puerto del administrador SNMP. Rango de valores: 1 a 65,534. El valor predeterminado es `162`.

8. En el campo **Comunidad**, ingrese la cadena de comunidad de SNMP. La cadena de comunidad de SNMP se utiliza como contraseña que el administrador de SNMP utiliza para establecer la conexión con los agentes de SNMP. Valor predeterminado: `público` significa que se otorga acceso de solo lectura. Recomendamos cambiar el valor predeterminado a una cadena de comunidad única para garantizar la seguridad de la comunicación entre el administrador de SNMP y los agentes de SNMP.

   > Debe especificar la misma cadena de comunidad de SNMP al configurar la conexión del administrador de SNMP a los agentes de SNMP y al crear o editar capturas.

9. En el campo **Capturas permitidas**, haga clic en **Editar** y desmarque las siguientes casillas para especificar qué capturas no envían los agentes de SNMP al administrador de SNMP:

   - Desmarque la casilla **Captura, cuando una interfaz está activa** para evitar que el agente de SNMP envíe una captura al administrador de SNMP cuando uno de los puertos del componente en el que está instalado el agente de SNMP se activa.
   - Desmarque la casilla **Captura, cuando una interfaz está inactiva** para evitar que el agente de SNMP envíe una captura al administrador de SNMP cuando uno de los puertos del componente en el que está instalado el agente de SNMP quede inactivo.
   - Desmarque la casilla **Captura, cuando el equipo está activo** para evitar que el agente de SNMP envíe una captura al administrador de SNMP cuando el componente en el que está instalado el agente de SNMP se active.
   - Desmarque la casilla **Captura, cuando el equipo está inactivo** para evitar que el agente de SNMP envíe una captura al administrador de SNMP cuando el componente en el que está instalado el agente de SNMP se quede inactivo.

   Las casillas están seleccionadas de manera predeterminada.

10. Haga clic en **Atrás** para continuar especificando la configuración de capturas.
11. En el campo **Descripción**, ingrese una breve descripción de la captura.
12. Haga clic en **Guardar**.

La captura se crea y se muestra en la tabla.

# Editar una captura

*Para editar una captura, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. Haga clic en **Administración → Configuración de implementación** junto al controlador al que están conectados los componentes que desea supervisar.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **SNMP**.

   Se muestra una tabla de capturas.

4. En **Parámetros de captura**, haga clic en **Editar**.
5. En la ventana que se abre, si es necesario, edite la configuración de la captura. Para obtener una descripción de la configuración, consulte las instrucciones para crear una captura.
6. Haga clic en **Guardar**.

La captura se modifica y actualiza en la tabla.

# Eliminar una captura

Las capturas eliminadas no se pueden restaurar.

*Para eliminar una captura, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores SD-WAN.

2. Haga clic en **Administración → Configuración de implementación** junto al controlador al que están conectados los componentes que desea supervisar.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **SNMP**.

   Se muestra una tabla de capturas.

4. En **Parámetros de captura**, haga clic en **Editar**.

5. En la ventana que se abre, haga clic en **Eliminar** junto a la captura que desea eliminar.

6. Haga clic en **Guardar**.

La captura se elimina y ya no se muestra en la tabla.

# Supervisión de vínculos

*Para habilitar la supervisión de vínculos, haga lo siguiente:*

1. Habilite la supervisión de vínculos de una de las siguientes maneras:

   - Si desea habilitar la supervisión de un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración → Configurar umbrales** junto al vínculo.

   - Si desea habilitar la supervisión de uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración → Configurar umbrales** junto al vínculo.

   - Si desea habilitar la supervisión de uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador, vaya a la sección **Topología**, haga clic en el vínculo y haga clic en **Configurar umbrales**.

2. Seleccione la casilla de verificación **Habilitar supervisión de umbral** para habilitar la supervisión de vínculos. Esta casilla está desactivada por defecto.

3. Si desea especificar umbrales para la supervisión de vínculos, haga lo siguiente:

   a. Para establecer los umbrales de supervisión de vínculos, haga clic en **Configurar como predeterminado**.

   b. Si desea que el controlador utilice el vínculo como último recurso para el cálculo de las rutas, independientemente de la supervisión de umbrales, seleccione la casilla de verificación **Último recurso**. Esta casilla está desactivada por defecto.

   c. En el campo **Intervalo para procesar tasa de utilización y errores (s)**, ingrese el intervalo de tiempo en segundos para medir la cantidad de errores en el vínculo y su nivel de utilización. Rango de valores: 1 a 300. El valor predeterminado es `60`.

   d. Si desea especificar un umbral para la cantidad de errores por segundo en el vínculo, seleccione la casilla de verificación **Habilitar la supervisión de errores** y, en el campo **Nivel de error crítico (errores/s)**, ingrese el valor del umbral. Rango de valores: 1 a 1 000 000. Está casilla de verificación está desactivada de manera predeterminada, y el valor en el campo es `1000`.

   e. Si desea especificar un umbral para la utilización de vínculos como un porcentaje de la tasa de bits de la interfaz de servicio de origen, seleccione la casilla de verificación **Habilitar supervisión de utilización** y, en el campo **Nivel de utilización crítico (%)**, ingrese el valor del umbral. Está casilla de verificación está desactivada de manera predeterminada, y el valor en el campo es `95`.

f. En el campo **Intervalo para procesar latencia, fluctuación y pérdida de paquetes (s)**, ingrese el intervalo de tiempo, en segundos, para la medición de la latencia, la fluctuación y la pérdida de paquetes en el vínculo. Rango de valores: 1 a 600. El valor predeterminado es `30`.

g. Si desea especificar el umbral de la latencia en milisegundos para la transmisión del tráfico a través del vínculo, seleccione la casilla de verificación **Habilitar supervisión de latencia** y, en el campo **Nivel de latencia crítico (ms)**, ingrese el valor del umbral. Rango de valores: 5 a 1000. Está casilla de verificación está desactivada de manera predeterminada, y el valor en el campo es `100`.

h. Si desea especificar el umbral del tiempo de fluctuación en milisegundos para la transmisión del tráfico a través del vínculo, seleccione la casilla de verificación **Habilitar supervisión de fluctuaciones** y, en el campo **Nivel de fluctuación crítico (ms)**, ingrese el valor del umbral. Rango de valores: 5 a 1000. Está casilla de verificación está desactivada de manera predeterminada, y el valor en el campo es `100`.

i. Si desea especificar un umbral para el porcentaje de paquetes de tráfico perdidos en el vínculo, seleccione la casilla de verificación **Habilitar supervisión de pérdida de paquetes** y, en el campo **Nivel de pérdida de paquetes crítico (%)**, ingrese el valor del umbral. Rango de valores: 1 a 100. Está casilla de verificación está desactivada de manera predeterminada, y el valor en el campo es `2`.

Las restricciones de umbral utilizan los umbrales de supervisión especificados.

4. Guarde la configuración de la supervisión de vínculos de una de las siguientes maneras:

   - Para guardar la configuración de la supervisión de vínculos, haga clic en **Guardar**.
   - Si desea guardar la configuración de la supervisión de vínculos y especificar la misma configuración en el vínculo en dirección opuesta, haga clic en **Guardar para ambos vínculos**.

5. Si especificó la configuración de la supervisión de vínculos para un vínculo que se estableció desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

# Crear una red de SD-WAN entre dispositivos CPE

Para transferir tráfico, debe crear una red de SD-WAN entre los dispositivos CPE utilizando vínculos que estén establecidos sobre la red subyacente. Los dispositivos CPE establecen vínculos desde todas las interfaces de SD-WAN disponibles del tipo WAN. Los vínculos son unidireccionales. Esto significa que, cuando se establece un vínculo de CPE 1 a CPE 2, se establece automáticamente un vínculo también de CPE 2 a CPE 1. Antes de crear una red de SD-WAN, debe garantizar la conectividad entre los dispositivos CPE.

Los vínculos se establecen según las funciones que le asigna a los dispositivos CPE. Puede asignar la función de puerta de enlace de SD-WAN o la función de un dispositivo CPE estándar a un dispositivo CPE. Las puertas de enlace SD-WAN establecen vínculos con todos los dispositivos CPE estándar y otras puertas de enlace SD-WAN. Los dispositivos CPE estándar establecen vínculos solo con puertas de enlace SD-WAN. De manera predeterminada, todos los dispositivos CPE tienen la función de dispositivo CPE estándar.

Si desea que se establezca un vínculo entre dos dispositivos CPE estándar, debe asignarles la misma etiqueta de topología. Puede convertir un dispositivo CPE estándar en un dispositivo de tránsito para permitir que otros dispositivos CPE establezcan vínculos a través de él.

Los vínculos entre los dispositivos CPE forman una topología. Las siguientes topologías son las más utilizadas en Kaspersky SD-WAN:

- En una topología de centro y radios, los vínculos entre los dispositivos CPE se establecen mediante las puertas de enlace de SD-WAN.

- En las topologías de malla completa y de malla parcial, los vínculos entre los dispositivos CPE se establecen directamente, o algunos vínculos se establecen directamente, mientras que otros se establecen mediante las puertas de enlace de SD-WAN.

Dentro de la red de SD-WAN, el tráfico de red entre los dispositivos CPE puede tomar varias rutas. Las rutas pasan por los vínculos entre los dispositivos CPE. La totalidad de todas las rutas posibles entre dos dispositivos CPE se denomina *segmento*. El dispositivo CPE de origen del segmento puede distribuir el tráfico vinculado al dispositivo CPE de destino del segmento a través de varias rutas. Un segmento puede contener entre 2 y 16 rutas.

Se admiten los siguientes tipos de ruta:

- *Auto SPF* (reenvío por la ruta más corta) es una ruta que el controlador calcula automáticamente. Puede reenviar el tráfico a lo largo de las rutas Auto SPF de dos modos:

  - En el modo *Activo/Activo*, se utilizan varias rutas Auto SPF simultáneamente para reenviar el tráfico entre los dispositivos CPE.

  - En el modo *Activo/En espera*, se utiliza una ruta Auto SPF con el costo más bajo para reenviar el tráfico entre los dispositivos CPE. Si la ruta Auto SPF que se está utilizando no está disponible, se usa la ruta Auto SPF con el siguiente costo más bajo. El costo de la ruta se calcula sumando el costo de cada vínculo atravesado por la ruta. Puede especificar el costo del vínculo de forma manual.

  Puede configurar el modo de reenvío del tráfico a lo largo de las rutas Auto SPF cuando se configuran las rutas.

- *Auto TE* (ingeniería de tráfico) es una ruta calculada automáticamente por el controlador, teniendo en cuenta las restricciones de umbral que especificó.

- *Manual-TE* es una ruta que se crea manualmente. Cuando se crea una ruta Manual-TE, especifique los vínculos que la ruta atraviesa en su camino desde el dispositivo CPE de origen del segmento hasta el dispositivo CPE de destino del segmento.

# Acerca de la topología de centro y radios

En una topología de centro y radios, el sitio central se conecta a varios sitios radiales para intercambiar tráfico. Esta topología es la más común para el diseño de las redes de SD-WAN, porque simplifica la administración de la red y proporciona un mayor nivel de seguridad al enrutar el tráfico a través del sitio central donde se realiza el análisis y la categorización del tráfico. La topología de centro y radios también permite un uso más eficiente del ancho de banda, ya que se optimiza y prioriza el tráfico en el sitio central.

Para crear una topología de centro y radios, debe asignar la puerta de enlace de SD-WAN y las funciones estándar de CPE a los dispositivos CPE. En este caso, las puertas de enlace de SD-WAN establecen vínculos con otras puertas de enlace de SD-WAN y dispositivos CPE estándar, mientras que los dispositivos CPE estándar establecen vínculos solo con las puertas de enlace de SD-WAN.

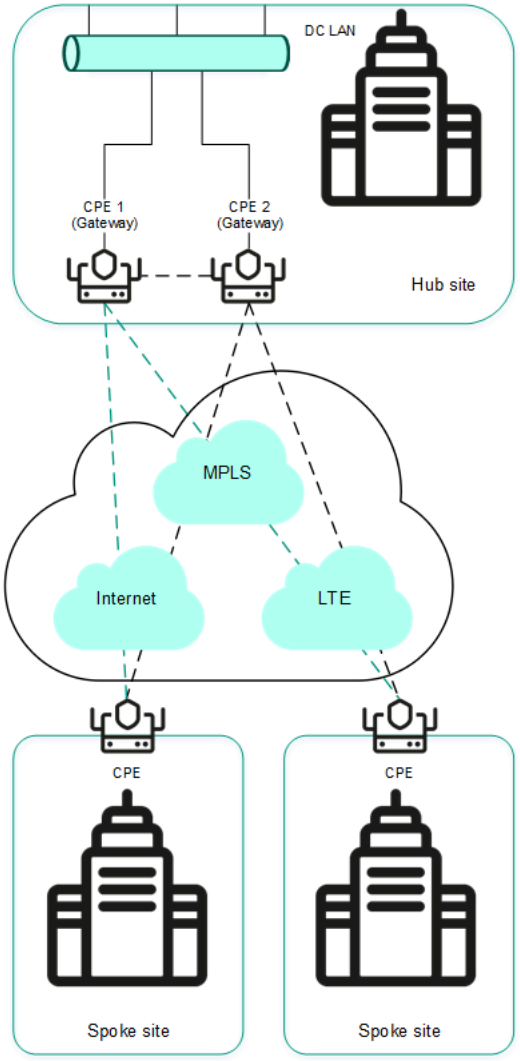
Puede utilizar la calidad del servicio para limitar el ancho de banda de los dispositivos CPE o las clases de tráfico.

Ejemplos de topologías de centro y radios:

- **Topología de centro y radios sin conexión entre los sitios radiales**.

  En la siguiente imagen, se muestra una topología de centro y radios en la que los sitios radiales se comunican con el sitio central, pero no entre sí. Las redes de SD-WAN creadas con esta topología son fáciles de diseñar y mantener, debido a que todos los servicios de red y aplicaciones necesarias se encuentran en el mismo centro de datos.

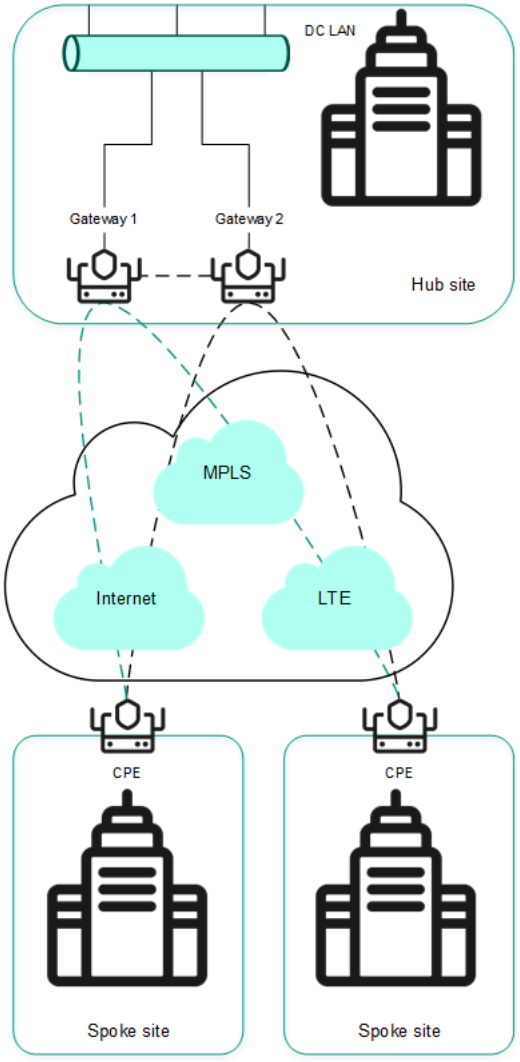
Los dispositivos CPE que se registran se incluyen automáticamente en el servicio de transporte de administración con el rol de hoja y pueden estar detrás de NAT (traducción de direcciones de red) y PAT (traducción de direcciones de puertos). En dicha topología de centro y radios, el tráfico no se puede transmitir directamente entre los dispositivos CPE.




Topología de centro y radios sin conexión entre los sitios radiales

- **Topología de centro y radios con conexión entre los sitios radiales mediante el sitio central**.

  En la siguiente imagen, se muestra una topología de centro y radios en la que los sitios radiales se comunican entre sí mediante el sitio central. Los dispositivos CPE que están registrados se agregan automáticamente al servicio de transporte de administración y pueden estar detrás de NAT y PAT.




Topología de centro y radios con conexión entre los sitios radiales mediante el sitio central

# Acerca de las topologías de malla completa y malla parcial

En las topologías de malla completa y malla parcial, los vínculos se establecen entre los dispositivos CPE estándar. El establecimiento de vínculos entre dispositivos CPE estándar tiene las siguientes ventajas sobre una topología Hub-and-Spoke en la que los dispositivos CPE estándar deben comunicarse entre sí a través de puertas de enlace de SD-WAN:

- Aspectos mejorados de la calidad del vínculo, como el retraso, la pérdida de paquetes y la fluctuación.
- Mayor ancho de banda de vínculos.
- Economía de los recursos de hardware de las puertas de enlace de SD-WAN.

Para crear una topología de malla completa, debe asignar la función del dispositivo CPE estándar a los dispositivos CPE y asignar la misma etiqueta de topología a los dispositivos CPE estándar. En este caso, los dispositivos CPE estándar con las mismas etiquetas de topología establecen vínculos entre sí.

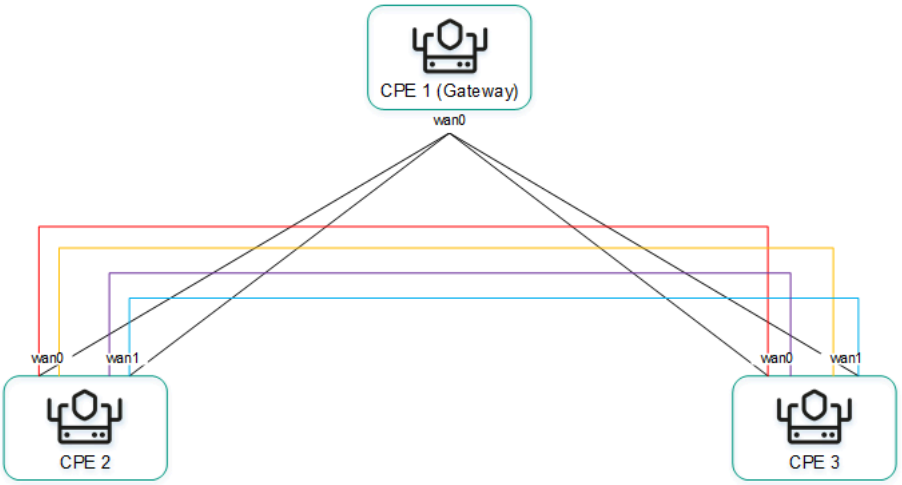
Para crear una topología de malla parcial, debe asignar la puerta de enlace de SD-WAN y las funciones del dispositivo CPE estándar a los dispositivos CPE y asignar la misma etiqueta de topología a los dispositivos CPE estándar. En este caso, las puertas de enlace de SD-WAN establecen vínculos con otras puertas de enlace de SD-WAN y con dispositivos CPE estándar, mientras que los dispositivos CPE estándar establecen vínculos con las puertas de enlace de SD-WAN y entre sí, siempre que se asigne la misma etiqueta de topología a los dispositivos CPE estándar. Si desea dividir los dispositivos CPE estándar en grupos, debe asignar una etiqueta de topología única a todos los dispositivos CPE estándar en cada grupo y también asignar una etiqueta de topología para que la comparta al menos un dispositivo CPE estándar en cada grupo.

Puede utilizar la calidad del servicio para limitar el ancho de banda de los dispositivos CPE o las clases de tráfico.

Ejemplos de topología de malla completa y malla parcial:

- **Topología de malla completa**.

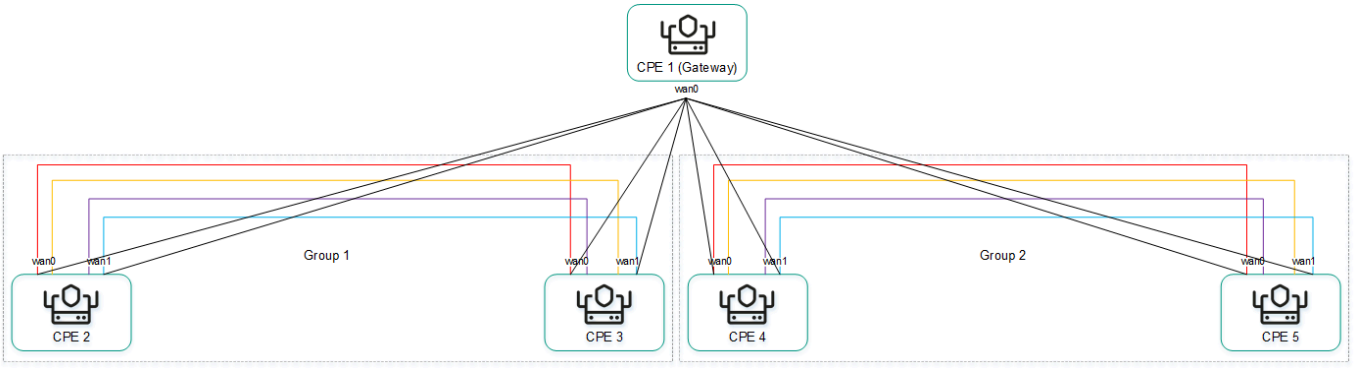
  En la siguiente figura se muestra una topología de malla completa en la que todos los dispositivos CPE establecen vínculos entre sí. El tráfico entre los dispositivos CPE 2 y CPE 3 se reenvía directamente. Con una gran cantidad de dispositivos y vínculos CPE, esta topología puede ser extremadamente exigente para los recursos del controlador.




Topología de malla completa

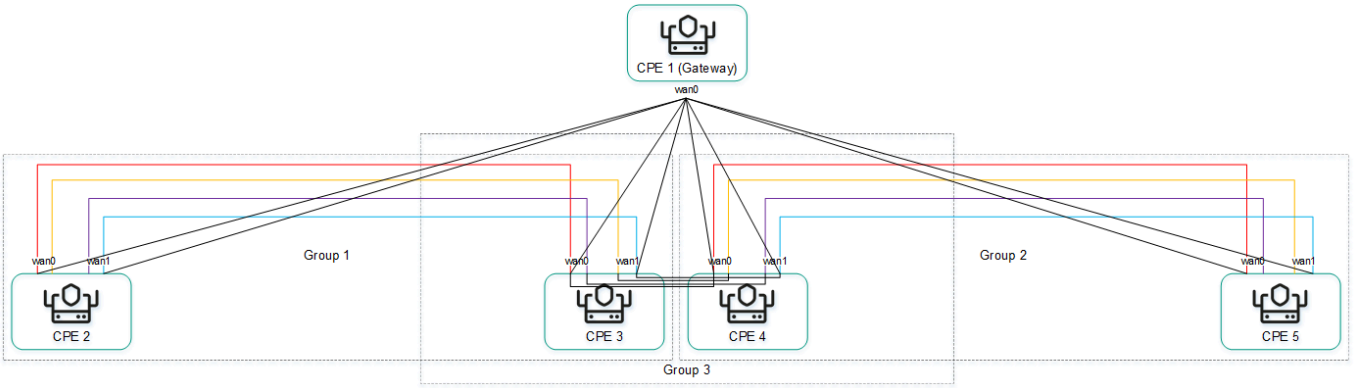
- **Topología de malla parcial**.

  En la siguiente figura se muestra una topología de malla parcial. Esta topología se utiliza cuando los vínculos directos entre algunos dispositivos CPE pueden ser indeseables por razones administrativas o imposibles por razones técnicas. En esta topología, puede agrupar dispositivos CPE de tal manera que los dispositivos CPE del mismo grupo se comuniquen directamente entre sí y se comuniquen con dispositivos CPE de otros grupos a través de un dispositivo CPE de tránsito.




Topología de malla parcial

  Un dispositivo CPE puede pertenecer a varios grupos al mismo tiempo, como se muestra en la siguiente figura.

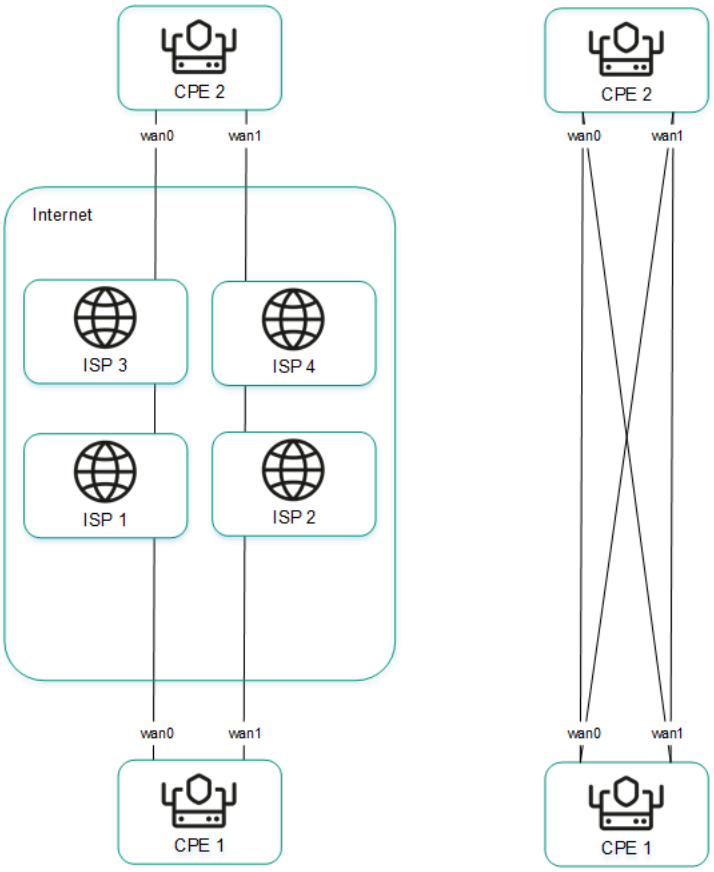



Topología de malla parcial, dispositivos CPE en varios grupos

Cuando crea vínculos directos entre dispositivos CPE, según el tipo de conectividad de los dispositivos CPE a través de vínculos físicos, son posibles las siguientes variantes de conectividad superpuesta:

- **Todos los vínculos físicos tienen conectividad IP directa entre sí**.

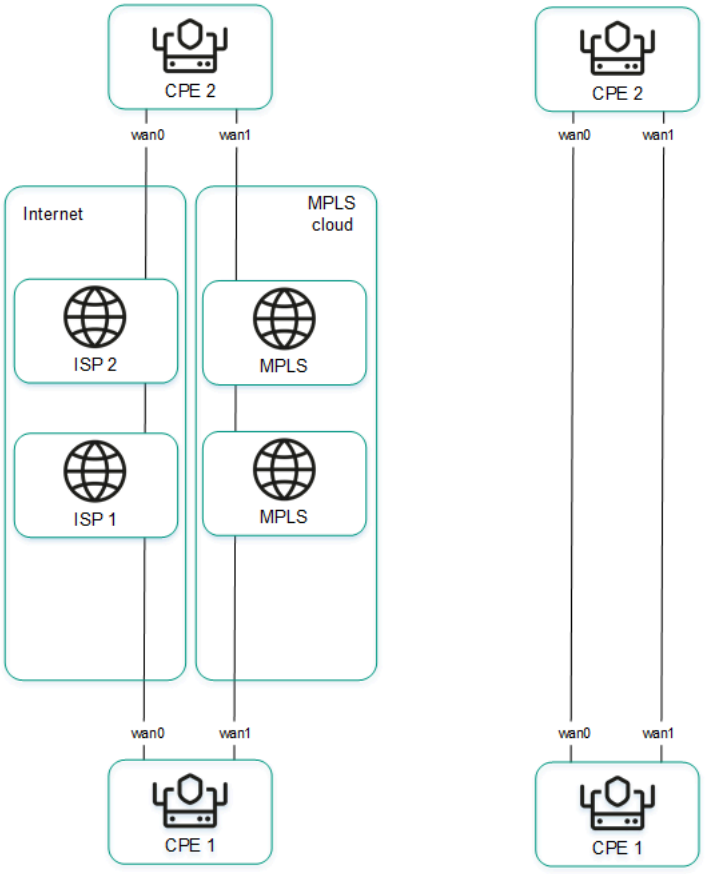
  Gracias a la conexión dentro de Internet, los dispositivos CPE pueden establecer el número máximo de vínculos entre sí (consulte la figura a continuación).




Conectividad física completa entre dispositivos CPE

- **Los vínculos físicos tienen conexión IP parcial entre sí**.

  En la siguiente figura, la nube de Internet y la nube MPLS no están conectadas entre sí, por lo que los vínculos solo se pueden establecer a través de interfaces SD-WAN del tipo WAN que pertenecen a la misma nube. No se pueden establecer los vínculos CPE1:WAN0 → CPE2:WAN1 y CPE1:WAN1 → CPE2:WAN0.



También son posibles otros escenarios de conectividad de red superpuesta si la conectividad IP entre las interfaces de SD-WAN del tipo WAN de los dispositivos CPE dentro de la misma nube es imposible por otras razones, por ejemplo, cuando se usa una topología MPLS que no admite la comunicación directa entre dispositivos CPE, o debido a la presencia de NAT/PAT o ACL en Internet.

# Asignar una función a un dispositivo CPE

Puede asignar una función a una plantilla de CPE o un dispositivo CPE. Una función asignada a una plantilla de CPE se asigna automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

*Para asignar una función a un dispositivo CPE, siga estos pasos:*

1. Asigne una función a un dispositivo CPE de una de las siguientes maneras:

   - Si desea asignar una función a una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Topología**.

   - Si desea asignar una función a un dispositivo CPE, realice una de las siguientes acciones:

     - En el menú, vaya a la sección **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Topología** y marque la casilla **Anular**.

     - En el menú, vaya a la sección **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador, vaya a la sección **Etiquetas de topología**, y en la lista desplegable **Conmutador**, seleccione el dispositivo CPE.

2. En la lista desplegable **Rol**, seleccione la función del dispositivo CPE:

   - **CPE** para un dispositivo CPE estándar. Esta es la configuración predeterminada.

   - **Gateway** para una puerta de enlace de SD-WAN. No puede asignar etiquetas de topología a las puertas de enlace de SD-WAN.

3. Guarde la función del dispositivo CPE de una de las siguientes maneras:

   - Si asignó un rol a una plantilla de CPE o a un dispositivo CPE en la sección **SD-WAN**, en la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE o del dispositivo CPE.

   - Si asignó una función a un dispositivo CPE en la sección **Etiquetas de topología**, haga clic en **Guardar**.

La función se asigna a los usuarios seleccionados.

# Asignar una etiqueta de topología a un dispositivo CPE

Puede asignar una etiqueta de topología a una plantilla de CPE o un dispositivo CPE. Una etiqueta de topología asignada a una plantilla de CPE se asigna automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE. Los dispositivos CPE con las mismas etiquetas de topología establecen vínculos entre sí automáticamente. No se puede asignar una etiqueta de topología a un dispositivo CPE si ha asignado la función de puerta de enlace SD-WAN al dispositivo CPE.

*Para asignar una etiqueta de topología a un dispositivo CPE:*

1. Asigne una etiqueta de topología a un dispositivo CPE de una de las siguientes maneras:

   - Si desea asignar una etiqueta de topología a una plantilla CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Topología**.

   - Si desea asignar una etiqueta de topología a un dispositivo CPE, realice una de las siguientes acciones:

     - En el menú, vaya a la sección **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Topología** y marque la casilla **Anular**.

     - En el menú, vaya a la sección **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador, vaya a la sección **Etiquetas de topología**, y en la lista desplegable **Conmutador**, seleccione el dispositivo CPE.

   Se muestran las etiquetas de topología.

2. En el campo **Etiquetas de topología**, ingrese la etiqueta de topología que desea asignar al dispositivo CPE y haga clic en el ícono de agregar +.

   La etiqueta de topología se asigna al dispositivo CPE. Puede asignar varias etiquetas de topología o eliminar una etiqueta de topología. Para eliminar una etiqueta de topología, haga clic en el ícono de eliminar ✕ junto a él.

3. Guarde las etiquetas de topología del dispositivo CPE de una de las siguientes maneras:

   - Si asignó una etiqueta de topología a una plantilla de CPE o un dispositivo CPE en la sección **SD-WAN**, en la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE o del dispositivo CPE.

   - Si asignó una etiqueta de topología a un dispositivo CPE en la sección **Etiquetas de topología**, haga clic en **Guardar**.

# Configuración de rutas

Puede configurar rutas en un segmento, plantilla CPE o en el dispositivo CPE. La configuración de ruta especificada en un segmento o una plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que pertenecen a este segmento o usan esta plantilla de CPE. La configuración de la ruta especificada en un dispositivo CPE se propaga automáticamente a todos los dispositivos CPE que pertenecen al mismo segmento que ese dispositivo CPE.

*Para configurar rutas:*

1. Configure rutas de una de las siguientes maneras:

   - Si desea configurar rutas en un segmento, vaya a la sección **Infraestructura**, haga clic en **Administración**→**Configuración de implementación** junto al controlador, vaya a la sección **Segmentos** y haga clic en **Administración**→ **Editar** junto al segmento.

   - Si desea configurar rutas en una plantilla CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Rutas múltiples**.

   - Si desea configurar rutas en un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Rutas múltiples**.

Se muestra la configuración de la ruta.

2. En el campo **Número máximo de rutas**, ingrese el número máximo de rutas admitidas por el dispositivo o segmento CPE. Rango de valores: 1 a 16. El valor por defecto es `8`.

3. En el campo **Límite máximo de Auto SPF**, ingrese el número máximo de rutas Auto SPF admitidas por el dispositivo o segmento CPE. El controlador calcula automáticamente las rutas Auto SPF. Rango de valores: 1 a 8. Valor predeterminado: `2`.

   Si desea que el tráfico se transmita entre dispositivos CPE en modo Activo/Activo, ingrese un valor mayor que `1` en este campo. Si desea que el tráfico se transmita entre dispositivos CPE en modo Activo/En espera, ingrese `1` en este campo.

4. En el campo **Multiplicador de variación de costos**, ingrese la relación máxima entre el costo de esta ruta y el costo más bajo de cualquier ruta en su red SD-WAN; si el costo de la ruta está por debajo de este límite, la ruta se puede agregar al segmento. Rango de valores: 1.0 a 10.0. Valor predeterminado: `10`. No puede ingresar un valor en este campo si la casilla de verificación **Equilibrio de peso múltiple** está seleccionada.

   Por ejemplo, si ingresa `2` en este campo, y el costo de ruta más bajo en su red SD-WAN es 10,000, se pueden agregar rutas con un costo de hasta 20,000 al segmento. En el modo Activo/En espera, el valor en este campo determina qué ruta Auto-SPF se usa si la ruta Auto-SPF anterior no está disponible.

5. Si desea agregar rutas al segmento independientemente de su costo, seleccione la casilla **Equilibrio de peso múltiple**. Esta casilla está desactivada por defecto.

6. Si está configurando rutas en un segmento, agregue o modifique las rutas TE manuales según sea necesario.

7. Guarde la configuración de la ruta de una de las siguientes maneras:

   - Si configuró rutas en el segmento, haga clic en **Guardar** para guardar la configuración del segmento.
   - Si configuró rutas en una plantilla CPE o en el dispositivo CPE:

     En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración del dispositivo CPE o programe un guardado diferido por haciendo clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionando la opción **Guardado programado**.

Se guarda la configuración de la ruta.

# Administrar vínculos

Puede ver los vínculos de una de las siguientes maneras:

- Para ver la tabla de vínculos establecidos desde un dispositivo CPE, vaya a la sección del menú **SD-WAN** → **CPE**, haga clic en el dispositivo CPE y seleccione la pestaña **Enlaces**.
- Para ver la tabla de todos los vínculos, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Enlaces**.
- Para ver la topología gráfica con todos los vínculos, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Topología**.

Cuando visualiza la tabla de vínculos, la información sobre los vínculos se muestra en las siguientes columnas de la tabla:

- **Origen** es el nombre, DPID y número de puerto de OpenFlow del dispositivo CPE que es el origen del vínculo.
- **IP/puerto de origen** es la dirección IP y el puerto del origen del vínculo, separados por dos puntos.
- **Origen de NAT/Desconexión** es el atributo topológico del origen del vínculo, responsable de enviar información sobre las interfaces de SD-WAN al controlador. Valores posibles:
  - **N** (Deshabilitado. La información de la interfaz de SD-WAN no se envía al controlador).
  - **NAT/PAT** (la interfaz de SD-WAN está detrás de NAT o PAT).
  - **Desconexión de WAN** (la interfaz de SD-WAN está conectada a una conexión de red aislada).
- **Destino** es el nombre, DPID y número de puerto de OpenFlow del dispositivo CPE que es el destino del vínculo.
- **IP/puerto de destino** es la dirección IP y el puerto del destino del vínculo, separados por dos puntos.
- **Destino de NAT/Desconexión** es el atributo topológico del destino del vínculo, responsable de enviar información sobre las interfaces de SD-WAN al controlador. Valores posibles:
  - **N** (Deshabilitado. La información de la interfaz de SD-WAN no se envía al controlador).
  - **NAT/PAT** (la interfaz de SD-WAN está detrás de NAT o PAT).
  - **Desconexión de WAN** (la interfaz de SD-WAN está conectada a una conexión de red aislada).

  Si es necesario, puede ocultar todas las columnas excepto**Origen**, **Origen de NAT/Desconexión**, **IP/puerto de origen**, **Destino**, **Destino de NAT/Desconexión**, **IP/puerto de destino**; para ello, haga clic en el ícono de configuración y seleccione **Mostrar túnel IP** en el menú.
- **Último recurso** indica si el controlador utiliza este vínculo como último recurso al calcular la ruta, independientemente de los indicadores de supervisión:
  - **Y**
  - **N**
- **Supervisión del umbral**determina si se utiliza la supervisión del umbral en los vínculos. Valores posibles:
  - **Y** (supervisión habilitada).
  - **N** (supervisión deshabilitada).
- **Cifrado** es el estado de cifrado del vínculo. Valores posibles:
  - **Configurado**
  - **Sí**
  - **No**

- **CFM** es el intervalo de tiempo para enviar paquetes de control cuando se está ejecutando la Administración de fallas de conexión. En esta columna se muestran dos valores en el formato **<valor 1>/<valor 2>**:

  - **<valor 1>** es el intervalo de tiempo para enviar paquetes de control que especificó cuando habilitó CFM en el dispositivo CPE.

  - **<valor 2>** es el intervalo de tiempo para enviar paquetes de control que se está utilizando actualmente. Se puede usar uno de los siguientes intervalos de tiempo para enviar paquetes de control:

    - El intervalo de tiempo para enviar paquetes de control que especificó cuando habilitó CFM en el dispositivo CPE. Si especifica diferentes intervalos de tiempo para enviar paquetes de control en dispositivos CPE, se utiliza el mayor de los intervalos de tiempo especificados. Por ejemplo, si especificó 300 milisegundos como intervalo de paquetes de control en CPE 1 y un segundo en CPE 2, el intervalo de paquetes de control es de 1 segundo.

    - El intervalo de tiempo para enviar paquetes de control que especificó cuando habilitó CFM en el vínculo. El intervalo de tiempo para enviar paquetes de control establecido para el vínculo anula los intervalos de tiempo para enviar paquetes de control establecidos en los dispositivos CPE. Por ejemplo, si especificó 300 milisegundos como intervalo de paquetes de control en CPE 1, un segundo en CPE 2 y 10 segundos en el vínculo entre CPE 1 y CPE 2, el intervalo de tiempo resultante para enviar paquetes de control es de 10 segundos.

  Los valores especificados manualmente en esta columna están subrayados.

- **MTU** es el valor MTU del vínculo.

- **Errores/segundo** es el número de errores por segundo en el vínculo.

- **Utilización (%)** es la carga del vínculo como un porcentaje del ancho de banda de la interfaz del servicio de origen.

- **Latencia (ms)** es el tiempo de retraso en milisegundos para el tráfico transmitido a través del vínculo.

- **Fluctuación (ms)** es el tiempo de fluctuación en milisegundos para el tráfico transmitido a través del vínculo.

- **Pérdida de paquetes (%)** es el porcentaje de pérdida de paquetes de tráfico en el vínculo.

- **Velocidad (Mbit/s)** es la velocidad de transmisión del tráfico a través del vínculo en Mbps.

- **Estado de configuración de FEC/Estado operativo de FEC** es el estado operativo/de configuración de la Corrección de errores de reenvío en la conexión (**Habilitado** o **Deshabilitado**).

- **Costo** es el costo del vínculo.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Ver estadísticas para un vínculo

*Para ver las estadísticas de un vínculo, siga estos pasos:*

1. Navegue hasta las estadísticas del vínculo de una de las siguientes maneras:

   - Si desea ver las estadísticas de un vínculo que se estableció desde un dispositivo CPE, vaya al menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, en la sección **Enlaces**, haga clic en el botón **Administración** del vínculo correspondiente y seleccione **Ver estadísticas**.

   - Si desea ver las estadísticas de uno de los vínculos en la tabla de todos los vínculos, vaya a la sección del menú **Infraestructura**, haga clic en el botón **Administración** junto al controlador y seleccione**Configuración de implementación**, luego en la sección **Enlaces**, haga clic en el botón **Administración** para el vínculo correspondiente y seleccione**Ver estadísticas**.

   - Si desea ver las estadísticas de uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección del menú **Infraestructura**, haga clic en el botón **Administración** junto al controlador y seleccione **Configuración de implementación**, luego, en la sección **Topología**, haga clic en el vínculo y seleccione**Ver estadísticas**.

   Se abre la ventana de estadísticas del vínculo. Las estadísticas se muestran en varias tablas en las pestañas correspondientes **Telemetría de vínculos**, **Cifrado**, CFM, FEC.

   Configuración vigente

   Fuente de configuración

   Conmutador

   Tipo

   Habilitado

   Intervalo

   1s

   Estado operativo

   Tipo

   Sí

   Intervalo

   1s

   FEC

   Configuración vigente

   Fuente de configuración

   Conmutador

   Tipo

   Deshabilitado

   Relación FEC

   Tiempo máximo en el búfer de reorganización (ms)

   Estado operativo

   Tipo

   Deshabilitado

Relación FEC

Tiempo máximo en el búfer de reorganización (ms)

Paquetes originales enviados

Paquetes de FEC enviados

Relación FEC en paquetes (%)

Bytes originales enviados

Bytes de FEC enviados

Relación FEC en bytes (%)

Tasa de transferencia de paquetes originales (paquetes/s)

Tasa de transferencia de paquetes totales (paquetes/s)

Tasa de transferencia de datos original (Kbps)

Tasa de transferencia de datos completos (Kbps)

Porcentaje de pérdida de paquetes originales (%)

Tasa de pérdida de paquetes totales (%)

# Actualizar automáticamente el costo del vínculo en función de la velocidad de datos máxima de la interfaz

Si la velocidad de datos de la interfaz WAN de la SD-WAN en el dispositivo CPE es mayor que la velocidad de red proporcionada por el ISP, debe limitar la velocidad máxima de esa interfaz para que coincida con la velocidad de la red.

Ejemplo:
El proveedor de servicios le da al cliente acceso a Internet a una velocidad de 50 Mbps y la velocidad de la conexión física en la interfaz del dispositivo CPE es de 100 Mbps. En este caso, para el cálculo correcto del costo del vínculo y la calidad del servicio, debe especificar la velocidad máxima de 50.

Puede especificar la velocidad máxima cuando crea o modifica una interfaz de SD-WAN saliente que participa en la conexión. El costo de la conexión se calcula en función del valor más bajo de la velocidad máxima de ambas interfaces en ambos extremos de la conexión. La relación de la velocidad máxima y los parámetros del costo es la siguiente:

- La velocidad máxima especifica el ancho de banda máximo de la interfaz para calcular correctamente las colas lógicas para QoS. Medido en Mbps.
- El costo determina el peso de la interfaz en la topología y se calcula mediante la fórmula: `Costo = 10 000 000 / Velocidad`, donde `Velocidad` equivale a la velocidad máxima. Cuanto menor sea el valor del costo, mayor será la prioridad del vínculo en la topología de la red.

Cuando cambia la velocidad máxima, el valor de costo cambia para los vínculos en ambas direcciones. El valor de la velocidad máxima más baja de las interfaces que participan en el vínculo se utiliza para el vínculo.

En lugar de calcular automáticamente el costo de la conexión, puede especificar su costo manualmente.

# Especificar el costo de un vínculo

*Para especificar el costo de un vínculo, siga estos pasos:*

1. Especifique el costo del vínculo de una de las siguientes maneras:

   - Si desea especificar el costo de un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN** → **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración** → **Configurar costo** junto al vínculo.

   - Si desea especificar el costo de uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración**→ **Configuración de implementación**junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración**→ **Configurar costo**junto al vínculo.

   - Si desea especificar el costo de uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración**→ **Configuración de implementación** junto al controlador, vaya a la sección **Topología**, haga clic en el vínculo y haga clic en**Configurar costo**.

2. En la ventana que se abre, seleccione la casilla **Anular** para especificar el costo del vínculo. Esta casilla está desactivada por defecto.

3. En el campo **Costo del vínculo**, ingrese el costo del vínculo. Si desea especificar el mismo costo para el vínculo en la dirección opuesta, seleccione la casilla **Guardar para ambos vínculos**. Esta casilla está desactivada por defecto.

4. Haga clic en **Guardar**.

   Se especifica el costo del vínculo.

5. Si especificó el costo del vínculo para un vínculo establecido desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

# Habilitar la amortiguación

La *amortiguación* es un mecanismo configurable que excluye los vínculos inestables cuyo estado cambia con demasiada frecuencia del cálculo de la ruta. Para determinar la inestabilidad del vínculo, se tienen en cuenta los siguientes cambios de estado:

- UP/LIVE → DOWN/NOT-LIVE.
- DOWN/NOT-LIVE → UP/LIVE.
- UP/LIVE → UP/NOT-LIVE.
- UP/NOT-LIVE → UP/LIVE.

Cuando se habilita la amortiguación en un vínculo, cada cambio de estado del vínculo aumenta el valor de penalización. Si la penalización alcanza el umbral dentro del tiempo especificado, se restringe el acceso al vínculo (su costo se incrementa 10 000 veces durante el período de tiempo especificado). El valor de cada uno de estos parámetros se especifica cuando habilita la amortiguación. De manera predeterminada, el acceso al vínculo se reanuda si el estado del vínculo no cambia durante 10 minutos.

*Para habilitar la amortiguación:*

1. Habilite la amortiguación de una de las siguientes maneras:

   - Si desea habilitar la amortiguación para un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración → Amortiguación** junto al vínculo.

   - Si desea habilitar la amortiguación para uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración → Amortiguación** junto al vínculo.

   - Si desea habilitar la amortiguación para uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic **Administración→ Configuración de implementación** junto al controlador, vaya a la sección **Topología**, haga clic en el vínculo y en**Amortiguación**.

2. En la ventana que se abre, seleccione la casilla **Habilitar** para habilitar la amortiguación en el vínculo. Esta casilla está desactivada por defecto.

3. En el campo **Tiempo de supresión máximo (ms)**, ingrese el tiempo, en milisegundos, durante el cual se puede restringir el acceso al vínculo. Cuando transcurre el tiempo especificado, todos los contadores de amortiguación del vínculo se restablecen. El valor predeterminado es `600000`.

4. En el campo **Penalidad**, ingrese el número en el que se incrementa la penalización cuando el vínculo cambia de estado. El valor predeterminado es `1`.

5. En el campo **Umbral de supresión**, ingrese el valor de penalización en el que se restringe el acceso al vínculo. El valor predeterminado es `4`.

6. En el campo **Intervalo de actualización (ms)**, ingrese el tiempo en milisegundos durante el cual la penalización debe alcanzar el valor especificado en el campo **Umbral de supresión** para que se restrinja el acceso al vínculo. El valor predeterminado es `120000`.

7. Si desea ver las estadísticas de amortiguación de un vínculo, haga clic en **Cargar estadísticas**.

8. Haga clic en **Guardar**.

   La amortiguación está habilitada para el vínculo.

9. Si habilitó la amortiguación para un vínculo establecido desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de la configuración para guardar la configuración del dispositivo CPE.

# Habilitar la corrección de errores de reenvío

La funcionalidad *Corrección de errores de reenvío (FEC)* reduce la pérdida de paquetes de tráfico en los vínculos, especialmente para las aplicaciones UDP, y el número de retransmisiones, que provocan retrasos, y también recupera los datos recibidos en el dispositivo CPE. La recuperación de datos se proporciona mediante la codificación redundante del flujo de datos en el dispositivo CPE de origen.

Si se habilita FEC en un vínculo, el dispositivo CPE de origen codifica el flujo de paquetes de tráfico transmitido a través del vínculo y agrega paquetes de tráfico redundantes. La codificación en dispositivos CPE puede causar retrasos debido al procesamiento de datos adicional.

El dispositivo CPE de destino almacena en búfer los paquetes de tráfico recibidos a través del vínculo y los decodifica para recuperar los paquetes de tráfico perdidos, si es posible. Recomendamos usar FEC en vínculos ruidosos para reducir la pérdida de paquetes y aumentar la velocidad de las conexiones TCP. El diagrama general de FEC se muestra en la siguiente figura.

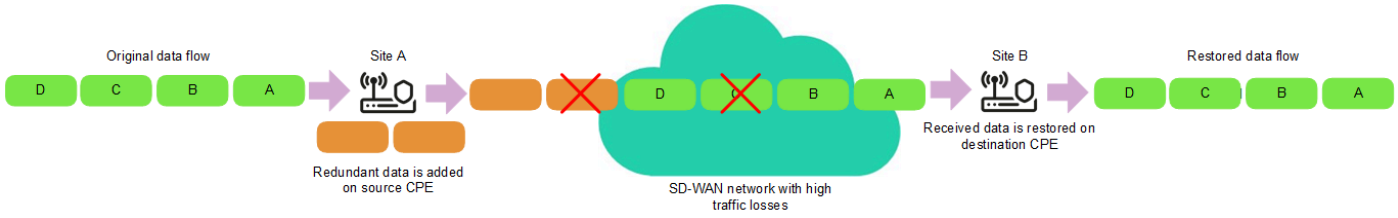



Diagrama de FEC

*Para habilitar FEC, siga estos pasos:*

1. Habilite FEC de una de las siguientes maneras:

   - Si desea habilitar FEC para un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en un dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración → FEC/reordenación** junto al vínculo.

   - Si desea habilitar FEC para uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura** , haga clic en **Administración → Configuración de implementación** junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración → FEC/reordenación** junto al vínculo.

   - Si desea habilitar FEC para uno de los vínculos en el la topografía gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic **Administración→ Configuración de implementación** junto al controlador, vaya a la sección **Topología**, haga clic en el vínculo y en **FEC/reordenación**.

   - Si desea habilitar la funcionalidad de FEC en uno de los vínculos cuando crea una interfaz SD-WAN del tipo WAN, vaya a la sección del menú **SD-WAN→ CPE**, haga clic en un dispositivo CPE, seleccione la pestaña **SD-WAN→ Interfaces** en la tabla de interfaces de SD-WAN, haga clic en el botón **+ Agregar** y seleccione la pestaña **Configuración del vínculo**.

2. En la ventana que se abre, habilite el conmutador **Anular** para anular la configuración del vínculo.

   Este conmutador está deshabilitado de manera predeterminada y no se muestra si está configurando FEC durante la creación de una interfaz SD-WAN del tipo WAN.

3. Habilite FEC para el vínculo con el conmutador **Habilitar FEC**. Este conmutador está deshabilitado de manera predeterminada.

4. En la lista desplegable **Proporción de redundancia (paquete original/redundante)**, seleccione la relación entre los paquetes de tráfico originales y los paquetes de tráfico adicionales con código redundante. Valor predeterminado: **0:0 (FEC desactivado)** significa que FEC no se utiliza. También puede especificar la relación entre los paquetes de tráfico originales y los paquetes de tráfico redundantes mediante la `propiedad del controlador` topology.link.fec.ratio.

5. En el campo **Tiempo de espera del búfer de reordenamiento (ms)**, ingrese el tiempo, en milisegundos, durante el cual un paquete de tráfico puede permanecer en la cola para que se aplique FEC. Rango de valores: de 1 a 1000.

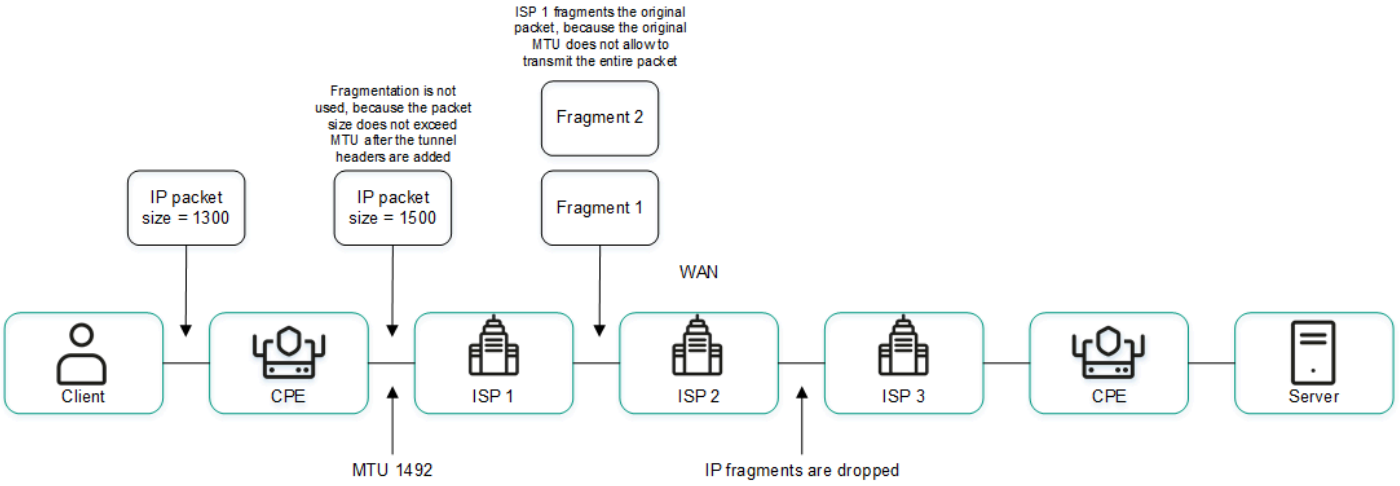
6. Haga clic en **Guardar**.

   Se habilita FEC.

7. Si habilitó FEC para un vínculo establecido desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

# Determinar el valor de MTU

Puede determinar el valor de MTU de un vínculo para averiguar por qué se bloquean los paquetes fragmentados en el vínculo (consulte la figura a continuación).




Vínculos con un tamaño de MTU reducido y paquetes fragmentados que se eliminarán

El valor de MTU se determina mediante el envío de paquetes LLDP con un tamaño de carga útil variable a través del vínculo. El tamaño mínimo de MTU detectable es de 1280 bytes y el máximo es de 1500 bytes. El valor de MTU se determina automáticamente cuando los dispositivos CPE están habilitados y periódicamente en un intervalo especificado en la `propiedad del controlador` topology.link.pmtud.scheduler.interval.sec.

Puede determinar el valor de MTU manualmente.

*Para determinar manualmente el valor de MTU,*

Determine el valor de MTU de una de las siguientes maneras:

- Si desea determinar manualmente el valor de MTU para un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN**→ **CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración**→ **Verificar MTU**junto al vínculo.

- Si desea determinar manualmente el valor de MTU para uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración**→ **Configuración de implementación**al lado del controlador, vaya a la sección **Enlaces** y haga clic en **Administración**→ **Verificar MTU**junto al vínculo.

El valor de MTU se muestra en la columna **MTU**.

# Cifrado de tráfico

El *cifrado de tráfico* es un mecanismo para proteger el intercambio de tráfico entre los dispositivos CPE a través de los vínculos. Por ejemplo, puede cifrar el tráfico que se transmite a través de vínculos no seguros.

El cifrado de tráfico no reemplaza la necesidad de usar otras medidas de seguridad de la información, como TLS, LDAPS y otros protocolos que protegen el tráfico dentro de la red superpuesta.

El controlador genera automáticamente claves para cifrar y descifrar el tráfico y envía las claves a los dispositivos CPE. El tráfico se cifra en el dispositivo CPE de origen mediante la clave de cifrado. El dispositivo CPE de destino descifra el tráfico mediante la clave de descifrado.

Las claves se actualizan periódicamente para privar a terceros de la oportunidad de cifrar o descifrar el tráfico transmitido si se intercepta una clave. Puede especificar el período después del cual se actualizan las claves en los dispositivos CPE mediante la `propiedad del controlador` topology.link.encryption.key.update.interval.minutes.

El cifrado de tráfico solo es compatible con dispositivos CPE que ejecutan el software Kaspersky SD-WAN.

Puede habilitar el cifrado de tráfico en un dispositivo CPE o en un vínculo. Un dispositivo CPE con el cifrado de tráfico habilitado reenvía el tráfico cifrado a través de todos sus vínculos, incluidos los nuevos vínculos que se establecerán en el futuro. Cuando el cifrado de tráfico está habilitado en un vínculo, el dispositivo CPE transmite tráfico cifrado a través de ese vínculo. Cuando el cifrado de tráfico está deshabilitado, las claves generadas por el controlador para cifrar y descifrar el tráfico se eliminan de todos los dispositivos CPE conectados. De manera predeterminada, el cifrado de tráfico está deshabilitado en dispositivos y vínculos CPE.

Por ejemplo, puede habilitar el cifrado de tráfico en un dispositivo CPE y deshabilitar el cifrado de tráfico en uno de los vínculos de ese dispositivo CPE. En este caso, el dispositivo CPE transmite tráfico cifrado a través de todos sus vínculos, excepto por el vínculo en el que el cifrado de tráfico está deshabilitado.

## Habilitar el cifrado de tráfico en un dispositivo CPE

Un dispositivo CPE con el cifrado de tráfico habilitado reenvía el tráfico cifrado a través de todos sus vínculos, incluidos los nuevos vínculos que se establecerán en el futuro. Puede habilitar o deshabilitar el cifrado de tráfico en una plantilla CPE o en un dispositivo CPE. La configuración de cifrado de tráfico especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos de CPE que utilizan esta plantilla de CPE.

*Para habilitar el cifrado de tráfico en un dispositivo CPE:*

1. Habilite el cifrado de tráfico en el dispositivo CPE de una de las siguientes maneras:

   - Si desea habilitar el cifrado de tráfico en una plantilla CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla CPE y seleccione la pestaña **Cifrado de vínculo**.

   - Si desea habilitar el cifrado de tráfico en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Cifrado de vínculo** y marque la casilla **Anular**.

   Se muestra la política de cifrado de tráfico.

2. En la lista desplegable **Habilitar cifrado**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

3. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla CPE o el dispositivo CPE, o programar un guardado diferido de la configuración del dispositivo CPE haciendo clic en el botón ⌄ a la derecha del botón **Guardar** y seleccionando la opción **Guardado programado**.

## Habilitar el cifrado de tráfico en un vínculo

Cuando el cifrado de tráfico está habilitado en un vínculo, el dispositivo CPE transmite tráfico cifrado a través de ese vínculo.

*Para habilitar el cifrado del tráfico en un vínculo, siga estos pasos:*

1. Habilite el cifrado de tráfico en el vínculo de una de las siguientes maneras:

   - Si desea habilitar el cifrado de tráfico para un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración → Configurar cifrado** junto al vínculo.

   - Si desea habilitar el cifrado de tráfico para uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración→ Configuración de implementación** junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración→ Configurar cifrado** junto al vínculo.

   - Si desea habilitar el cifrado de tráfico para uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración→ Configuración de implementación** junto al controlador, vaya a la sección **Topología**, haga clic en el vínculo y haga clic en**Configurar cifrado**.

2. Esto abre una ventana, en esa ventana, seleccione la casilla de verificación **Anular**. Esta casilla está desactivada por defecto.

3. Seleccione la casilla **Habilitar cifrado** para habilitar el cifrado de tráfico para el vínculo. Esta casilla está desactivada por defecto.

4. Haga clic en **Guardar**.

   El cifrado de tráfico se habilita en el vínculo.

5. Si habilitó el cifrado de tráfico para un vínculo establecido desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

# Administración de errores de conectividad (CFM)

La funcionalidad *Administración de fallas de conectividad* (en adelante también CFM) permite detectar vínculos no disponibles entre dispositivos CPE. Cuando CFM está habilitada, el dispositivo CPE envía paquetes de control de Mensajes de verificación de continuidad (CCM) a través de sus vínculos en los intervalos especificados y escucha los paquetes de control de respuesta en los vínculos de dirección opuesta. Si los paquetes de control de respuesta no llegan, el dispositivo CPE considera que el vínculo no está disponible y comienza a transmitir tráfico a través de un vínculo disponible seleccionado al azar.

El tiempo de espera de respuesta es igual al intervalo de envío del paquete de control 3.5 veces. El tiempo que se tarda en cambiar un dispositivo CPE a una nueva conexión cuando no se reciben paquetes de respuesta es igual al intervalo de envío de paquetes de control multiplicado por un número en el rango de 3.5 a 7. Por ejemplo, si especificó 300 milisegundos como el intervalo de tiempo para enviar paquetes de control, el tiempo de espera de respuesta es de 1,05 segundos y el tiempo que se tarda en cambiar el dispositivo CPE a un nuevo vínculo es de 1,05 a 2,1 segundos.

Cuando usa el mecanismo de CFM, recomendamos configurar el intervalo de CFM y la `propiedad del controlador core.link.liveness.timeout` de modo que `core.link.liveness.timeout` >= intervalo de CFM * 10.

Puede habilitar CFM en un dispositivo CPE o en un vínculo:

- Un dispositivo CPE con CFM habilitada envía paquetes de control sobre todos sus vínculos, incluidos los nuevos vínculos que se establecerán en el futuro. Si especifica diferentes intervalos de tiempo para enviar paquetes de control en dispositivos CPE, se utiliza el mayor de los intervalos de tiempo especificados. Por ejemplo, si especificó 300 milisegundos como intervalo de paquetes de control en CPE 1 y un segundo en CPE 2, el intervalo de paquetes de control es de 1 segundo.

  Cuando CFM está habilitada en un dispositivo CPE y deshabilitada en el otro dispositivo CPE, el dispositivo CPE con CFM habilitada tiene prioridad. En este caso, los dispositivos CPE se envían paquetes de control entre sí a través de todos sus vínculos.

- Cuando CFM está habilitado para un vínculo, el dispositivo CPE envía paquetes de control solo a través de ese vínculo. Cuando habilita CFM para un vínculo, también debe habilitar CFM en el vínculo de dirección opuesta. El intervalo de tiempo para enviar paquetes de control establecido para el vínculo anula los intervalos de tiempo para enviar paquetes de control establecidos en los dispositivos CPE. Por ejemplo, si especificó 300 milisegundos como intervalo de paquetes de control en CPE 1, un segundo en CPE 2 y 10 segundos en el vínculo entre CPE 1 y CPE 2, el intervalo de tiempo resultante para enviar paquetes de control es de 10 segundos.

Por ejemplo, puede habilitar CFM en un dispositivo CPE y deshabilitar CFM en uno de los vínculos de ese dispositivo CPE. En este caso, el dispositivo CPE envía paquetes de control a través de todos sus vínculos, excepto por el vínculo en el que CFM está deshabilitada. De manera predeterminada, CFM está deshabilitada en dispositivos CPE y vínculos.

Cambiar la configuración de CFM en una conexión activa puede causar interrupciones en el tráfico.

## Habilitar CFM en un dispositivo CPE

Un dispositivo CPE con CFM habilitada envía paquetes de control sobre todos sus vínculos, incluidos los nuevos vínculos que se establecerán en el futuro. Puede habilitar o deshabilitar CFM en una plantilla de CPE o en un dispositivo CPE. La configuración de CFM especificada en la plantilla de CPE se propaga automáticamente a todos los dispositivos CPE que utilizan esta plantilla de CPE.

Cuando CFM está habilitada en un dispositivo CPE y deshabilitada en el otro dispositivo CPE, el dispositivo CPE con CFM habilitada tiene prioridad. En este caso, los dispositivos CPE se envían paquetes de control entre sí a través de todos sus vínculos.

Cambiar la configuración de CFM en una conexión activa puede causar interrupciones en el tráfico.

*Para habilitar CFM en un dispositivo CPE, siga estos pasos:*

1. Habilite CFM en el dispositivo CPE de una de las siguientes maneras:

   - Si desea habilitar CFM en una plantilla de CPE, vaya a la sección del menú **SD-WAN→ Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **CFM**.

   - Si desea habilitar CFM en un dispositivo CPE, vaya a la sección del menú **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **CFM** y seleccione la casilla de verificación **Anular**.

2. En la lista desplegable **CFM**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

3. En la lista desplegable **Intervalo**, seleccione el intervalo de tiempo para enviar paquetes de control:

   - **300 ms**.

   - **1 s**. Esta es la configuración predeterminada.

   - **10 s**.

   - **1 min**.

   El tiempo de espera de respuesta es igual al intervalo de envío del paquete de control 3.5 veces. El tiempo que se tarda en cambiar un dispositivo CPE a una nueva conexión cuando no se reciben paquetes de respuesta es igual al intervalo de envío de paquetes de control multiplicado por un número en el rango de 3.5 a 7. Por ejemplo, si en la lista desplegable **Intervalo**seleccionó **300 ms**, el tiempo de espera de respuesta es de 1.05 segundos y el tiempo que tarda en cambiar el dispositivo CPE a un nuevo vínculo es de 1.05 a 2.1 segundos.

   Si especificó diferentes intervalos de paquetes de control en los dispositivos CPE, se utiliza el mayor de los intervalos especificados. Por ejemplo, si en la lista desplegable **Intervalo** para CPE 1, seleccionó **300 ms** y para CPE 2 seleccionó **1 s**, el intervalo de tiempo para enviar paquetes de control es de 1 segundo.

4. En la parte inferior del área de configuración, haga clic en el botón **Guardar** para guardar inmediatamente la configuración de la plantilla de CPE o el dispositivo CPE, o programe un guardado diferido de la configuración del dispositivo CPE al hacer clic en el ícono ⌄ a la derecha del botón **Guardar** y seleccionar la opción **Guardado programado**.

## Habilitar CFM en un vínculo

Cuando CFM está habilitada para un vínculo, el dispositivo CPE envía paquetes de control solo a través de ese vínculo. Cuando habilita CFM para un vínculo, también debe habilitar CFM en el vínculo de dirección opuesta.

Cambiar la configuración de CFM en una conexión activa puede causar interrupciones en el tráfico.

*Para habilitar CFM en un vínculo:*

1. Habilite CFM en el vínculo de una de las siguientes maneras:

   - Si desea habilitar CFM para un vínculo que se estableció desde un dispositivo CPE, vaya a la sección **SD-WAN → CPE**, haga clic en el dispositivo CPE, seleccione la pestaña **Enlaces** y haga clic en **Administración → Configurar CFM** junto al vínculo.

   - Si desea habilitar CFM para uno de los vínculos en la tabla de todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador, vaya a la sección **Enlaces** y haga clic en **Administración → Configurar CFM** junto al vínculo.

2. Si desea habilitar CFM para uno de los vínculos en la topología gráfica con todos los vínculos, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto controlador, vaya a la sección **Topología**, haga clic en el vínculo y haga clic en**Configurar CFM**.

3. Esto abre una ventana, en esa ventana, seleccione la casilla de verificación **Anular**. Esta casilla está desactivada por defecto.

4. Seleccione **Guardar para ambos vínculos** para habilitar CFM en el vínculo de dirección opuesta. Esta casilla está desactivada por defecto.

5. En la lista desplegable **CFM**, seleccione **Habilitado**. El valor predeterminado es **Deshabilitado**.

6. En la lista desplegable **Intervalo**, seleccione el intervalo de tiempo para enviar paquetes de control:

   - **300 ms**.

   - **1 s**. Esta es la configuración predeterminada.

   - **10 s**.

   - **1 min**.

   El tiempo de espera de respuesta es igual al intervalo de envío del paquete de control 3.5 veces. El tiempo que se tarda en cambiar un dispositivo CPE a una nueva conexión cuando no se reciben paquetes de respuesta es igual al intervalo de envío de paquetes de control multiplicado por un número en el rango de 3.5 a 7. Por ejemplo, si en la lista desplegable **Intervalo**seleccionó **300 ms**, el tiempo de espera de respuesta es de 1.05 segundos y el tiempo que tarda en cambiar el dispositivo CPE a un nuevo vínculo es de 1.05 a 2.1 segundos.

   El intervalo de tiempo para enviar paquetes de control establecido para el vínculo anula los intervalos de tiempo para enviar paquetes de control que especificó al habilitar CFM en dispositivos CPE. Por ejemplo, si en la lista desplegable **Intervalo** para CPE 1 seleccionó **300 ms**, para CPE 2 seleccionó **1 s** y para el vínculo entre CPE 1 y CPE 2 seleccionó **10 s**, el intervalo de tiempo resultante para enviar paquetes de control es de 10 segundos.

7. Haga clic en **Guardar**.

   CFM está habilitado para el vínculo.

8. Si habilitó CFM para un vínculo establecido desde el dispositivo CPE, haga clic en **Guardar** en la parte superior del área de configuración para guardar la configuración del dispositivo CPE.

# Administrar segmentos

Para ver la tabla de segmentos, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Segmentos**. La información sobre los segmentos y las rutas que contienen se muestra en las siguientes columnas de la tabla:

- **Remitente** es el nombre y el DPID del dispositivo CPE del origen del segmento.
- **Destinatario** es el nombre y el DPID del dispositivo CPE del destino del segmento.
- **Rutas/máximo** es la cantidad de rutas creadas y la cantidad máxima de rutas admitidas por el segmento.
- **#** es el número secuencial de la ruta. Cuanto menor sea el número de la ruta, antes se construyó.
- **Tipo de ruta** es el tipo de ruta:
  - **Auto SPF**
  - **Auto TE**
  - **Manual TE**
- **Rutas** son nombres, DPID y números de puertos de OpenFlow de dispositivos CPE a través de los cuales pasa la ruta.
- **Estado administrativo** es el estado administrativo de la ruta:
  - **arriba**
  - **abajo**
- **Estado operativo** es el estado operativo de la ruta:
  - **arriba**
  - **abajo**
- **Costo** es el costo de la ruta.
- **Cantidad de saltos** es el número de saltos de la ruta.
- **Peso equilibrado** es el peso de la ruta calculado en función del costo total de los vínculos.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una ruta Manual-TE

Cuando crea una ruta Manual-TE, debe especificar manualmente los vínculos por los que pasa la ruta en el camino del dispositivo CPE de origen del segmento al dispositivo CPE de destino del segmento. Se admiten dos tipos de rutas Manual-TE:

- Una *ruta Manual-TE completamente definida* especifica cada dispositivo CPE e interfaz de servicio a través de la cual pasa la ruta Manual-TE.

- Una *ruta híbrida Manual-TE* especifica uno o más dispositivos CPE e interfaces de servicio a través de las cuales pasa la ruta Manual-TE. En este caso, el tráfico entre las secciones de la ruta Manual-TE que no se especifican manualmente se transmite de forma automática (se utiliza una ruta Auto-SPF).

Puede usar restricciones de Manual-TE para agregar rutas Manual-TE a los servicios de transporte.

Ejemplos de posibles rutas Manual-TE:
En los ejemplos, se especifica un número de puerto de OpenFlow después del número de dispositivo CPE, separado por dos puntos.

**Ruta Manual-TE completamente definida**: CPE 1:3 → CPE 2:1, CPE 2:2 → CPE 4:1, CPE 4:5 → CPE N:2.

**Ruta híbrida Manual-TE**: CPE 1 → CPE 5, CPE 5:3 → CPE 4:3, CPE 4 → CPE N. En este caso, la ruta de CPE 1 a CPE N se construye como una ruta Auto-SPF CPE 1 → CPE 5, una ruta Manual-TE CPE 5:3 → CPE 4:3 y una ruta Auto-SPF CPE 4 → CPE N.

*Para crear una ruta Manual-TE, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Segmentos**.

   Se muestra una tabla de segmentos.

4. Haga clic en **Administración** → **Editar** junto al segmento en el que desea crear una ruta Manual-TE.

   Se muestran la configuración y la tabla de rutas.

   La información sobre las rutas se muestra en las siguientes columnas de la tabla:

   - **Tipo de ruta** es el tipo de ruta:

     - **Auto SPF**

     - **Auto TE**

     - **Manual TE**

- **Estado administrativo** es el estado administrativo de la ruta:
  - **arriba**
  - **abajo**
- **Estado operativo** es el estado operativo de la ruta:
  - **arriba**
  - **abajo**
- **Costo** es el costo de la ruta.
- **Cantidad de saltos** es el número de saltos de la ruta.
- **Equilibrio de carga** indica si el equilibrio de carga está habilitado para la ruta.
- **Peso equilibrado** es el peso de la ruta para el equilibrio calculado en función del costo total de los vínculos.

5. Haga clic en **+ Ruta Manual-TE**.

   Se muestran la configuración de la ruta Manual-TE y la tabla de saltos.

   La información sobre los saltos se muestra en las siguientes columnas de la tabla:

   - **#** es el número secuencial del salto. Cuanto menor sea el número del salto, antes se agregó.
   - **Remitente** es el nombre, DPID y número de puerto de OpenFlow del dispositivo CPE que es el origen del salto.
   - **Destinatario** es el nombre, DPID y número de puerto de OpenFlow del dispositivo CPE que es el destino del salto.
   - **Costo** es el costo del salto.

   El costo total de la ruta Manual-TE se muestra en la parte superior de la tabla.

6. En el campo **Nombre** del área de configuración, ingrese el nombre de la ruta Manual-TE.

7. En el campo **Número máximo de saltos**, ingrese el número máximo de saltos en la ruta Manual-TE. Rango de valores: 1 a 8. Valor predeterminado: `4`.

8. Agregue el salto a la ruta Manual-TE:

   a. En la lista desplegable **Remitente** a la izquierda, seleccione el dispositivo CPE de origen para el salto.

      Si está agregando el primer salto a la ruta Manual-TE, puede seleccionar solo el dispositivo CPE de origen del segmento como el dispositivo CPE de origen del salto. Si agregó al menos un salto a la ruta Manual-TE, solo puede seleccionar el dispositivo CPE de destino del salto anterior como el dispositivo CPE de origen del salto actual.

   b. Si es necesario, en la lista desplegable **Puerto** a la izquierda, seleccione el puerto de OpenFlow del origen del salto. Valor predeterminado: **Automáticamente** significa que el puerto de OpenFlow se determina automáticamente.

   c. En la lista desplegable **Destinatario** a la derecha, seleccione el dispositivo CPE al final del salto.

Si en la lista desplegable **Puerto** seleccionó **Automáticamente** como dispositivo CPE de origen del salto, puede seleccionar cualquier dispositivo CPE que no se esté utilizando en otros saltos como destino del salto. En este caso, en la lista desplegable **Puerto**, se selecciona **Automáticamente** para el dispositivo CPE de destino del salto y el puerto de OpenFlow se detecta automáticamente. Por lo tanto, el salto utiliza una ruta Auto-SPF.

Si en la lista desplegable **Puerto**, seleccionó un puerto de OpenFlow para el dispositivo CPE de origen del salto, para el dispositivo CPE de destino del salto, solo puede usar un dispositivo CPE que tenga un vínculo creado a partir de ese puerto de OpenFlow. En este caso, en la lista desplegable **Puerto**, el puerto de OpenFlow al que se construye el vínculo se selecciona automáticamente como el dispositivo CPE de destino del salto. Por lo tanto, el salto utiliza el vínculo especificado entre los dos dispositivos CPE.

d. Si es necesario, en la lista desplegable **Puerto** a la derecha, seleccione el puerto de OpenFlow del dispositivo CPE de destino del salto. Valor predeterminado: **Automáticamente** significa que el puerto de OpenFlow se determina automáticamente.

e. Haga clic en **Agregar**.

El salto se crea y se muestra en la tabla. Puede agregar varios saltos o eliminarlos. Para eliminar un salto, selecciónelo en la tabla y haga clic en el botón **Eliminar**.

9. Haga clic en **Crear**.

Se realiza una verificación para asegurarse de que el dispositivo CPE de destino del último salto coincida con el dispositivo CPE de destino del segmento en el que está creando la ruta Manual-TE. Si la verificación es correcta, se crea la ruta Manual-TE y se muestra en la tabla, y la columna **Costo** muestra el costo de la ruta Manual-TE, que es la suma total del costo de todos los saltos que agregó a esta ruta Manual-TE.

10. Haga clic en **Guardar** para guardar la configuración del segmento.

# Editar una ruta Manual-TE

*Para editar una ruta Manual-TE, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Segmentos**.

Se muestra una tabla de segmentos.

4. Haga clic en **Administración** → **Editar** junto al segmento en el que desea editar una ruta Manual-TE.

Se muestran la configuración y la tabla de rutas.

5. Haga clic en **Editar** junto a la ruta Manual-TE que desea editar.

Se muestran la configuración de la ruta Manual-TE y la tabla de saltos.

6. Si es necesario, edite la configuración de la ruta Manual-TE. Para obtener una descripción de la configuración, consulte las instrucciones para crear una ruta de TE manual.

7. Haga clic en **Guardar**.

   La ruta Manual-TE se modifica y actualiza en la tabla.

8. Haga clic en **Guardar** para guardar la configuración del segmento.

# Eliminar una ruta Manual-TE

Las rutas Manual-TE eliminadas no se pueden restaurar.

*Para eliminar una ruta de TE manual:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Segmentos**.

   Se muestra una tabla de segmentos.

4. Haga clic en **Administración** → **Editar** junto al segmento en el que desea eliminar una ruta Manual-TE.

   Se muestran la configuración y la tabla de rutas.

5. Haga clic en **Eliminar** junto a la ruta Manual-TE que desea eliminar.

   La ruta Manual-TE se elimina y ya no se muestra en la tabla.

6. Haga clic en **Guardar** para guardar la configuración del segmento.

# Calidad de servicio (QoS)

Una directiva de *Calidad de servicio* (QoS) garantiza la transferencia de datos de acuerdo con los requisitos establecidos para las *clases de tráfico*. En Kaspersky SD-WAN, los siguientes componentes contribuyen a la calidad del servicio:

- Clases de tráfico: indican la prioridad del procesamiento del tráfico y distribuyen el tráfico entre las colas. Por ejemplo, puede usar una de las clases de tráfico para el tráfico en tiempo real que requiere minimizar la pérdida de paquetes. Puede asignar el tráfico a las clases de tráfico cuando crea o edita un clasificador de tráfico.

- Los clasificadores de tráfico determinan si los valores de DSCP especificados en los campos del encabezado del paquete de tráfico deben ser de confianza. Si un clasificador de tráfico no confía en los valores de DSCP, los asigna a las clases de tráfico. Puede especificar un clasificador de tráfico cuando crea o edita una regla de calidad de servicio para que la regla de calidad de servicio utilice este clasificador de tráfico.

- Las reglas de calidad de servicio determinan si el ancho de banda del tráfico procesado por los clasificadores de tráfico es limitado. Puede especificar una regla de calidad de servicio cuando crea o edita un servicio de transporte para que el servicio de transporte utilice esta regla de calidad de servicio.

- Las *restricciones* se utilizan para configurar cómo se crean las rutas en los servicios de transporte. Puede crear dos tipos de restricciones:

  - Las restricciones de Manual-TE agregan rutas Manual-TE a los servicios de transporte.

  - Las restricciones de umbral especifican los umbrales de supervisión de vínculos que se utilizan para crear rutas de Auto-TE en los servicios de transporte.

  Puede especificar una restricción cuando crea o edita un servicio de transporte para que el servicio de transporte use esta restricción.

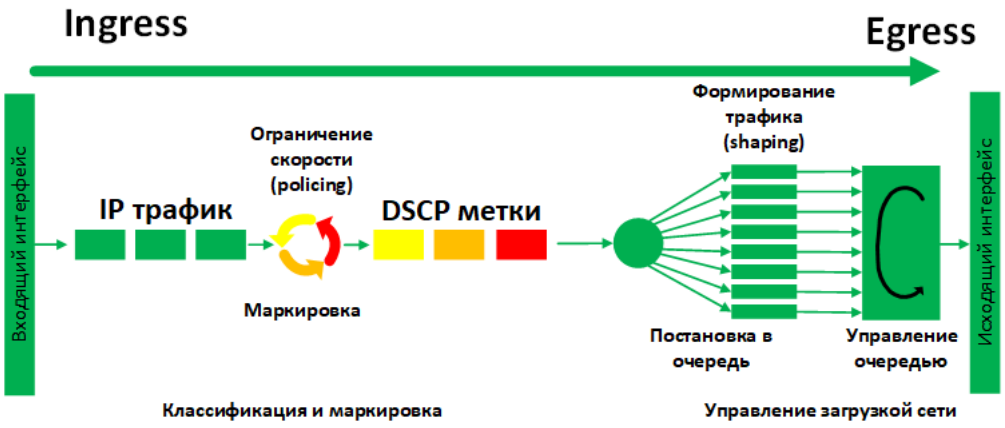
- Las reglas de clasificación de tráfico identifican el tráfico con valores particulares de los campos de encabezado L2-L4, así como el tráfico de las aplicaciones especificadas, en el flujo general de tráfico. Puede especificar una regla de clasificación de tráfico al crear o editar un filtro de tráfico para que el filtro de tráfico utilice esta regla de clasificación de tráfico.

- Los filtros de tráfico filtran el tráfico según las reglas de clasificación de tráfico especificadas. Puede especificar un filtro de tráfico cuando crea o edita un servicio de transporte o una interfaz de ACL para que el servicio de transporte o la interfaz de ACL utilicen este filtro de tráfico.

# Mecanismos de la calidad del servicio

Una directiva de QoS permite clasificar y administrar las prioridades del procesamiento del tráfico de tránsito entre cualquier interfaz CPE, incluidas las interfaces de puente, las interfaces SD-WAN y los servicios de transporte.

En la siguiente figura, se muestra un diagrama de la aplicación de herramientas de calidad de servicio.



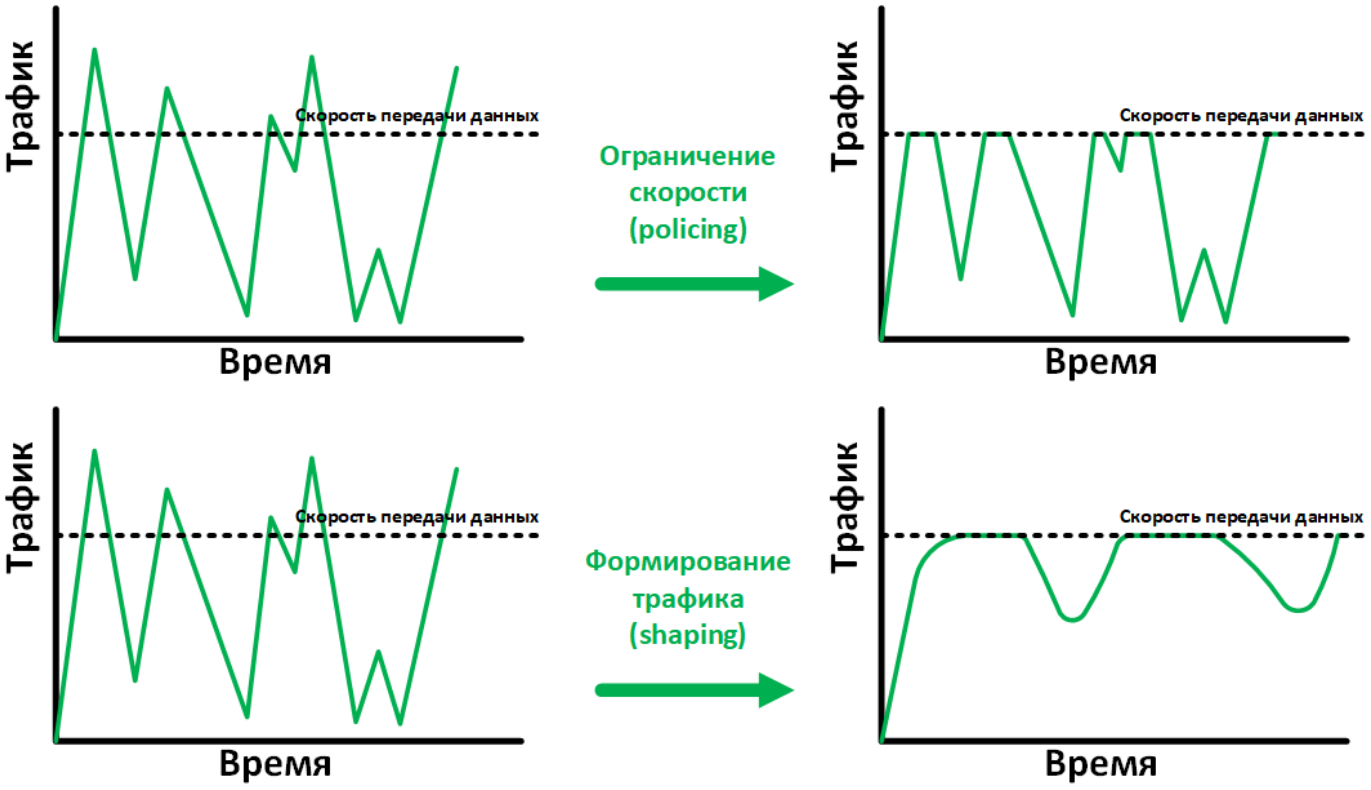

Herramientas de QoS de la solución SD-WAN

El tráfico que ingresa a la interfaz entrante se puede marcar en función de varios atributos para que coincidan con las clases de tráfico predefinidas. Esto también puede modificar la marca que se aplica actualmente al tráfico entrante.

Se puede aplicar un mecanismo de limitación de velocidad (*vigilancia*) al tráfico marcado entrante de acuerdo con las clases de tráfico.

La *configuración* del tráfico se puede aplicar al tráfico marcado saliente de acuerdo con las clases de tráfico.

En la siguiente figura, se muestra el principio de funcionamiento de la regulación y el modelado. La vigilancia elimina el tráfico que excede el umbral de velocidad de datos. El modelado suaviza las ráfagas de tráfico mediante un retraso adicional.



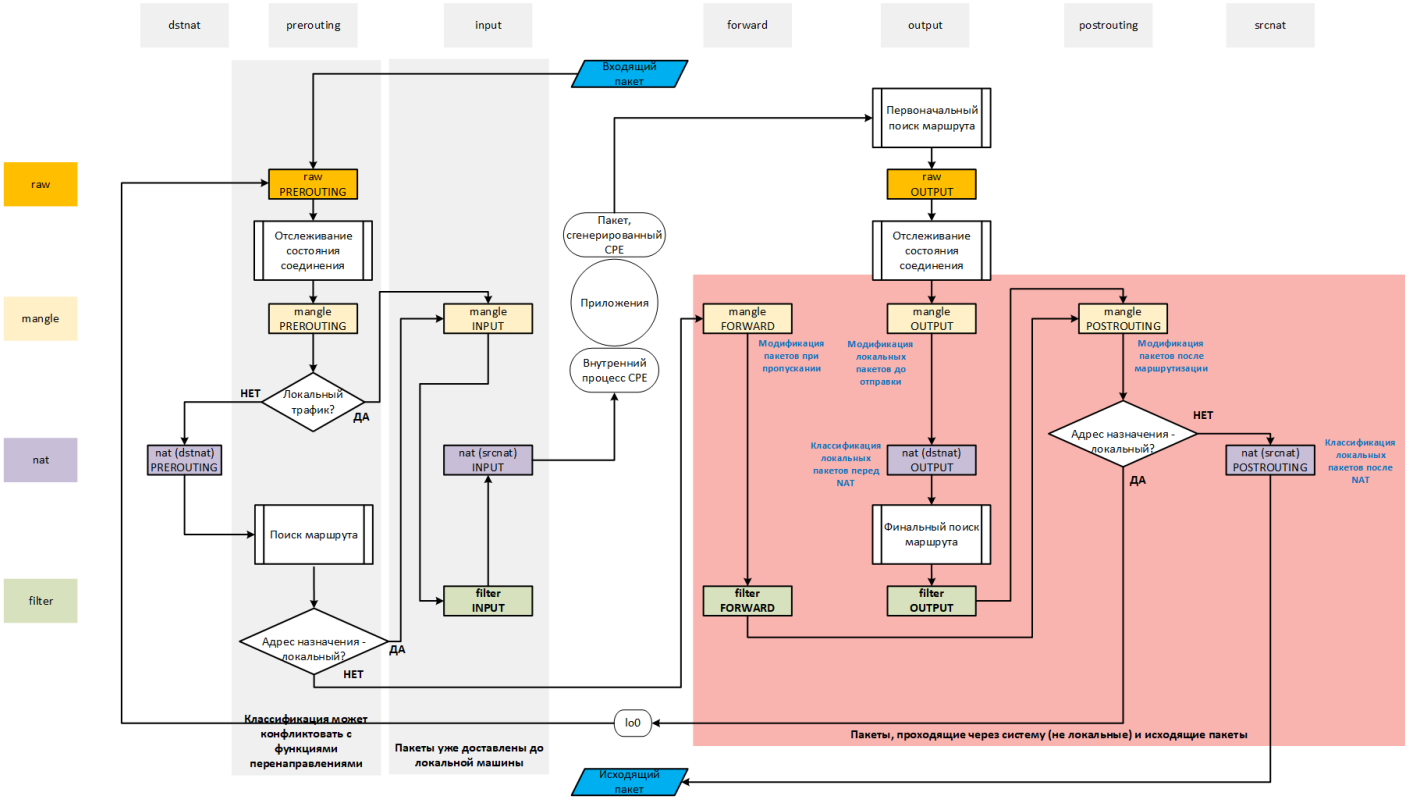

Mecanismos de procesamiento de tráfico

# Marcado y remarcado del tráfico

## Marcado mediante CLASSIFY

Para asignar el tráfico de la aplicación a las clases de tráfico adecuadas para su posterior procesamiento mediante los mecanismos de QoS, puede usar la funcionalidad CLASSIFY de las reglas de firewall avanzadas.

En el siguiente diagrama, se muestra cómo procesa el firewall el tráfico en el formato clásico de filtro de paquetes iptables. La función CLASSIFY está disponible en varias tablas y cadenas.




Puntos de clasificación (CLASSIFY) de las reglas de firewall avanzadas

Para el tráfico de tránsito, recomendamos usar la tabla MANGLE, la cadena FORWARD.

Puede crear una regla avanzada que identifique algún tipo de tráfico de acuerdo con varios criterios en la tabla MANGLE, la cadena FORWARD, la acción CLASSIFY y asignar este tráfico a un número de cola.

> Puede seleccionar solo las colas 0 a 6, que corresponden a las clases de tráfico: *Mejor esfuerzo*, *Normal para el negocio*, *Crítico para el negocio*, *Video*, *Conferencia*, *Señalización*, *Tiempo real*. No puede colocar el tráfico de la aplicación en la cola 7 (la clase *Control de red*).

El tráfico marcado de esta manera se coloca directamente en la cola de salida. El marcado de tráfico es completamente local y se usa solo dentro del dispositivo CPE para distribuir el tráfico a las colas.

# Marcado mediante TOS

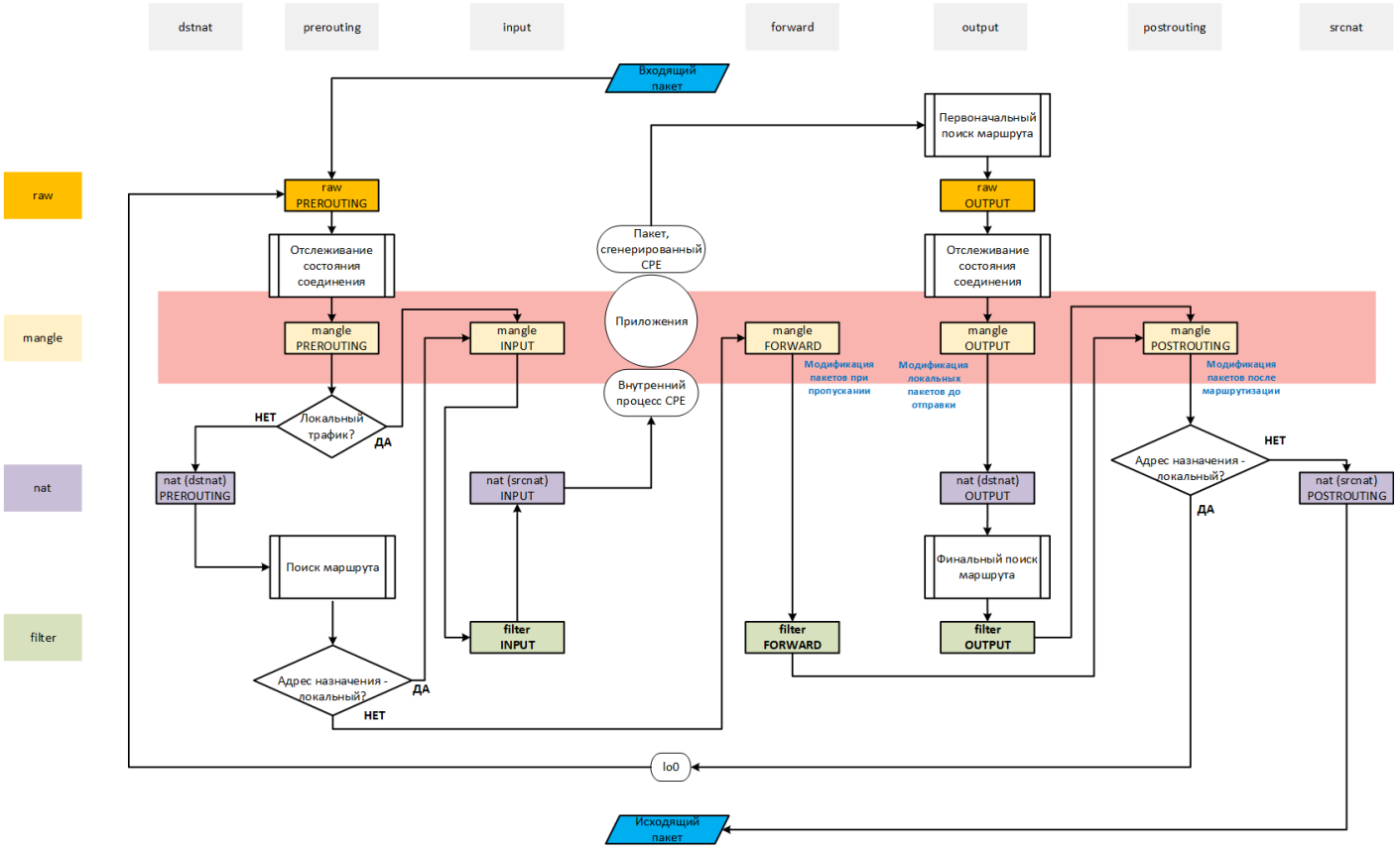
Puede marcar o volver a marcar el tráfico entrante para que coincida con las clases de tráfico configuradas mediante la acción TOS de las reglas de firewall avanzadas.

A diferencia de la marca CLASSIFY, los valores TOS/DSCP son parte del encabezado IP, lo que significa que se pueden ver fuera del dispositivo y afectar el enrutamiento y la prioridad en las redes.

En la siguiente tabla, se muestra la correspondencia entre las marcas DSCP y TOS, y las clases de tráfico preconfiguradas.

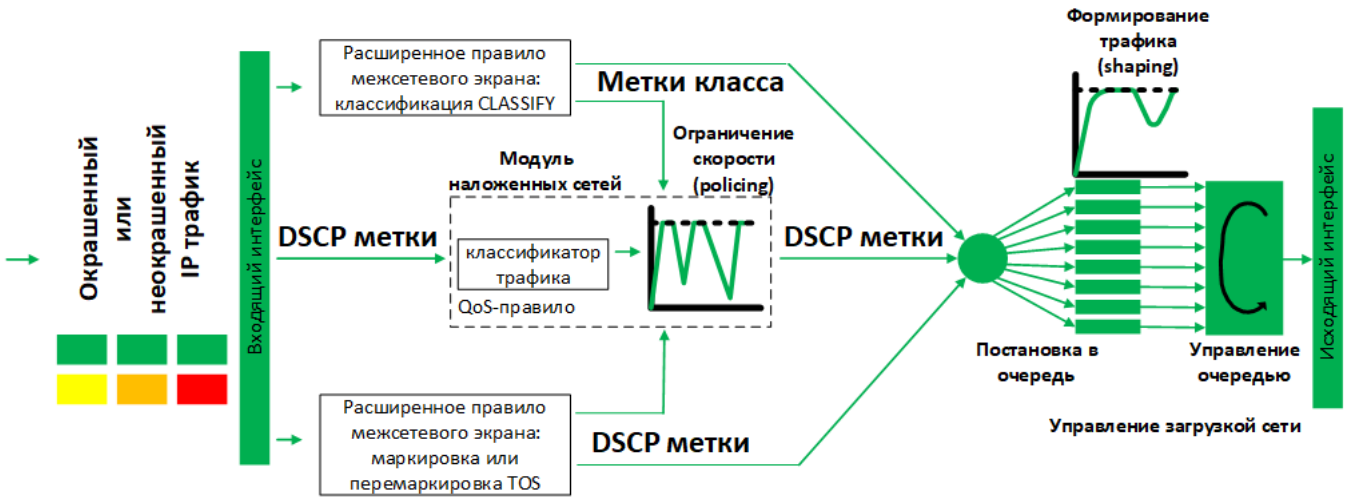
Correspondencia de las marcas DSCP y TOS con las clases de tráfico preconfiguradas

| Clase de etiqueta de tráfico | Cola | Marcado DSCP | Marcado TOS |
|---|---|---|---|
| 0 | Mejor esfuerzo | BE | 0 |
| 1 | Normal para el negocio | CS1 | 32 |
| 2 | Crítico para el negocio | CS2 | 64 |
| 3 | Señalización | AF21 | 72 |
| 4 | Video | AF42 | 144 |
| 5 | Conferencia | EF | 184 |
| 6 | Tiempo real | AF22 | 80 |




Puntos de marcado (TOS) de reglas de firewall avanzadas

En el siguiente diagrama detallado, se muestra cómo la aplicación utiliza los mecanismos de calidad de servicio (QoS) de Kaspersky SD-WAN teniendo en cuenta las redes superpuestas.




Herramientas de QoS de Kaspersky SD-WAN

## Modelado del tráfico

Puede configurar el modelado de tráfico en función de las marcas de clase o de las marcas DSCP en las interfaces de red físicas o lógicas del dispositivo CPE. El modelado del tráfico se habilita por separado para cada interfaz de red. Para las interfaces SD-WAN, esta función siempre está habilitada y puede configurar los ajustes de modelado de tráfico individuales.

*Para configurar el modelado de tráfico en las interfaces de red, siga estos pasos:*

1. Configure el modelado de tráfico de red en las interfaces de red de una de las siguientes maneras:

   - Si desea configurar el modelado del tráfico de red en las interfaces de red de una plantilla de CPE, vaya a la sección del menú SD-WAN → Plantillas de CPE, haga clic en la plantilla de CPE y seleccione la pestaña Red.

   - Si desea configurar el modelado del tráfico de red en las interfaces de red de un dispositivo CPE, vaya a la sección del menú SD-WAN → CPE, haga clic en el dispositivo CPE y seleccione la pestaña Red. Si desea editar una interfaz de red heredada de la plantilla de CPE, seleccione la casilla de verificación **Anular** junto a la interfaz de red.

2. Seleccione la interfaz de red que desee editar y haga clic en el botón Editar.

3. Seleccione la pestaña **QoS**.

4. Habilite el botón de alternancia Habilitado.

5. Si es necesario, cambie la velocidad máxima total en la interfaz y la configuración de ancho de banda mínimo y máximo para cada cola de tráfico.

6. Guarde los cambios.

*Para configurar el modelado de tráfico en las interfaces SD-WAN, siga estos pasos:*

1. Configure el modelado de tráfico de una de las siguientes maneras:

   - Si desea configurar el modelado de tráfico de red en las interfaces SD-WAN de una plantilla CPE, vaya a la sección del menú SD-WAN → Plantillas de CPE, haga clic en la plantilla de CPE y seleccione la pestaña SD-WAN.

   - Si desea configurar el modelado de tráfico de red en las interfaces SD-WAN de un dispositivo CPE, vaya a la sección del menú SD-WAN → CPE, haga clic en el dispositivo CPE y seleccione la pestaña SD-WAN. Si desea editar una interfaz de SD-WAN heredada de la plantilla CPE, seleccione la casilla **Anular** junto a esa interfaz.

2. Haga clic en la interfaz SD-WAN que desee editar, o selecciónela en la tabla y haga clic en el botón Editar.

3. Seleccione la pestaña **QoS**.

4. Cambie la configuración de las colas de tráfico: etiquetas de clases de tráfico, ToS, ancho de banda mínimo y máximo.

5. Guarde los cambios.

# Administrar clases de tráfico

## Acerca de las clases de tráfico

Puede ver la tabla de las clases de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador.

- Para ver la tabla de clases de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clases de tráfico**.

- Para ver la tabla de clases de tráfico en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS**.

De manera predeterminada, se crean las siguientes clases de tráfico:

- **Mejor esfuerzo**
- **Normal para el negocio**
- **Crítico para el negocio**
- **Video**
- **Conferencia**
- **Señalización**

- **Tiempo real**
- **Control de red**

La información sobre las clases de tráfico se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la clase de tráfico.
- **Clase de etiqueta** es la etiqueta interna de la clase de tráfico.
- **Número de cola** es el número de la cola a la que se dirige el tráfico de la clase de tráfico.
- **KOver** es la relación de sobrecompromiso del ancho de banda del tráfico, que establece el multiplicador por el cual el ancho de banda dedicado a la clase de tráfico puede aumentarse si el ancho de banda total no se utiliza por completo.
- **Excluir en el cómputo de la ruta** indica si el ancho de banda disponible para la clase de tráfico se tiene en cuenta para el cálculo de la ruta:
  - **Sí**.
  - **No**.

Los siguientes parámetros se muestran en la parte inferior de la tabla:

- **Clase de tráfico predeterminada** es la clase de tráfico en la que se coloca todo el tráfico que no está incluido en otras clases.
- **Clase de tráfico de control** es la clase de tráfico en la que se coloca el tráfico de control que se utiliza para administrar los componentes de la solución. Recomendamos asignar la máxima prioridad al tráfico de control para asegurarse de que la red funcione de manera confiable.
- **Ancho de banda reservado máximo (%)** es el porcentaje de la velocidad máxima de transferencia de tráfico que puede estar disponible para la clase de tráfico.

Kaspersky SD-WAN no admite la creación de clases de tráfico, pero puede editar las clases de tráfico predeterminadas en la plantilla de instancia SD-WAN o en el menú de configuración del controlador.

## Editar una clase de tráfico

Puede editar una clase de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si edita una clase de tráfico en una plantilla de instancia SD-WAN, esa clase de tráfico no se modifica en el menú de configuración del controlador de las instancias SD-WAN ya implementadas.

> Las clases de tráfico predeterminadas son adecuadas para la mayoría de los escenarios de implementación y no recomendamos editarlas.

*Para editar una clase de tráfico, siga estos pasos:*

1. Edite una clase de tráfico de una de las siguientes maneras:

   - Si desea editar la clase de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clases de tráfico**.

   - Si desea cambiar la clase de tráfico en la sección de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS**.

   Se muestra una tabla de clases de tráfico.

2. Haga clic en **Editar**.

3. En la columna **Nombre**, ingrese el nombre de la clase de tráfico.

4. En la columna **Número de cola**, seleccione el número de la cola en el tráfico de la clase seleccionada. Cuanto mayor sea el valor, mayor será la prioridad de la clase de tráfico. No puede especificar la misma prioridad para varias clases de tráfico.

5. En la columna **KOver**, seleccione la relación de sobrecompromiso del ancho de banda del tráfico, que establece el multiplicador por el cual el ancho de banda dedicado a la clase de tráfico puede aumentarse si el ancho de banda total no se utiliza por completo.

6. Si desea ignorar el ancho de banda disponible para la clase de tráfico durante la creación de la ruta, seleccione la casilla **Excluir en el cómputo de la ruta**. Cuando se selecciona esta casilla, no se puede seleccionar la relación **KOver** para la clase de tráfico. De manera predeterminada, esta casilla está seleccionada junto a la clase de tráfico **Mejor esfuerzo**.

7. En la lista desplegable **Clase de tráfico predeterminada**, seleccione la clase de tráfico en la que se coloca todo el tráfico que no está incluido en otras clases. De manera predeterminada, la clase de tráfico **Mejor esfuerzo** está seleccionada.

8. En la lista desplegable **Clase de tráfico de control**, seleccione la clase de tráfico en la que desea que se coloque el tráfico de control. De manera predeterminada, la clase de tráfico **Control de red** está seleccionada.

9. En la lista desplegable **Ancho de banda reservado máximo (%)**, seleccione el porcentaje de la velocidad máxima de transferencia de tráfico que puede estar disponible para la clase de tráfico. Rango de valores: de 10 a 90. El valor predeterminado es **90**.

10. Haga clic en **Guardar**.

    Se modifica la clase de tráfico.

# Administrar clasificadores de tráfico

Puede ver la tabla de los clasificadores de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador.

- Para ver la tabla de los clasificadores de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN → Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clasificadores de tráfico**.

- Para ver la tabla de clasificadores de tráfico en el menú de configuración del controlador, vaya a la sección del menú**Infraestructura** y abra la configuración del despliegue del controlador; para ello, haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS** y seleccione la pestaña **Clasificadores de tráfico**.

De manera predeterminada, se crea **Untrust-BE-Classifier**, que no confía en los valores DSCP de los campos de encabezado de los paquetes de tráfico y coloca todo el tráfico en la clase de tráfico **Mejor esfuerzo**. La información sobre las clases de tráfico se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del clasificador de tráfico.

- **Tipo** indica si el clasificador confía en los valores DSCP establecidos en los campos de encabezado de los paquetes de tráfico:

  - **Sí**.

  - **No**.

- **Clase de tráfico** son las clases de tráfico en las que el clasificador coloca el tráfico.

- **Campo de paquete** son los encabezados de los paquetes de tráfico.

- **Etiqueta externa** es el valor DSCP que los encabezados del paquete de tráfico deben contener para que el clasificador coloque el tráfico en la clase de tráfico.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un clasificador de tráfico

Puede crear un clasificador de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si crea un clasificador de tráfico en una plantilla de instancia SD-WAN, ese clasificador de tráfico no se crea en el menú de configuración del controlador de las instancias SD-WAN ya implementadas.

*Para crear un clasificador de tráfico, siga estos pasos:*

1. Cree un clasificador de tráfico de una de las siguientes maneras:

   - Si desea crear un clasificador de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN**→ **Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clasificadores de tráfico**.

   - Si desea crear un clasificador de tráfico en el menú de configuración del controlador, vaya a la sección **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **QoS** y seleccione la pestaña **Clasificadores de tráfico**.

   Se muestra una tabla de clases de tráfico.

2. Haga clic en **+ Clasificador**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del clasificador de tráfico.

4. En la lista **Tipo**, seleccione uno de estos valores:

   - **Confiar** significa que el clasificador de tráfico confía en los valores de DSCP establecidos en los campos de encabezado de los paquetes de tráfico. Esta es la configuración predeterminada.

   - **No confiar** significa que el clasificador de tráfico no confía en los valores de DSCP establecidos en los campos de encabezado de los paquetes de tráfico.

5. Si seleccionó **Confiar** en la lista **Tipo**, asigne las clases de tráfico a los valores de DSCP en los encabezados de los paquetes de tráfico:

   a. En la columna **Clase de tráfico**, seleccione la clase de tráfico en la que el clasificador de tráfico coloca el tráfico.

   b. En la columna **Etiqueta externa**, haga clic en **Seleccionar** junto al campo de encabezado del paquete de tráfico.

   c. Seleccione las casillas de verificación junto a los valores de DSCP mostrados que deben estar presentes en el campo de encabezado del paquete de tráfico para que el clasificador de tráfico coloque el tráfico en la clase de tráfico.

   d. Haga clic en **Aceptar**.

6. En la lista **Tipo** que seleccionó **No confiar**, seleccione la clase de tráfico en la que el clasificador de tráfico coloca todo el tráfico en la lista desplegable **Clase de tráfico**.

7. Haga clic en **Crear**.

   El clasificador de tráfico se crea y se muestra en la tabla.

8. Si creó un clasificador de tráfico en la plantilla de instancias SD-WAN, en la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancias SD-WAN.

Puede especificar un clasificador de tráfico cuando crea o edita una regla de calidad de servicio para que la regla de calidad de servicio utilice este clasificador de tráfico.

# Editar un clasificador de tráfico

Puede editar un clasificador de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si edita un clasificador de tráfico en una plantilla de instancia SD-WAN, ese clasificador de tráfico no se edita en el menú de configuración del controlador de instancias SD-WAN ya implementadas.

*Para editar un clasificador de tráfico:*

1. Edite un clasificador de tráfico de una de las siguientes maneras:

   - Si desea editar un clasificador de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clasificadores de tráfico**.

   - Si desea editar un clasificador de tráfico en el menú de configuración del controlador, vaya a la sección **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **QoS** y seleccione la pestaña **Clasificadores de tráfico**.

   Se muestra una tabla de clases de tráfico.

2. Haga clic en **Administración** → **Editar** junto al clasificador de tráfico que desea editar.

3. En la ventana que se abre, si es necesario, edite la configuración del clasificador de tráfico. Para obtener una descripción de la configuración, consulte las instrucciones para crear un clasificador de tráfico.

4. Haga clic en **Guardar**.

   El clasificador de tráfico se modifica y actualiza en la tabla.

5. Si ha editado un clasificador de tráfico en la plantilla de instancias SD-WAN, en la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancias SD-WAN.

# Eliminar un clasificador de tráfico

Puede eliminar un clasificador de tráfico en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si elimina un clasificador de tráfico en una plantilla de instancia SD-WAN, ese clasificador de tráfico no se elimina en el menú de configuración del controlador de las instancias SD-WAN ya implementadas.

Los clasificadores de tráfico eliminados no se pueden restaurar.

*Para eliminar un clasificador de tráfico, siga estos pasos:*

1. Elimine un clasificador de tráfico de una de las siguientes maneras:

   - Si desea eliminar un clasificador de tráfico en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Clasificadores de tráfico**.

   - Si desea eliminar un clasificador de tráfico en el menú de configuración del controlador, vaya a la sección **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador y vaya a la sección **QoS** y seleccione la pestaña **Clasificadores de tráfico**.

   Se muestra una tabla de clases de tráfico.

2. Haga clic en **Administración → Eliminar** junto al clasificador de tráfico que desea eliminar.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   El clasificador de tráfico se elimina y ya no se muestra en la tabla.

4. Si eliminó un clasificador de tráfico en la plantilla de instancias SD-WAN, en la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancias SD-WAN.

# Administrar las reglas de calidad del servicio

Puede ver la tabla de las reglas de calidad del servicio en una plantilla de instancia SD-WAN o en el menú de configuración del controlador.

- Para ver la tabla de las reglas de calidad del servicio en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN → Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Reglas de QoS**.

- Para ver la tabla de reglas de calidad de servicio en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración del despliegue del controlador; para ello, haga clic en el nombre del controlador o selecciónelo en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS** y seleccione la pestaña **Reglas de QoS**.

De manera predeterminada, se crea la regla de calidad del servicio **Unlimited-QoS**, que utiliza el clasificador de tráfico predeterminado, **Untrust-BE-Classifier**, no limita el ancho de banda y ofrece el 100 % de la totalidad del ancho de banda a la clase de tráfico **Mejor esfuerzo**. La información sobre las reglas de calidad del servicio se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la regla de calidad del servicio.

- **MBR** es el ancho de banda máximo permitido por la regla de calidad del servicio.

- Las siguientes columnas muestran el porcentaje del ancho de banda total disponible para las clases de tráfico:

  - **Mejor esfuerzo**

  - **Normal para el negocio**

  - **Crítico para el negocio**

- **Video**
- **Conferencia**
- **Señalización**
- **Tiempo real**

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una regla de calidad de servicio

Puede crear una regla de calidad de servicio en la plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si crea una regla de calidad de servicio en una plantilla de instancia SD-WAN, esa regla de calidad de servicio no se crea en el menú de configuración del controlador de instancias SD-WAN ya implementadas.

*Para crear una regla de calidad de servicio, siga estos pasos:*

1. Cree una regla de calidad de servicio:

   - Si desea crear una regla de calidad de servicio en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Reglas de QoS**.

   - Si desea crear una regla de calidad de servicio en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o selecciónelo en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS** y seleccione la pestaña **Reglas de QoS**.

   Se muestra la tabla de reglas de calidad del servicio.

2. Haga clic en **+ Regla de QoS**.

3. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la regla de calidad de servicio.

4. En la lista desplegable **Clasificador**, seleccione el clasificador de tráfico creado que desea usar en la regla de calidad de servicio.

5. Si desea que la regla de calidad de servicio limite el ancho de banda para el tráfico procesado por el clasificador de tráfico, desmarque la casilla **Sin límite**. Esta casilla está seleccionada por defecto.

6. Si desmarcó la casilla **Sin límite**, configure el límite de ancho de banda de tráfico:

   a. En el campo **MBR**, ingrese la tasa de bits máxima. El valor predeterminado es `1`.

   b. En la lista desplegable **Tipo de velocidad**, seleccione las unidades de medida para la tasa de bits máxima:

   - **Kbit/s**. Esta es la configuración predeterminada.
   - **Mbit/s**.
   - **Gbit/s**

   c. Si en la lista desplegable **Clasificador**, seleccionó un clasificador del tipo **Confianza**, en la columna **Ancho de banda reservado máximo (%)**, especifique el porcentaje de la tasa de bits total disponible para las clases de tráfico. La suma total de los valores especificados debe ser igual al 100 %.

7. Haga clic en **Crear**.

   La regla de calidad de servicio se crea y se muestra en la tabla.

8. Si creó una regla de calidad de servicio en la plantilla de instancia SD-WAN, en la parte inferior del área de configuración, haga clic en Guardar para guardar la configuración de la plantilla de la instancia SD-WAN.

Puede especificar una regla de calidad de servicio cuando crea o edita un servicio de transporte para que el servicio de transporte utilice esta regla de calidad de servicio.

# Editar una regla de calidad de servicio

Puede editar una regla de calidad del servicio en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si edita una regla de calidad de servicio en una plantilla de instancia SD-WAN, esa regla de calidad de servicio no se crea en el menú de configuración del controlador de instancias SD-WAN ya implementadas.

*Para editar una regla de calidad de servicio, siga estos pasos:*

1. Edite una regla de calidad de servicio:

   - Si desea editar una regla de calidad de servicio en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Reglas de QoS**.
   - Si desea editar una regla de calidad de servicio en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS** y seleccione la pestaña **Reglas de QoS**.

   Se muestra la tabla de reglas de calidad del servicio.

2. Haga clic en el nombre de la regla de calidad de servicio que desea editar o selecciónela en la tabla y haga clic en el botón **Editar**.

3. En la ventana que se abre, si es necesario, edite la configuración de la calidad de servicio. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla de calidad de servicio.

4. Haga clic en **Guardar**.

   La regla de calidad de servicio se modifica y actualiza en la tabla.

5. Si editó una regla de calidad de servicio en la plantilla de instancia SD-WAN, en la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancia SD-WAN.

# Eliminar una regla de calidad del servicio

Puede eliminar una regla de calidad del servicio en una plantilla de instancia SD-WAN o en el menú de configuración del controlador. Si elimina una regla de calidad del servicio en una plantilla de instancia SD-WAN, esa regla de calidad del servicio no se elimina del menú de configuración del controlador de las instancias SD-WAN ya implementadas.

Las reglas de calidad del servicio eliminadas no se pueden restaurar.

*Para eliminar una regla de calidad del servicio, haga lo siguiente:*

1. Elimine una regla de calidad del servicio:

   - Si desea eliminar una regla de calidad del servicio en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN → Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Reglas de QoS**.

   - Si desea eliminar una regla de calidad de servicio en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **QoS** y seleccione la pestaña **Reglas de QoS**.

   Se muestra la tabla de reglas de calidad del servicio.

2. Seleccione la regla de calidad de servicio que desea eliminar y haga clic en el botón **Eliminar**.

3. En la ventana de confirmación, haga clic en **Eliminar**.

   La regla de calidad de servicio se eliminará y ya no se mostrará en la tabla.

4. Si eliminó una regla de calidad del servicio en la plantilla de instancia SD-WAN, en la parte inferior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de instancia SD-WAN.

# Administrar restricciones de Manual-TE

Para ver la tabla de restricciones de Manual-TE, vaya a la sección del menú **Infraestructura**, haga clic en **Administración → Configuración de implementación** junto al controlador y vaya a la sección **Restricciones**. La información sobre las restricciones de Manual-TE se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la restricción de Manual-TE.
- **Segmento** es el segmento de las rutas de Manual-TE agregadas a la restricción de Manual-TE.
- **Rutas** son las rutas de Manual-TE que se agregaron a la restricción de Manual-TE.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una restricción de Manual-TE

*Para crear una restricción de Manual-TE, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. En la parte superior de la página, haga clic en **+ Agregar**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la restricción de Manual-TE.

6. Seleccione la casilla de verificación **Utilizar ruta Manual-TE** junto a las rutas Manual-TE creadas que desea agregar a la restricción de Manual-TE. Estas casillas de verificación están desactivadas de manera predeterminada.

7. Si desea permitir el uso de una ruta Auto-SPF cuando las rutas Manual-TE especificadas no están disponibles, seleccione la casilla **Ignorar si no se encontró una ruta restringida** junto a las rutas Manual-TE. Solo puede seleccionar la casilla junto a una ruta Manual-TE que tenga seleccionada la casilla **Utilizar ruta Manual-TE**. Estas casillas de verificación están desactivadas de manera predeterminada.

8. Haga clic en **Crear**.

La restricción de Manual-TE se crea y se muestra en la tabla.

Puede especificar una restricción de Manual-TE cuando crea o edita un servicio de transporte para que el servicio de transporte use esta restricción de Manual-TE.

# Editar una restricción de Manual-TE

*Para editar una restricción de Manual-TE, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. Haga clic en el nombre de la regla de Manual-TE que desea editar, o selecciónela en la tabla y haga clic en el botón **Editar**.

5. En la ventana que se abre, si es necesario, edite la configuración de la restricción de Manual-TE. Para obtener una descripción de la configuración, consulte las instrucciones para crear una restricción de Manual-TE.

6. Haga clic en **Guardar**.

La restricción de Manual-TE se modifica y actualiza en la tabla.

# Eliminar una restricción de Manual-TE

Las restricciones de Manual-TE eliminadas no se pueden restaurar.

*Para eliminar una restricción de Manual-TE, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. En la tabla, seleccione la restricción de Manual-TE que desea eliminar y haga clic en el botón **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

La restricción de Manual-TE se elimina y ya no se muestra en la tabla.

# Administrar restricciones de umbral

Para ver la tabla de restricciones de umbral en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o selecciónelo en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **Restricciones** y seleccione la pestaña **Umbrales**. La información sobre las restricciones de umbral se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la restricción de umbral.
- **Último recurso** indica si la restricción de umbral excluye un vínculo del cálculo de la ruta Auto-TE si la casilla de verificación **Último recurso** está seleccionada en la configuración de supervisión de vínculos:
  - Y
  - N
- **Nivel de error** indica si la restricción de umbral excluye un vínculo del cálculo de ruta Auto-TE si se alcanza el umbral de errores por segundo en el vínculo:
  - Y
  - N
- **Utilización** indica si la restricción de umbral excluye un vínculo del cálculo de ruta Auto-TE si el umbral de utilización se alcanza en el vínculo, como un porcentaje del ancho de banda de la interfaz del servicio de origen:
  - Y
  - N
- **Latencia** indica si la restricción de umbral excluye un vínculo del cálculo de la ruta Auto-TE si el umbral de retardo (en milisegundos) se alcanza para el tráfico que pasa a través del vínculo:
  - Y
  - N
- **Fluctuación** indica si la restricción de umbral excluye un vínculo del cálculo de ruta Auto-TE si se alcanza el umbral de fluctuación (en milisegundos) para el tráfico que pasa a través del vínculo:
  - Y
  - N

- **Pérdida de paquetes** indica si la restricción de umbral excluye un vínculo del cálculo de ruta Auto-TE si se alcanza el umbral de pérdida de paquetes (como un valor porcentual) en el vínculo:
  - Y
  - N

Puede especificar umbrales de supervisión cuando configura la supervisión del vínculo.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una restricción de umbral

*Para crear una restricción de umbral, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. Seleccione la pestaña **Umbrales**.

   Se muestra una tabla de restricciones de umbral.

5. En la parte superior de la página, haga clic en **+ Restricción de umbral**.

6. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la restricción de umbral.

7. Seleccione la casilla **No utilice vínculos si se alcanzó el umbral** junto a los indicadores de supervisión de vínculos para que la restricción de umbral excluya los vínculos que alcanzaron el valor de umbral de estos indicadores de supervisión del cálculo de la ruta Auto-TE. Esta casilla está desactivada por defecto.

8. Si no desea que la restricción de umbral excluya los vínculos con umbrales alcanzados del cálculo de ruta Auto-TE cuando no existen vínculos alternativos, seleccione la casilla **Ignorar si no se encontró una ruta restringida** junto a los valores de supervisión. Esta casilla está desactivada por defecto. Solo puede seleccionar la casilla junto a los valores de supervisión que tienen seleccionada la casilla **No utilice vínculos si se alcanzó el umbral**.

   Por ejemplo, si seleccionó la casilla **No utilice vínculos si se alcanzó el umbral** junto al valor de supervisión **Nivel de error**, la restricción de umbral excluye un vínculo en el que se alcanza el umbral de errores por segundo del cálculo de la ruta Auto-TE. Si también seleccionó la casilla **Ignorar si no se encontró una ruta restringida** y todos los vínculos alcanzaron el umbral de errores por segundo, la restricción de umbral no excluye el vínculo del cálculo de la ruta Auto-TE.

9. Haga clic en **Crear**.

La restricción de umbral se crea y se muestra en la tabla.

Puede especificar una restricción de umbral cuando crea o edita un servicio de transporte para que el servicio de transporte utilice esta restricción de umbral.

# Editar una restricción de umbral

*Para editar una restricción de umbral, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. Seleccione la pestaña **Umbrales**.

   Se muestra una tabla de restricciones de umbral.

5. Haga clic en el nombre de la restricción de umbral que desea editar o selecciónela en la tabla y haga clic en el botón **Editar**.

6. En la ventana que se abre, si es necesario, edite la configuración de la restricción de umbral. Para obtener una descripción de la configuración, consulte las instrucciones para crear una restricción de umbral.

7. Haga clic en **Guardar**.

La restricción de umbral se modifica y se actualiza en la tabla.

# Eliminar una restricción de umbral

Las restricciones de umbral eliminadas no se pueden restaurar.

*Para eliminar una restricción de umbral, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Restricciones**.

   La pestaña **Manual-TE** con la tabla de restricciones de Manual-TE está seleccionada de manera predeterminada.

4. Seleccione la pestaña **Umbrales**.

   Se muestra una tabla de restricciones de umbral.

5. En la tabla, seleccione la restricción de umbral que desea eliminar y haga clic en el botón **Eliminar**.

6. En la ventana de confirmación, haga clic en **Eliminar**.

La restricción de umbral se elimina y ya no se muestra en la tabla.

# Administrar reglas de clasificación de tráfico

Para ver la tabla de reglas de clasificación de tráfico, en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú y abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o selecciónelo en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **Filtros de tráfico**.

La información sobre las reglas de clasificación de tráfico se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre de la regla de clasificación de tráfico.
- **Campos L2** son campos L2 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general.
- **Campos L3** son campos L3 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general.
- **Campos L4** son campos L4 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear una regla de clasificación de tráfico

*Para crear una regla de clasificación de tráfico:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. En la parte superior de la página, haga clic en **+ Regla de clasificación**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre de la regla de clasificación del tráfico.

6. En la pestaña **Campos L2**, seleccione las casillas junto a los campos L2 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general. Si la casilla está seleccionada, ingrese o seleccione el valor del campo. Puede utilizar los valores de los siguientes campos para identificar el tráfico en el flujo de datos general:

   - **ID de VLAN exterior**. Rango de valores: 1 a 2094.
   - **PCP de VLAN exterior**. Rango de valores: 0 a 7.
   - **MAC de origen**.
   - **Máscara de MAC de origen**.
   - **MAC de destino**.
   - **Máscara de MAC de destino**.
   - **Ethertype**:
     - **0x0800**. Esta es la configuración predeterminada.
     - **0x86dd**
     - **0x0806**

7. En la pestaña **Campos L3**, seleccione las casillas junto a los campos L3 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general. Si la casilla está seleccionada, ingrese o seleccione el valor del campo. Puede usar los valores de los siguientes campos para identificar el tráfico en el flujo de datos general.

   - **Protocolo**:
     - **IPv4**
     - **IPv6**
   - **IP de origen**.
   - **Longitud del prefijo de IP de origen**. Rango de valores para la dirección IPv4: 0 a 32; para la dirección IPv6: 0 a 128
   - **IP de destino**.
   - **Longitud del prefijo de IP de destino**. Rango de valores para la dirección IPv4: 0 a 32; para la dirección IPv6: 0 a 128

- **DSCP**
- **TOS**

8. En la pestaña **Campos L4**, seleccione las casillas junto a los campos L4 cuyos valores utiliza la regla de clasificación de tráfico para identificar el tráfico en el flujo de datos general. Si la casilla está seleccionada, ingrese o seleccione el valor del campo. Puede utilizar los valores de los siguientes campos para identificar el tráfico en el flujo de datos general:
   - **Protocolo de IP**
   - **Lista de puertos de origen**
   - **Lista de puertos de destino**
   - **Número de tipo de ICMP**
9. En la pestaña **DPI**, seleccione la casilla **Aplicación** y la aplicación cuyo tráfico identifica la regla de clasificación de tráfico en el flujo de datos general.
10. Haga clic en **Crear**.

    La regla de clasificación del tráfico se crea y se muestra en la tabla.

Puede especificar una regla de clasificación de tráfico al crear o editar un filtro de tráfico para que el filtro de tráfico utilice esta regla de clasificación de tráfico.

Ejemplo de una regla de clasificación de tráfico creada:
Puede crear una regla de clasificación de tráfico con los siguientes parámetros:

- En la pestaña **Campos L2**, en el campo **ID de VLAN exterior**, ingrese `1`.
- En la pestaña **Campos L2**, en el campo **PCP de VLAN exterior**, ingrese `3`.
- En la pestaña **Campos L3**, en la lista desplegable **Protocolo**, seleccione **IPv4**.
- En la pestaña **Campos L3**, en el campo **IP de origen**, ingrese la dirección IP `192.168.2.0/24`.

La regla de clasificación de tráfico identifica el tráfico con las siguientes propiedades en el flujo de datos general:

- Etiqueta de la VLAN externa: 1
- Etiqueta del PCP externa: 3
- Protocolo: IPv4
- Dirección IP de origen: 192.168.2.0/24

La regla de clasificación de tráfico no identifica el tráfico que carece de al menos una de estas propiedades en el flujo de datos general.

# Editar una regla de clasificación de tráfico

*Para editar una regla de clasificación de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. Haga clic en el nombre de la regla de clasificación de tráfico que desea editar o selecciónela en la tabla y haga clic en el botón **Editar**.

5. En la ventana que se abre, si es necesario, edite la configuración de la regla de clasificación de tráfico. Para obtener una descripción de la configuración, consulte las instrucciones para crear una regla de clasificación de tráfico.

6. Haga clic en **Guardar**.

La regla de clasificación del tráfico se modifica y se actualiza en la tabla.

# Eliminar una regla de clasificación de tráfico

Las reglas de clasificación de tráfico eliminadas no se pueden restaurar.

*Para eliminar una regla de clasificación de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. En la tabla, seleccione la regla de clasificación de tráfico que desea eliminar y haga clic en el botón **Eliminar**.

5. En la ventana de confirmación, haga clic en **Eliminar**.

La regla de clasificación de tráfico se elimina y ya no se muestra en la tabla.

# Administrar filtros de tráfico

Para ver la tabla de filtros de tráfico en el menú de configuración del controlador, vaya a la sección **Infraestructura** del menú, abra la configuración de despliegue del controlador; para ello, haga clic en el nombre del controlador o selecciónelo en la tabla y haga clic en **Configuración de implementación**. Luego, vaya a la sección **Filtros de tráfico** y seleccione la pestaña **Filtros**. La información sobre los filtros de tráfico se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del filtro de tráfico.
- **Reglas agregadas** son reglas de clasificación de tráfico que se agregaron al filtro de tráfico.
- **Acción** es la acción que el filtro de tráfico aplica al tráfico:
  - **Permitir**: permitir un mayor enrutamiento del tráfico.
  - **Denegar**: bloquear un mayor enrutamiento del tráfico.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un filtro de tráfico

*Para crear un filtro de tráfico, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. Seleccione la pestaña **Filtros**.

   Se muestra una tabla de filtros de tráfico.

5. En la parte superior de la página, haga clic en **+ Filtro de tráfico**.

6. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del filtro de tráfico.

7. Agregue la regla de clasificación de tráfico creada al filtro de tráfico.

   a. En el campo **Secuencia**, ingrese el número secuencial de la regla de clasificación de tráfico. La primera regla de clasificación de tráfico que el filtro de tráfico aplica es la regla con el número de secuencia más bajo. Rango de valores: 1 a 998. El valor predeterminado es `10`.

      No puede especificar el mismo número de secuencia para varias reglas de clasificación de tráfico.

   b. En la lista desplegable **Regla de clasificación**, seleccione la regla de clasificación de tráfico que desea agregar al filtro de tráfico.

   c. En la lista desplegable **Acción**, seleccione la acción que el filtro aplica al tráfico:

      - **Permitir**: permitir un mayor enrutamiento del tráfico. Esta es la configuración predeterminada.
      - **Denegar**: bloquear un mayor enrutamiento del tráfico.

   d. Haga clic en **Agregar**.

   Se agrega la regla de clasificación de tráfico. Puede agregar varias reglas de clasificación de tráfico o eliminar reglas de clasificación de tráfico. Para eliminar una regla de clasificación de tráfico, haga clic en **Eliminar** junto a ella.

8. En la lista desplegable **Acción predeterminada**, seleccione la acción que el filtro de tráfico aplica a todo el resto del tráfico:

   - **Permitir**: permitir un mayor enrutamiento del tráfico. Esta es la configuración predeterminada.
   - **Denegar**: bloquear un mayor enrutamiento del tráfico.

9. Haga clic en **Crear**.

Se crea el filtro de tráfico y se muestra en la tabla.

Puede especificar un filtro de tráfico cuando crea o edita un servicio de transporte o una interfaz de ACL para que el servicio de transporte o la interfaz de ACL utilicen este filtro de tráfico.

# Editar un filtro de tráfico

*Para editar un filtro de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. Seleccione la pestaña **Filtros**.

   Se muestra una tabla de filtros de tráfico.

5. Haga clic en el nombre del filtro de tráfico que desea editar o selecciónelo en la tabla y haga clic en el botón **Editar**.

6. En la ventana que se abre, si es necesario, edite la configuración del filtro de tráfico. Para obtener una descripción de la configuración, consulte las instrucciones para crear un filtro de tráfico.

7. Haga clic en **Guardar**.

El filtro de tráfico se modifica y actualiza en la tabla.

# Eliminar un filtro de tráfico

Los filtros de tráfico eliminados no se pueden restaurar.

*Para eliminar un filtro de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Filtros de tráfico**.

   De manera predeterminada, está seleccionada la pestaña **Reglas**, que muestra la tabla de reglas de clasificación de tráfico.

4. Seleccione la pestaña **Filtros**.

   Se muestra una tabla de filtros de tráfico.

5. En la tabla, seleccione el filtro de tráfico que desea eliminar y haga clic en el botón **Eliminar**.

6. En la ventana de confirmación, haga clic en **Eliminar**.

El filtro de tráfico se elimina y ya no se muestra en la tabla.

# Transmisión de tráfico entre dispositivos CPE y dispositivos cliente mediante servicios de transporte

## Acerca de los servicios de transporte

Puede utilizar los *servicios de transporte* para transmitir tráfico entre los dispositivos CPE y los dispositivos del cliente que estén conectados a ellos. Los servicios de transporte se desarrollan sobre los segmentos y constan de interfaces de servicio. Kaspersky SD-WAN admite la creación de los siguientes servicios de transporte:

- L2:
  - Punto a punto (E-line en la clasificación MEF, en adelante también denominado servicio P2P) es un servicio de transporte estático en el que el tráfico se transmite entre dos interfaces de servicio.
  - Punto a multipunto (E-Tree en la clasificación MEF, en adelante también denominado servicio P2M) es un servicio de transporte en el que el tráfico se transmite entre varias interfaces de servicio de acuerdo con una topología de árbol. Para cada interfaz de servicio agregada al servicio P2M, debe asignar una de las siguientes funciones:
    - **Raíz** significa que la interfaz de servicio puede enviar tráfico a las interfaces de servicio con cualquier función.
    - **Hoja** significa que la interfaz de servicio puede enviar tráfico solo a las interfaces de servicio con la función **Raíz**.
  - Multipunto a multipunto (E-LAN en la clasificación MEF, en adelante también denominado servicio M2M) es un servicio de transporte en el que el tráfico se transmite entre varias interfaces de servicio sin una jerarquía.

  El servicio P2P es un servicio de transporte estático y no utiliza el mecanismo de aprendizaje MAC para completar la tabla MAC en el Controlador. Las direcciones MAC se agregan automáticamente a la tabla MAC en el controlador cuando un servicio P2P se crea o se modifica. El mecanismo de aprendizaje de las direcciones MAC se utiliza para los servicios P2M y los servicios M2M.
- La multidifusión de IP (en adelante también denominada servicio de multidifusión de IP) es un servicio de transporte en el que se crea un árbol de multidifusión para la distribución del tráfico entre varias interfaces de servicio.
- La VPN L3 (en adelante también denominada servicio de VPN L3) es un servicio de transporte en el que el tráfico se enruta entre varias interfaces L3, que se asignan a las interfaces de servicio o los servicios M2M.

Cuando se crean o editan servicios de transporte, puede agregar interfaces de servicio de respaldo. Una interfaz de servicio de respaldo permite continuar con la transferencia de datos en caso de una falla en la interfaz de servicio principal. Las interfaces de servicio principal y de respaldo se pueden crear en el mismo dispositivo CPE o en diferentes dispositivos CPE.

El tráfico se puede duplicar o reenviar entre las interfaces de servicio de los dispositivos CPE. En este caso, las interfaces de servicio se pueden agregar al servicio de transporte.

### Administrar los servicios de transporte en una plantilla de instancia SD-WAN o en una plantilla de CPE

Puede crear servicios P2M y servicios M2M así como servicios de VPN L3 en una plantilla de instancia SD-WAN y, luego, utilizarla cuando se implemente una plantilla de SD-WAN. Los servicios de transporte creados en la plantilla de instancia SD-WAN se crean automáticamente para la instancia SD-WAN implementada. De esta manera, puede crear servicios de transporte antes de implementar la instancia SD-WAN.

Los servicios de transporte creados para una instancia SD-WAN implementada se pueden agregar a una plantilla de CPE y, luego, puede especificar la plantilla cuando se agreguen o se registren manualmente los dispositivos CPE. Esto crea automáticamente las interfaces de servicio que se asignan a los puertos OpenFlow, que se asignan a las interfaces de SD-WAN del tipo LAN de los dispositivos CPE. Las interfaces de servicio creadas automáticamente se agregan a los servicios de transporte que agregó a la plantilla de CPE. De esta manera, no es necesario que conecte manualmente cada dispositivo CPE a los servicios de transporte.

### Servicio de transporte de administración

Cuando se registra un dispositivo CPE, se conecta automáticamente a un servicio de transporte de administración. El servicio de transporte de administración transmite el tráfico de la consola SSH, ejecuta scripts y envía los comandos de la API para administrar el VIM implementado en un dispositivo uCPE.

De manera predeterminada, se crea un servicio de transporte de administración P2M en cada plantilla de instancia SD-WAN. Cuando se crea o se edita un servicio P2M o un servicio M2M en la plantilla de instancia SD-WAN, puede establecer ese servicio P2M o servicio M2M como el servicio de administración.

Si es necesario, el tráfico de supervisión de Zabbix, así como el tráfico de protocolo syslog y NetFlow, se puede transmitir mediante el servicio de transporte de administración. El tráfico de supervisión de Zabbix está cifrado de manera predeterminada, pero para cifrar el tráfico de syslog y NetFlow, dicho tráfico debe transmitirse a través del servicio de transporte de administración. La transmisión del tráfico de syslog y NetFlow a través del servicio de transporte de administración se rige por la configuración de la tabla de enrutamiento y reenvío del dispositivo CPE.

## Duplicación de paquetes de tráfico

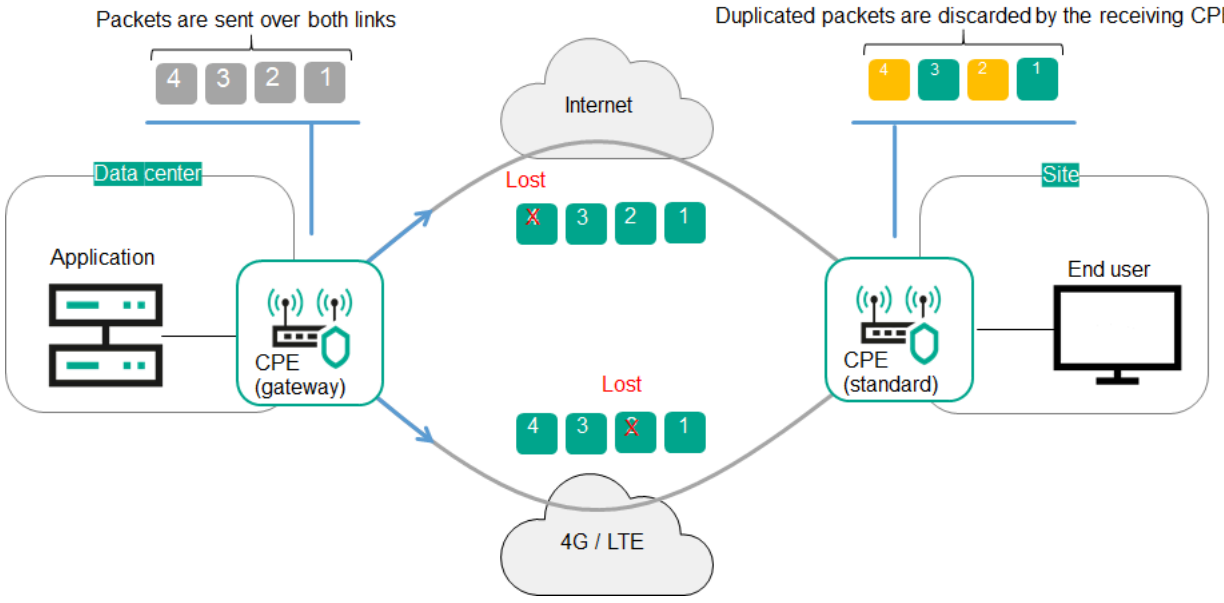
Puede habilitar la duplicación de paquetes de tráfico para evitar pérdidas al transmitir paquetes de tráfico mediante los siguientes servicios de transporte:

- Servicios de P2P
- Servicios de P2M
- Servicios de M2M
- Servicios de VPN L3
- Servicios de TAP

Si la duplicación de paquetes de tráfico está habilitada para un servicio de transporte, el dispositivo CPE de origen duplica los paquetes de tráfico y los envía a través de todas las conexiones. El dispositivo CPE de destino recibe los paquetes de tráfico y descarta los paquetes de tráfico superfluos. Si un paquete de tráfico enviado a través de una conexión se pierde, el dispositivo CPE de destino puede recibir ese paquete de tráfico a través de una conexión diferente. La duplicación de paquetes de tráfico se puede utilizar para aplicaciones que tienen una gran demanda, como cajeros automáticos y terminales POS.

Para habilitar la duplicación de paquetes de tráfico, seleccione **Transmisión** en la lista desplegable **Modo de equilibrio** al crear o editar un servicio de transporte.

Por ejemplo, la siguiente figura muestra un dispositivo CPE con la función de puerta de enlace en un centro de datos; este dispositivo CPE utiliza dos conexiones para enviar paquetes de tráfico a un dispositivo CPE estándar en una ubicación remota. El dispositivo CPE estándar en la ubicación remota luego transmite los paquetes de tráfico a los usuarios finales. Ambos dispositivos CPE se agregan a un servicio de transporte que tiene habilitada la duplicación de paquetes de tráfico, lo que significa que los paquetes de tráfico se duplican y se transmiten de manera simultánea a través de dos conexiones.




Duplicación de paquetes de tráfico entre dispositivos CPE

# Escenario: dirigir el tráfico de la aplicación a un servicio de transporte

El escenario para dirigir el tráfico de la aplicación a un servicio de transporte implica los siguientes pasos:

1. **Crear un servicio de transporte**

   Cree un servicio de transporte al que desee dirigir el tráfico de la aplicación. Puede usar las siguientes instrucciones para completar este paso:

   - Crear un servicio P2P
   - Crear un servicio P2M
   - Crear un servicio M2M
   - Crear un servicio de multidifusión IP
   - Crear un servicio VPN L3

2. **Crear una regla de clasificación de tráfico**

   Cree una regla de clasificación de tráfico para identificar el tráfico de la aplicación en el flujo de datos general. Cuando crea una regla de clasificación de tráfico, debe seleccionar el protocolo L3 en la pestaña **Campos L3** y seleccionar la aplicación cuyo tráfico desea dirigir al servicio de transporte en la pestaña **DPI**.

   Si desea dirigir el tráfico de varias aplicaciones a un servicio de transporte, debe crear una regla de clasificación de tráfico para cada aplicación.

3. **Crear un filtro de tráfico**

   Cree un filtro de tráfico para determinar si se permite el enrutamiento del tráfico de la aplicación. Cuando crea un filtro de tráfico, debe agregar las reglas de clasificación de tráfico que creó para el tráfico de la aplicación al filtro de tráfico.

4. **Crear una interfaz de ACL**

   Cree una interfaz de ACL para aplicar el filtro de tráfico al tráfico que se transmite a través de esta interfaz de ACL. Cuando crea una interfaz de ACL, debe seleccionar un filtro de tráfico que creó para el tráfico de la aplicación.

5. **Agregar la interfaz de ACL al servicio de transporte**

   Edite el servicio de transporte para agregar la interfaz de ACL que creó para el tráfico de la aplicación. Puede usar las siguientes instrucciones para completar este paso:

   - Editar un servicio P2P
   - Editar un servicio P2M
   - Editar un servicio M2M
   - Editar un servicio de multidifusión IP
   - Editar un servicio de VPN L3

El tráfico de la aplicación se dirige al servicio de transporte.

# Escenario: establecer la conexión L2 entre dispositivos CPE

Puede establecer una conectividad L2 entre los dispositivos CPE para los siguientes propósitos:

- Crear un dominio L2 que incluya varias ubicaciones remotas.
- Transmitir tráfico L2 para vínculos keepalive entre los dispositivos CPE instalados en diferentes ubicaciones remotas.
- Implementar escenarios de duplicación de tráfico personalizados.

El escenario para establecer la conectividad L2 entre dispositivos CPE implica los siguientes pasos:

1. **Crear puertos de OpenFlow en los conmutadores virtuales de los dispositivos CPE**

1. Cuando crea o edita una interfaz de red sin una dirección IP en los dispositivos CPE entre los que desea establecer una conectividad L2, seleccione la casilla de verificación **Modo L2**. Cuando se selecciona la casilla, se crea automáticamente un puerto de OpenFlow asignado a la interfaz de red en el conmutador virtual del dispositivo CPE. Esta casilla está desactivada por defecto. No puede seleccionar esta casilla en los siguientes casos:

   - Seleccionó las siguientes casillas durante la creación de una interfaz de red:
     - **Puente**
     - **NetFlow**
     - **Forzar dirección IP, ruta y gateway**
   - La interfaz de red se utiliza en una ruta estática.
   - BGP utiliza la interfaz de red.
   - El protocolo OSPF utiliza la interfaz de red.
   - El protocolo VRRP utiliza la interfaz de red.
   - La interfaz de red se utiliza para transmitir tráfico de multidifusión.
   - Una tabla de enrutamiento y reenvío virtuales (VRF) utiliza la interfaz de red.
   - La interfaz de red se utiliza para el diagnóstico de dispositivos CPE mediante la utilidad ping, traceroute, tcpdump o sweep.

   El número del puerto de OpenFlow creado automáticamente en el conmutador virtual del dispositivo CPE se muestra en el campo **Puerto OpenFlow**. Puede cambiar el número de puerto de OpenFlow. Rango de valores: de 11 a 20.

2. **Crear interfaces de servicio asignadas a puertos de OpenFlow**

   Cree interfaces de servicio asignadas a puertos de OpenFlow que se crearon automáticamente en el paso anterior de este escenario. Debe seleccionar el puerto de OpenFlow al que está asignada la interfaz de servicio en la lista desplegable **Puerto**.

3. **Agregar interfaces de servicio al servicio de transporte**

   Agregue las interfaces de servicio que creó en el paso anterior de este escenario al servicio de transporte que desea usar para establecer la conexión L2 entre los dispositivos CPE. Puede usar las siguientes instrucciones para completar este paso:

   - Crear un servicio P2P y Editar un servicio P2P.
   - Crear un servicio P2M y Editar un servicio P2M.
   - Crear un servicio M2M y Editar un servicio M2M.
   - Crear un servicio VPN L3 y Editar un servicio VPN L3.

- Crear un servicio de multidifusión IP y Editar un servicio de multidifusión IP.
- Crear un servicio TAP y Editar un servicio TAP.

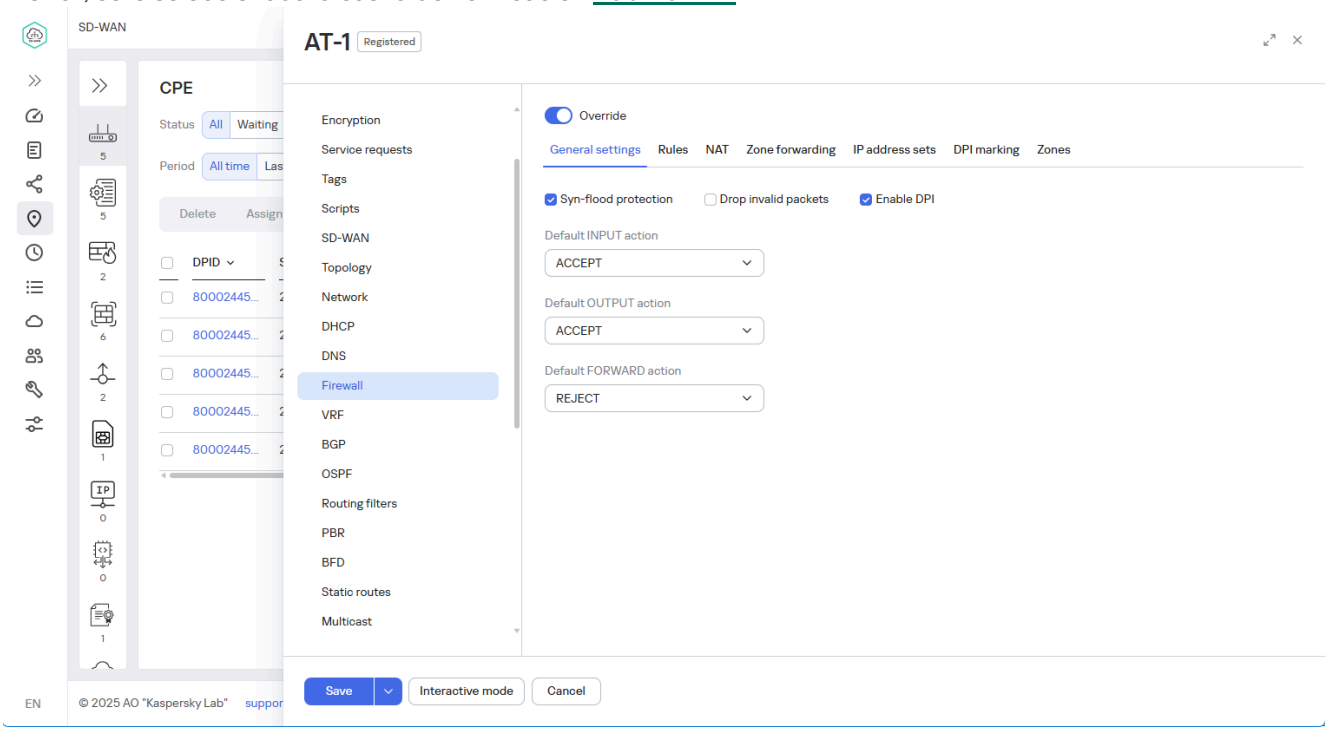
Se establece la conectividad L2 entre dispositivos CPE.

# Escenario: administración del tráfico de aplicaciones de acuerdo con un SLA

El escenario para gestionar la administración del tráfico de aplicaciones de acuerdo con un SLA implica los siguientes pasos:

1. **Habilitación de la DPI (Inspección profunda de paquete) globalmente en la configuración del firewall**

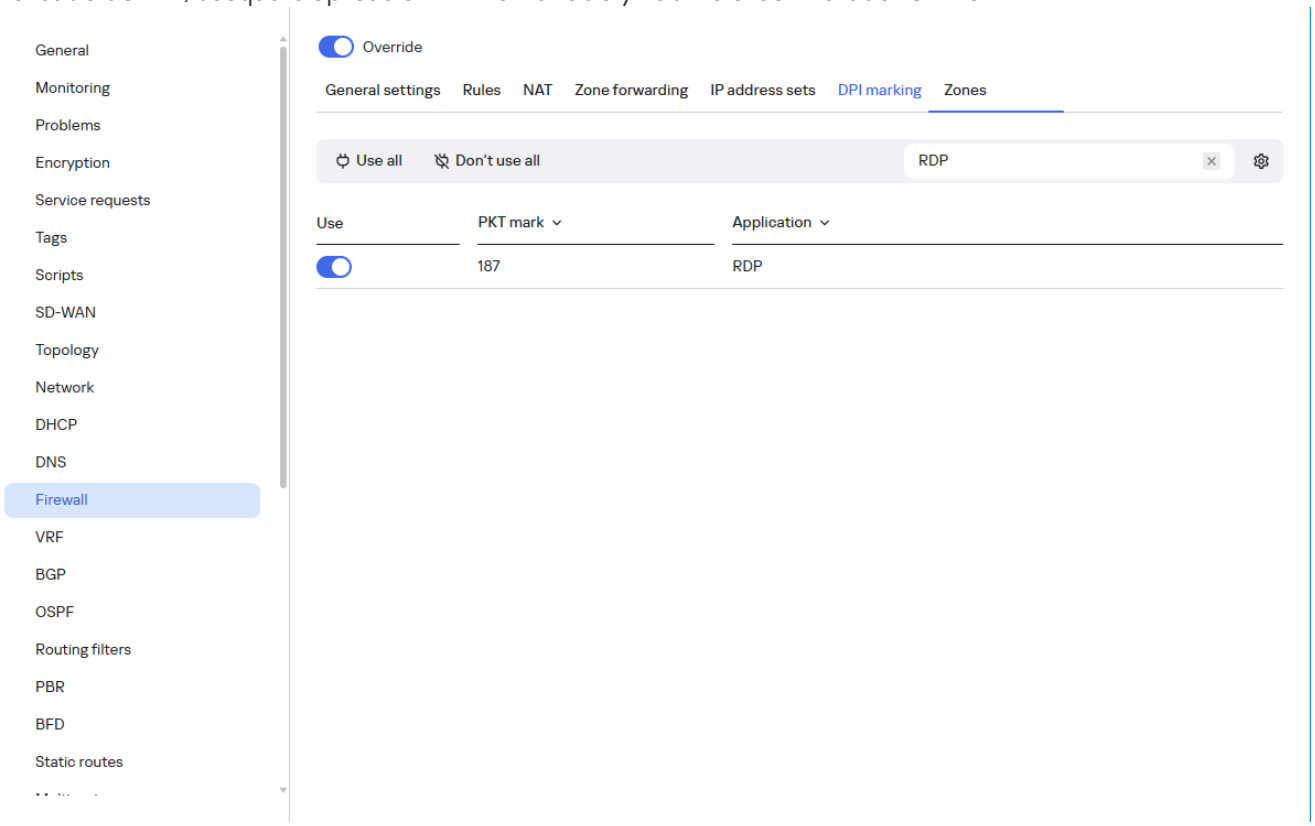
   Asegúrese de que en el área de **configuración principal del firewall** del dispositivo CPE o de la plantilla del firewall, esté seleccionada la casilla de verificación Habilitar DPI:




Ventana de configuración de CPE. Habilitación de la funcionalidad de DPI.

2. **Habilitación del reconocimiento de aplicaciones mediante DPI para RDP**

En el área de configuración del firewall del dispositivo CPE o de la plantilla del firewall, seleccione la pestaña **Marcado de DPI**, busque la aplicación **RDP** en la tabla y habilite el conmutador **Utilizar**:

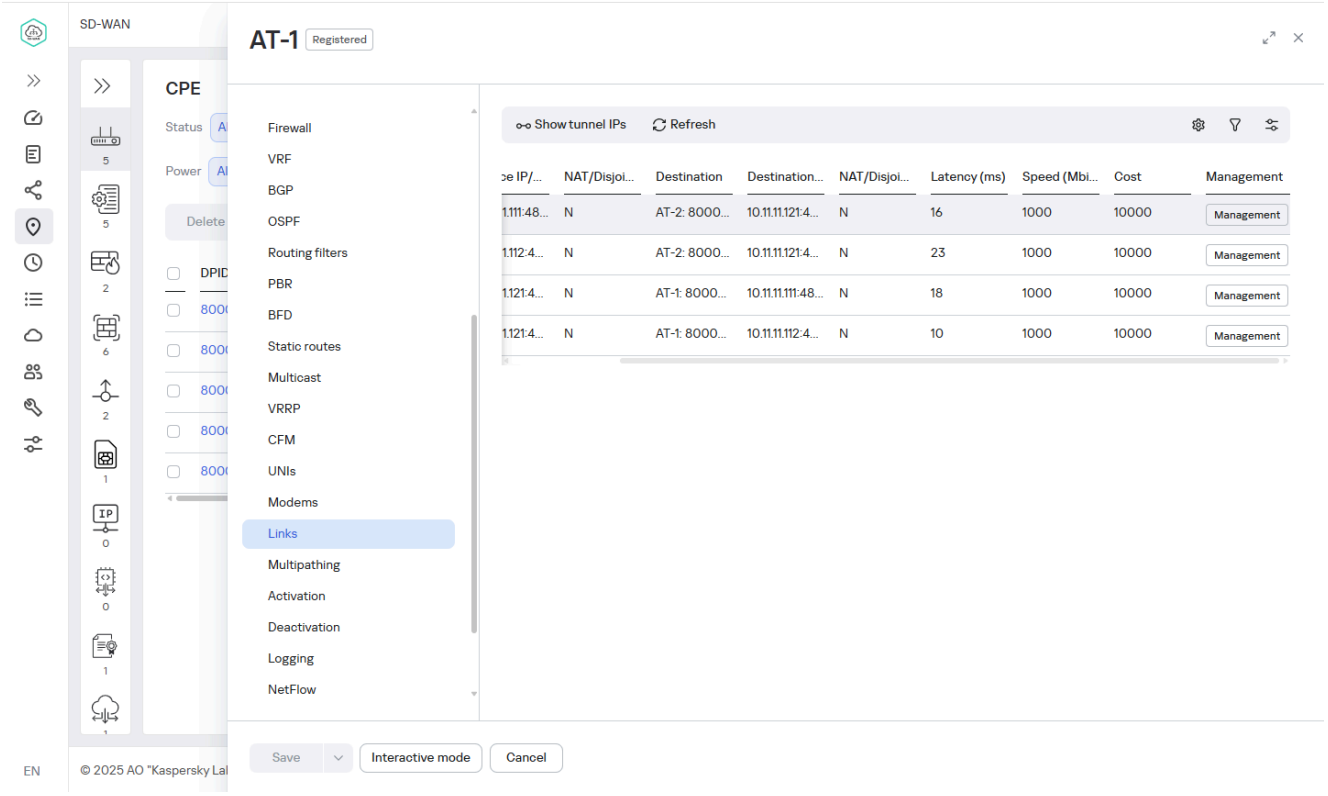



Habilitación de la DPI para el reconocimiento de RDP

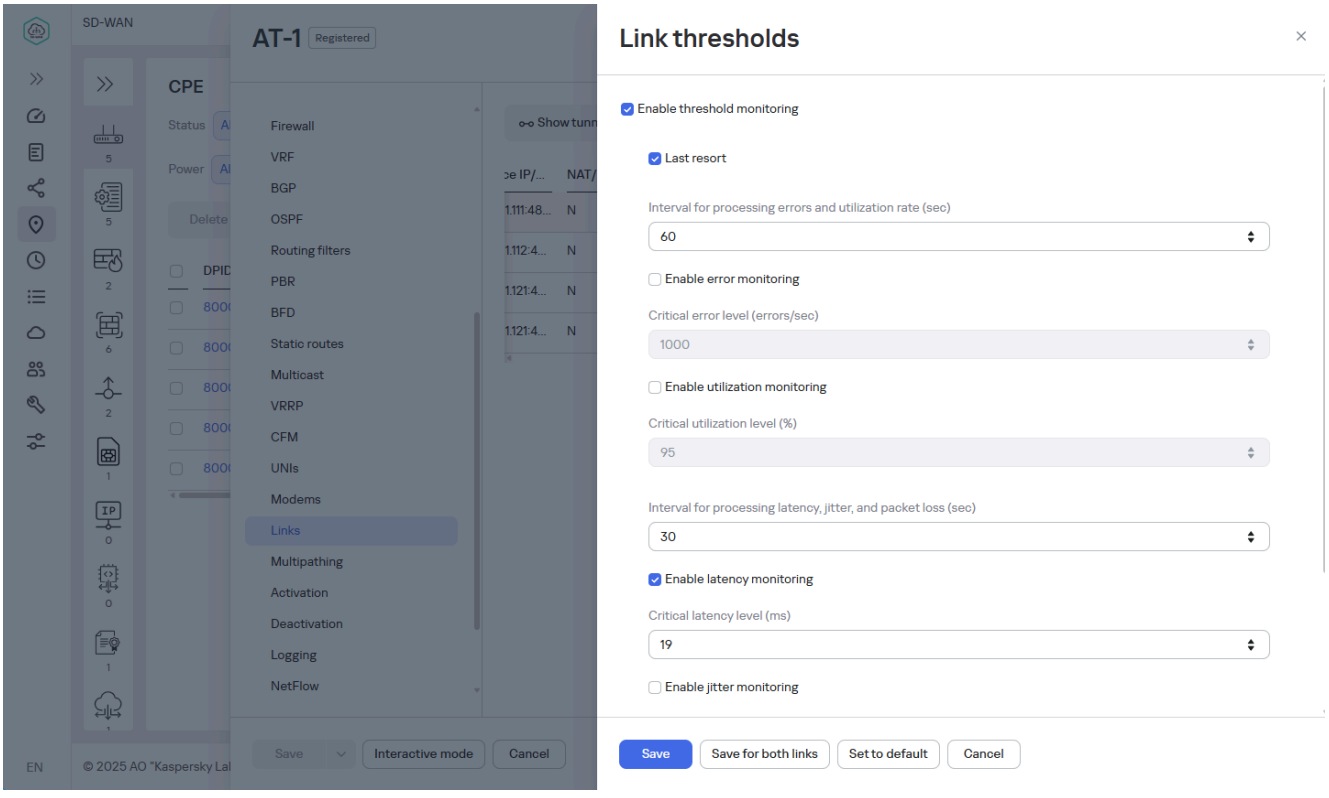
Para obtener más información sobre la configuración de la DPI, consulte Configuración del marcado de DPI.

3. **Habilitación de la supervisión del tráfico en los vínculos del CPE**

   Siga las instrucciones de Supervisión de vínculos para habilitar la supervisión del umbral en el vínculo relevante del dispositivo CPE, seleccione la casilla de verificación Último recurso y, para la configuración Nivel de latencia crítico (ms), especifique un valor ligeramente mayor que la latencia en el vínculo seleccionado:



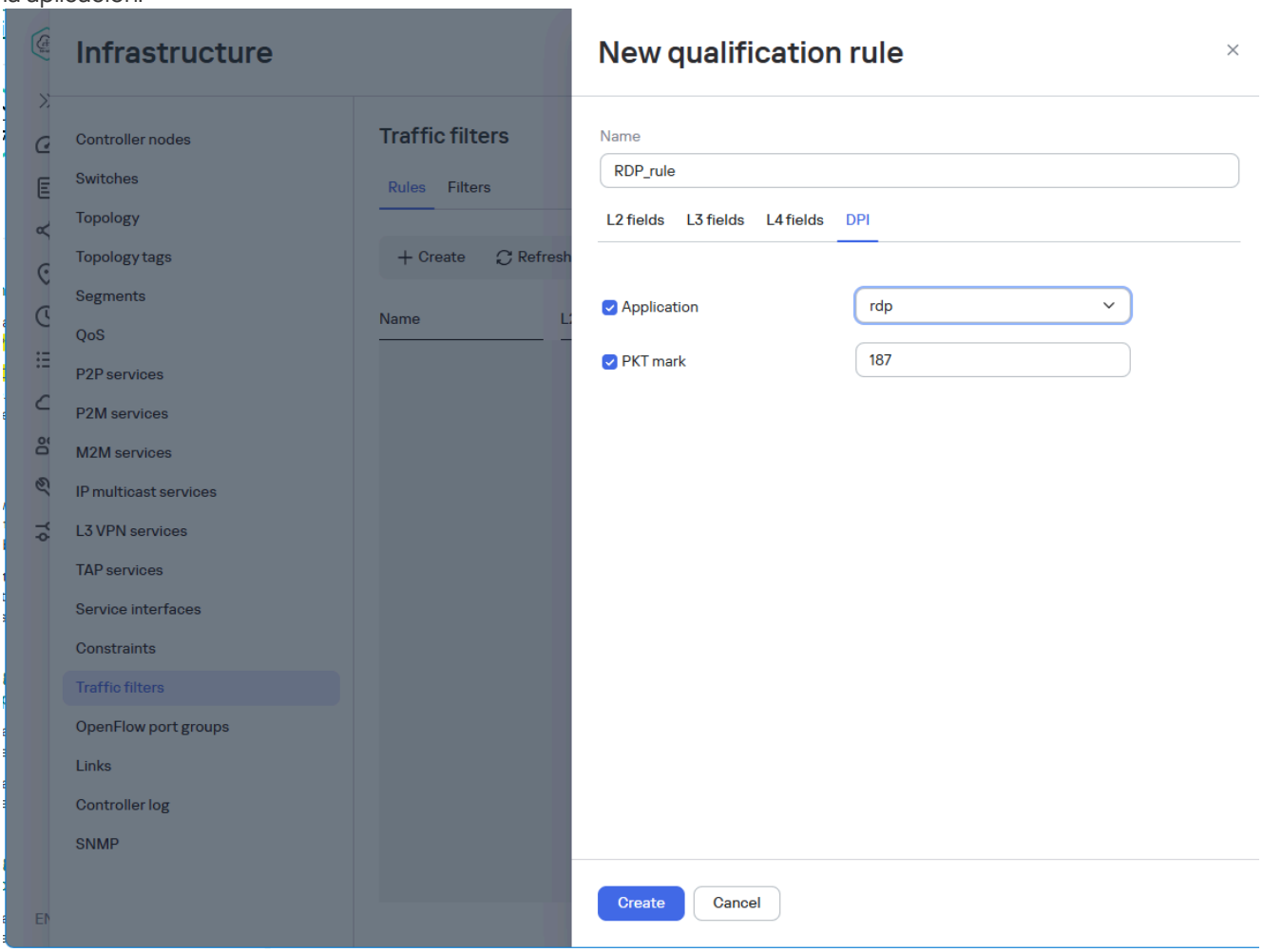

Procedimiento para crear umbrales en el vínculo de un dispositivo CPE




Habilitación de la supervisión de demoras y establecimiento de un nivel de latencia crítico

4. **Creación de una regla de clasificación de tráfico de aplicaciones**

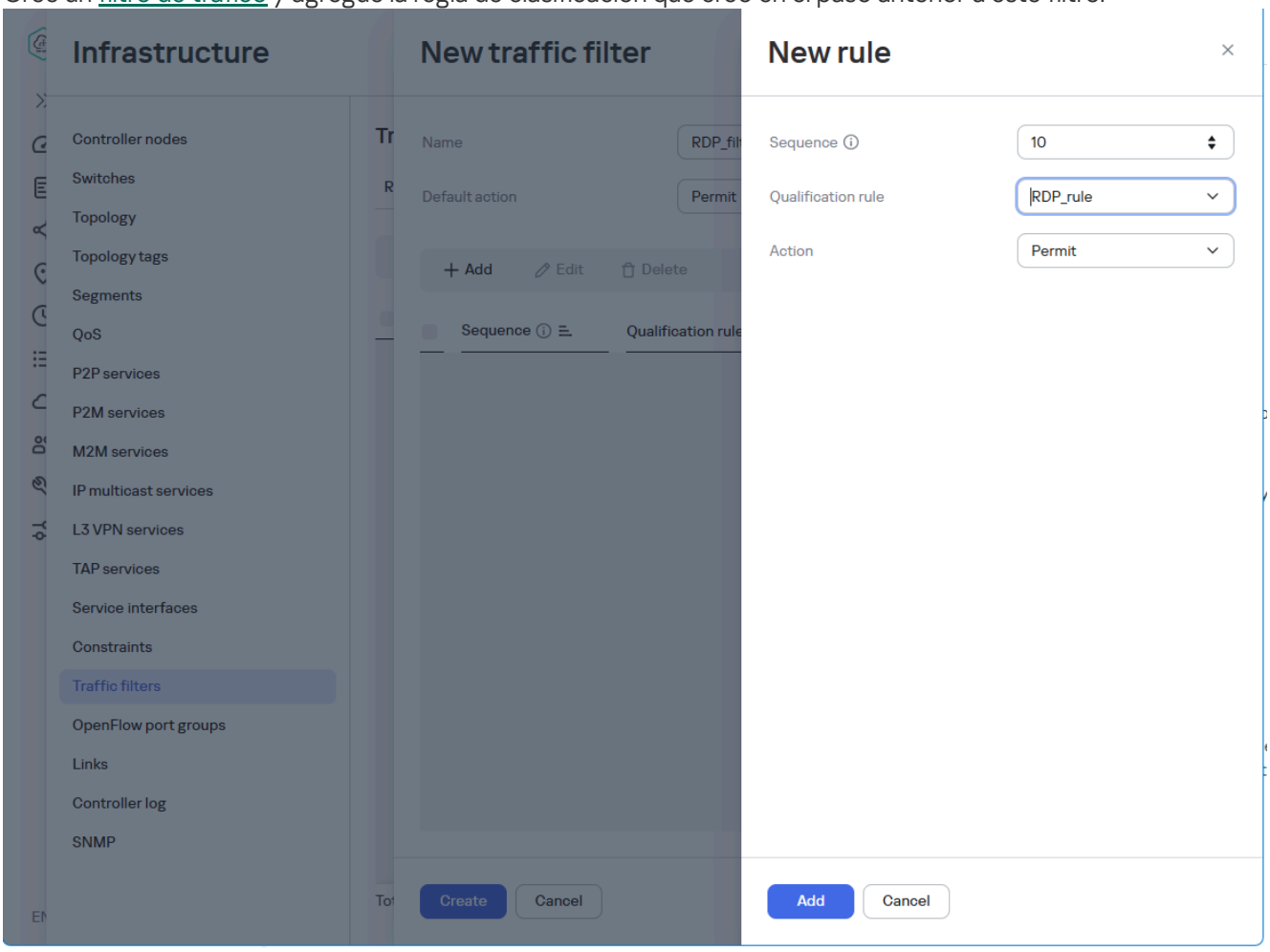
Para crear una regla de clasificación de tráfico, en la pestaña **DPI**, especifique el valor **dpi** para la clasificación de la aplicación:




Creación de una regla de clasificación de tráfico para la aplicación RDP

### 5 Creación de un filtro para identificar el tráfico de la aplicación

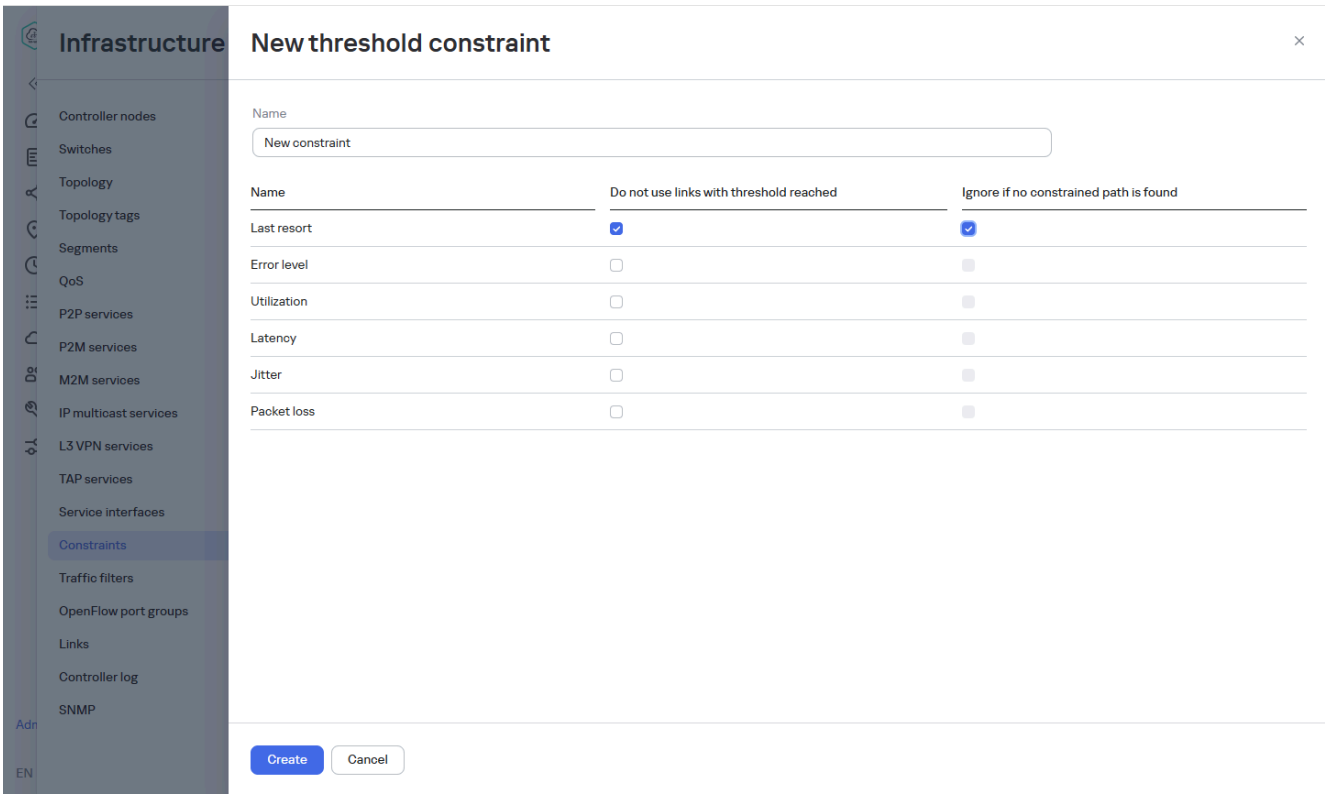
Cree un filtro de tráfico y agregue la regla de clasificación que creó en el paso anterior a este filtro:




Crear un filtro de tráfico

### 6 Creación de restricciones de umbral

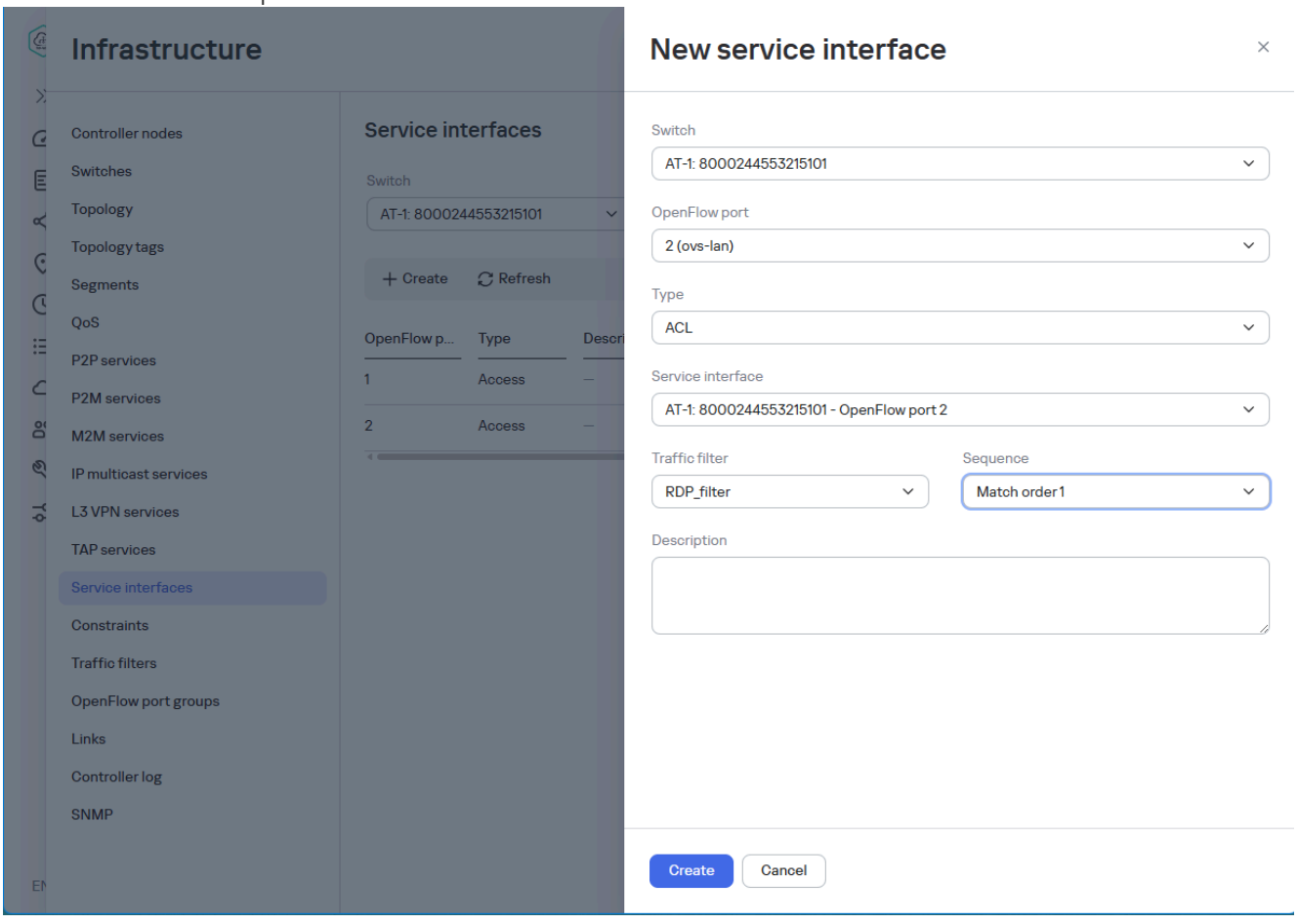
Cree una restricción de umbral para el controlador, seleccione **Último recurso** como el indicador de supervisión y seleccione las casillas de verificación **No utilice vínculos si se alcanzó el umbral** y **Ignorar si no se encontró una ruta restringida**:




Creación de un umbral con el indicador de supervisión "Último recurso"

### 7 Creación de interfaces de servicio ACL

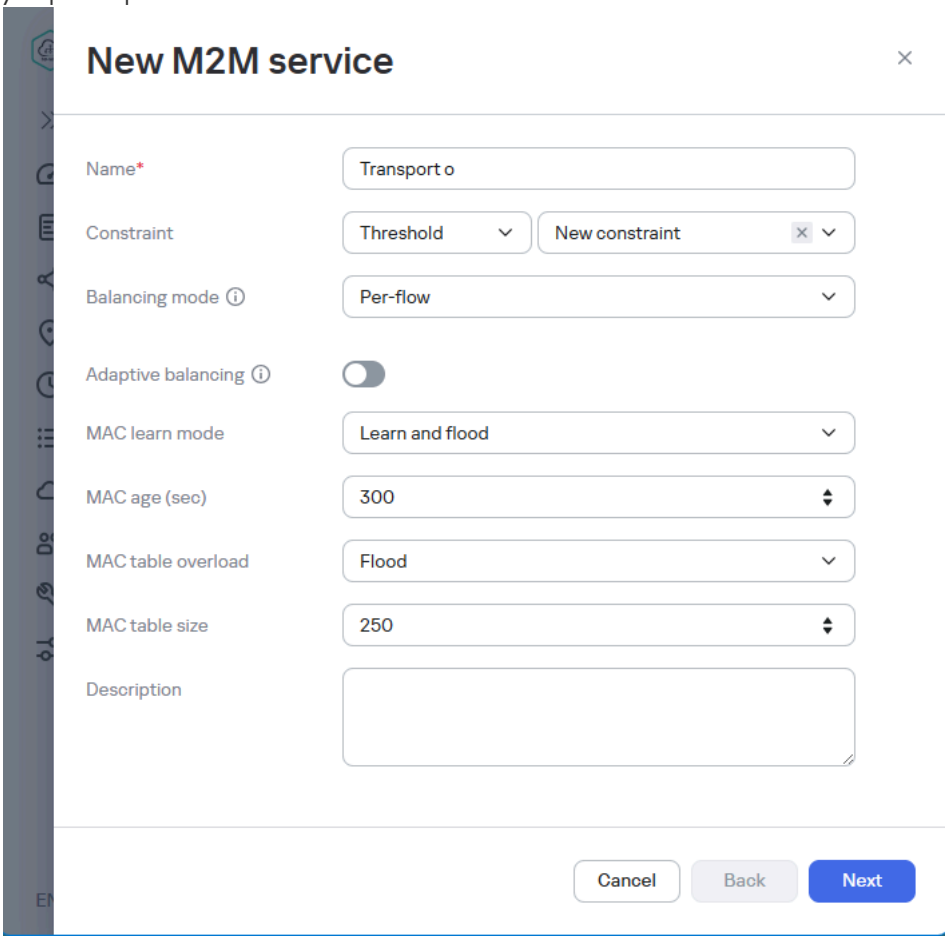
Cree interfaces de servicio del tipo ACL para el dispositivo CPE con el rol de puerta de enlace y el dispositivo CPE estándar. Cuando cree las interfaces, especifique la interfaz de servicio del servicio M2M principal y el filtro creado anteriormente para el tráfico RDP:




Adición de una interfaz de ACL con el filtro de tráfico creado anteriormente

8 **Creación de un servicio M2M independiente**

Cree un servicio M2M que solo reciba tráfico RDP. Incluya en este servicio solo las interfaces de ACL creadas en el paso anterior y especifique la restricción de umbral "Nueva restricción" creada anteriormente:




Adición de un servicio M2M con una restricción de umbral

El tráfico RDP ahora termina en el nuevo servicio M2M. El resto del tráfico se dirige a la interfaz de servicio principal para distribuirse entre los vínculos disponibles.

# Administrar servicios de transporte punto a punto (P2P)

Para ver la tabla de servicios P2P, vaya a la sección del menú **Infraestructura**, haga clic en **Administración**→ **Configuración de implementación**al lado del controlador y vaya a la sección **Servicios de P2P**. La información sobre los servicios P2P se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio P2P.
- **Origen** contiene información sobre la interfaz de servicio de origen del servicio P2P:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio
- **Destino** contiene información sobre la interfaz del servicio de destino del servicio P2P:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio

- **QoS** es la regla de calidad de servicio especificada para la interfaz de servicio de origen del servicio P2P.
- **Interfaz de servicio de respaldo** contiene información sobre la interfaz del servicio de respaldo del servicio P2P:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio
- **Estado**es el estado del servicio P2P:
  - **Arriba**
  - **Abajo**

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un servicio P2P

*Para crear un servicio P2P, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

   Se muestra una tabla de servicios P2P.

4. En la parte superior de la página, haga clic en **+ Servicio de P2P**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio P2P.

6. En la lista desplegable **Restricción**, seleccione la restricción de Manual-TE o la restricción de umbral que desea agregar al servicio P2P.

7. En la lista desplegable **Modo de equilibrio**, seleccione el modo de equilibrio para la distribución del tráfico entre los vínculos:
   - **Por flujo** significa que los flujos de tráfico (5 tuplas) se distribuyen entre los vínculos de acuerdo con el costo del vínculo. Esta es la configuración predeterminada.
   - **Por paquete** significa que los paquetes de tráfico se distribuyen entre los vínculos de acuerdo con el costo del vínculo.
   - **Transmisión** significa que los paquetes de tráfico se duplican y se transmiten en simultáneo a través de todos los vínculos para evitar pérdidas.

Puede especificar el costo del vínculo de forma manual.

8. Opcionalmente, configure el modo de equilibrio adaptativo si desea que el peso de la ruta se ajuste de manera dinámica según el nivel de pérdida de los paquetes de la ruta:

   a. Active el conmutador **Equilibrio adaptado**.

   b. En el campo **Tasa de pérdida mínima (%)**, especifique el porcentaje mínimo de pérdida de los paquetes en la ruta en la que comienza el equilibrio adaptativo para ajustar el peso. Rango de valores: 0.01 a 100.

   c. En el campo **Tasa de pérdida máxima (%)**, especifique el porcentaje máximo de pérdida de los paquetes en el que la ruta se excluye del equilibrio de carga.

   d. En la lista desplegable **Velocidad de convergencia**, seleccione la tasa de convergencia de los pesos adaptativos a los valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0.75
      - **Rápido**: 0.5

9. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del servicio P2P.

10. En las listas desplegables **Conmutador** y **Interfaz del servicio** de la izquierda, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de origen del servicio P2P.

11. En las listas desplegables **Conmutador** y **Interfaz del servicio** a la derecha, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de destino del servicio P2P.

12. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en las listas desplegables **Interfaz del servicio**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

13. Si desea intercambiar los valores seleccionados en las listas desplegables **Interfaz del servicio**, seleccione la casilla **Interfaces del conmutador**. Esta casilla está desactivada por defecto.

14. Si desea agregar una interfaz de servicio de reserva del origen del servicio P2P a través de la cual se transmite el tráfico si falla la interfaz de servicio principal:

    a. Seleccione la casilla **Utilizar interfaz de respaldo**. Esta casilla está desactivada por defecto.

    b. En las listas desplegables **Conmutador de respaldo** y **Interfaz de servicio de respaldo**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de reserva.

    c. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en la lista desplegable **Interfaz de servicio de respaldo**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

       Si la interfaz del servicio de origen principal del servicio P2P vuelve a funcionar, el servicio P2P sigue utilizando la interfaz del servicio de origen de respaldo.

15. En las listas desplegables **Filtro entrante** a la izquierda y a la derecha, seleccione el filtro de tráfico creado para las interfaces de origen y destino del servicio P2P.

16. En la lista desplegable **QoS**, seleccione la regla de calidad de servicio creada para la interfaz de servicio del origen del servicio P2P.

17. Si desea rastrear el estado de las interfaces de servicio de origen y destino del servicio P2P y, cuando falla una de las interfaces, deshabilitar automáticamente la otra, seleccione la casilla **Propagar estado de la interfaz**. Esta casilla está desactivada por defecto. Esta casilla no se puede seleccionar cuando la casilla **Utilizar interfaz de respaldo** está seleccionada.

    Cuando la interfaz de servicio que se deshabilitó por primera vez vuelve a estar en línea, la segunda interfaz de servicio que se deshabilitó automáticamente también reanuda su funcionamiento. Esta funcionalidad solo funciona en interfaces de servicio con clasificación de tráfico de acceso. Puede seleccionar el tipo de clasificación de tráfico cuando crea una interfaz de servicio.

18. Haga clic en **Crear**.

El servicio P2P se crea y se muestra en la tabla.

# Ver estadísticas de un servicio P2P

*Para ver las estadísticas de un servicio P2P, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

    Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

    Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

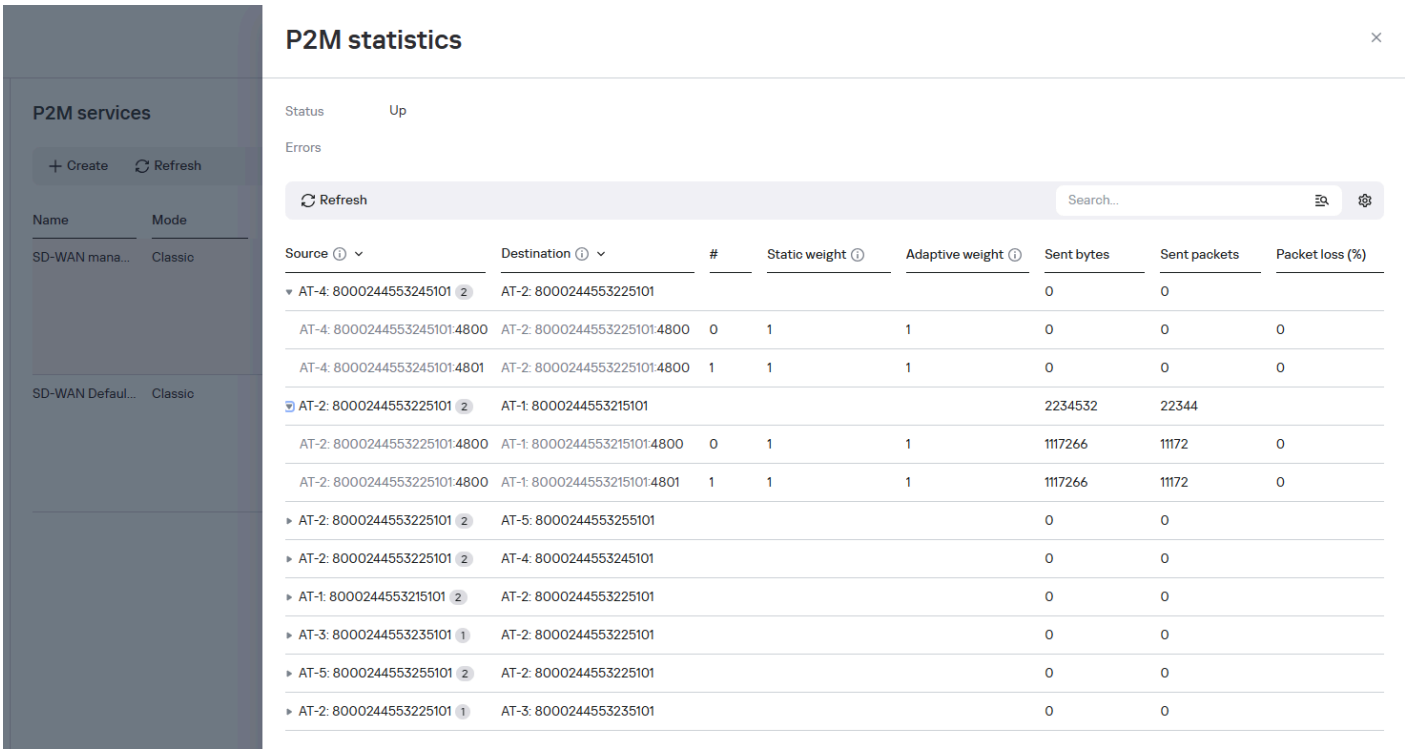
    Se muestra una tabla de servicios P2P.

4. Haga clic en **Administración** → **Estadísticas** junto al servicio P2P cuyas estadísticas desea ver.

Se abre una ventana con las estadísticas del servicio P2P.

En la parte superior de la ventana de estadísticas, el campo **Estado** muestra el estado operativo del servicio. El campo **Errores** muestra los posibles errores que pueden ocurrir para el servicio.

Las estadísticas de los segmentos, las rutas y los vínculos del servicio se muestran jerárquicamente en una tabla. Las filas de la tabla están agrupadas por segmento. Las filas dentro de cada grupo contienen estadísticas para las rutas incluidas en el segmento correspondiente. Para expandir un grupo, haga clic en el triángulo (▸). Para los servicios que no tienen límites establecidos, las filas muestran todas las rutas con el equilibrio de carga habilitado en el segmento. Para los servicios con límites, las filas muestran las rutas de Auto-TE que cumplen el límite.




Visualización de estadísticas, usando un servicio P2M como ejemplo

La información estadística detallada sobre los segmentos y las rutas se muestra en las siguientes columnas de la tabla:

**Origen**: para filas agregadas, el host de origen del segmento; para filas en grupos expandibles, el host de origen de la ruta en el segmento.

**Destino**: para filas agregadas, el host de destino del segmento; para filas en grupos expandibles, el host de destino de la ruta en el segmento.

**#** es el número secuencial de la ruta. Cuanto menor sea el número de la ruta, antes se construyó. Este valor se muestra solo para filas en grupos expandibles.

**Peso estático** es el peso de la ruta estática en función del costo. Este valor se muestra solo para filas en grupos expandibles.

**Peso adaptado** es el peso dinámico de la ruta basado en el análisis de la pérdida de paquetes en esta ruta. Este valor se muestra solo para filas en grupos expandibles. Si no se utiliza el equilibrio adaptativo, esta columna no se muestra.

**Bytes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de bytes enviados al depósito del grupo OF.

**Paquetes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de paquetes enviados al depósito del grupo OF.

**Pérdida de paquetes (%)** es el porcentaje de pérdida de paquetes en una ruta determinada (la relación entre el número de paquetes perdidos y el número total de paquetes enviados). Este valor se muestra solo para filas en grupos expandibles.

# Ver y configurar la visualización de la topología de un servicio P2P

*Para ver y configurar la visualización de una topología de servicio P2P, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

   Se muestra una tabla de servicios P2P.

4. Haga clic en **Administración** → **Topología del servicio** junto al servicio P2P cuya topología desea ver.

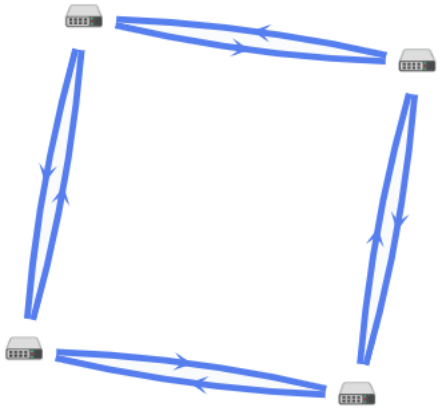
   Se abre una ventana con la topología del servicio P2P.

5. Si necesita mover dispositivos CPE, realice una de las siguientes acciones:

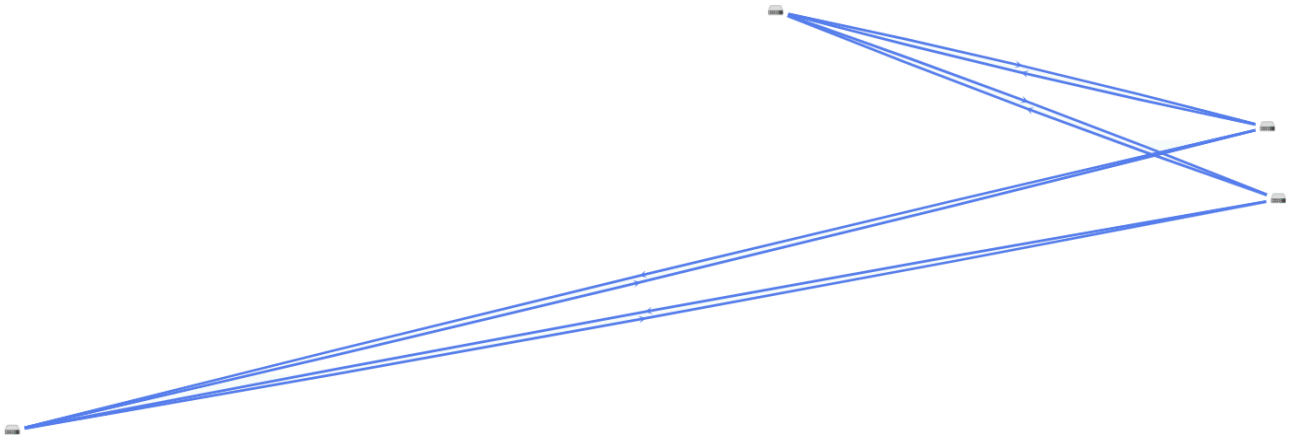
   - Si desea cambiar manualmente la posición de los dispositivos CPE, haga clic en **Manual** y ajuste la posición de los dispositivos CPE.

   - Si desea organizar automáticamente los dispositivos CPE, haga clic en **Automáticamente** y seleccione uno de los siguientes valores de la lista desplegable que se muestra:

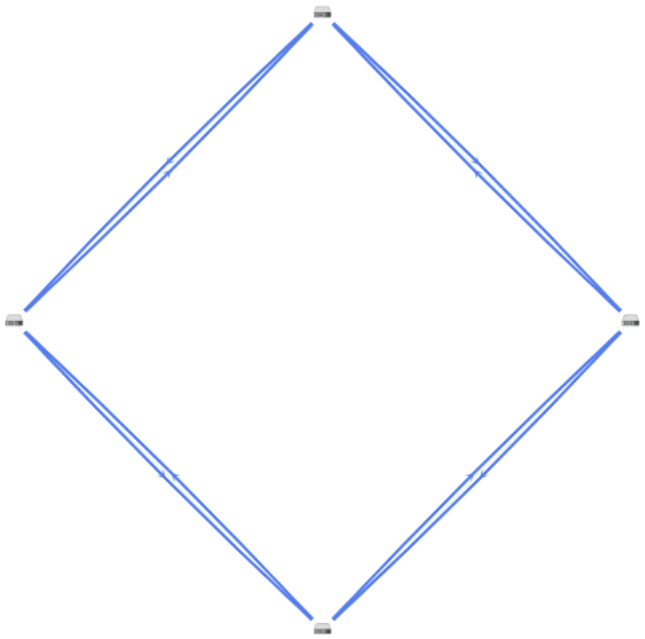
     - **Simulación física**: los dispositivos CPE se disponen aproximadamente de acuerdo con su ubicación real entre sí, por ejemplo:

- **Aleatorio**: la disposición de los dispositivos CPE es aleatoria, por ejemplo:



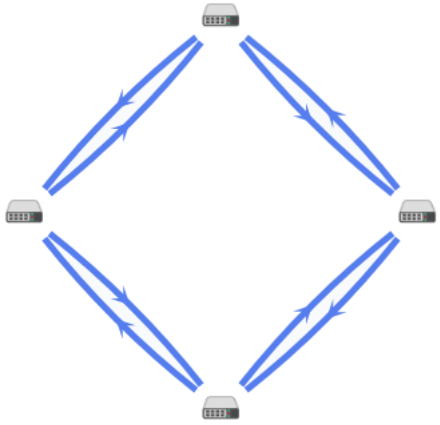
- **Círculo**: los dispositivos CPE se organizan de acuerdo con una topología en anillo, por ejemplo:



- **Búsqueda en anchura**: los dispositivos CPE están dispuestos horizontalmente, por ejemplo:



- **Concéntrico**: los dispositivos CPE están dispuestos de forma concéntrica, por ejemplo:



- **Cuadrícula**: los dispositivos CPE se organizan de acuerdo con una topología de cuadrícula, por ejemplo:

6. Si desea mostrar información sobre los dispositivos CPE, seleccione las siguientes casillas:

   - **Nombre** muestra los nombres de los dispositivos CPE.
   - **Dirección IP** muestra las direcciones IP de los dispositivos CPE.

   Estas casillas de verificación están desactivadas de manera predeterminada.

7. Si desea mostrar un segmento entre dos dispositivos CPE:

   a. Seleccione la casilla **Segmentos**. Esta casilla está desactivada por defecto.

   b. En las listas desplegables que se muestran, seleccione los dispositivos CPE de origen y destino del segmento.

   Se muestra el segmento entre los dispositivos CPE.

# Editar un servicio P2P

*Para editar un servicio P2P, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

   Se muestra una tabla de servicios P2P.

4. Haga clic en **Administración** → **Editar** junto al servicio P2P que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio P2P. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio P2P.

6. Haga clic en **Guardar**.

El servicio P2P se modifica y actualiza en la tabla.

# Reiniciar un servicio P2P

Puede reiniciar un servicio P2P para restaurarlo en caso de mal funcionamiento. Cuando reinicia un servicio P2P, el controlador elimina automáticamente y vuelve a crear las reglas asociadas con este servicio P2P en las tablas de OpenFlow de los dispositivos CPE. Esto afecta a los dispositivos CPE cuyas interfaces de servicio se agregan al servicio P2P.

*Para reiniciar un servicio P2P, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

   Se muestra una tabla de servicios P2P.

4. Haga clic en **Administración** → **Reaprovisionar** junto al servicio P2P que desea reaprovisionar.

5. En la ventana de confirmación, haga clic en **Reaprovisionar**.

Se reiniciará el servicio P2P.

# Eliminar un servicio P2P

Los servicios P2P eliminados no se pueden restaurar

*Para eliminar un servicio P2P, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2P**.

   Se muestra una tabla de servicios P2P.

4. Haga clic en **Administración** → **Eliminar** junto al servicio P2P que desea eliminar.

5. Para eliminar las interfaces de servicio agregadas al servicio P2P, seleccione la casilla **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.

6. Haga clic en **Eliminar**.

El servicio P2P se elimina y ya no se muestra en la tabla.

# Administrar servicios de transporte punto a multipunto (P2M)

Para ver la tabla de servicios P2M, vaya a la sección del menú **Infraestructura**, haga clic en **Administración→ Configuración de implementación** al lado del controlador y vaya a la sección **Servicios de P2M**. La información sobre los servicios P2M se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio P2M.
- **Modo** indica si se utiliza una DFI (interfaz de reenvío predeterminada) en el servicio P2M, al cual se envía tráfico de unidifusión desconocido:
  - **Clásico** si no desea utilizar una DFI. Esta es la configuración predeterminada.
  - **DFI con FIB en la raíz y las hojas** si desea utilizar una DFI en la interfaz de servicio con el rol raíz.
  - **DFI con FIB en la hoja** si desea utilizar una DFI en la interfaz de servicio con el rol raíz. Las interfaces de servicio con el rol de hoja deben crearse en el mismo dispositivo CPE. Las interfaces de servicio de respaldo con el rol de hoja deben crearse en el mismo dispositivo CPE, que debe ser diferente del dispositivo CPE en el que se crean las interfaces de servicio principales.
- **Antigüedad de MAC (s)** es el período en segundos durante el cual las entradas se mantienen en la tabla MAC del controlador.
- **Modo de aprendizaje de MAC** es la acción que se aplica a una serie de marcos cuando el primer marco se envía al controlador para obtener la dirección MAC de origen:
  - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio P2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos.
  - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

  Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.
- **Tamaño de la tabla MAC** es el número máximo de entradas en la tabla MAC del controlador.
- **Sobrecarga en tabla MAC** es la directiva para procesar nuevas direcciones MAC cuando la tabla MAC del controlador está llena:
  - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión).
  - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

- **Endpoints** es la información sobre las interfaces de servicio que se agregaron al servicio P2M:
  - Nombres y DPID de los dispositivos CPE en los que se crearon las interfaces de servicio
  - Números de puertos OpenFlow a los que se asignan las interfaces de servicio
  - Funciones de las interfaces de servicio:
    - **Raíz** significa que la interfaz de servicio puede enviar tráfico a las interfaces de servicio con cualquier función.
    - **Hoja** significa que la interfaz de servicio puede enviar tráfico solo a las interfaces de servicio con la función **Raíz**.
- **Estado** es el estado del servicio P2M:
  - **Arriba**
  - **Abajo**
- **Descripción** es una breve descripción del servicio P2M.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un servicio P2M

*Para crear un servicio P2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. En la parte superior de la página, haga clic en **+ Servicio de P2M**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio P2M.

6. En la lista desplegable **Restricción**, seleccione la restricción de Manual-TE o la restricción de umbral que desea agregar al servicio P2M.

7. En la lista desplegable **Modo de equilibrio**, seleccione el modo de equilibrio para la distribución del tráfico entre los vínculos:

   - **Por flujo** significa que los flujos de tráfico (5 tuplas) se distribuyen entre los vínculos de acuerdo con el costo del vínculo. Esta es la configuración predeterminada.
   - **Por paquete** significa que los paquetes de tráfico se distribuyen entre los vínculos de acuerdo con el costo del vínculo.
   - **Transmisión** significa que los paquetes de tráfico se duplican y se transmiten en simultáneo a través de todos los vínculos para evitar pérdidas.

   Puede especificar el costo del vínculo de forma manual.

8. Opcionalmente, configure el modo de equilibrio adaptativo si desea que el peso de la ruta se ajuste de manera dinámica según el nivel de pérdida de los paquetes de la ruta:

   a. Active el conmutador **Equilibrio adaptado**.

   b. En el campo **Tasa de pérdida mínima (%)**, especifique el porcentaje mínimo de pérdida de los paquetes en la ruta en la que comienza el equilibrio adaptativo para ajustar el peso. Rango de valores: 0.01 a 100.

   c. En el campo **Tasa de pérdida máxima (%)**, especifique el porcentaje máximo de pérdida de los paquetes en el que la ruta se excluye del equilibrio de carga.

   d. En la lista desplegable **Velocidad de convergencia**, seleccione la tasa de convergencia de los pesos adaptativos a los valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0.75
      - **Rápido**: 0.5

9. En la lista desplegable **Modo**, seleccione si el servicio P2M utiliza una DFI (Interfaz de reenvío predeterminada), a la que se envía el tráfico de unidifusión desconocido:

   - **Clásico** si no desea utilizar una DFI. Esta es la configuración predeterminada.
   - **DFI con FIB en la raíz y las hojas** si desea utilizar una DFI en la interfaz de servicio con el rol raíz.
   - **DFI con FIB en la hoja** si desea utilizar una DFI en la interfaz de servicio con el rol raíz. Las interfaces de servicio con el rol de hoja deben crearse en el mismo dispositivo CPE. Las interfaces de servicio de respaldo con el rol de hoja deben crearse en el mismo dispositivo CPE, que debe ser diferente del dispositivo CPE en el que se crean las interfaces de servicio principales.

10. En la lista desplegable **Modo de aprendizaje de MAC**, seleccione la acción que desea aplicar a una serie de marcos cuando el primer marco se envíe al controlador para conocer la dirección MAC de origen:

    - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio P2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos. Esta es la configuración predeterminada.

    - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

    Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

11. En el campo **Antigüedad de MAC (s)**, ingrese el período de tiempo en segundos en el que las entradas se mantienen en la tabla MAC del controlador. Rango de valores: 10 a 65 535. El valor predeterminado es `300`.

12. En la lista desplegable **Sobrecarga en tabla MAC**, seleccione la directiva para el procesamiento de las nuevas direcciones MAC cuando la tabla MAC del controlador esté completa:

    - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.

    - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

13. En el campo **Tamaño de la tabla MAC**, ingrese la cantidad máxima de entradas en la tabla MAC del controlador. Rango de valores: 0 a 65 535. `0` significa que la cantidad de registros en la tabla MAC del controlador no está limitada. El valor predeterminado es `100`.

14. Si es necesario, en el campo **Descripción**, ingrese una breve descripción del servicio P2M.

15. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

16. Agregue la interfaz de servicio al servicio P2M:

    a. Haga clic en **+ Agregar**.

    Se mostrará la configuración de la interfaz de servicio.

    b. En las listas desplegables **Conmutador** y **Interfaz del servicio** a la derecha, seleccione el dispositivo CPE y la interfaz de servicio creada que desea agregar al servicio P2M.

    c. En la lista desplegable **QoS**, seleccione la calidad de la regla de servicio creada para la interfaz de servicio.

    d. En la lista desplegable **Filtro entrante**, seleccione el filtro de tráfico creado para la interfaz de servicio.

    e. En la lista desplegable **Rol**, seleccione la función de la interfaz de servicio:

    - **Raíz** significa que la interfaz de servicio puede enviar tráfico a las interfaces de servicio con cualquier función.

    - **Hoja** significa que la interfaz de servicio puede enviar tráfico solo a las interfaces de servicio con la función **Raíz**.

    - **Interfaz de reenvío raíz predeterminada** significa que la interfaz de servicio puede enviar tráfico a las interfaces de servicio con cualquier función, y la función de DFI se asigna a esta interfaz de servicio.

f. Si desea agregar una interfaz de servicio de respaldo a través de la cual se deba enviar el tráfico cuando falle la interfaz de servicio principal, en las listas desplegables **Conmutador de respaldo** y **Interfaz de servicio de respaldo**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea utilizar como interfaz de servicio de respaldo.

Si la interfaz de servicio principal vuelve a estar en línea, el servicio P2M continúa utilizando la interfaz de servicio de respaldo.

La interfaz de servicio se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias interfaces de servicio o eliminar interfaces de servicio. Para eliminar una interfaz de servicio, haga clic en el ícono de eliminar ✕ junto a ella.

17. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

18. Si desea agregar varias interfaces de red a un servicio P2M al mismo tiempo, debe agregar un grupo de puertos OpenFlow. Para hacerlo, haga lo siguiente:

a. Haga clic en **+ Agregar**.

Se mostrará la configuración del grupo de puertos OpenFlow.

b. En la lista desplegable **Grupo**, seleccione el grupo de puertos OpenFlow creado que desea agregar al servicio P2M. Cuando se guarda la configuración del servicio P2M, se crean las interfaces de servicio automáticamente que se asignan a los puertos OpenFlow en el grupo de puertos OpenFlow, y, luego, estas interfaces de servicio se agregan automáticamente al servicio P2M.

c. En la lista desplegable **QoS**, seleccione la calidad de la regla de servicio creada para las interfaces de servicio automáticamente creadas que se asignaron a los puertos OpenFlow.

d. En el campo **ID de VLAN**, ingrese el valor de la etiqueta de la VLAN exterior para las interfaces de servicio automáticamente creadas que se asignaron a los puertos OpenFlow. Las interfaces de servicio con el tipo de clasificación de tráfico VLAN solo se pueden crear automáticamente. Se asigna la misma etiqueta de la VLAN exterior a cada interfaz de servicio.

e. En la lista desplegable **Rol**, seleccione la función para las interfaces de servicio creadas automáticamente asignadas a los puertos OpenFlow:

- **Raíz** significa que la interfaz de servicio puede enviar tráfico a las interfaces de servicio con cualquier función.
- **Hoja** significa que la interfaz de servicio puede enviar tráfico solo a las interfaces de servicio con la función **Raíz**.

Se agrega el grupo de OpenFlow y se muestra en la parte inferior de la ventana. Puede agregar varios grupos de puertos OpenFlow o eliminar los grupos de puertos OpenFlow. Para eliminar un grupo de puertos OpenFlow, haga clic en el ícono de eliminar ✕ junto a él.

19. Haga clic en **Crear**.

El servicio P2M se crea y se muestra en la tabla.

# Ver estadísticas de un servicio P2M

*Para ver las estadísticas de un servicio P2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

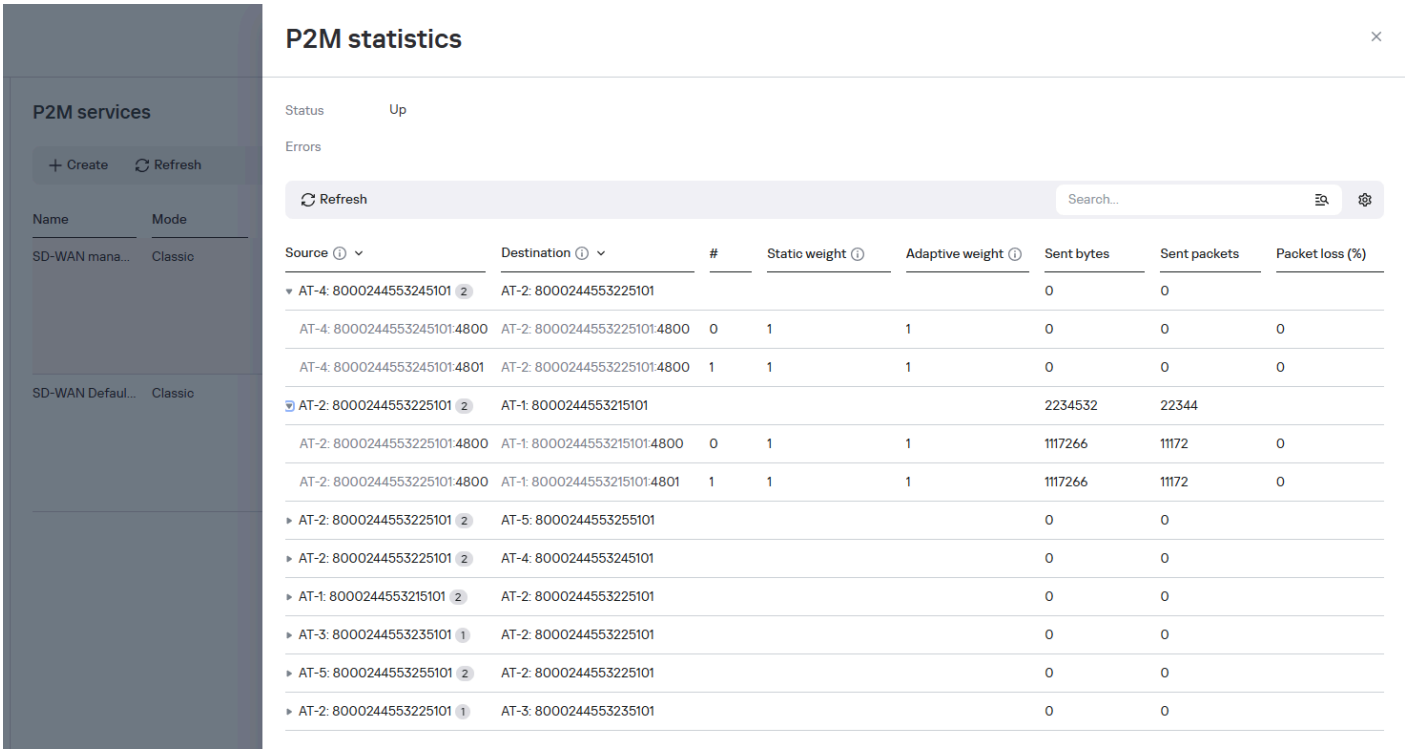
   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Estadísticas** junto al servicio P2M cuyas estadísticas desea ver.

Se abre una ventana con las estadísticas del servicio P2M.

En la parte superior de la ventana de estadísticas, el campo **Estado** muestra el estado operativo del servicio. El campo **Errores** muestra los posibles errores que pueden ocurrir para el servicio.

Las estadísticas de los segmentos, las rutas y los vínculos del servicio se muestran jerárquicamente en una tabla. Las filas de la tabla están agrupadas por segmento. Las filas dentro de cada grupo contienen estadísticas para las rutas incluidas en el segmento correspondiente. Para expandir un grupo, haga clic en el triángulo (▸). Para los servicios que no tienen límites establecidos, las filas muestran todas las rutas con el equilibrio de carga habilitado en el segmento. Para los servicios con límites, las filas muestran las rutas de Auto-TE que cumplen el límite.




Visualización de estadísticas, usando un servicio P2M como ejemplo

La información estadística detallada sobre los segmentos y las rutas se muestra en las siguientes columnas de la tabla:

**Origen**: para filas agregadas, el host de origen del segmento; para filas en grupos expandibles, el host de origen de la ruta en el segmento.

**Destino**: para filas agregadas, el host de destino del segmento; para filas en grupos expandibles, el host de destino de la ruta en el segmento.

**#** es el número secuencial de la ruta. Cuanto menor sea el número de la ruta, antes se construyó. Este valor se muestra solo para filas en grupos expandibles.

**Peso estático** es el peso de la ruta estática en función del costo. Este valor se muestra solo para filas en grupos expandibles.

**Peso adaptado** es el peso dinámico de la ruta basado en el análisis de la pérdida de paquetes en esta ruta. Este valor se muestra solo para filas en grupos expandibles. Si no se utiliza el equilibrio adaptativo, esta columna no se muestra.

**Bytes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de bytes enviados al depósito del grupo OF.

**Paquetes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de paquetes enviados al depósito del grupo OF.

**Pérdida de paquetes (%)** es el porcentaje de pérdida de paquetes en una ruta determinada (la relación entre el número de paquetes perdidos y el número total de paquetes enviados). Este valor se muestra solo para filas en grupos expandibles.

# Ver la tabla MAC de un servicio P2M

*Para ver la tabla MAC de un servicio P2M, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Tabla MAC** junto al servicio P2M cuya tabla MAC desea ver.

Esto abre una ventana con la tabla MAC del servicio P2M. La información sobre las direcciones MAC se muestra en las siguientes columnas de la tabla:

- **MAC** es la dirección MAC.
- **Nombre de host** es el DPID del conmutador detrás del cual se encuentra la dirección MAC.
- **Puerto** es el número del puerto detrás del cual se encuentra la dirección MAC.
- **VLAN** es el segmento de la VLAN en el que se encuentra la dirección MAC.
- **Antigüedad (segundos)** es el tiempo en segundos durante el cual la dirección MAC ha estado presente en la tabla de direcciones MAC.

5. Si desea encontrar una dirección MAC específica, escríbala en el campo y haga clic en **Buscar por MAC**.
6. Si desea borrar la tabla MAC, haga clic en **Borrar**.

# Visualización y configuración de la visualización de una topología de servicio P2M

*Para ver y configurar la visualización de una topología de servicio P2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Topología del servicio** junto al servicio P2M cuya topología desea ver.

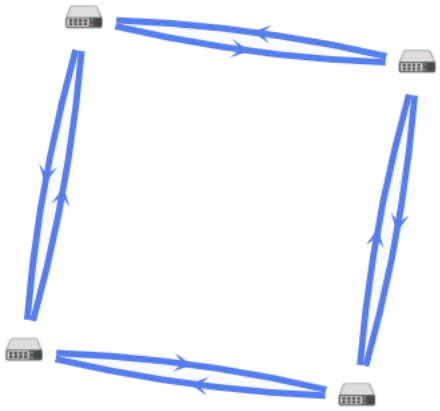
   Se abre una ventana con la topología del servicio P2M.

5. Si necesita mover dispositivos CPE, realice una de las siguientes acciones:

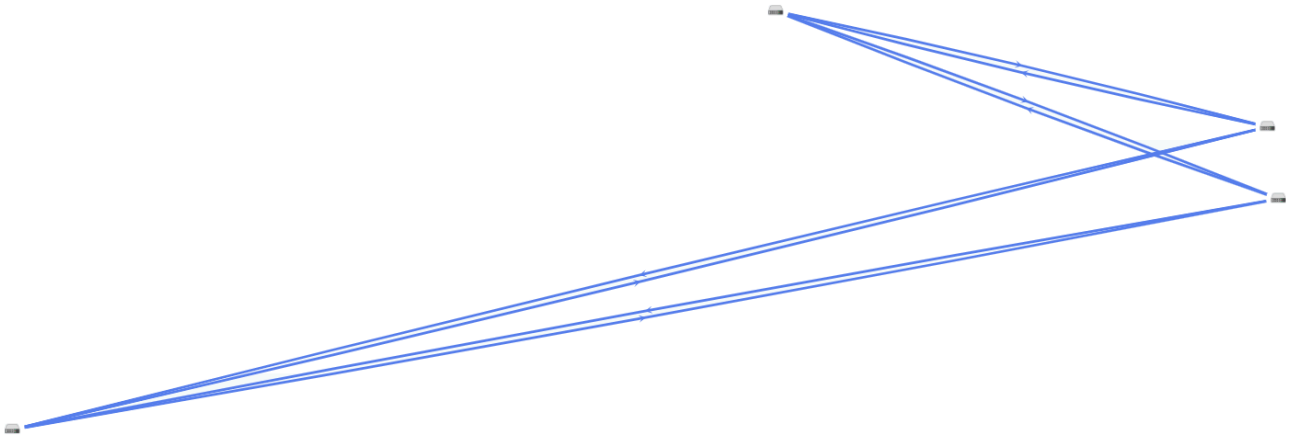
- Si desea cambiar manualmente la posición de los dispositivos CPE, haga clic en **Manual** y ajuste la posición de los dispositivos CPE.

- Si desea organizar automáticamente los dispositivos CPE, haga clic en **Automáticamente** y seleccione uno de los siguientes valores de la lista desplegable que se muestra:

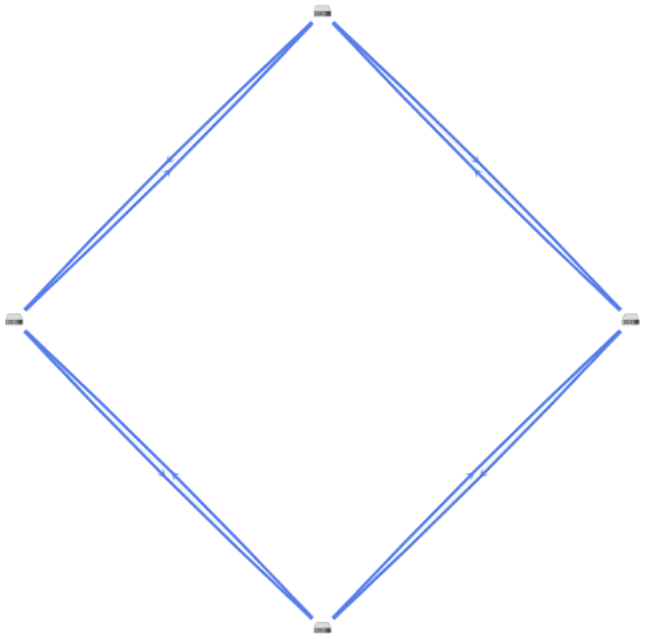
  - **Simulación física**: los dispositivos CPE se disponen aproximadamente de acuerdo con su ubicación real entre sí, por ejemplo:



  - **Aleatorio**: la disposición de los dispositivos CPE es aleatoria, por ejemplo:



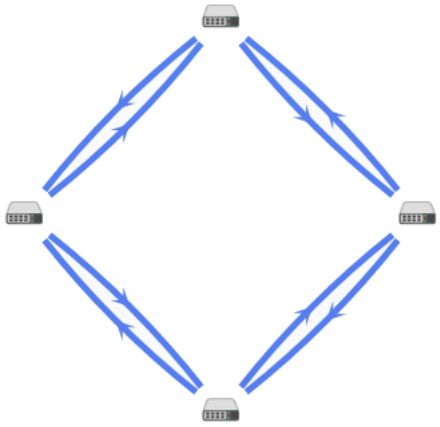
  - **Círculo**: los dispositivos CPE se organizan de acuerdo con una topología en anillo, por ejemplo:



- **Búsqueda en anchura**: los dispositivos CPE están dispuestos horizontalmente, por ejemplo:



- **Concéntrico**: los dispositivos CPE están dispuestos de forma concéntrica, por ejemplo:



- **Cuadrícula**: los dispositivos CPE se organizan de acuerdo con una topología de cuadrícula, por ejemplo:



6. Si desea mostrar información sobre los dispositivos CPE, seleccione las siguientes casillas:

   - **Nombre** muestra los nombres de los dispositivos CPE.
   - **Dirección IP** muestra las direcciones IP de los dispositivos CPE.

   Estas casillas de verificación están desactivadas de manera predeterminada.

7. Si desea mostrar un segmento entre dos dispositivos CPE:

   a. Seleccione la casilla **Segmentos**. Esta casilla está desactivada por defecto.

   b. En las listas desplegables que se muestran, seleccione los dispositivos CPE de origen y destino del segmento.

   Se muestra el segmento entre los dispositivos CPE.

# Editar un servicio P2M

*Para editar un servicio P2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Editar** junto al servicio P2M que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio P2M. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio P2M.

6. Haga clic en **Guardar**.

El servicio P2M se modifica y actualiza en la tabla.

# Reiniciar un servicio P2M

Puede reiniciar un servicio P2M para restaurarlo en caso de mal funcionamiento. Cuando reinicia un servicio P2M, el controlador elimina y vuelve a crear automáticamente las reglas asociadas con este servicio P2M en las tablas de OpenFlow de los dispositivos CPE. Esto afecta a los dispositivos CPE cuyas interfaces de servicio se agregan al servicio P2M.

*Para reiniciar un servicio P2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Reaprovisionar** junto al servicio P2M que desea reaprovisionar.

5. En la ventana de confirmación, haga clic en **Confirmar**.

Se reinicia el servicio P2M.

# Eliminar un servicio P2M

Los servicios P2M eliminados no se pueden restaurar.

*Para eliminar un servicio P2M, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de P2M**.

   Se muestra una tabla de servicios P2M.

4. Haga clic en **Administración** → **Eliminar** junto al servicio P2M que desea eliminar.

5. Si desea eliminar las interfaces de servicio agregadas al servicio P2M, seleccione la casilla de verificación **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.

6. Haga clic en **Eliminar**.

El servicio P2M se eliminará y ya no se mostrará en la tabla.

# Administrar servicios de transporte multipunto a multipunto (M2M)

Para ver la tabla de servicios M2M, vaya a la sección del menú **Infraestructura**, haga clic en **Administración**→ **Configuración de implementación** junto al controlador y vaya a la sección **Servicios de M2M**. La información sobre los servicios M2M se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio M2M.
- **Antigüedad de MAC (s)** es el período en segundos durante el cual las entradas se mantienen en la tabla MAC del controlador.
- **Modo de aprendizaje de MAC** es la acción que se aplica a una serie de marcos cuando el primer marco se envía al controlador para obtener la dirección MAC de origen:
  - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio M2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos.
  - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

  Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.
- **Tamaño de la tabla MAC** es el número máximo de entradas en la tabla MAC del controlador.

- **Sobrecarga en tabla MAC** es la directiva para procesar nuevas direcciones MAC cuando la tabla MAC del controlador está llena:
  - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.
  - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.
- **Endpoints** es la información sobre las interfaces de servicio que se agregaron al servicio M2M:
  - Nombres y DPID de los dispositivos CPE en los que se crearon las interfaces de servicio
  - Números de puertos OpenFlow a los que se asignan las interfaces de servicio
  - Funciones de las interfaces de servicio
- **Estado** es el estado del servicio M2M:
  - **Arriba**
  - **Abajo**
- **Descripción** es una breve descripción del servicio M2M.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un servicio M2M

*Para crear un servicio M2M, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.

4. En la parte superior de la página, haga clic en **+ Servicio de M2M**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio M2M.

6. En la lista desplegable **Restricción**, seleccione la restricción de Manual-TE creada o la restricción de umbral que desea agregar al servicio M2M.

7. En la lista desplegable **Modo de equilibrio**, seleccione el modo de equilibrio para la distribución del tráfico entre los vínculos:

   - **Por flujo** significa que los flujos de tráfico (5 tuplas) se distribuyen entre los vínculos de acuerdo con el costo del vínculo. Esta es la configuración predeterminada.
   - **Por paquete** significa que los paquetes de tráfico se distribuyen entre los vínculos de acuerdo con el costo del vínculo.
   - **Transmisión** significa que los paquetes de tráfico se duplican y se transmiten en simultáneo a través de todos los vínculos para evitar pérdidas.

   Puede especificar el costo del vínculo de forma manual.

8. Opcionalmente, configure el modo de equilibrio adaptativo si desea que el peso de la ruta se ajuste de manera dinámica según el nivel de pérdida de los paquetes de la ruta:

   a. Active el conmutador **Equilibrio adaptado**.

   b. En el campo **Tasa de pérdida mínima (%)**, especifique el porcentaje mínimo de pérdida de los paquetes en la ruta en la que comienza el equilibrio adaptativo para ajustar el peso. Rango de valores: 0.01 a 100.

   c. En el campo **Tasa de pérdida máxima (%)**, especifique el porcentaje máximo de pérdida de los paquetes en el que la ruta se excluye del equilibrio de carga.

   d. En la lista desplegable **Velocidad de convergencia**, seleccione la tasa de convergencia de los pesos adaptativos a los valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0.75
      - **Rápido**: 0.5

9. En la lista desplegable **Modo de aprendizaje de MAC**, seleccione la acción que desea aplicar a una serie de marcos cuando el primer marco se envíe al controlador para conocer la dirección MAC de origen:

   - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio M2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos. Esta es la configuración predeterminada.
   - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

   Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

10. En el campo **Antigüedad de MAC (s)**, ingrese el período de tiempo en segundos en el que las entradas se mantienen en la tabla MAC del controlador. Rango de valores: 10 a 65 535. El valor predeterminado es `300`.

11. En la lista desplegable **Sobrecarga en tabla MAC**, seleccione la directiva para el procesamiento de las nuevas direcciones MAC cuando la tabla MAC del controlador esté completa:

    - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.
    - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

12. En el campo **Tamaño de la tabla MAC**, ingrese la cantidad máxima de entradas en la tabla MAC del controlador. Rango de valores: 0 a 65 535. `0` significa que la cantidad de registros en la tabla MAC del controlador no está limitada. El valor predeterminado es `100`.

13. Si es necesario, en el campo **Descripción**, escriba una breve descripción del servicio M2M.

14. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

15. Agregue la interfaz de servicio al servicio M2M:

    a. Haga clic en **+ Agregar**.

    Se mostrará la configuración de la interfaz de servicio.

    b. En las listas desplegables **Conmutador** y **Interfaz del servicio** a la derecha, seleccione el dispositivo CPE y la interfaz de servicio creada que desea agregar al servicio M2M.

    c. En la lista desplegable **QoS**, seleccione la calidad de la regla de servicio creada para la interfaz de servicio.

    d. En la lista desplegable **Filtro entrante**, seleccione el filtro de tráfico creado para la interfaz de servicio.

    e. Si desea agregar una interfaz de servicio de respaldo a través de la cual se deba enviar el tráfico cuando falle la interfaz de servicio principal, en las listas desplegables **Conmutador de respaldo** y **Interfaz de servicio de respaldo**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea utilizar como interfaz de servicio de respaldo.

    Si la interfaz de servicio principal vuelve a estar en línea, el servicio M2M continúa utilizando la interfaz de servicio de respaldo.

    La interfaz de servicio se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias interfaces de servicio o eliminar interfaces de servicio. Para eliminar una interfaz de servicio, haga clic en el ícono de eliminar ✕ junto a ella.

16. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

17. Si desea agregar varias interfaces de red a un servicio M2M al mismo tiempo, tiene que agregar un grupo de puertos OpenFlow. Para hacerlo, haga lo siguiente:

    a. Haga clic en **+ Agregar**.

    Se mostrará la configuración del grupo de puertos OpenFlow.

    b. En la lista desplegable **Grupo**, seleccione el grupo de puertos OpenFlow creado que desea agregar al servicio M2M. Cuando se guarda la configuración del servicio M2M, se crean las interfaces de servicio automáticamente que se asignan a los puertos OpenFlow en el grupo de puertos OpenFlow, y, luego, estas interfaces de servicio se agregan automáticamente al servicio M2M.

c. En la lista desplegable **QoS**, seleccione la calidad de la regla de servicio creada para las interfaces de servicio automáticamente creadas que se asignaron a los puertos OpenFlow.

d. En el campo **ID de VLAN**, ingrese el valor de la etiqueta de la VLAN exterior para las interfaces de servicio automáticamente creadas que se asignaron a los puertos OpenFlow. Las interfaces de servicio con el tipo de clasificación de la VLAN solo se pueden crear automáticamente. Se asigna la misma etiqueta de la VLAN exterior a cada interfaz de servicio.

Se agrega el grupo de OpenFlow y se muestra en la parte inferior de la ventana. Puede agregar varios grupos de puertos OpenFlow o eliminar los grupos de puertos OpenFlow. Para eliminar un grupo de puertos OpenFlow, haga clic en el ícono de eliminar ✕ junto a él.

18. Haga clic en **Crear**.

Se crea el servicio M2M y se muestra en la tabla.

# Ver las estadísticas de un servicio M2M

*Para ver las estadísticas de un servicio M2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

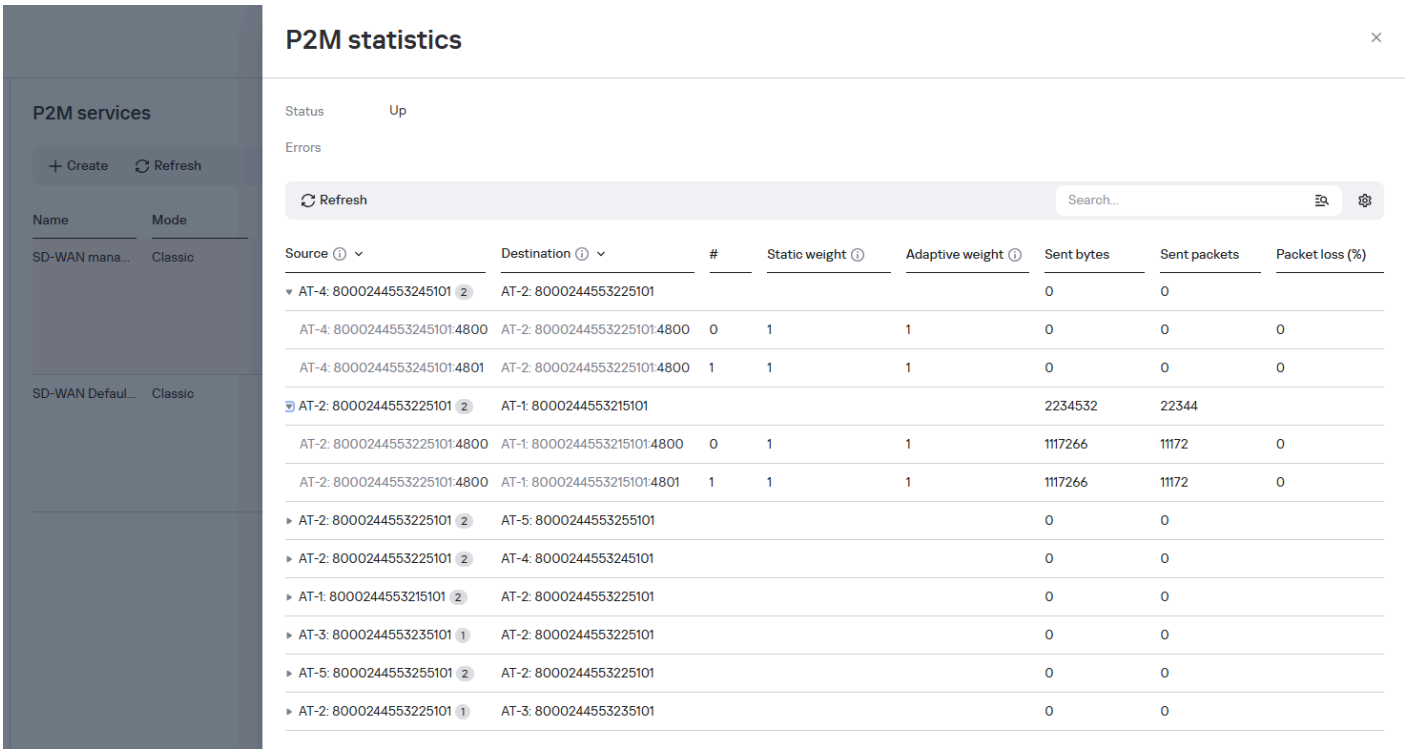
   Se mostrará una tabla de servicios M2M.

4. Haga clic en **Administración** → **Estadísticas** junto al servicio M2M cuyas estadísticas desea ver.

Se abre una ventana con las estadísticas del servicio M2M.

En la parte superior de la ventana de estadísticas, el campo **Estado** muestra el estado operativo del servicio. El campo **Errores** muestra los posibles errores que pueden ocurrir para el servicio.

Las estadísticas de los segmentos, las rutas y los vínculos del servicio se muestran jerárquicamente en una tabla. Las filas de la tabla están agrupadas por segmento. Las filas dentro de cada grupo contienen estadísticas para las rutas incluidas en el segmento correspondiente. Para expandir un grupo, haga clic en el triángulo (▸). Para los servicios que no tienen límites establecidos, las filas muestran todas las rutas con el equilibrio de carga habilitado en el segmento. Para los servicios con límites, las filas muestran las rutas de Auto-TE que cumplen el límite.




Visualización de estadísticas, usando un servicio P2M como ejemplo

La información estadística detallada sobre los segmentos y las rutas se muestra en las siguientes columnas de la tabla:

**Origen**: para filas agregadas, el host de origen del segmento; para filas en grupos expandibles, el host de origen de la ruta en el segmento.

**Destino**: para filas agregadas, el host de destino del segmento; para filas en grupos expandibles, el host de destino de la ruta en el segmento.

**#** es el número secuencial de la ruta. Cuanto menor sea el número de la ruta, antes se construyó. Este valor se muestra solo para filas en grupos expandibles.

**Peso estático** es el peso de la ruta estática en función del costo. Este valor se muestra solo para filas en grupos expandibles.

**Peso adaptado** es el peso dinámico de la ruta basado en el análisis de la pérdida de paquetes en esta ruta. Este valor se muestra solo para filas en grupos expandibles. Si no se utiliza el equilibrio adaptativo, esta columna no se muestra.

**Bytes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de bytes enviados al depósito del grupo OF.

**Paquetes enviados**: para filas agregadas, el valor de la ventana de estadísticas del servicio actual; para filas en grupos expandibles, la cantidad de paquetes enviados al depósito del grupo OF.

**Pérdida de paquetes (%)** es el porcentaje de pérdida de paquetes en una ruta determinada (la relación entre el número de paquetes perdidos y el número total de paquetes enviados). Este valor se muestra solo para filas en grupos expandibles.

# Ver la tabla MAC de un servicio M2M

*Para ver la tabla MAC de un servicio M2M, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.

4. Haga clic en **Administración** → **Tabla MAC** junto al servicio M2M cuyas estadísticas desea ver.

   Esto abre una ventana con la tabla MAC del servicio M2M. La información sobre las direcciones MAC se muestra en las siguientes columnas de la tabla:

   - **MAC** es la dirección MAC.
   - **Nombre de host** es el DPID del conmutador detrás del cual se encuentra la dirección MAC.
   - **Puerto** es el número del puerto detrás del cual se encuentra la dirección MAC.
   - **VLAN** es el segmento de la VLAN en el que se encuentra la dirección MAC.
   - **Antigüedad (segundos)** es el tiempo en segundos durante el cual la dirección MAC ha estado presente en la tabla de direcciones MAC.

5. Si desea encontrar una dirección MAC específica, escríbala en el campo y haga clic en **Buscar por MAC**.

6. Si desea borrar la tabla MAC, haga clic en **Borrar**.

# Ver y configurar la visualización de una topología de servicio M2M

*Para ver y configurar la visualización de una topología de servicio M2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.

4. Haga clic en **Administración** → **Topología del servicio** junto al servicio M2M cuya topología desea ver.

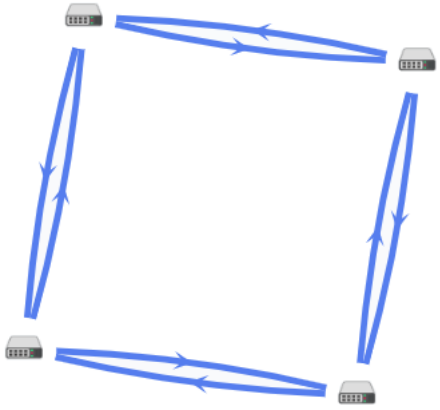
   Se abre una ventana con la topología del servicio M2M.

5. Si necesita mover dispositivos CPE, realice una de las siguientes acciones:

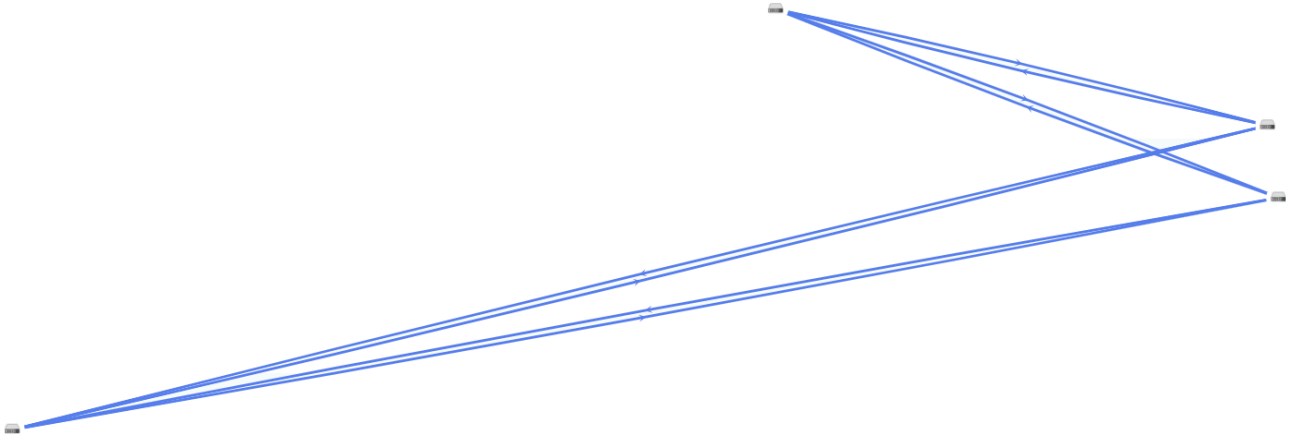
   - Si desea cambiar manualmente la posición de los dispositivos CPE, haga clic en **Manual** y ajuste la posición de los dispositivos CPE.

   - Si desea organizar automáticamente los dispositivos CPE, haga clic en **Automáticamente** y seleccione uno de los siguientes valores de la lista desplegable que se muestra:

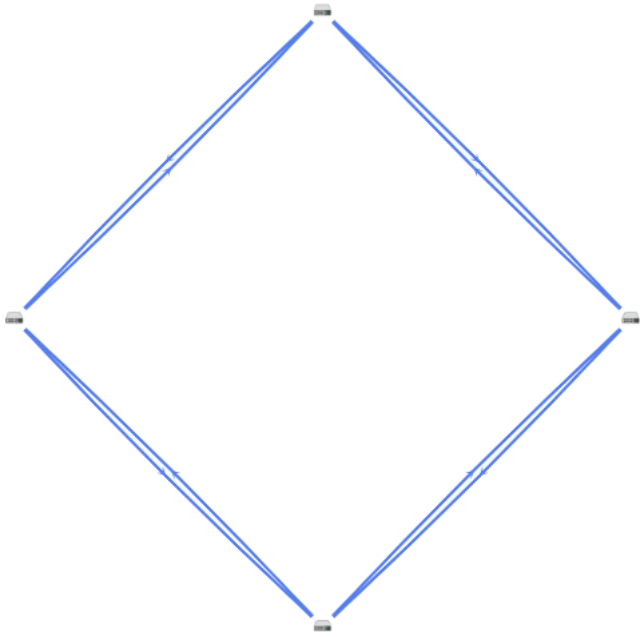
     - **Simulación física**: los dispositivos CPE se disponen aproximadamente de acuerdo con su ubicación real entre sí, por ejemplo:

     - **Aleatorio**: la disposición de los dispositivos CPE es aleatoria, por ejemplo:

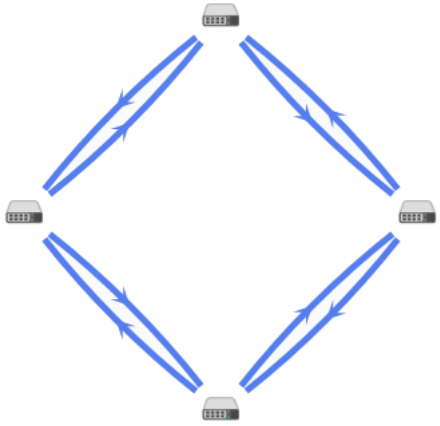
- **Círculo**: los dispositivos CPE se organizan de acuerdo con una topología en anillo, por ejemplo:



- **Búsqueda en anchura**: los dispositivos CPE están dispuestos horizontalmente, por ejemplo:



- **Concéntrico**: los dispositivos CPE están dispuestos de forma concéntrica, por ejemplo:



- **Cuadrícula**: los dispositivos CPE se organizan de acuerdo con una topología de cuadrícula, por ejemplo:



6. Si desea mostrar información sobre los dispositivos CPE, seleccione las siguientes casillas:

   - **Nombre** muestra los nombres de los dispositivos CPE.
   - **Dirección IP** muestra las direcciones IP de los dispositivos CPE.

   Estas casillas de verificación están desactivadas de manera predeterminada.

7. Si desea mostrar un segmento entre dos dispositivos CPE:

   a. Seleccione la casilla **Segmentos**. Esta casilla está desactivada por defecto.

   b. En las listas desplegables que se muestran, seleccione los dispositivos CPE de origen y destino del segmento.

   Se muestra el segmento entre los dispositivos CPE.

# Editar un servicio M2M

*Para editar un servicio M2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.

4. Haga clic en **Administración** → **Editar** junto al servicio M2M que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio M2M. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio M2M.

6. Haga clic en **Guardar**.

El servicio M2M se modifica y actualiza en la tabla.

# Reiniciar un servicio M2M

Puede reiniciar un servicio M2M para restaurarlo en caso de mal funcionamiento. Cuando reinicia un servicio M2M, el controlador elimina y vuelve a crear automáticamente las reglas asociadas con este servicio M2M en las tablas de OpenFlow de los dispositivos CPE. Esto afecta a los dispositivos CPE cuyas interfaces de servicio se agregan al servicio M2M.

*Para reiniciar un servicio M2M, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.

4. Haga clic en **Administración** → **Reaprovisionar** junto al servicio M2M que desea reaprovisionar.
5. En la ventana de confirmación, haga clic en **Confirmar**.

Se reinicia el servicio M2M.

# Eliminación de un servicio M2M

Los servicios M2M eliminados no se pueden restaurar.

*Para eliminar un servicio M2M:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.
2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.
3. Vaya a la sección **Servicios de M2M**.

   Se mostrará una tabla de servicios M2M.
4. Haga clic en **Administración** → **Eliminar** junto al servicio M2M que desea eliminar.
5. Si desea eliminar las interfaces de servicio agregadas al servicio M2M, seleccione la casilla de verificación **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.
6. Haga clic en **Eliminar**.

El servicio M2M se elimina y ya no se muestra en la tabla.

# Administrar servicios de transporte de multidifusión IP

Para ver la tabla de servicios de multidifusión IP, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Servicios de multidifusión de IP**. La información sobre los servicios de multidifusión IP se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio de multidifusión IP.
- **Interfaz de servicio de origen** contiene información sobre la interfaz de servicio de origen del servicio de multidifusión IP:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio

- a **Interfaz de servicio de respaldo** contiene información sobre la interfaz de servicio de origen de respaldo del servicio de multidifusión IP:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio
- **IP del enrutador de consulta** es la dirección IP de la interfaz de servicio de origen del servicio de multidifusión IP.
- **Interfaces de servicio del consumidor** contiene información sobre las interfaces de servicio de destino del servicio de multidifusión IP:
  - Nombres y DPID de los dispositivos CPE en los que se crearon las interfaces de servicio
  - Números de puertos OpenFlow a los que se asignan las interfaces de servicio
- **Grupos**Contiene información sobre los grupos de multidifusión que se agregaron al servicio de multidifusión IP:
  - Direcciones IP de los grupos de multidifusión
  - Longitud de prefijo de los grupos de multidifusión
  - Ancho de banda garantizado para los grupos de multidifusión
- **Estado** es el estado del servicio de multidifusión IP:
  - **Arriba**
  - **Abajo**
- **Errores** son errores que ocurrieron mientras se estaba ejecutando el servicio de multidifusión IP.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un servicio de multidifusión IP

*Para crear un servicio de multidifusión IP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de multidifusión de IP**.

   Se muestra una tabla de servicios de multidifusión IP.

4. En la parte superior de la página, haga clic en **+ Servicio de multidifusión de IP**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio de multidifusión IP.

6. En las listas desplegables **Conmutador de origen** y **Interfaz de servicio de origen**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de origen del servicio de multidifusión IP.

7. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en la lista desplegable **Interfaz de servicio de origen**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

8. En el campo **IP del enrutador de consulta**, ingrese la dirección IP de la interfaz del servicio de origen del servicio de multidifusión IP.

9. Si desea agregar una interfaz de servicio de reserva del origen del servicio de multidifusión IP a través de la cual se transmite el tráfico si falla la interfaz de servicio principal:

    a. Seleccione la casilla **Utilizar interfaz de respaldo**. Esta casilla está desactivada por defecto.

    b. En las listas desplegables **Conmutador de respaldo** y **Interfaz de servicio de respaldo**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de reserva.

    c. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en la lista desplegable **Interfaz de servicio de respaldo**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

    d. Si desea que el servicio de multidifusión IP vuelva a utilizar la interfaz del servicio de origen principal cuando esa interfaz de servicio vuelva a funcionar, seleccione la casilla **Restablecimiento automático de recuperación**. Esta casilla está desactivada por defecto.

    e. Si desea que el árbol de distribución de tráfico de multidifusión se cree en la interfaz del servicio de respaldo, seleccione la casilla **Árbol de multidifusión de respaldo**. Mientras la interfaz del servicio principal permanezca activa, los paquetes de tráfico en la interfaz del servicio de respaldo se descartan. Esta casilla está seleccionada por defecto.

10. Seleccione la casilla **Proxy IGMP** para usar un servidor proxy IGMP. Esto le permite mantener la transmisión de tráfico a los grupos de multidifusión activos a los que está conectada al menos una interfaz de servicio de destino del servicio de multidifusión IP. Esta casilla está desactivada por defecto.

11. En la lista desplegable **QoS**, seleccione la regla de calidad de servicio creada para la interfaz de servicio del origen del servicio de multidifusión IP.

12. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

13. Agregue la interfaz del servicio de destino al servicio de multidifusión IP:

    a. En las listas desplegables **Conmutador del consumidor** y **Interfaz de servicio del consumidor**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como interfaz de servicio de destino del servicio de multidifusión IP.

    b. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en la lista desplegable **Interfaz de servicio del consumidor**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

    c. Haga clic en **+ Agregar**.

La interfaz de servicio se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias interfaces de servicio o eliminar interfaces de servicio. Para eliminar una interfaz de servicio, haga clic en **Eliminar** junto a ella.

14. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

15. Agregue el grupo de multidifusión al servicio de multidifusión IP:

    a. En el campo **Dirección IP**, ingrese la dirección IP del grupo de multidifusión. Rango de valores: 224.0.0.0 a 239.255.255.255.

    b. En la lista desplegable **Máscara**, seleccione la longitud del prefijo del grupo de multidifusión. Rango de valores: 24 a 32.

    c. En la lista desplegable **GBR**, seleccione la velocidad de bits garantizada (GBR) para el grupo de multidifusión.

    d. Haga clic en **+ Agregar**.

    El grupo de multidifusión se agrega y se muestra en la parte inferior de la ventana. Puede agregar varios grupos de multidifusión o eliminar grupos de multidifusión. Para eliminar un grupo de multidifusión, haga clic en **Eliminar** junto a él.

16. Haga clic en **Crear**.

El servicio de multidifusión IP se crea y se muestra en la tabla.

# Ver las estadísticas de un servicio de multidifusión IP

*Para ver las estadísticas de un servicio de multidifusión IP:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de multidifusión de IP**.

   Se muestra una tabla de servicios de multidifusión IP.

4. Haga clic en **Administración** → **Estadísticas** junto al servicio de multidifusión IP cuyas estadísticas desea ver.

Se abre una ventana con las estadísticas del servicio de multidifusión IP.

# Editar un servicio de multidifusión IP

*Para editar un servicio de multidifusión IP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de multidifusión de IP**.

   Se muestra una tabla de servicios de multidifusión IP.

4. Haga clic en **Administración**→ **Editar interfaces de origen**,**Editar interfaces del consumidor** o **Editar grupos de multidifusión** junto al servicio de multidifusión IP que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio de multidifusión IP. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio de multidifusión IP.

6. Haga clic en **Guardar**.

El servicio de multidifusión IP se modifica y actualiza en la tabla.

# Eliminar un servicio de multidifusión IP

Los servicios de multidifusión IP eliminados no se pueden restaurar.

*Para eliminar un servicio de multidifusión IP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de multidifusión de IP**.

   Se muestra una tabla de servicios de multidifusión IP.

4. Haga clic en **Administración** → **Eliminar** junto al servicio de multidifusión IP que desea eliminar.

5. Si desea eliminar las interfaces de servicio agregadas al servicio de multidifusión IP, seleccione la casilla de verificación **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.

6. Haga clic en **Eliminar**.

El servicio de multidifusión IP se elimina y ya no se muestra en la tabla.

# Administrar servicios de transporte VPN L3

Para ver la tabla de servicios VPN L3, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Servicios de VPN L3**. La información sobre los servicios VPN L3 se muestra en las siguientes columnas de la tabla:

- **Nombre** es el servicio VPN L3.
- **Tipo** es el tipo de topología del servicio VPN L3.
- **Inter-spoke a través del centro de conectividad** indica si es posible la comunicación entre sitios radiales a través del sitio concentrador:
  - **Sí**.
  - **No**.
- **Endpoints** es la información sobre las interfaces L3 que se agregaron al servicio VPN L3:
  - Si las interfaces L3 están asignadas a servicios M2M, se muestran los nombres de los servicios M2M.
  - Si las interfaces L3 están asignadas a interfaces de servicio, se muestra la siguiente información:
    - Nombres y DPID de los dispositivos CPE en los que se crearon las interfaces de servicio
    - Números de puertos OpenFlow a los que se asignan las interfaces de servicio
    - Reglas de calidad de servicio especificadas para las interfaces de servicio
    - Filtros de tráfico especificados para las interfaces de servicio
  - Longitudes de los prefijos de la interfaz L3.
  - Direcciones MAC de las interfaces L3
  - Período en segundos durante el cual las entradas se mantienen en la tabla ARP en el controlador
- **Rutas** es la información sobre las rutas estáticas que se agregaron al servicio VPN L3:
  - Prefijos IPv4 de destino de las rutas estáticas
  - Direcciones IPv4 de puerta de enlace para enrutar paquetes de tráfico a los prefijos IPv4 de las rutas estáticas

- Interfaces L3 detrás de las cuales están los prefijos IPv4 de destino de las rutas estáticas
- Métricas de las rutas estáticas

- **Estado** es el estado del servicio VPN L3:
  - **Arriba**
  - **Abajo**
- **Errores** son errores que ocurrieron mientras se estaba ejecutando el servicio VPN L3.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

# Crear un servicio VPN L3

*Para crear un servicio de VPN L3, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. En la parte superior de la página, haga clic en **+ Servicio de VPN L3**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio VPN L3.

6. En la lista desplegable **Restricción**, seleccione la restricción de Manual-TE o la restricción de umbral que desea agregar al servicio VPN L3.

7. En la lista desplegable **Modo de equilibrio**, seleccione el modo de equilibrio para equilibrar el tráfico entre los vínculos:
   - **Por flujo** significa que los flujos de tráfico (5 tuplas) se distribuyen entre los vínculos de acuerdo con el costo del vínculo. Esta es la configuración predeterminada.
   - **Por paquete** significa que los paquetes de tráfico se distribuyen entre los vínculos de acuerdo con el costo del vínculo.
   - **Transmisión** significa que los paquetes de tráfico se duplican y se transmiten en simultáneo a través de todos los vínculos para evitar pérdidas.

   Puede especificar el costo del vínculo de forma manual.

8. Opcionalmente, configure el modo de equilibrio adaptativo si desea que el peso de la ruta se ajuste de manera dinámica según el nivel de pérdida de los paquetes de la ruta:

    a. Active el conmutador **Equilibrio adaptado**.

    b. En el campo **Tasa de pérdida mínima (%)**, especifique el porcentaje mínimo de pérdida de los paquetes en la ruta en la que comienza el equilibrio adaptativo para ajustar el peso. Rango de valores: 0.01 a 100.

    c. En el campo **Tasa de pérdida máxima (%)**, especifique el porcentaje máximo de pérdida de los paquetes en el que la ruta se excluye del equilibrio de carga.

    d. En la lista desplegable **Velocidad de convergencia**, seleccione la tasa de convergencia de los pesos adaptativos a los valores calculados:

    - **Rápido**: 1
    - **Rápido**: 0.75
    - **Rápido**: 0.5

9. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

10. Agregue la interfaz L3 al servicio VPN L3:

    a. En la lista desplegable **Modo**, seleccione el tipo de interfaz L3:

    - **Servicio de M2M** significa que la interfaz L3 está asignada a un servicio M2M.
    - **Interfaz del servicio** significa que la interfaz L3 está asignada a una interfaz de servicio.

    b. Si en la lista desplegable **Modo**, seleccionó **Servicio de M2M**, en la lista desplegable **Servicio de M2M**, seleccione el servicio M2M creado que está asignado a la interfaz L3.

    c. Si en la lista desplegable **Modo**, seleccionó **Interfaz del servicio**, configure la interfaz de servicio:

    1. En las listas desplegables **Conmutador** y **Interfaz del servicio**, seleccione el dispositivo CPE y la interfaz de servicio creada a la que se asigna la interfaz L3.
    2. En la lista desplegable **QoS**, seleccione la regla de calidad de servicio creada para la interfaz L3.
    3. En la lista desplegable **Filtro entrante**, seleccione el filtro de tráfico creado para la interfaz L3.
    4. Si desea mostrar las interfaces de servicio que se agregaron a los servicios de transporte en la lista desplegable **Interfaz del servicio**, seleccione la casilla **Mostrar interfaces utilizadas**. Esta casilla está desactivada por defecto.

    d. En el campo **Dirección IP**, ingrese la dirección IP de la interfaz L3.

    e. En el campo **Longitud del prefijo**, ingrese la longitud del prefijo de la interfaz L3. Rango de valores: de 0 a 32.

    f. En el campo **Dirección MAC**, ingrese la dirección MAC de la interfaz L3. Para generar una dirección MAC, haga clic en **Generate**.

g. En el campo **Antigüedad de ARP (s)**, ingrese el período en segundos durante el cual las entradas se mantienen en la tabla ARP en el servicio VPN L3. Rango de valores: de 1 a 65 535. El valor predeterminado es `200`.

h. Haga clic en **+ Agregar**.

La interfaz L3 se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias interfaces L3 o eliminarlas. Para eliminar una interfaz L3, haga clic en **Eliminar** junto a ella.

11. Haga clic en **Siguiente** para pasar al siguiente grupo de configuraciones.

12. Si desea agregar una ruta estática al servicio VPN L3:

a. En el campo **Dirección IP**, ingrese la dirección IPv4 de destino de la ruta estática.

b. En el campo **Longitud del prefijo**, ingrese la longitud del prefijo IPv4 de la ruta estática. Rango de valores: de 0 a 32.

c. En la lista desplegable **SVI**, seleccione la interfaz L3 agregada seguida del prefijo IPv4 del destino de la ruta estática. Agregó una interfaz L3 en el paso 9 de estas instrucciones.

d. En el campo **Gateway**, ingrese la dirección IPv4 de la puerta de enlace para enrutar paquetes de tráfico al prefijo IPv4 del destino de la ruta estática.

e. En el campo **Métrica**, ingrese una métrica para la ruta estática. El valor predeterminado es `0`.

f. Haga clic en **+ Agregar**.

La ruta estática se agrega y se muestra en la parte inferior de la ventana. Puede agregar varias rutas estáticas o eliminar rutas estáticas. Para eliminar una ruta estática, haga clic en **Eliminar** junto a ella.

13. Haga clic en **Crear**.

El servicio VPN L3 se crea y se muestra en la tabla.

# Administrar la tabla ARP de un servicio VPN L3

Para ver la tabla ARP del servicio de VPN L3, vaya a la sección **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador, vaya a la sección **Servicios de VPN L3** y haga clic en **Administración** → **Tabla ARP** junto al servicio de VPN L3. La información sobre los registros se muestra en las siguientes columnas de la tabla:

- **Dirección IP** es la dirección IP de la interfaz de servicio.
- **MAC** es la dirección MAC de la interfaz de servicio.
- **Interfaz del servicio** es la información sobre la interfaz de servicio:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio
- **Tiempo de espera máximo (s)** es el tiempo en segundos que ha transcurrido desde que se creó el registro.

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Crear un registro estático en la tabla ARP de un servicio VPN L3

*Para crear un registro estático en la tabla ARP de un servicio VPN L3, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Tabla ARP** junto al servicio de VPN L3 en cuya tabla ARP desea crear el registro estático.

   Se muestra la página con la tabla ARP del servicio VPN L3.

5. En la parte superior de la página, haga clic en **+ Registro ARP estático**.

6. En la ventana que se abre, en las listas desplegables **Conmutador** y **Interfaz del servicio**, seleccione el dispositivo CPE y la interfaz de servicio creada para la que desea especificar una dirección IP y una dirección MAC.

7. En el campo **Dirección IP**, ingrese la dirección IP de la interfaz de servicio.

8. En el campo **MAC**, ingrese la dirección MAC de la interfaz de servicio.

9. Haga clic en **Crear**.

Se crea el registro estático y se muestra en la tabla ARP del servicio VPN L3.

## Editar un registro estático en la tabla ARP de un servicio VPN L3

*Para editar un registro estático en la tabla ARP de un servicio VPN L3, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Tabla ARP** junto al servicio VPN L3 en cuya tabla ARP desea editar un registro estático.

   Se muestra la página con la tabla ARP del servicio VPN L3.

5. Haga clic en **Administración** → **Editar** junto al registro estático que desea editar.

6. En la ventana que se abre, si es necesario, edite la dirección IP o la dirección MAC de la interfaz de servicio.

7. Haga clic en **Guardar**.

El registro estático se modifica y actualiza en la tabla.

## Eliminar un registro estático en la tabla ARP de un servicio VPN L3

Los registros estáticos eliminados en la tabla ARP de un servicio VPN L3 no se pueden restaurar.

*Para eliminar un registro estático en la tabla ARP de un servicio VPN L3, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Tabla ARP** junto al servicio VPN L3 en cuya tabla ARP desea eliminar un registro estático.

   Se muestra la página con la tabla ARP del servicio VPN L3.

5. Haga clic en **Administración** → **Eliminar** junto al registro estático que desea eliminar.

6. En la ventana de confirmación, haga clic en **Eliminar**.

El registro estático se elimina y ya no se muestra en la tabla.

# Ver la tabla de enrutamiento y reenvío de un servicio de VPN L3

*Para ver la tabla de enrutamiento y reenvío de un servicio de VPN L3, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Tabla de enrutamiento** junto al servicio de VPN L3 cuya tabla de enrutamiento desea ver.

Esto abre una ventana con la tabla de enrutamiento y reenvío del servicio de VPN L3.

# Editar un servicio de VPN L3

*Para editar un servicio de VPN L3, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Editar** junto al servicio de VPN L3 que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio de VPN L3. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio de VPN L3.

6. Haga clic en **Guardar**.

El servicio de VPN L3 se modificará y se actualizará en la tabla.

# Reiniciar un servicio de VPN L3

Puede reiniciar un servicio VPN L3 para restaurarlo en caso de que no funcione correctamente. Cuando reinicia un servicio de VPN L3, el controlador elimina y vuelve a crear automáticamente las reglas asociadas con este servicio de VPN L3 en las tablas de OpenFlow de los dispositivos CPE. Esto afecta a los dispositivos CPE cuyas interfaces de servicio se agregan al servicio VPN L3.

*Para reiniciar un servicio VPN L3:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Reaprovisionar** junto al servicio de VPN L3 que desea reaprovisionar.

5. En la ventana de confirmación, haga clic en **Confirmar**.

Se reinicia el servicio de VPN L3.

# Eliminación de un servicio de VPN L3

Los servicios VPN L3 eliminados no se pueden restaurar.

*Para eliminar un servicio VPN L3:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de VPN L3**.

   Se muestra una tabla de servicios de VPN L3.

4. Haga clic en **Administración** → **Eliminar** junto al servicio de VPN L3 que desea eliminar.

5. Si desea eliminar las interfaces de servicio agregadas al servicio de VPN L3, seleccione la casilla **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.

6. Haga clic en **Eliminar**.

El servicio de VPN L3 se elimina y ya no se muestra en la tabla.

# Administrar servicios de transporte en una plantilla de instancia SD-WAN

Para ver la tabla de servicios P2M y servicios M2M en una plantilla de instancia SD-WAN, vaya a la sección **SD-WAN→ Plantillas de instancia SD-WAN**, haga clic en la plantilla de instancia SD-WAN y seleccione la pestaña **Servicios de transporte**. La información sobre los servicios P2M y M2M se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio P2M o del servicio M2M.
- **Tipo** es el tipo de servicio de transporte:
  - **P2M**
  - **M2M**
- **Servicio de transporte de administración** indica si el servicio P2M o el servicio M2M es un servicio de administración:
  - **Sí**.
  - **No**.
- **Modo** indica si se utiliza una DFI (interfaz de reenvío predeterminada) en el servicio P2M, al cual se envía tráfico de unidifusión desconocido:
  - **Clásico** si no desea utilizar una DFI. Esta es la configuración predeterminada.
  - **DFI con FIB en la raíz y las hojas** si desea utilizar una DFI en la interfaz de servicio con el rol raíz.
  - **DFI con FIB en la hoja** si desea utilizar una DFI en la interfaz de servicio con el rol raíz. Las interfaces de servicio con el rol de hoja deben crearse en el mismo dispositivo CPE. Las interfaces de servicio de respaldo con el rol de hoja deben crearse en el mismo dispositivo CPE, que debe ser diferente del dispositivo CPE en el que se crean las interfaces de servicio principales.

  El valor de esta columna solo se muestra si el valor de la columna **Tipo** es **P2M**.
- **Antigüedad de MAC (s)** es el período en segundos durante el cual las entradas se mantienen en la tabla MAC del controlador.

- **Modo de aprendizaje de MAC** es la acción que se aplica a una serie de marcos cuando el primer marco se envía al controlador para obtener la dirección MAC de origen:

  - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio M2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos.

  - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

  Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

- **Tamaño de la tabla MAC** es el número máximo de entradas en la tabla MAC del controlador.

- **Sobrecarga en tabla MAC** es la directiva para procesar nuevas direcciones MAC cuando la tabla MAC del controlador está llena:

  - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.

  - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

- **Acciones** contiene las acciones que se pueden realizar con el servicio de transporte.

Para ver una lista de servicios VPN L3, seleccione la pestaña **Servicios L3**.

# Crear un servicio P2M o un servicio M2M en una plantilla de instancia SD-WAN

*Para crear un servicio P2M o un servicio M2M en una plantilla de instancia SD-WAN, haga lo siguiente:*

1. En el menú, vaya a la sección **SD-WAN → Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancias SD-WAN en la que desea crear un servicio P2M o un servicio M2M.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Seleccione la pestaña **Servicios de transporte**.

   La pestaña **Servicios X2M** con la tabla de servicios de P2M y M2M está seleccionada de manera predeterminada.

4. Haga clic en **+ Servicio de transporte**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio P2M o M2M.

6. En la lista desplegable **Tipo**, seleccione el tipo de servicio de transporte:

   - **P2M** Si selecciona esta opción en la lista desplegable **Modo**, seleccione si el servicio P2M utiliza una DFI (interfaz de reenvío predeterminada), a la que se envía el tráfico de unidifusión desconocido:

     - **Clásico** si no desea utilizar una DFI. Esta es la configuración predeterminada.

     - **DFI con FIB en la raíz y las hojas** si desea utilizar una DFI en la interfaz de servicio con el rol raíz.

     - **DFI con FIB en la hoja** si desea utilizar una DFI en la interfaz de servicio con el rol raíz. Las interfaces de servicio con el rol de hoja deben crearse en el mismo dispositivo CPE. Las interfaces de servicio de respaldo con el rol de hoja deben crearse en el mismo dispositivo CPE, que debe ser diferente del dispositivo CPE en el que se crean las interfaces de servicio principales.

   - **M2M**

7. Si desea que un servicio P2M o M2M sea el servicio de administración, seleccione la casilla de verificación **Servicio de transporte de administración**. Esta casilla está desactivada por defecto. Solo un servicio de transporte puede ser el servicio de administración.

8. En la lista desplegable **Modo de aprendizaje de MAC**, seleccione la acción que desea aplicar a una serie de marcos cuando el primer marco se envíe al controlador para conocer la dirección MAC de origen:

   - **Aprender e inundar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se envía a todas las interfaces de servicio agregadas al servicio P2M, excepto por la interfaz de servicio a la que llegó originalmente la serie de marcos. Esta es la configuración predeterminada.

   - **Aprender y desconectar** significa que el controlador recuerda la dirección MAC del origen y comprueba la presencia de la dirección MAC de destino en la tabla MAC. Si la dirección MAC de destino no está en la tabla MAC, la serie de marcos se descarta.

   Si la dirección MAC de destino está presente en la tabla MAC, la serie de marcos se envía a la interfaz de servicio de destino.

9. En el campo **Tamaño de la tabla MAC**, ingrese la cantidad máxima de entradas en la tabla MAC del controlador. Rango de valores: 0 a 65 535. `0` significa que la cantidad de registros en la tabla MAC del controlador no está limitada. El valor predeterminado es `100`.

10. En el campo **Antigüedad de MAC (s)**, ingrese el período de tiempo en segundos en el que las entradas se mantienen en la tabla MAC del controlador. Rango de valores: 10 a 65 535. El valor predeterminado es `300`.

11. En la lista desplegable **Sobrecarga en tabla MAC**, seleccione la directiva para el procesamiento de las nuevas direcciones MAC cuando la tabla MAC del controlador esté completa:

    - **Inundación** significa que el tráfico con direcciones MAC de destino que no se obtuvieron se transmite como tráfico BUM (difusión, unidifusión desconocida y multidifusión). Esta es la configuración predeterminada.

    - **Desconectar** significa que se descarta el tráfico con direcciones MAC de destino que no se obtuvieron.

12. Haga clic en **Crear**.

    Se creará un servicio P2M o un servicio M2M y se mostrará en la tabla.

13. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Crear un servicio VPN L3 en una plantilla de instancia SD-WAN

*Para crear un servicio VPN L3 en una plantilla de instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN en la que desea crear un servicio VPN L3.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Seleccione la pestaña **Servicios de transporte** → **Servicios L3**.

   Se muestra una lista de servicios de VPN L3.

4. Haga clic en **+ Servicio de transporte**.

5. En la ventana que se abre, ingrese el nombre del servicio VPN L3.

6. Haga clic en **Crear**.

   El servicio VPN L3 se crea y se muestra en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Editar un servicio de transporte en una plantilla de instancia SD-WAN

*Para editar un servicio de transporte en una plantilla de instancia SD-WAN:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

   Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN en la que desea editar un servicio de transporte.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Si desea editar un servicio de P2M o un servicio de M2M:

   a. Seleccione la pestaña **Servicios de transporte**.

      La pestaña **Servicios X2M** con la tabla de servicios de P2M y M2M está seleccionada de manera predeterminada.

b. Haga clic en **Editar** junto al servicio de P2M o M2M que desea editar.

c. En la ventana que se abre, si es necesario, edite la configuración del servicio de P2M o M2M. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio de P2M o un servicio de M2M en una plantilla de instancia SD-WAN.

4. Si desea editar un servicio de VPN L3:

a. Seleccione la pestaña **Servicios de transporte** → **Servicios L3**.

Se muestra una lista de servicios de VPN L3.

b. Haga clic en **Editar** junto al servicio de VPN L3 que desea editar.

c. En la ventana que se abre, si es necesario, edite el nombre del servicio de VPN L3.

5. Haga clic en **Guardar**.

El servicio de transporte se modifica y actualiza en la tabla.

6. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Eliminar un servicio de transporte en una plantilla de instancia SD-WAN

Los servicios de transporte que se eliminan en la plantilla de instancias SD-WAN no se pueden restaurar.

*Para eliminar un servicio de transporte en una plantilla de instancia SD-WAN, siga estos pasos:*

1. En el menú, vaya a la sección **SD-WAN** → **Plantillas de instancia SD-WAN**.

Se muestra una tabla de plantillas de instancias SD-WAN.

2. Haga clic en la plantilla de instancia SD-WAN en la que desea eliminar un servicio de transporte.

Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, se selecciona la pestaña **Información**, que muestra el nombre de la plantilla de instancia SD-WAN.

3. Si desea eliminar un servicio P2M o un servicio M2M, siga estos pasos:

a. Seleccione la pestaña **Servicios de transporte**.

La pestaña **Servicios X2M** con la tabla de servicios de P2M y M2M está seleccionada de manera predeterminada.

b. Haga clic en **Eliminar** junto al servicio P2M o el servicio M2M que desea eliminar.

El servicio P2M o el servicio M2M se elimina y ya no se muestra en la tabla.

4. Si desea eliminar un servicio VPN L3, siga estos pasos:

   a. Seleccione la pestaña **Servicios de transporte** → **Servicios L3**.

      Se muestra una lista de servicios de VPN L3.

   b. Haga clic en **Eliminar** junto al servicio VPN L3 que desea eliminar.

   El servicio de VPN L3 se elimina y ya no se muestra en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de la instancia SD-WAN.

# Administrar servicios de transporte en una plantilla de CPE

Para ver la tabla de servicios de transporte en una plantilla de CPE, vaya a la sección del menú **SD-WAN** → **Plantillas de CPE**, haga clic en la plantilla de CPE y seleccione la pestaña **Servicios de transporte**. La información sobre los servicios de transporte se muestra en las siguientes columnas de la tabla:

- **Nombre** es el nombre del servicio de transporte.
- **Nombre de QoS** es el nombre de la regla de calidad de servicio para la interfaz de servicio, que se crea automáticamente para la conexión del dispositivo CPE al servicio de transporte.
- **Etapa** es el estado en el que el dispositivo CPE se conecta al servicio de transporte:
  - **Antes de la habilitación** significa que el dispositivo CPE se conecta al servicio de transporte antes de que se habilite este dispositivo CPE.
  - **Después de la habilitación** significa que el dispositivo CPE se conecta al servicio de transporte después de que se habilita este dispositivo CPE.

  Puede seleccionar en qué estado se encuentra el dispositivo CPE después del registro al agregar un dispositivo CPE.
- **Tipo** es el tipo de servicio de transporte:
  - **P2M**
  - **M2M**
  - **VPN L3**
- **Configuración de la conexión** contiene información sobre la interfaz de servicio que se crea automáticamente para conectar un dispositivo CPE al servicio de transporte:
  - Función de la interfaz de servicio:
    - **Hoja**
    - **Raíz**

Se muestra solo si el valor en la columna Tipo es P2M.

- Tipo de clasificación del tráfico en la interfaz de servicio:
  - **Acceso**
  - **VLAN**
  - **Q-in-Q**
- Etiqueta de VLAN externa de la interfaz de servicio. Solo se muestra si el tipo de clasificación del tráfico en la interfaz de servicio es **VLAN** o **Q-in-Q**.
- Etiqueta de VLAN interna de la interfaz de servicio. Solo se muestra si el tipo de clasificación del tráfico en la interfaz de servicio es **Q-in-Q**.

- **Acciones** contiene las acciones que se pueden realizar con el servicio de transporte.

# Agregar un servicio de transporte a una plantilla de CPE

*Para agregar un servicio de transporte a una plantilla de CPE, siga estos pasos:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE a la que desea agregar un servicio de transporte.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ⤢. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Servicios de transporte**.

   Se muestra una tabla de servicios de transporte.

4. Haga clic en **+ Servicio de transporte**.

5. En la ventana que se abre, en el campo **Nombre**, ingrese el nombre del servicio de transporte creado. Si el nombre real del servicio de transporte no coincide con el nombre especificado en la plantilla de CPE, el dispositivo CPE no establece la conexión al servicio de transporte.

6. En el campo **Nombre de QoS**, ingrese el nombre de la regla de calidad de servicio creada para la interfaz de servicio, que se crea automáticamente para la conexión del dispositivo CPE al servicio de transporte. Si el nombre real de la regla de calidad de servicio no coincide con el nombre especificado en la plantilla de CPE, la regla de calidad de servicio no se aplica a la interfaz de servicio.

7. En la lista desplegable **Etapa**, seleccione el estado en el que el dispositivo CPE se conecta al servicio de conexión de transporte:

   - **Antes de la habilitación** significa que el dispositivo CPE se conecta al servicio de transporte antes de que se habilite este dispositivo CPE.
   - **Después de la habilitación** significa que el dispositivo CPE se conecta al servicio de transporte después de que se habilita este dispositivo CPE.

Puede seleccionar en qué estado se encuentra el dispositivo CPE después del registro cuando agrega o registra manualmente un dispositivo CPE.

8. En la lista desplegable **Tipo**, seleccione el tipo de servicio de transporte:

   - **P2M** Si selecciona esta opción en la lista desplegable **Rol**, seleccione la función de la interfaz de servicio que se crea automáticamente para conectar el dispositivo CPE al servicio de transporte:
     - **Hoja**
     - **Raíz**
   - **M2M**
   - **VPN L3** Si selecciona esta opción, haga lo siguiente:
     a. En el campo **Dirección IP**, ingrese la dirección IP de la interfaz L3.
     b. En el campo **Máscara**, ingrese la longitud del prefijo de la interfaz L3. Rango de valores: de 0 a 32.

   Si el tipo real del servicio de transporte no coincide con el tipo especificado en la plantilla de CPE, el dispositivo CPE no establece la conexión al servicio de transporte.

9. En la lista desplegable **Clasificación**, seleccione el tipo de clasificación de tráfico en la interfaz de servicio que se crea automáticamente para la conexión del dispositivo CPE al servicio de transporte:

   - **Acceso** Esta es la configuración predeterminada.
   - **VLAN** Si selecciona esta opción, en el campo **ID de VLAN**, ingrese la etiqueta de la VLAN externa de la interfaz de servicio. Rango de valores: 1 a 4094.
   - **Q-in-Q** Si selecciona este valor, configure la interfaz L3 que se crea automáticamente y se asigna a la interfaz de servicio:
     a. En el campo **ID de VLAN**, ingrese la etiqueta de la VLAN externa de la interfaz de servicio. Rango de valores: 1 a 4094.
     b. En el campo **ID de VLAN interna**, ingrese la etiqueta de la VLAN interna de la interfaz de servicio. Rango de valores: 1 a 4094.

10. Haga clic en **Crear**.

    El servicio de transporte se crea y se muestra en la tabla.

11. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Editar un servicio de transporte en una plantilla de CPE

*Para editar un servicio de transporte en una plantilla de CPE:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea editar un servicio de transporte.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Servicios de transporte**.

   Se muestra una tabla de servicios de transporte.

4. Haga clic en **Editar** junto al servicio de transporte que desea editar.

5. En la ventana que se abre, si es necesario, edite la configuración del servicio de transporte. Para obtener una descripción de la configuración, consulte las instrucciones para agregar un servicio de transporte a una plantilla de CPE.

6. Haga clic en **Guardar**.

   El servicio de transporte se modifica y actualiza en la tabla.

7. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Eliminar un servicio de transporte de una plantilla de CPE

Los servicios de transporte que se eliminan en la plantilla de CPE no se pueden restaurar.

*Para eliminar un servicio de transporte en una plantilla de CPE, haga lo siguiente:*

1. En el menú, vaya a la subsección **SD-WAN → Plantillas de CPE**.

   Se muestra una tabla de plantillas de CPE.

2. Haga clic en la plantilla de CPE en la que desea eliminar un servicio de transporte.

   Se muestra el área de configuración. Puede expandir el área de configuración para llenar toda la página haciendo clic en el ícono de expandir ↙↗. De manera predeterminada, está seleccionada la pestaña **Información**, que muestra información general sobre la plantilla de CPE.

3. Seleccione la pestaña **Servicios de transporte**.

   Se muestra una tabla de servicios de transporte.

4. Haga clic en **Eliminar** junto al servicio de transporte que desea eliminar.

   El servicio de transporte se eliminará y ya no se mostrará en la tabla.

5. En la parte superior del área de configuración, haga clic en **Guardar** para guardar la configuración de la plantilla de CPE.

# Duplicación y reenvío de tráfico entre dispositivos CPE

Kaspersky SD-WAN admite el reenvío y la duplicación de tráfico entre dispositivos CPE. Puede redirigir o duplicar el tráfico de los puntos de recopilación de tráfico al destino del tráfico mediante los servicios TAP. El reenvío significa enviar el tráfico que llega a los puntos de recopilación de tráfico al punto de destino del tráfico, y la duplicación significa enviar una copia del tráfico.

Las interfaces de servicio se utilizan como puntos de recopilación y destinos del tráfico. Tanto las interfaces de servicio individuales como las interfaces de servicio agregadas a un servicio de transporte pueden ser puntos de recopilación de tráfico.

Debe crear un destino de tráfico y luego especificar este destino de tráfico y los puntos de recopilación de tráfico cuando crea o edita un servicio TAP. No es necesario crear puntos de recopilación de tráfico con antelación.

## Administrar destinos de tráfico

Para ver la lista de destinos de tráfico, vaya a la sección del menú **Infraestructura** haga clic en **Administración** → **Configuración de implementación** junto al controlador y vaya a la sección **Servicios de TAP**.

En las instrucciones de Administrar las tablas de los componentes de la solución, se describen las acciones que puede realizar con la lista.

### Crear un destino de tráfico

*Para crear un destino de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. En la parte superior de la página, haga clic en **+ Destino de duplicación**.

5. En la ventana que se abre, en las listas desplegables **Conmutador** y **Interfaz del servicio**, seleccione el dispositivo CPE y la interfaz de servicio creada que desea usar como destino de tráfico.

6. Haga clic en **Crear**.

El destino de tráfico se crea y se muestra en la tabla.

## Eliminar un destino de tráfico

Los destinos de tráfico eliminados no se pueden restaurar.

*Para eliminar un destino de tráfico, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. Haga clic en **Eliminar** junto al destino de tráfico que desea eliminar.

5. En la ventana de confirmación, haga clic en **Eliminar**.

El destino del tráfico se elimina y ya no se muestra en la tabla.

# Administrar servicios de TAP

Para ver la tabla de servicios de TAP, vaya a la sección del menú **Infraestructura**, haga clic en **Administración** → **Configuración de implementación** junto al controlador, vaya a la sección **Servicios de TAP** y seleccione la pestaña **Servicios de TAP**. La información sobre los servicios de TAP se muestra en las siguientes columnas de la tabla:

- **Destino de duplicación** contiene información sobre la interfaz de servicio utilizada como destino del tráfico:
  - Nombre y DPID del dispositivo CPE en el que se creó la interfaz de servicio
  - El número del puerto OpenFlow al que se asigna la interfaz de servicio
- **Duplicar tráfico** indica si el servicio TAP duplica el tráfico desde los puntos de recopilación de tráfico hasta el destino del tráfico:
  - **Sí**.
  - **No**.

- **Tipo** es el tipo de puntos de recopilación de tráfico:
  - **SI** significa que las interfaces de servicio individuales se utilizan como puntos de recopilación de tráfico.
  - Si las interfaces de servicio utilizadas como puntos de recopilación de tráfico se agregan a un servicio de transporte, se muestra el tipo de servicio de transporte:
    - **P2P**
    - **Multidifusión de IP**
    - **VPN L3**
    - **P2M**
    - **M2M**
- **Servicio de transporte** es el servicio de transporte al que se agregaron las interfaces de servicio que se utilizan como puntos de recopilación de tráfico. El valor de esta columna se muestra solo si la columna **Tipo de punto de origen** muestra el tipo de servicio de transporte.
- **Puntos de origen** contiene información sobre las interfaces de servicio que se utilizan como puntos de recopilación de tráfico:
  - Nombres y DPID de los dispositivos CPE en los que se crearon las interfaces de servicio
  - Números de puertos OpenFlow a los que se asignan las interfaces de servicio
- **Estado** es el estado del servicio TAP:
  - **Arriba**
  - **Abajo**

Las acciones que puede realizar con la tabla se describen en el artículo Administrar las tablas de componentes de la solución.

## Crear un servicio de TAP

*Para crear un servicio TAP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. Seleccione la pestaña **Servicios de TAP**.

   Se muestra una tabla de servicios de TAP.

5. En la parte superior de la página, haga clic en **+ Servicio de TAP**.

6. Si desea que el servicio TAP refleje el tráfico de los puntos de recopilación de tráfico al destino del tráfico, seleccione la casilla **Duplicar tráfico**. Cuando se selecciona esta casilla, se envía una copia del tráfico al destino; cuando se desmarca la casilla, el tráfico se reenvía. Esta casilla está desactivada por defecto.

7. En la lista desplegable **Modo de equilibrio**, seleccione el modo de equilibrio para la distribución del tráfico entre los vínculos:

   - **Por flujo** significa que los flujos de tráfico (5 tuplas) se distribuyen entre los vínculos de acuerdo con el costo del vínculo. Esta es la configuración predeterminada.
   - **Por paquete** significa que los paquetes de tráfico se distribuyen entre los vínculos de acuerdo con el costo del vínculo.
   - **Transmisión** significa que los paquetes de tráfico se duplican y se transmiten en simultáneo a través de todos los vínculos para evitar pérdidas.

   Puede especificar el costo del vínculo de forma manual.

8. Opcionalmente, configure el modo de equilibrio adaptativo si desea que el peso de la ruta se ajuste de manera dinámica según el nivel de pérdida de los paquetes de la ruta:

   a. Active el conmutador **Equilibrio adaptado**.

   b. En el campo **Tasa de pérdida mínima (%)**, especifique el porcentaje mínimo de pérdida de los paquetes en la ruta en la que comienza el equilibrio adaptativo para ajustar el peso. Rango de valores: 0.01 a 100.

   c. En el campo **Tasa de pérdida máxima (%)**, especifique el porcentaje máximo de pérdida de los paquetes en el que la ruta se excluye del equilibrio de carga.

   d. En la lista desplegable **Velocidad de convergencia**, seleccione la tasa de convergencia de los pesos adaptativos a los valores calculados:

      - **Rápido**: 1
      - **Rápido**: 0.75
      - **Rápido**: 0.5

9. En la lista desplegable **Destino de duplicación**, seleccione el destino de tráfico creado.

10. En la lista desplegable **Tipo de punto de origen**, seleccione el tipo de punto de recopilación de tráfico:

    - **Interfaz del servicio** significa que las interfaces de servicio individuales se utilizan como puntos de recopilación de tráfico.
    - **Servicio de transporte** significa que las interfaces de servicio que se agregan a un servicio de transporte se utilizan como puntos de recopilación de tráfico.

11. Si en la lista desplegable **Tipo de punto de origen** seleccionó **Servicio de transporte**, siga estos pasos:

    a. En la lista desplegable **Tipo**, seleccione el tipo de servicio de transporte:

    - **P2P**
    - **Multidifusión de IP**
    - **VPN L3**
    - **P2M**
    - **M2M**

    b. En la lista desplegable **Servicio de transporte**, seleccione el servicio de transporte.

12. En la lista desplegable **Puntos de origen**, seleccione la interfaz de servicio creada que desea usar como punto de recopilación de tráfico.

    El punto de recopilación de tráfico se agrega y se muestra en la parte inferior de la ventana. Puede agregar varios puntos de recopilación de tráfico o eliminarlos. Para eliminar un punto de recopilación de tráfico, haga clic en **Eliminar** junto a él.

13. Haga clic en **Siguiente** y seleccione las reglas de clasificación de tráfico creadas para los puntos de recopilación de tráfico.

14. Haga clic en **Crear**.

El servicio TAP se crea y se muestra en la tabla.

## Ver estadísticas de un servicio de TAP

*Para ver las estadísticas de un servicio TAP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. Seleccione la pestaña **Servicios de TAP**.

   Se muestra una tabla de servicios de TAP.

5. Haga clic en **Administración** → **Estadísticas** junto al servicio TAP cuyas estadísticas desea ver.

Se abre una ventana con las estadísticas del servicio TAP.

## Editar un servicio de TAP

*Para editar un servicio de TAP, haga lo siguiente:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. Seleccione la pestaña **Servicios de TAP**.

   Se muestra una tabla de servicios de TAP.

5. Haga clic en **Administración** → **Editar** junto al servicio de TAP que desea editar.

6. En la ventana que se abre, edite la configuración del servicio de TAP, si es necesario. Para obtener una descripción de la configuración, consulte las instrucciones para crear un servicio de TAP.

7. Haga clic en **Guardar**.

El servicio de TAP se modificará y se actualizará en la tabla.

## Eliminar un servicio de TAP

Los servicios TAP eliminados no se pueden restaurar.

*Para eliminar un servicio TAP, siga estos pasos:*

1. En el menú, vaya a la sección **Infraestructura**.

   Esto abre la página de administración de recursos. De manera predeterminada, está seleccionada la pestaña **Recursos de la red**, que muestra la tabla de controladores.

2. Haga clic en el nombre del controlador o seleccione el controlador en la tabla y haga clic en**Configuración de implementación**.

   Esto abre el menú para administrar la configuración de despliegue del controlador. De manera predeterminada, se le dirige a la sección **Nodos del controlador**, que muestra una tabla de nodos de controlador.

3. Vaya a la sección **Servicios de TAP**.

   De manera predeterminada, la pestaña **Destinos de duplicación** está seleccionada, que muestra la tabla de los destinos de tráfico.

4. Seleccione la pestaña **Servicios de TAP**.

   Se muestra una tabla de servicios de TAP.

5. Haga clic en **Administración** → **Eliminar** junto al servicio TAP que desea eliminar.

6. Para eliminar las interfaces de servicio agregadas al servicio TAP, seleccione la casilla **Eliminar interfaces de servicio asociadas** en la ventana de confirmación. Esta casilla está desactivada por defecto.

7. Haga clic en **Eliminar**.

El servicio TAP se elimina y ya no se muestra en la tabla.

# Integración con la Kaspersky Unified Monitoring and Analysis Platform

Puede usar Kaspersky Unified Monitoring and Analysis Platform (KUMA) para recibir notificaciones acerca de eventos de seguridad que ocurrieron en el orquestador y los dispositivos CPE. Esta sección describe los pasos para instalar y configurar KUMA.

Kaspersky SD-WAN no actúa como un agente de KUMA, solo envía eventos a KUMA sin marcado.

Para instalar KUMA, necesita una imagen del sistema operativo Astra Linux 1.8.5. Para obtener una lista de los sistemas operativos compatibles con KUMA, consulte la Ayuda de KUMA.

## Instalación de KUMA

*Para instalar KUMA:*

1. Configure el nombre de host en el servidor en el que desea instalar KUMA:

```
sudo hostnamectl set-hostname kuma.local
```

2. Asegúrese de que el host tenga una lista de servidores DNS; adminístrela si es necesario:

```
cat /etc/resolv.conf
```

3. En el servidor en el que desea instalar KUMA, especifique la dirección IP del servidor en el formato `<dirección IP> kuma.local` en el archivo para asignar direcciones IP a nombres de dominio:

```
vi /etc/hosts
```

4. Instale los paquetes requeridos:

```
sudo yum install python3
sudo pip3 install netaddr
sudo yum install firewalld
sudo yum install compat-openssl11
sudo yum install nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm at-spi2-atk mesa-libgbm alsa-lib
cups-libs libXcomposite libXdamage libXrandr
```

5. Si el servidor usa el mecanismo SELINUX, configure `SELINUX=disabled` para deshabilitarlo:

```
vi /etc/selinux/config
```

6. Habilite la sincronización horaria y confirme que está funcionando:

```
sudo systemctl enable --now chronyd sudo timedatectl | grep 'System clock synchronized'
```

7. Si desea usar la cuenta raíz para iniciar sesión en el servidor, especifique `PermitRootLogin yes` en el archivo de configuración SSH:

```
vi /etc/ssh/sshd_config
```

8. Reinicie el servidor.

9. Copie el archivo comprimido con el instalador `kuma-ansible-installer-<número de versión>.tar.gz` en el servidor y descomprímalo con el siguiente comando. Para descomprimir el archivo comprimido, necesitará aproximadamente 2 GB de espacio en disco.

```
sudo tar -xpf kuma-ansible-installer-<número de versión>.tar.gz
```

10. Cambie al directorio del instalador:

```
cd kuma-ansible-installer
```

11. Copie la plantilla `single.inventory.yml.template` y cree un archivo de inventario llamado `single.inventory.yml` basado en la plantilla:

```
cp single.inventory.yml.template single.inventory.yml
```

12. Abra el archivo `single.inventory.yml` para editarlo.

```
vi single.inventory.yml
```

13. Edite el contenido del archivo siguiendo el ejemplo siguiente:

```
all:
 vars:
 deploy_to_k8s: false
 need_transfer: false
 deploy_example_services: true
 no_firewall_actions: false
kuma:
 vars:
 ansible_connection: local
 ansible_user: root
 children:
 kuma_core:
 hosts:
 kuma.local:
 raft_node_addr: ""
 kuma_metrics:
 hosts:
 kuma.local:
 kuma_collector:
 hosts:
 kuma.local:
 kuma_correlator:
 hosts:
 kuma.local:
 kuma_storage:
 hosts:
 kuma.local:
 shard: 1
 replica: 1
 keeper: 1
```

14. Prepare el archivo de clave de KUMA.

15. Copie el archivo de clave al directorio:

```
sudo cp <archivo de clave>.key <directorio de instalación>/roles/kuma/files/license.key
```

16. Ejecute el instalador:

```
sudo ./install.sh single.inventory.yml
```

Espere hasta que finalice la instalación de KUMA.

17. Inicie sesión en la interfaz web de KUMA:

a. En su navegador, vaya a `https://<FQDN del host en el que está instalado KUMA>:7220`

b. Ingrese las credenciales de usuario predeterminadas:

- nombre de usuario: `admin`
- contraseña: `mustB3Ch@ng3d!`

18. Cambie la contraseña de la cuenta de administrador.

Para obtener más información acerca de la instalación de KUMA, consulte la Ayuda de KUMA.

# Escenario: configuración de KUMA

Este escenario describe el procedimiento para configurar Kaspersky Unified Monitoring and Analysis Platform para la integración con Kaspersky SD-WAN.

El proceso de configuración de KUMA incluye los siguientes pasos:

1. **Inicie sesión en la interfaz web de KUMA**

   Inicie sesión en la interfaz web de KUMA si aún no lo hizo. Asegúrese de cambiar la contraseña predeterminada.

2. Configuración del almacenamiento
3. Creación y configuración de un normalizador para mensajes de syslog
4. Configuración del correlacionador y las reglas de correlación
5. Configuración de un recopilador para mensajes de syslog
6. Configuración del servicio snmpd
7. Configuración de las reglas de notificación

Para obtener más información acerca de la configuración de KUMA, consulte la Ayuda de KUMA.

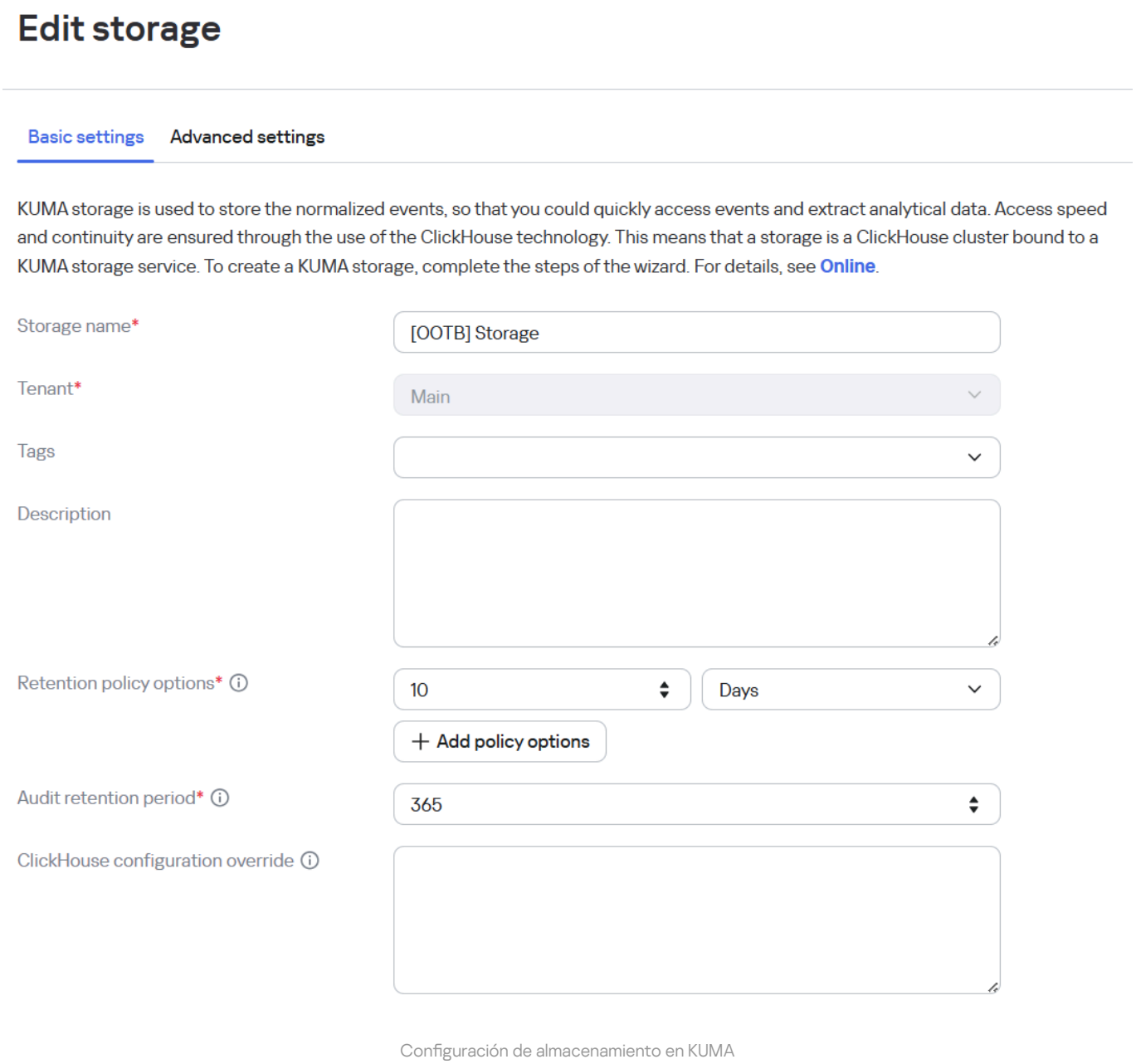
# Configuración de almacenamiento en KUMA

De manera predeterminada, el `almacenamiento [OOTB]` está configurado para retener eventos durante un máximo de 2 días, después de lo cual se eliminan los eventos.

*Para aumentar el período de retención:*

1. Vaya a la sección **Recursos** → **Almacenamientos**.
2. Abra el `almacenamiento [OOTB]` creado de manera predeterminada.
3. Seleccione la pestaña **Configuración básica**.
4. Cambie la configuración de las **opciones de directiva de retención**.

Puede especificar el valor en días, gigabytes o como porcentaje. Establezca el valor dictado por la directiva de seguridad de su empresa (por ejemplo, 10 días).




Configuración de almacenamiento en KUMA

5. Para guardar los cambios, haga clic en el botón **Guardar**.

6. Para aplicar los cambios, actualice la configuración del servicio:

   a. Vaya a la sección **Recursos** → **Servicios activos**.

   El servicio de `almacenamiento [OOTB]` se muestra en la lista con el estado **Actualización requerida**.

   b. Seleccione la casilla junto al servicio de `almacenamiento [OOTB]` y haga clic en **Actualizar configuración**.

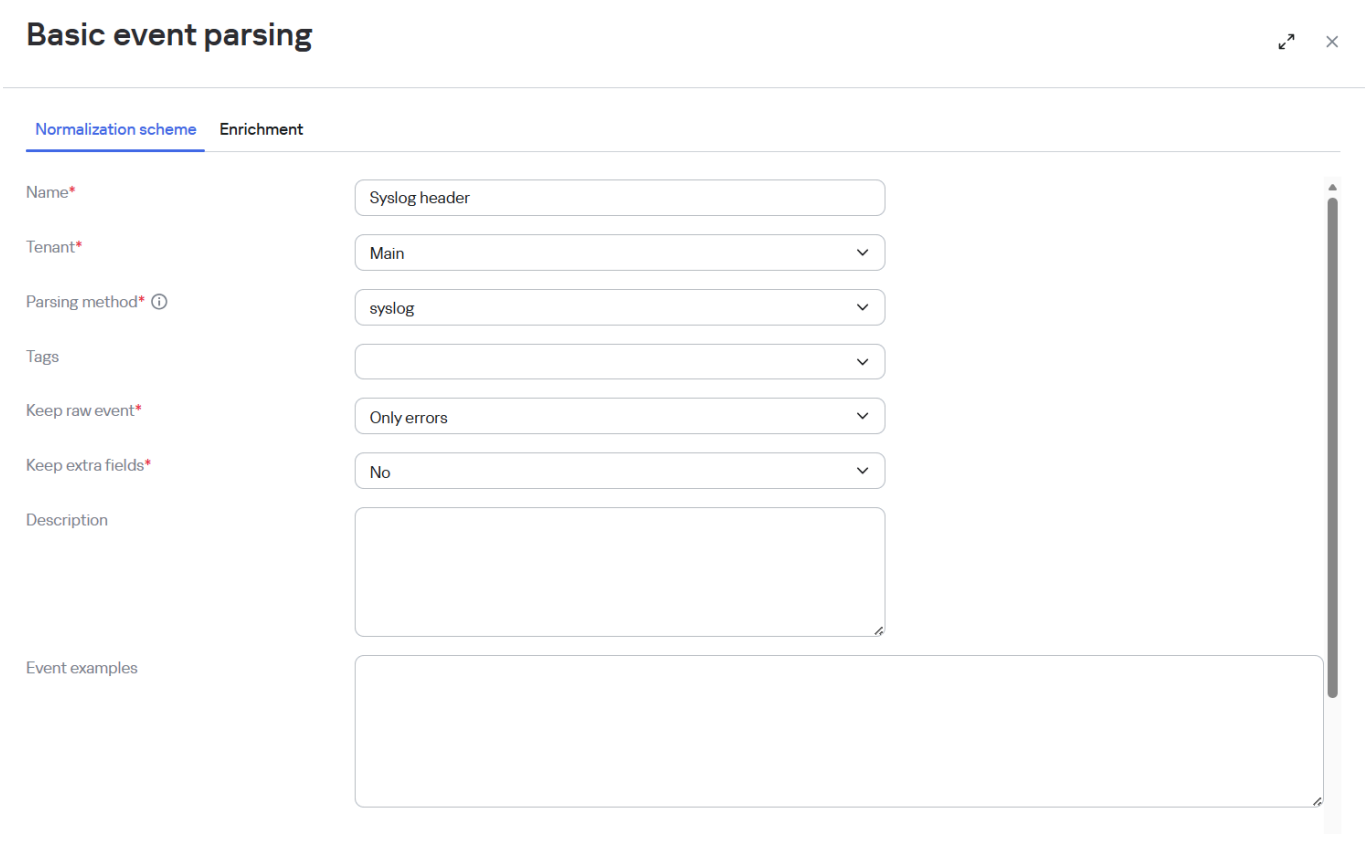
La configuración del servicio se actualiza sin reiniciar el equipo, y los cambios entran en vigor.

# Creación y configuración de un normalizador en KUMA para mensajes de syslog

Para recibir mensajes de syslog del orquestador de SD-WAN y los CPE y convertirlos al modelo de datos de KUMA, debe crear un normalizador.

*Para crear un normalizados, haga lo siguiente:*

1. Vaya a la sección **Recursos** → **Normalizador**.
2. Haga clic en **+ Crear**.
3. Complete los campos en la pestaña **Esquema de normalización**:
   - En el campo **Nombre**, ingrese un nombre para el normalizador, por ejemplo, `Encabezado syslog`.
   - En el campo **Inquilino**, seleccione `Principal`.
   - En el campo **Método de análisis**, seleccione `syslog`.
   - En el campo **Mantener evento sin formato**, seleccione `Solo errores`.
   - En los **campos Conservar adicionales**, seleccione `No`.

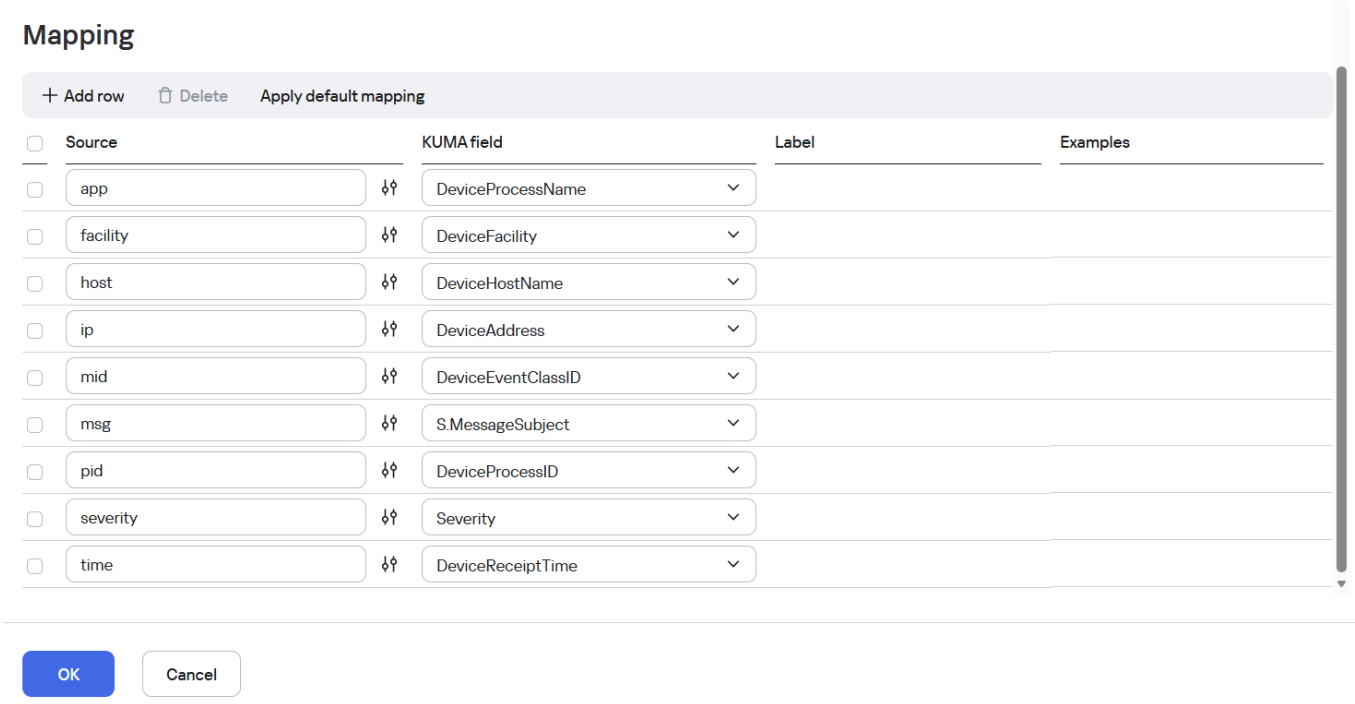



Ajuste de la configuración básica del normalizador en KUMA

4. Configure la asignación de campos:

   a. En la pestaña **Esquema de normalización**, en **Asignación**, haga clic en **Aplicar asignación predeterminada**.

   b. Para el valor `msg` en el campo **Origen**, cambie el valor en el campo **KUMA** a `S.MessageSubject` (admite más caracteres que el estándar 1024).




Configuración de la asignaciónde campos en KUMA

   a. Haga clic en **Aceptar**.

5. Haga clic en **Crear una nueva**.

Se guardan los cambios.

# Configuración del correlacionador y reglas de correlación en KUMA

Para recibir notificaciones de alerta acerca de eventos de seguridad del orquestador SD-WAN y los CPE en KUMA, debe configurar un correlacionador y reglas de correlación.

Un *correlacionador* es un servicio que analiza los eventos recibidos del servicio del recopilador (syslog) de acuerdo con la configuración de las reglas de correlación y genera una notificación de eventos.

Una *regla de correlación* es una regla que describe el indicador de activación y el nivel de gravedad asignado.

## Configuración de reglas de correlación

*Para configurar reglas de correlación:*

1. Vaya a la sección **Recursos** → **Reglas de correlación**.
2. Haga clic en **+ Crear**.
3. En la ventana que se muestra, complete la configuración de la regla de correlación de acuerdo con la tabla.
4. Seleccione la pestaña **Acciones** y active la regla usando el resultado.
5. Repita los pasos para el resto de las reglas de correlación.

Se guardan los cambios.

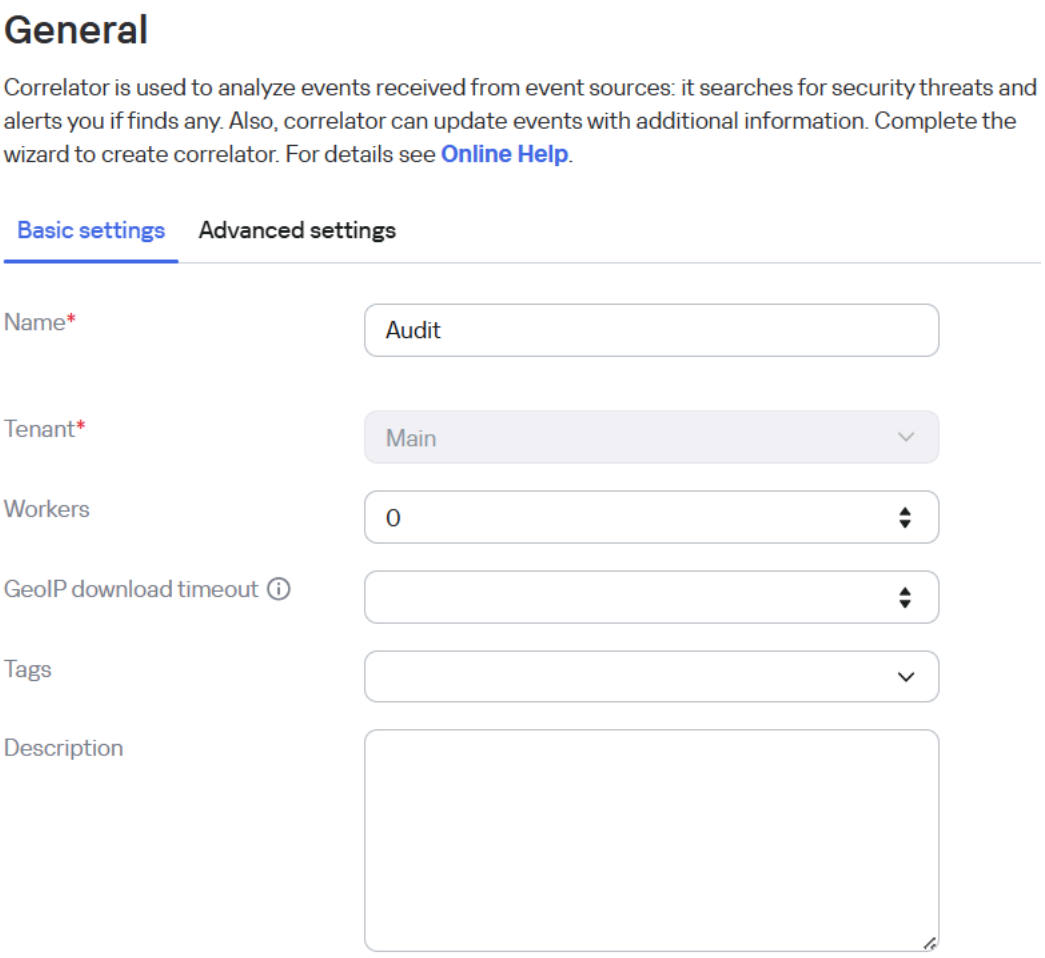
## Configuración de un correlacionador

*Para configurar un correlacionador, siga estos pasos:*

1. Vaya a **Recursos** → **Correlacionadores**.
2. Haga clic en **+ Crear**.

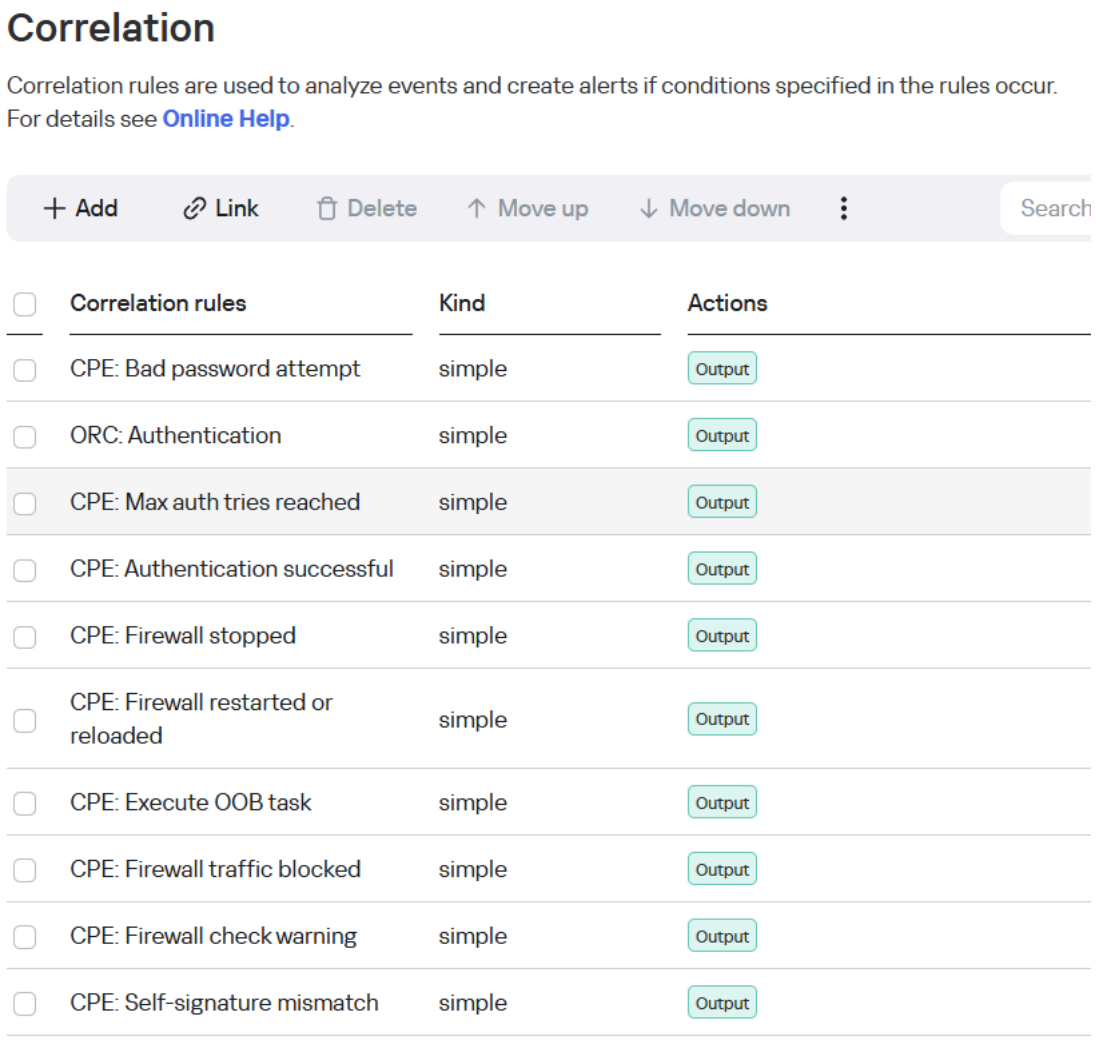
3. En la pestaña **General**, complete los siguientes campos:

- En el campo **Nombre**, escriba un nombre para el correlacionador (por ejemplo, `Auditoría`).
- En el campo **Inquilino**, seleccione `Principal` (seleccione un inquilino diferente si es necesario).




Configuración de correlación en la pestaña **General** en KUMA

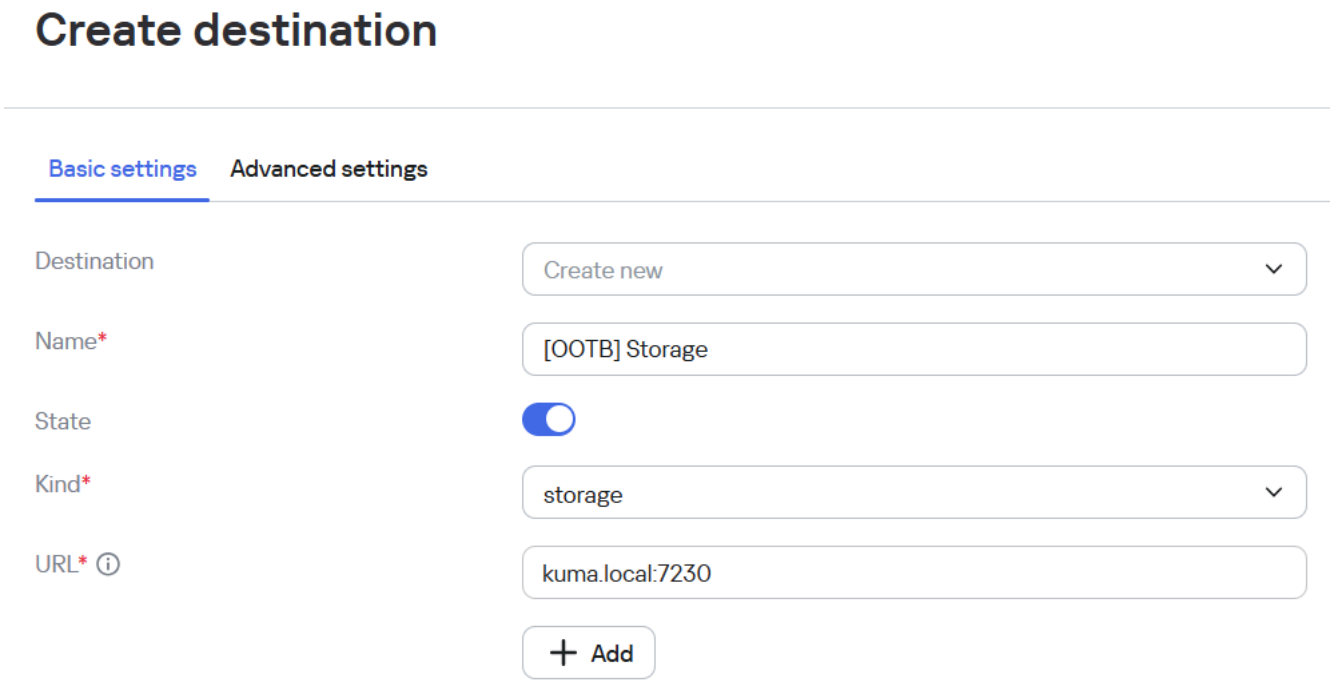
4. En la pestaña **Correlación**, haga clic en **Vínculo** y, en la ventana que se muestra, seleccione todas las reglas de correlación creadas anteriormente de la lista.




Configuración de reglas de correlación en el correlacionador de KUMA

5. En la pestaña **Enrutamiento**, haga clic en **+ Agregar** y complete los campos:

   - En el campo **Tipo**, seleccione `almacenamiento`. Esto hace que se muestre el campo **URL**.
   - En el campo **URL**, seleccione el "Almacenamiento [OOTB]" disponible (seleccione otro si es necesario).
   - El campo **Nombre** se completa automáticamente después de seleccionar una **URL**.




Configuración del correlacionador en la pestaña **Enrutamiento** en KUMA

6. En la pestaña **Validación de la configuración**, haga clic en **Crear y guardar servicio** y obtenga un comando de inicio que debe ejecutar en la línea de comandos del servidor KUMA.

7. Haga clic en **Guardar**.

   Se guardan los cambios.

# Tabla de referencia para crear reglas de correlación KUMA

| Nombre | Tipo | Campos heredados | Nivel de importancia | Selectores | Acciones | Correlacionador |
|---|---|---|---|---|---|---|
| ORC: Auditoría iniciada | simple | Mensaje | Bajo | Message contain SYS-AUD Started: | Procesamiento adicional | Auditoría |
| ORC: Auditoría detenida | simple | Mensaje | Promedio | Message contain SYS-AUD Stopped: | Procesamiento adicional | Auditoría |
| ORC: Cambio de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Any: | Procesamiento adicional | Auditoría |
| ORC: Error de cambio de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE AnyError: | Procesamiento adicional | Auditoría |
| ORC: Creación de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Create: | Procesamiento adicional | Auditoría |
| ORC: Error de creación de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE CreateError: | Procesamiento adicional | Auditoría |

| Nombre | Tipo | Campos heredados | Nivel de importancia | Selectores | Acciones | Correlacionador |
|---|---|---|---|---|---|---|
| ORC: Registro de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Registration: | Procesamiento adicional | Auditoría |
| ORC: Error de registro de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE RegistrationError: | Procesamiento adicional | Auditoría |
| ORC: Eliminación de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Delete: | Procesamiento adicional | Auditoría |
| ORC: Error de eliminación de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE DeleteError: | Procesamiento adicional | Auditoría |
| ORC: Deshabilitación de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Disable: | Procesamiento adicional | Auditoría |
| ORC: Error de deshabilitación de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE DisableError: | Procesamiento adicional | Auditoría |
| ORC: Habilitación de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE Enable: | Procesamiento adicional | Auditoría |
| ORC: Error de habilitación de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE EnableError: | Procesamiento adicional | Auditoría |
| ORC: Plantilla de firewall de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-GEN FirewallTemplate: | Procesamiento adicional | Auditoría |
| ORC: Error de plantilla de firewall de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-GEN FirewallTemplateError: | Procesamiento adicional | Auditoría |
| ORC: Cifrado de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-ENC Encryption: | Procesamiento adicional | Auditoría |
| ORC: Error de cifrado de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-ENC EncryptionError: | Procesamiento adicional | Auditoría |
| ORC: Scripts de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-SCR Scripts: | Procesamiento adicional | Auditoría |
| ORC: Error de scripts de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-SCR ScriptsError: | Procesamiento adicional | Auditoría |
| ORC: Interfaz de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-NET Interface: | Procesamiento adicional | Auditoría |
| ORC: Error de interfaz de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-NET InterfaceError: | Procesamiento adicional | Auditoría |
| ORC: Firewall de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-FW Firewall: | Procesamiento adicional | Auditoría |
| ORC: Error de firewall de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-FW FirewallError: | Procesamiento adicional | Auditoría |
| ORC: Ruta estática de CPE | simple | Mensaje | Bajo | Message contain SDW-CPE-STR StaticRoute: | Procesamiento adicional | Auditoría |
| ORC: Error de ruta estática de CPE | simple | Mensaje | Promedio | Message contain SDW-CPE-STR StaticRouteError: | Procesamiento adicional | Auditoría |
| ORC: Cambio de plantilla de CPE | simple | Mensaje | Bajo | Message contain SDW-CPET Any: | Procesamiento adicional | Auditoría |
| ORC: Error de cambio de plantilla de CPE | simple | Mensaje | Promedio | Message contain SDW-CPET AnyError: | Procesamiento adicional | Auditoría |
| ORC: Cifrado de plantilla de CPE | simple | Mensaje | Bajo | Message contain SDW-CPET-ENC Encryption: | Procesamiento adicional | Auditoría |
| ORC: Error de cifrado de plantilla de CPE | simple | Mensaje | Promedio | Message contain SDW-CPET-ENC EncryptionError: | Procesamiento adicional | Auditoría |
| ORC: Scripts de plantilla de CPE | simple | Mensaje | Bajo | Message contain SDW-CPET-SCR Scripts: | Procesamiento adicional | Auditoría |
| ORC: Error de scripts de plantilla de CPE | simple | Mensaje | Promedio | Message contain SDW-CPET-SCR ScriptsError: | Procesamiento adicional | Auditoría |

| Nombre | Tipo | Campos heredados | Nivel de importancia | Selectores | Acciones | Correlacionador |
|---|---|---|---|---|---|---|
| ORC: Interfaz de plantilla de CPE | simple | Mensaje | Bajo | Message contain SDW-CPET-NET Interface: | Procesamiento adicional | Auditoría |
| ORC: Error de interfaz de plantilla de CPE | simple | Mensaje | Promedio | Message contain SDW-CPET-NET InterfaceError: | Procesamiento adicional | Auditoría |
| ORC: Ruta estática de plantilla de CPE | simple | Mensaje | Bajo | Message contain SDW-CPET-STR StaticRoute: | Procesamiento adicional | Auditoría |
| ORC: Error de ruta estática de plantilla de CPE | simple | Mensaje | Promedio | Message contain SDW-CPET-STR StaticRouteError: | Procesamiento adicional | Auditoría |
| ORC: Plantilla de firewall | simple | Mensaje | Bajo | Message contain SDW-FWT Firewall: | Procesamiento adicional | Auditoría |
| ORC: Error de plantilla de firewall | simple | Mensaje | Promedio | Message contain SDW-FWT FirewallError: | Procesamiento adicional | Auditoría |
| ORC: Plantilla de zona | simple | Mensaje | Bajo | Message contain SDW-FWZ Zone: | Procesamiento adicional | Auditoría |
| ORC: Error de plantilla de zona | simple | Mensaje | Promedio | Message contain SDW-FWZ ZoneError: | Procesamiento adicional | Auditoría |
| ORC: Firmware | simple | Mensaje | Bajo | Message contain SDW-FMW Firmware: | Procesamiento adicional | Auditoría |
| ORC: Error de firmware | simple | Mensaje | Promedio | Message contain SDW-FMW FirmwareError: | Procesamiento adicional | Auditoría |
| ORC: Actualización de firmware | simple | Mensaje | Bajo | Message contain SCH-FMWU FirmwareUpdate: | Procesamiento adicional | Auditoría |
| ORC: Error de actualización de firmware | simple | Mensaje | Promedio | Message contain SCH-FMWU FirmwareUpdateError: | Procesamiento adicional | Auditoría |
| ORC: Configuración de actualización programada | simple | Mensaje | Bajo | Message contain SCH-UPDS UpdateSettings: | Procesamiento adicional | Auditoría |
| ORC: Error de configuración de actualización programada | simple | Mensaje | Promedio | Message contain SCH-UPDS UpdateSettingsError: | Procesamiento adicional | Auditoría |
| ORC: Autenticación de usuario | simple | Mensaje | Bajo | Message contain USR-USR Authentication: | Procesamiento adicional | Auditoría |
| ORC: Error de autenticación de usuario | simple | Mensaje | Promedio | Message contain USR-USR AuthenticationError: | Procesamiento adicional | Auditoría |
| ORC: Cambio de usuario | simple | Mensaje | Bajo | Message contain USR-USR UserChange: | Procesamiento adicional | Auditoría |
| ORC: Permiso de usuario | simple | Mensaje | Bajo | Message contain USR-PERM UserPermissions: | Procesamiento adicional | Auditoría |
| ORC: Llamada de API | simple | Mensaje | Bajo | Message contain SYS-API Call: | Procesamiento adicional | Auditoría |
| ORC: Llamada de API completada | simple | Mensaje | Bajo | Message contain SYS-API CallComplete: | Procesamiento adicional | Auditoría |
| CPE: La autenticación se realizó correctamente | simple | Mensaje | Bajo | DeviceFacility = 10,<br>Severity = 5,<br>Message contains Password auth succeeded | Procesamiento adicional | Auditoría |
| CPE: Se alcanzó el número máximo de intentos de autenticación | simple | Mensaje | Alto | DeviceFacility = 10,<br>Severity = 6,<br>Message contains Max auth tries reached | Procesamiento adicional | Auditoría |
| CPE: Intento de contraseña incorrecto | simple | Mensaje | Promedio | DeviceFacility = 10<br>Severity = 4<br>Message contains Bad password attempt | Procesamiento adicional | Auditoría |

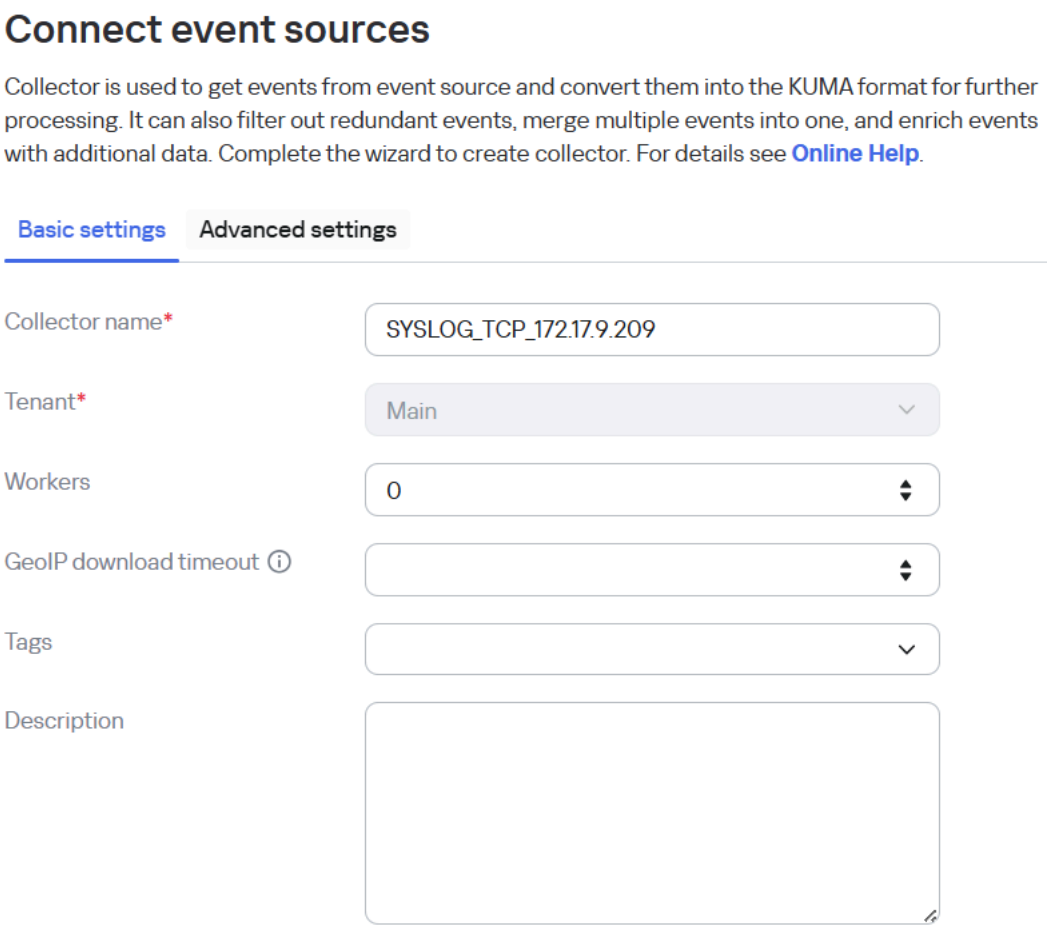
| Nombre | Tipo | Campos heredados | Nivel de importancia | Selectores | Acciones | Correlacionador |
|---|---|---|---|---|---|---|
| CPE: Ejecutar tarea OOB | simple | Mensaje | Bajo | DeviceFacility = 1,<br>Severity = 6,<br>Message contains sdwan-oob: | Procesamiento adicional | Auditoría |
| CPE: Firewall detenido | simple | Mensaje | Crítico | DeviceFacility = 1,<br>Severity = 2,<br>Message contains Firewall stopped | Procesamiento adicional | Auditoría |
| CPE: Firewall iniciado | simple | Mensaje | Bajo | DeviceFacility = 1,<br>Severity = 6,<br>Message contains Firewall started | Procesamiento adicional | Auditoría |
| CPE: Firewall reiniciado o recargado | simple | Mensaje | Promedio | DeviceFacility = 1,<br>Severity = 4,<br>OR<br>Message contains Firewall reloaded<br>Message contains Firewall restarted | Procesamiento adicional | Auditoría |
| CPE: Auditoría de firewall | simple | Mensaje | Bajo | DeviceFacility = 0,<br>Severity = 6,<br>Message contains FW-AUD | Procesamiento adicional | Auditoría |
| CPE: La comprobación de integridad se realizó correctamente | simple | Mensaje | Bajo | DeviceFacility = 1,<br>Severity = 6,<br>Message contains Integrity check successful | Procesamiento adicional | Auditoría |
| CPE: La verificación de integridad falló | simple | Mensaje | Crítico | DeviceFacility = 1,<br>Severity = 2,<br>Message endsWith Integrity check failed | Procesamiento adicional | Auditoría |
| CPE: Incompatibilidad de comprobación | simple | Mensaje | Crítico | DeviceFacility = 1,<br>Severity = 2,<br>Message contains Verification mismatch | Procesamiento adicional | Auditoría |
| CPE: Tráfico de firewall bloqueado | simple | Mensaje | Crítico | DeviceFacility = 1,<br>Severity = 2,Message contains Integrity check failed. Reenvío de tráfico bloqueado | Procesamiento adicional | Auditoría |
| CPE: La comprobación automática de firewall se realizó correctamente | simple | Mensaje | Bajo | DeviceFacility = 1,<br>Severity = 6,<br>Message contains Successful firewall self test | Procesamiento adicional | Auditoría |
| CPE: La comprobación automática de firewall falló | simple | Mensaje | Crítico | DeviceFacility = 1,<br>Severity = 2,<br>Message contains Firewall self test failed | Procesamiento adicional | Auditoría |
| CPE: Dispositivo USB insertado | simple | Mensaje | Promedio | DeviceFacility = 0,<br>Severity = 6,<br>OR<br>Message contains USB deviceMessage contains Storage device detected | Procesamiento adicional | Auditoría |
| CPE: Dispositivo USB montado | simple | Mensaje | Alto | DeviceFacility = 0,<br>Severity = 6,<br>Message contains mounted filesystem | Procesamiento adicional | Auditoría |
| CPE: Salto de tiempo detectado | simple | Mensaje | Promedio | DeviceFacility = 3,<br>Severity = 4,<br>Message contains time jump detected | Procesamiento adicional | Auditoría |

# Configuración de un recopilador para eventos syslog en KUMA

Para recibir mensajes de syslog del orquestador SD-WAN y los dispositivos CPE, debe crear un recopilador de KUMA.

*Para configurar un recopilador de KUMA:*

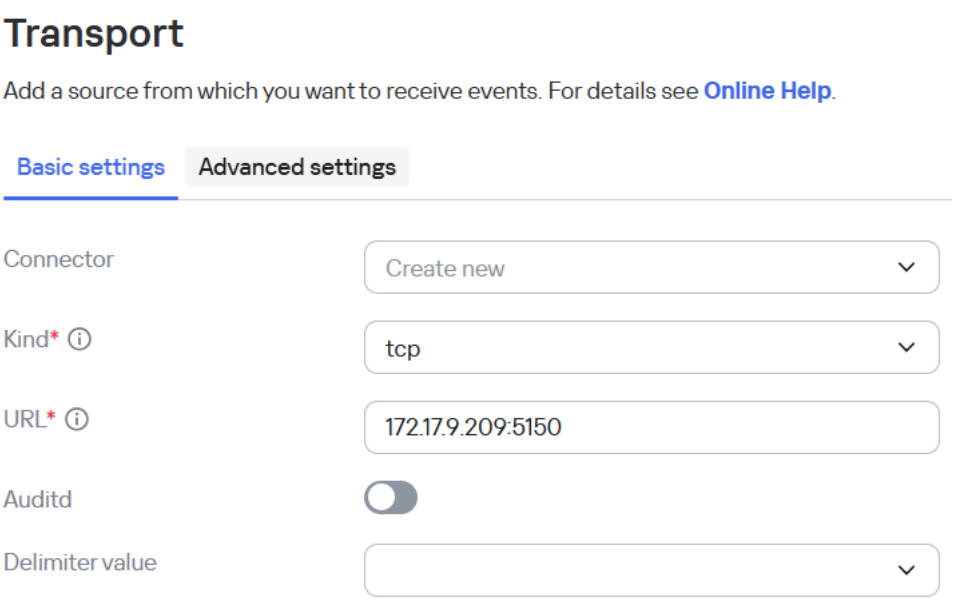
1. Vaya a **Recursos** → **Recopiladores**.
2. Haga clic en **+ Crear**.
3. En la pestaña **Conectar orígenes de eventos** → **Configuración básica**, complete los campos:
   - En el campo **Nombre del recopilador**, ingrese un nombre para el recopilador (por ejemplo, `SYSLOG_TCP_172.17.9.209`).
   - En el campo **Inquilino**, seleccione `Principal` (seleccione un inquilino diferente si es necesario).




Configuración del recopilador en la pestaña **Conectar orígenes de eventos** → **Configuración básica** en KUMA

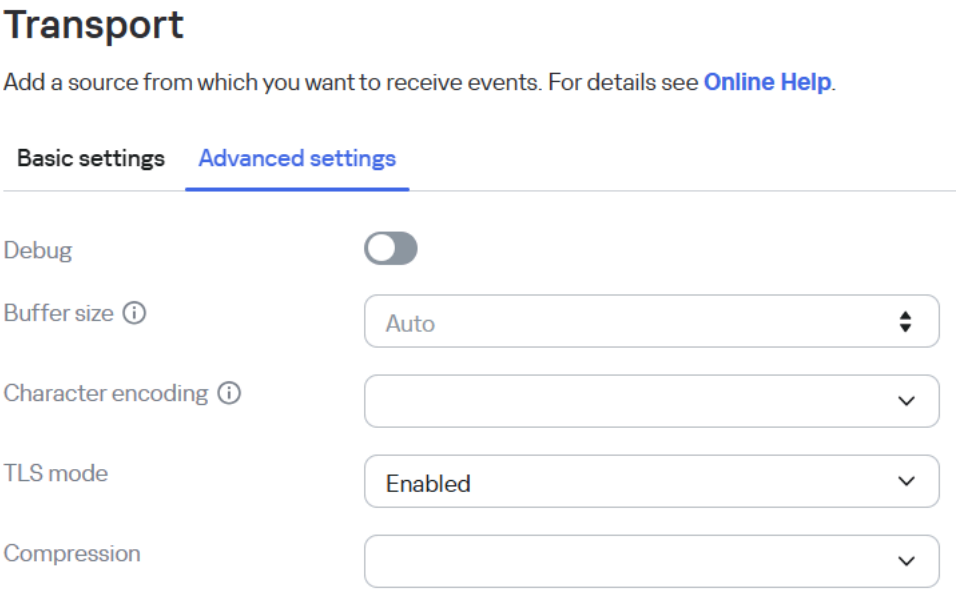
4. En la pestaña **Transporte** → **Configuración básica**, complete los siguientes campos:

   - En el campo **Tipo**, seleccione `tcp`.
   - En el campo **URL**, ingrese `<dirección IP>:<puerto>` (por ejemplo, 172.17.9.209:5150).




Configuración del recopilador en la pestaña **Transporte** → **Configuración básica** en KUMA

5. En la pestaña **Transporte** → **Configuración avanzada**, en el campo **Modo TLS**, seleccione **Habilitado**.

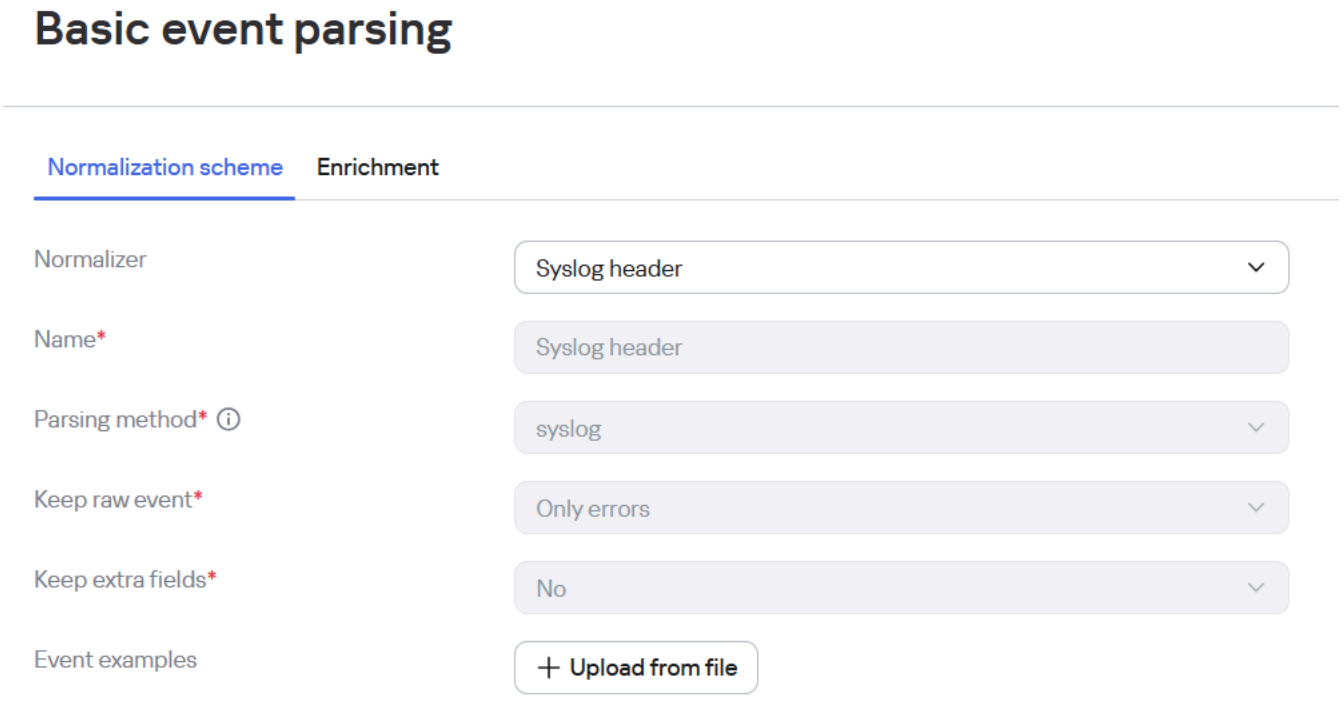



Configuración del recopilador en la pestaña **Transporte** → **Configuración avanzada** en KUMA

6. En la pestaña **Análisis de eventos**, haga clic en **+ Agregar análisis de eventos** y, en el campo **Normalizador**, seleccione la plantilla `encabezado syslog` creada anteriormente.

   Todos los demás campos se completan automáticamente.

7. Haga clic en **Aceptar**.




Configuración del recopilador en la pestaña **Análisis de eventos** en KUMA

8. En la pestaña **Enrutamiento**, haga clic en **+ Agregar** y complete los campos:

   - En el campo **Tipo**, seleccione `almacenamiento`. Esto hace que se muestre el campo **URL**.
   - En el campo **URL**, seleccione el "Almacenamiento [OOTB]" disponible (seleccione otro si es necesario).
   - El campo **Nombre** se completa automáticamente después de seleccionar una **URL**.

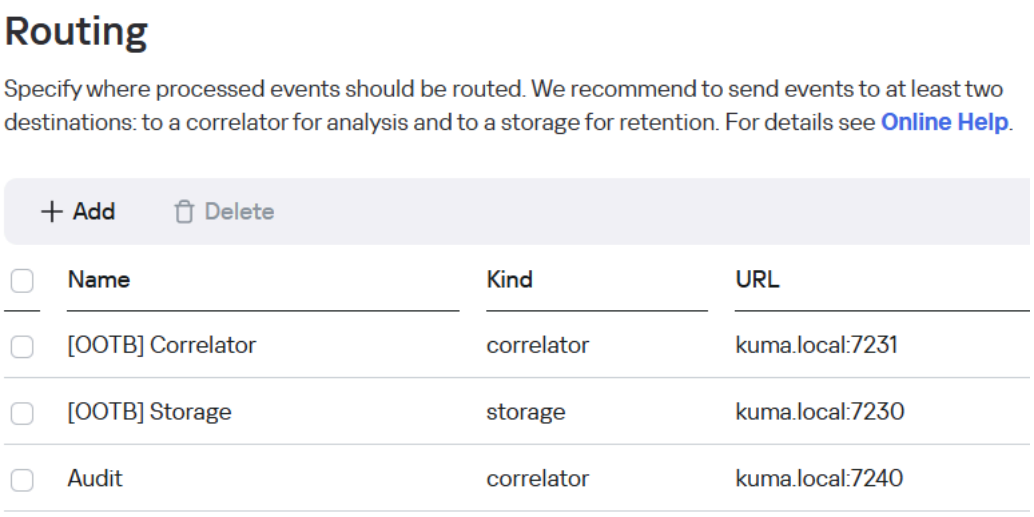
9. En la pestaña **Enrutamiento**, haga clic en **+ Agregar** y complete los campos:

   - En el campo **Tipo**, seleccione `correlacionador`. Esto hace que se muestre el campo **URL**.
   - En el campo **URL**, seleccione un correlacionador [OOTB] disponible.

     Si se requiere un procesamiento adicional de los eventos recibidos, deberá configurar el correlacionador de auditoría. Puede crear un nuevo correlacionador más adelante.
   - El campo **Nombre** se completa automáticamente después de seleccionar una **URL**.

10. En la pestaña **Enrutamiento**, haga clic en **+ Agregar** y complete los campos:

    - En el campo **Tipo**, seleccione `correlacionador`. Esto hace que se muestre el campo **URL**.
    - En el campo **URL**, seleccione `Auditoría`.
    - El campo **Nombre** se completa automáticamente después de seleccionar una **URL**.




Configuración del recopilador en la pestaña **Enrutamiento** en KUMA

11. En la pestaña **Validación de la configuración**, haga clic en **Crear y guardar servicio** y obtenga un comando de inicio que debe ejecutar en la línea de comandos del servidor KUMA.

12. Haga clic en **Guardar**.

    Se guardan los cambios.

# Configuración del servicio de correo en KUMA

Para recibir notificaciones por correo electrónico de los servicios del sistema KUMA y eventos configurados por el usuario, debe configurar un servidor SMTP.

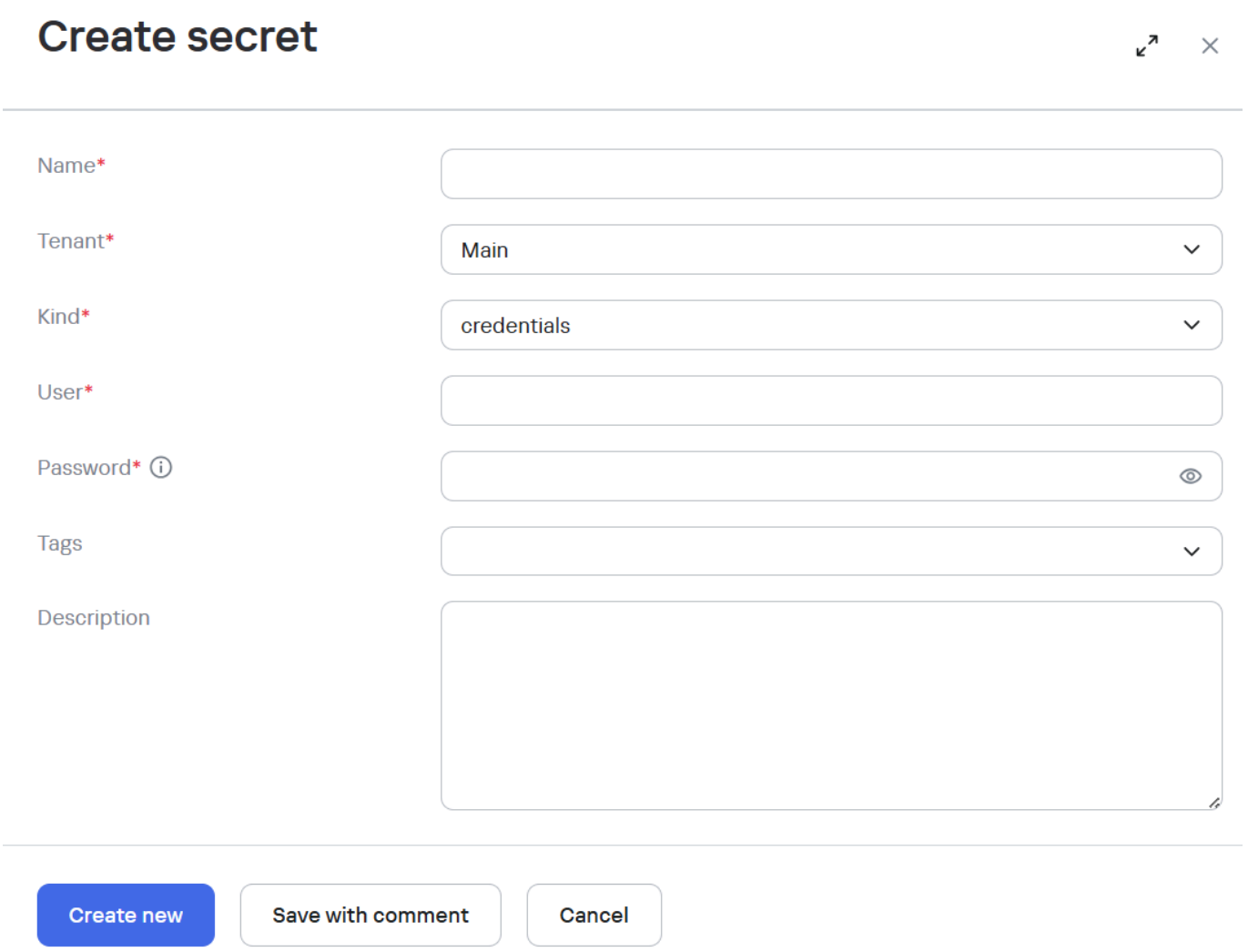
*Para configurar el servicio de correo:*

1. Vaya a **Recursos** → **Secretos**.

2. Haga clic en **+ Crear** y complete los campos:

    - En el campo **Nombre**, ingrese un nombre para la directiva.
    - En el campo **Inquilino**, seleccione `Principal` (seleccione un inquilino diferente si es necesario).
    - En el campo **Tipo**, seleccione `credenciales`.
    - En el campo **Usuario**, especifique la cuenta en el servidor SMTP.
    - En el campo **Contraseña**, ingrese la contraseña de la cuenta en el servidor SMTP.

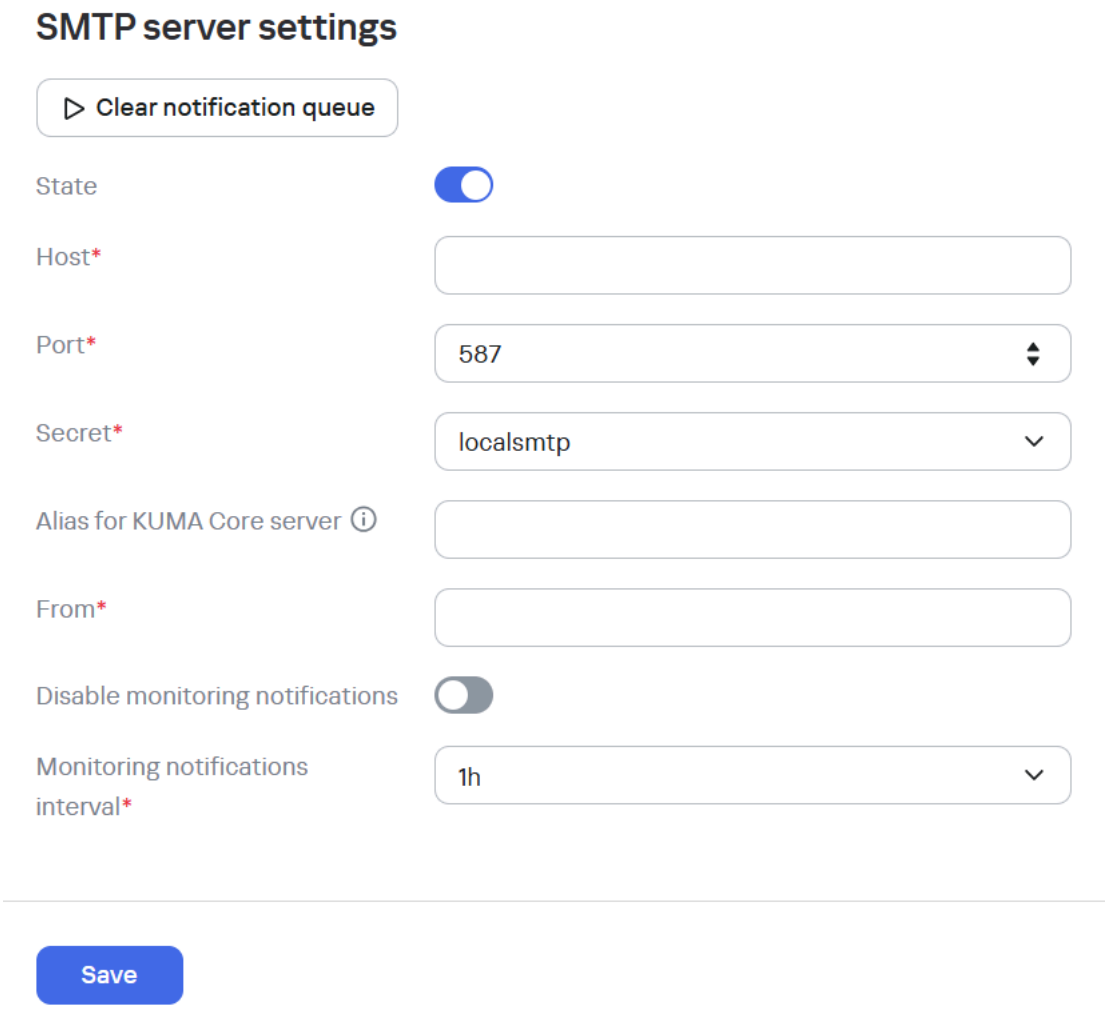
- El campo **Etiquetas** es opcional.
- El campo **Descripción** es opcional.




Configuración del servicio de correo en **Recursos** → **Secretos** en KUMA

3. Vaya a la sección **Configuración** → **Otro** → **Común**.
4. En la sección **Configuración del servidor SMTP**, complete los siguientes campos:
   - Habilite el botón de alternancia **Estado**.
   - En el campo **Host**, especifique la dirección IP o el nombre de dominio del servidor SMTP.
   - En el campo **Puerto**, ingrese el número de puerto del servidor SMTP.
   - En el campo **Secreto**, seleccione la directiva configurada anteriormente.
   - El campo **Alias para el servidor KUMA Core** es opcional.
   - En el campo **De**, ingrese la dirección de correo electrónico desde la cual se enviarán los mensajes al usuario.

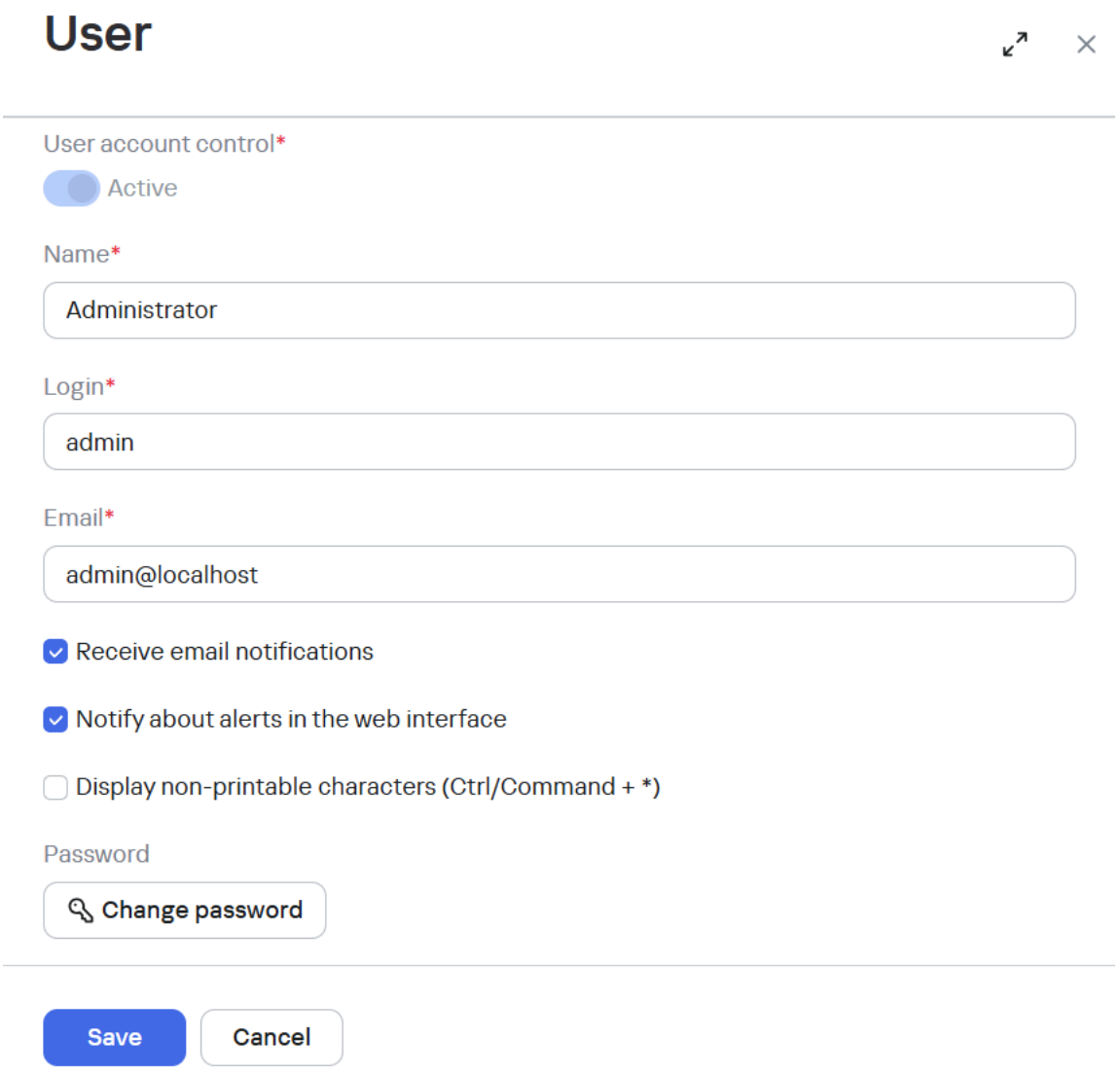
- No modifique el campo **Deshabilitar notificaciones de supervisión**.
- Establezca el **Intervalo de notificaciones de supervisión** en 1h (o un valor diferente si es necesario).




Configuración del servicio de correo en la sección **Configuración** → **Otro** → **Común** en KUMA

5. Para activar el envío de mensajes de correo electrónico, vaya al perfil de Administrador (**Administrador** → **Perfil**) y complete los siguientes campos:

   - En el campo **Correo electrónico**, especifique la dirección de correo electrónico del Administrador.
   - Seleccione la casilla **Recibir notificaciones por correo electrónico**.
   - Seleccione la casilla **Notificar acerca de alertas en la interfaz web**.




Perfil de administrador en KUMA

Se guardan los cambios.

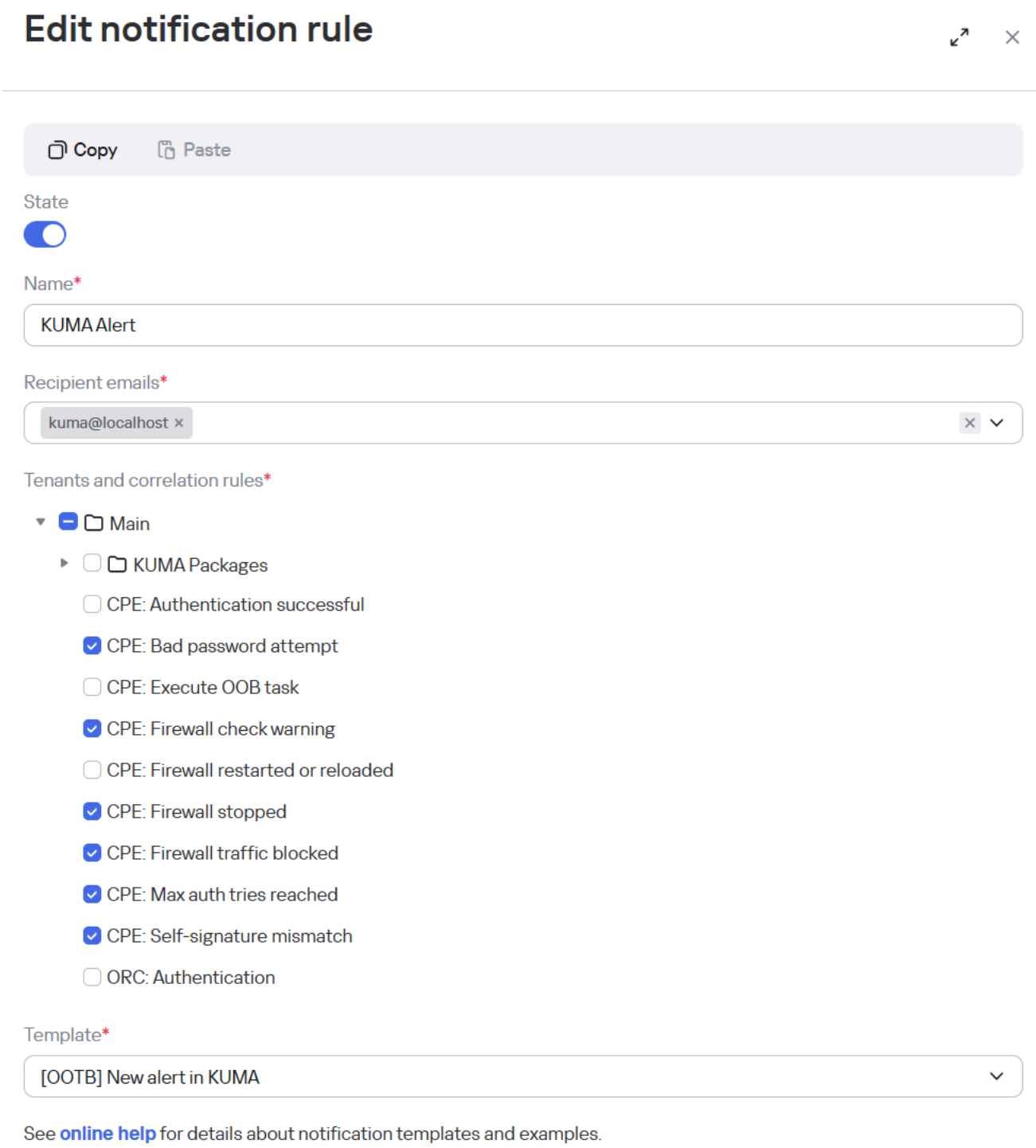
# Configuración de reglas de notificación en KUMA

Para recibir notificaciones por correo electrónico del orquestador de SD-WAN y los CPE, debe configurar las reglas de notificación.

*Para configurar las reglas de notificación:*

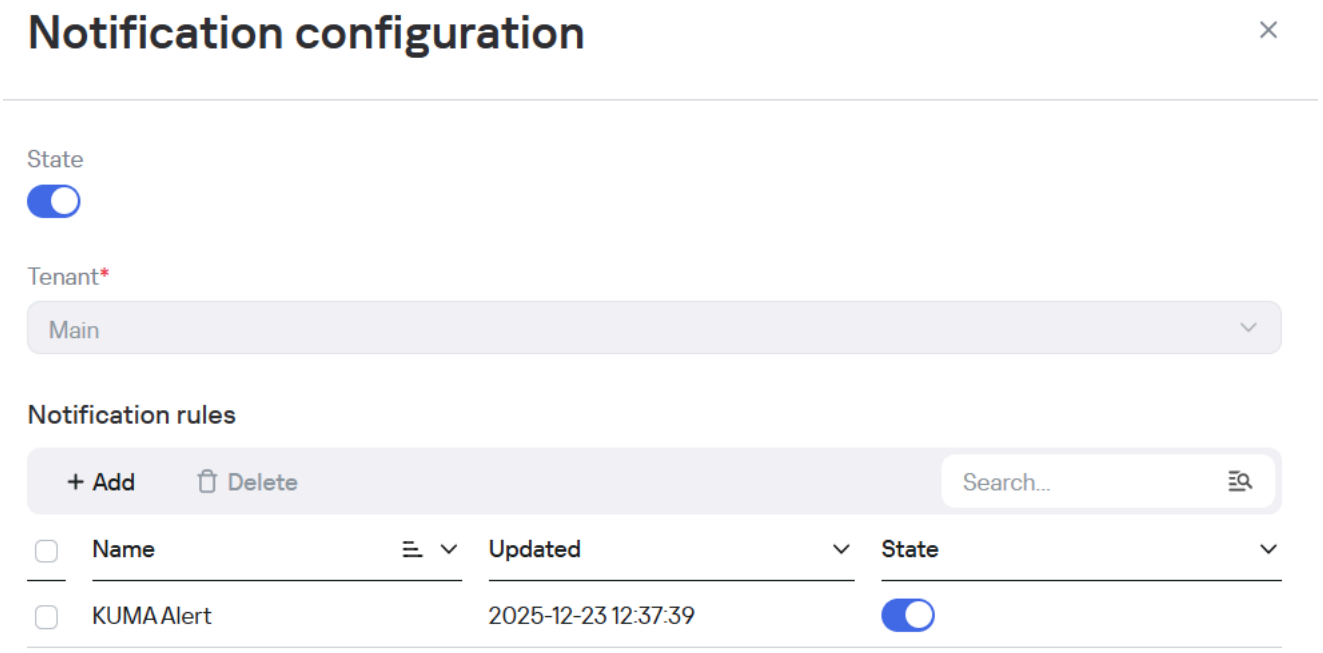
1. Vaya a la sección **Configuración** → **Otro** → **Alertas** y seleccione la pestaña **Reglas de notificación**
2. Haga clic en **+ Agregar configuración para un nuevo inquilino** y complete los campos.
   - Habilite el botón de alternancia **Estado**.
   - En el campo **Inquilino**, seleccione `Principal` (seleccione un inquilino diferente si es necesario).
3. Haga clic en **+ Agregar** y complete los campos:
   - Habilite el botón de alternancia **Estado**.
   - En el campo **Nombre**, ingrese un nombre para la regla (por ejemplo, "Alerta KUMA").
   - En el campo **Correos electrónicos de los destinatarios**, especifique las direcciones de correo electrónico de los usuarios.
   - En **Inquilinos y reglas de correlación**, seleccione las reglas para las que desea recibir notificaciones por correo electrónico.
   - En el campo **Plantilla**, seleccione la plantilla de correo electrónico predeterminada `[OOTB] Nueva alerta en KUMA` o cree una propia

4. Haga clic en **Guardar**.




Configuración de la regla de notificación en KUMA

5. Haga clic en **Guardar**.




Configuración de la regla de notificación en KUMA

Se guardan los cambios.

# Ejemplos de configuración para la búsqueda por eventos clave en KUMA

Para buscar ciertos eventos de seguridad, puede usar una consulta SQL a la base de datos (en la sección **Eventos** → **SQL Builder**). Con SQL Builder, puede crear consultas y guardarlas para reutilizarlas rápidamente.

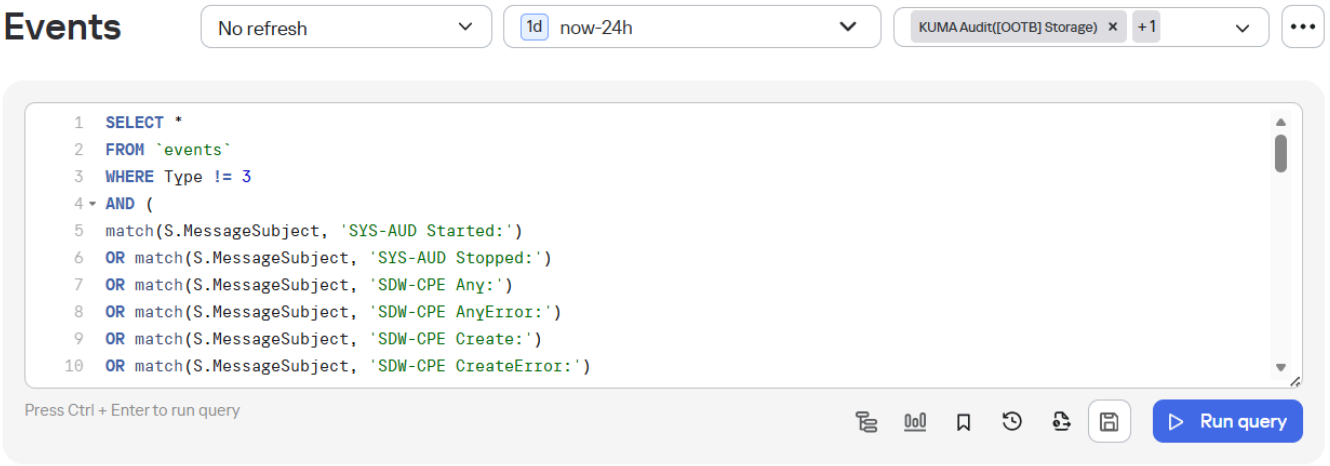
## Creación de una consulta SQL

*Para crear una consulta SQL:*

1. Vaya a la sección **Eventos** y busque el campo **Eventos** con la consulta SQL predeterminado.

2. Elimine el contenido de la consulta SQL predeterminado.

3. Copie y pegue una consulta SQL de los ejemplos en esta sección.

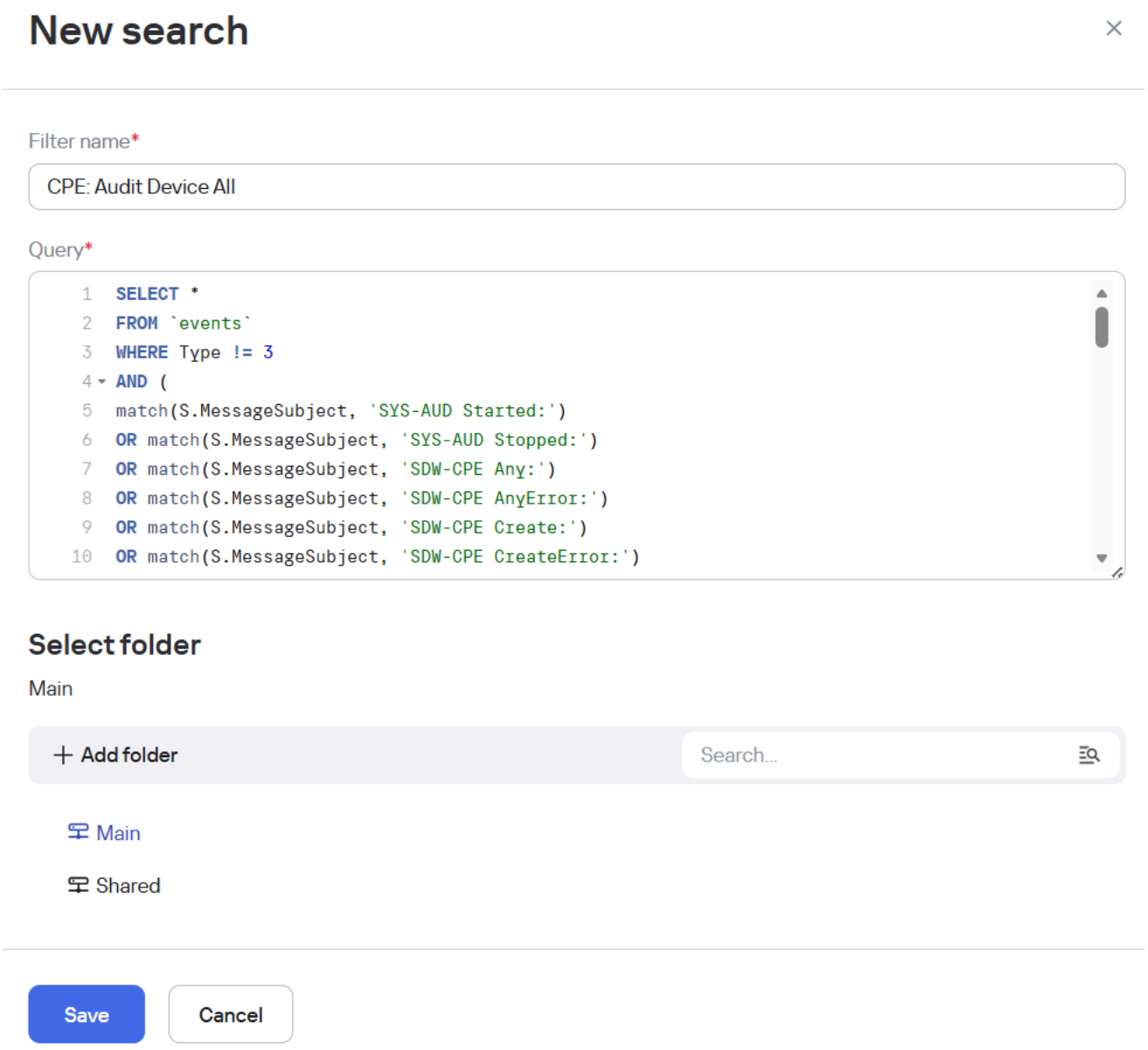



Sección **Eventos** en KUMA

4. Haga clic en **Guardar filtro actual** y complete los campos:

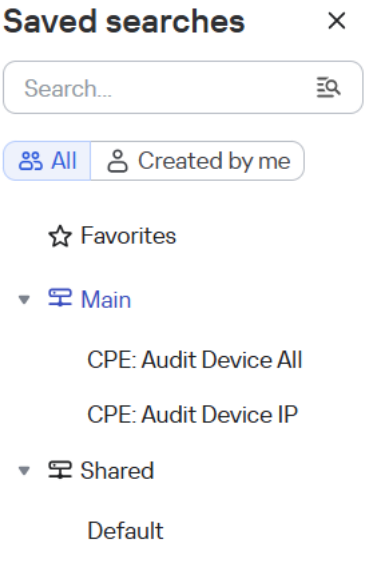
- En el campo **Nombre de filtro**, escriba un nombre para la consulta SQL.
- En el campo **Consulta**, ingrese el texto de la consulta SQL.
- En el campo **Seleccionar carpeta**, seleccione `Principal`.

5. Haga clic en **Guardar** para guardar la consulta.



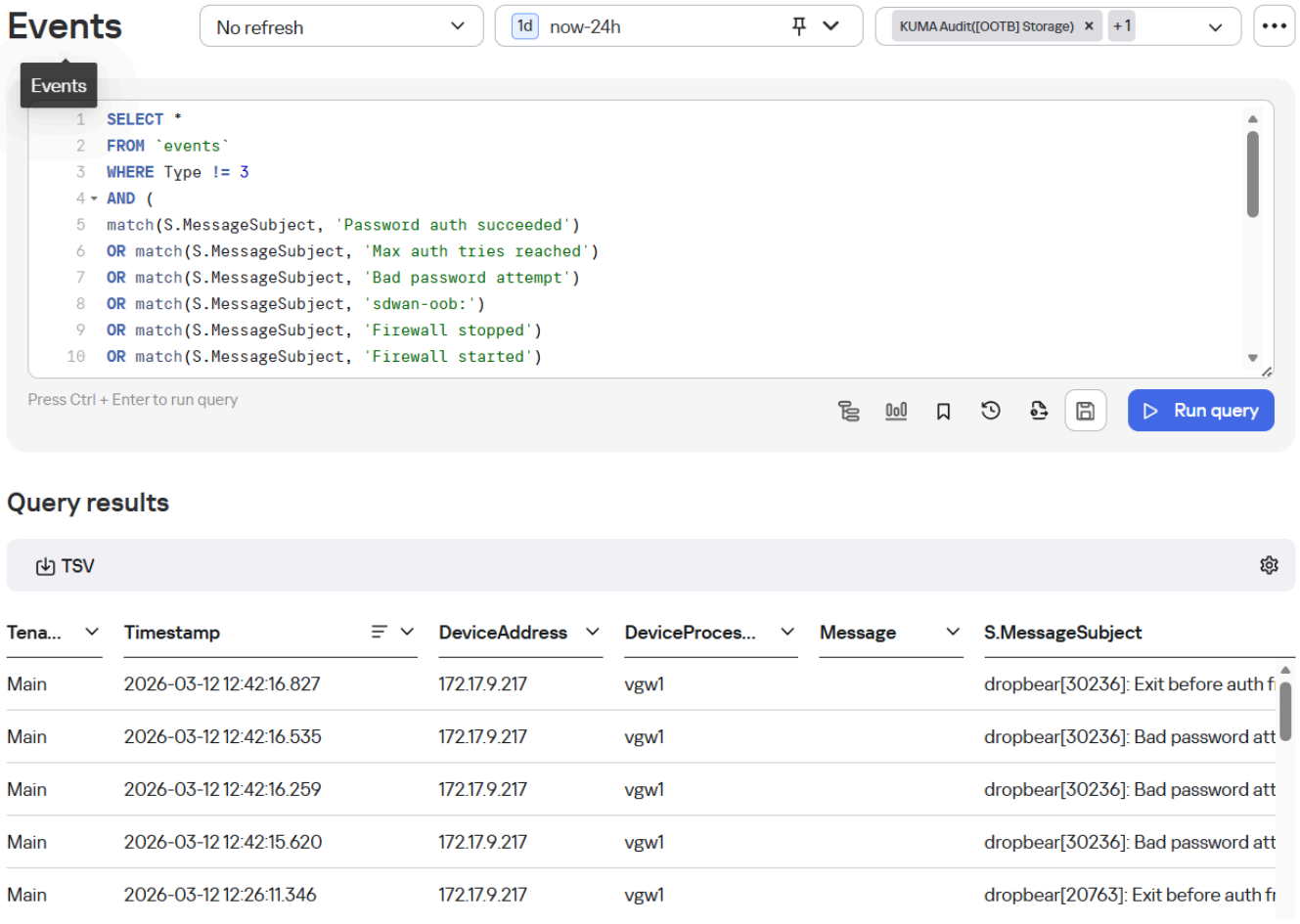

Configuración de la consulta SQL en KUMA

6. Haga clic en **Búsquedas guardadas** para ver las consultas SQL guardadas.




Consultas SQL guardadas en KUMA

7. Seleccione una consulta SQL y haga clic en **Ejecutar consulta** para mostrar todos los eventos que coinciden con la consulta.




Resultado de una consulta SQL en KUMA

## Ejemplos de consultas SQL

Nombre: ORC: Auditar todas las notificaciones de seguridad

Descripción: Buscar todos los eventos de seguridad en el CPE (excluir las reglas de correlación que informan acerca de la creación del Tipo de alarma !=3)

```
SELECT *
FROM `events`
WHERE Type != 3
AND (
match(S.MessageSubject, 'SYS-AUD Started:')
OR match(S.MessageSubject, 'SYS-AUD Stopped:')
OR match(S.MessageSubject, 'SDW-CPE Any:')
OR match(S.MessageSubject, 'SDW-CPE AnyError:')
OR match(S.MessageSubject, 'SDW-CPE Create:')
OR match(S.MessageSubject, 'SDW-CPE CreateError:')
OR match(S.MessageSubject, 'SDW-CPE Registration:')
OR match(S.MessageSubject, 'SDW-CPE RegistrationError:')
OR match(S.MessageSubject, 'SDW-CPE Delete:')
OR match(S.MessageSubject, 'SDW-CPE DeleteError:')
OR match(S.MessageSubject, 'SDW-CPE Disable:')
OR match(S.MessageSubject, 'SDW-CPE DisableError:')
OR match(S.MessageSubject, 'SDW-CPE Enable:')
OR match(S.MessageSubject, 'SDW-CPE EnableError:')
OR match(S.MessageSubject, 'SDW-CPE-GEN FirewallTemplate:')
OR match(S.MessageSubject, 'SDW-CPE-GEN FirewallTemplateError:')
OR match(S.MessageSubject, 'SDW-CPE-ENC Encryption:')
OR match(S.MessageSubject, 'SDW-CPE-ENC EncryptionError:')
OR match(S.MessageSubject, 'SDW-CPE-SCR Scripts:')
OR match(S.MessageSubject, 'SDW-CPE-SCR ScriptsError:')
OR match(S.MessageSubject, 'SDW-CPE-NET Interface:')
OR match(S.MessageSubject, 'SDW-CPE-NET InterfaceError:')
OR match(S.MessageSubject, 'SDW-CPE-FW Firewall:')
OR match(S.MessageSubject, 'SDW-CPE-FW FirewallError:')
OR match(S.MessageSubject, 'SDW-CPE-STR StaticRoute:')
OR match(S.MessageSubject, 'SDW-CPE-STR StaticRouteError:')
OR match(S.MessageSubject, 'SDW-CPET Any:')
OR match(S.MessageSubject, 'SDW-CPET AnyError:')
OR match(S.MessageSubject, 'SDW-CPET-ENC Encryption:')
OR match(S.MessageSubject, 'SDW-CPET-ENC EncryptionError:')
OR match(S.MessageSubject, 'SDW-CPET-SCR Scripts:')
OR match(S.MessageSubject, 'SDW-CPET-SCR ScriptsError:')
OR match(S.MessageSubject, 'SDW-CPET-NET Interface:')
OR match(S.MessageSubject, 'SDW-CPET-NET InterfaceError:')
OR match(S.MessageSubject, 'SDW-CPET-STR StaticRoute:')
OR match(S.MessageSubject, 'SDW-CPET-STR StaticRouteError:')
OR match(S.MessageSubject, 'SDW-FWT Firewall:')
OR match(S.MessageSubject, 'SDW-FWT FirewallError:')
OR match(S.MessageSubject, 'SDW-FWZ Zone:')
OR match(S.MessageSubject, 'SDW-FWZ ZoneError:')
OR match(S.MessageSubject, 'SDW-FMW Firmware:')
OR match(S.MessageSubject, 'SDW-FMW FirmwareError:')
OR match(S.MessageSubject, 'SCH-FMWU FirmwareUpdate:')
OR match(S.MessageSubject, 'SCH-FMWU FirmwareUpdateError:')
OR match(S.MessageSubject, 'SCH-UPDS UpdateSettings:')
OR match(S.MessageSubject, 'SCH-UPDS UpdateSettingsError:')
OR match(S.MessageSubject, 'USR-USR Authentication:')
OR match(S.MessageSubject, 'USR-USR AuthenticationError:')
OR match(S.MessageSubject, 'USR-USR UserChange:')
OR match(S.MessageSubject, 'USR-PERM UserPermissions:')
OR match(S.MessageSubject, 'SYS-API Call:')
OR match(S.MessageSubject, 'SYS-API CallComplete:')
)
ORDER BY Timestamp DESC
LIMIT 500;
```

Nombre: CPE: Auditar todos los dispositivos

Descripción: Buscar todos los eventos de seguridad en el CPE

```
SELECT *
FROM `events`
WHERE Type != 3
AND (
match(S.MessageSubject, 'Password auth succeeded')
OR match(S.MessageSubject, 'Max auth tries reached')
OR match(S.MessageSubject, 'Bad password attempt')
OR match(S.MessageSubject, 'sdwan-oob:')
OR match(S.MessageSubject, 'Firewall stopped')
OR match(S.MessageSubject, 'Firewall started')
OR match(S.MessageSubject, 'Firewall reloaded')
OR match(S.MessageSubject, 'Firewall restarted')
OR match(S.MessageSubject, 'FW-AUD')
OR match(S.MessageSubject, 'Integrity check successful')
OR match(S.MessageSubject, 'Integrity check failed')
OR match(S.MessageSubject, 'Verification mismatch')
OR match(S.MessageSubject, 'Traffic forwarding blocked')
OR match(S.MessageSubject, 'Successful firewall self test')
OR match(S.MessageSubject, 'Firewall self test failed')
OR match(S.MessageSubject, 'USB device')
OR match(S.MessageSubject, 'Storage device detected')
OR match(S.MessageSubject, 'mounted filesystem')
OR match(S.MessageSubject, 'time jump detected')
)
ORDER BY Timestamp DESC
LIMIT 500;
```

Nombre: CPE: Auditar todas las direcciones IP del dispositivo

Descripción: Buscar todos los eventos de seguridad en el CPE por una dirección IP específica

```
SELECT *
FROM `events`
WHERE DeviceAddress = '172.17.9.223' AND Type != 3
AND (
match(S.MessageSubject, 'Password auth succeeded')
OR match(S.MessageSubject, 'Max auth tries reached')
OR match(S.MessageSubject, 'Bad password attempt')
OR match(S.MessageSubject, 'sdwan-oob:')
OR match(S.MessageSubject, 'Firewall stopped')
OR match(S.MessageSubject, 'Firewall started')
OR match(S.MessageSubject, 'Firewall reloaded')
OR match(S.MessageSubject, 'Firewall restarted')
OR match(S.MessageSubject, 'FW-AUD')
OR match(S.MessageSubject, 'Integrity check successful')
OR match(S.MessageSubject, 'Integrity check failed')
OR match(S.MessageSubject, 'Verification mismatch')
OR match(S.MessageSubject, 'Traffic forwarding blocked')
OR match(S.MessageSubject, 'Successful firewall self test')
OR match(S.MessageSubject, 'Firewall self test failed')
OR match(S.MessageSubject, 'USB device')
OR match(S.MessageSubject, 'Storage device detected')
OR match(S.MessageSubject, 'mounted filesystem')
OR match(S.MessageSubject, 'time jump detected')
)
ORDER BY Timestamp DESC
LIMIT 500;
```

# Integración con Kaspersky CyberSecurity for Networks

Puede integrar Kaspersky SD-WAN con Kaspersky Industrial CyberSecurity for Networks para reenviar el tráfico SPAN desde las interfaces de servicio de los dispositivos CPE a las interfaces de red de los nodos de Kaspersky Industrial CyberSecurity for Networks. Antes de configurar la integración, tendrá que habilitar el cifrado de tráfico en los dispositivos CPE desde cuyas interfaces de servicio desea reenviar el tráfico SPAN. Recomendamos asignar los dispositivos CPE a una red específica de Kaspersky Industrial CyberSecurity

https://support.kaspersky.com/help/KICSforNetworks/4.2/en-US/102350.htm

.

El tráfico SPAN se identifica con etiquetas de la VLAN que se agregan a los paquetes de tráfico de acuerdo con el estándar IEEE 802.1q. Debe asegurarse de que las etiquetas de la VLAN que coinciden se utilicen en las interfaces de servicio de los dispositivos CPE y en las interfaces de red de los nodos de Kaspersky Industrial CyberSecurity for Networks.

Para lograr una integración eficaz de Kaspersky SD-WAN con Kaspersky Industrial CyberSecurity for Networks, puede aumentar el límite en la cantidad de puntos de control con la configuración adicional de los componentes de Kaspersky Industrial CyberSecurity for Networks. Límites máximos posibles:

- Hasta 100 puntos de control en un nodo de Kaspersky Industrial CyberSecurity for Networks
- Hasta 100 puntos de control en total en un nodo de Kaspersky Industrial CyberSecurity for Networks

El resto de los requisitos para la implementación de los componentes de Kaspersky Industrial CyberSecurity for Networks son similares a los de otros escenarios de implementación, por ejemplo, la instalación de un servidor sin sensores externos

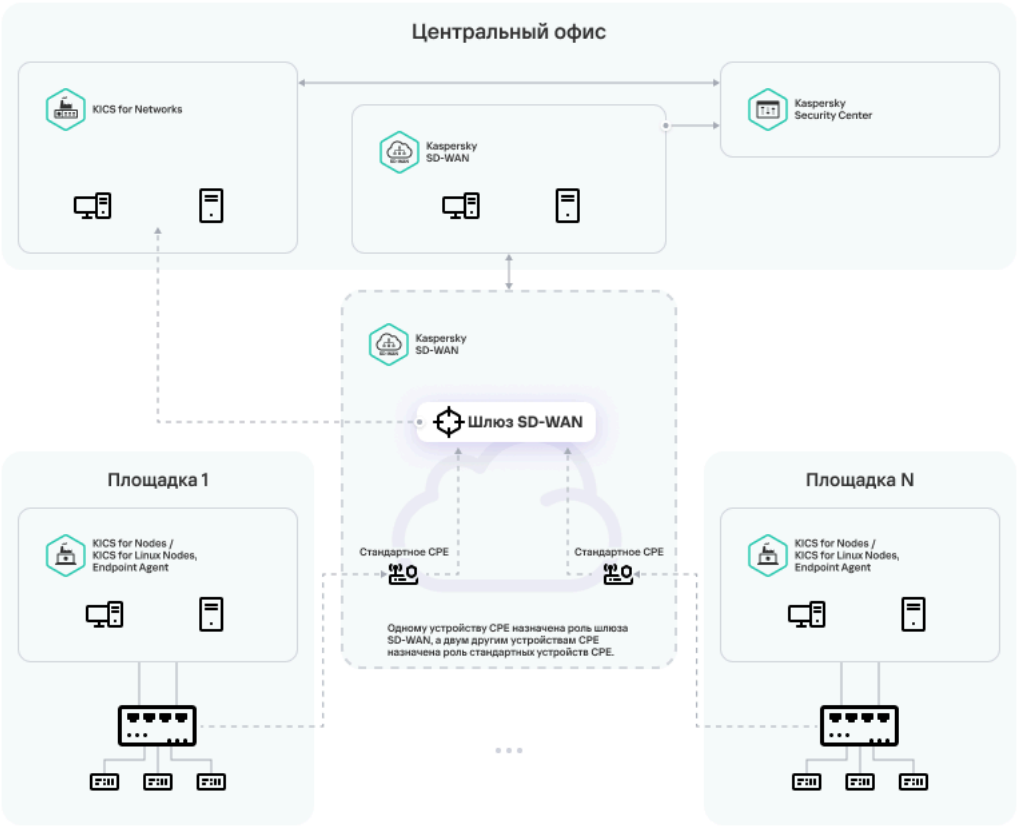
https://support.kaspersky.com/help/KICSforNetworks/4.2/en-US/206298.htm

.

> Si necesita más información sobre cómo configurar los componentes de Kaspersky Industrial CyberSecurity for Networks para que se integren con Kaspersky SD-WAN, comuníquese con su administrador técnico de cuentas (TAM).

También puede obtener más información acerca de la integración de Kaspersky SD-WAN y Kaspersky Industrial CyberSecurity for Networks en la sección Apéndices.

En la siguiente figura, se muestra un escenario de implementación de ejemplo en el caso de Kaspersky SD-WAN y Kaspersky Industrial CyberSecurity for Networks. Las líneas de puntos indican la ruta del tráfico SPAN. Primero, los conmutadores de red de las ubicaciones remotas 1 y N duplican el tráfico a los dispositivos CPE con la función del dispositivo CPE estándar. Luego, los dispositivos CPE estándar reenvían el tráfico SPAN al dispositivo CPE con la función de la puerta de enlace de SD-WAN, que a su vez reenvía el tráfico SPAN al servidor de Kaspersky Industrial CyberSecurity for Networks. Los componentes de Kaspersky SD-WAN y Kaspersky Industrial CyberSecurity for Networks se encuentran en la oficina central de la organización.




Ejemplo de integración de Kaspersky SD-WAN con Kaspersky Industrial CyberSecurity for Networks

# Ponerse en contacto con el Servicio de soporte técnico

En esta sección se describe cómo obtener soporte técnico y las condiciones en las que está disponible.

## Cómo obtener Servicio de soporte técnico

Si no puede encontrar una solución para su problema en la documentación del programa o en una de las otras fuentes de información sobre Kaspersky SD-WAN, comuníquese con Soporte técnico. El equipo de Soporte técnico responderá a sus preguntas sobre la instalación y el uso de Kaspersky SD-WAN.

Kaspersky ofrece soporte para Kaspersky SD-WAN durante todo su ciclo de vida (consulte la página del ciclo de vida de la aplicación). Antes de ponerse en contacto con el Servicio de soporte técnico, lea las reglas de soporte.

Puede comunicarse con el Servicio de soporte técnico de una de las siguientes maneras:

- Visitando el sitio web del Soporte técnico.
- Enviando una solicitud al Servicio de soporte técnico a través del portal de Kaspersky CompanyAccount.

## Soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las organizaciones que utilizan las aplicaciones de Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky a través de solicitudes en línea. El portal de Kaspersky CompanyAccount le permite supervisar el progreso de las solicitudes electrónicas que procesan los especialistas de Kaspersky, así como llevar un historial de las solicitudes electrónicas.

Puede registrar a todos los empleados de su organización en una cuenta única en Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas por los empleados registrados a Kaspersky y además administrar los privilegios de estos empleados a través de Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- Inglés
- Español
- Italiano
- Alemán

- Polaco
- Portugués
- Ruso
- Francés
- Japonés

Puede obtener más información acerca de Kaspersky CompanyAccount en el sitio web del Servicio de soporte técnico.

# Fuentes de información acerca de la solución

Esta sección enumera las fuentes de información acerca de la solución.

Puede seleccionar la fuente de información más adecuada, según el nivel de importancia y urgencia del problema.

## Página de Kaspersky SD-WAN en el sitio web de Kaspersky

En la página de Kaspersky SD-WAN, puede ver información general acerca de la aplicación, sus funciones y características.

La página de Kaspersky SD-WAN contiene un vínculo a la tienda en línea. Allí puede comprar la solución o renovar su licencia para usar la solución.

## Página de Kaspersky SD-WAN en la Base de conocimientos

La *Base de conocimientos* es una sección en el sitio web de Soporte técnico.

En la página de Kaspersky SD-WAN en la Base de conocimientos, podrá leer artículos que proporcionan información útil, recomendaciones y respuestas a las preguntas frecuentes sobre cómo comprar, instalar y usar la solución.

Los artículos de la Base de conocimientos pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky SD-WAN como con otras aplicaciones de Kaspersky. Los artículos de la Base de conocimientos también pueden incluir novedades de Soporte técnico.

## Foro sobre aplicaciones Kaspersky

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky y con otros usuarios en nuestro Foro.

En el Foro, puede ver los hilos publicados, agregar sus comentarios y crear nuevos hilos.

# Apéndices

Puede obtener información adicional sobre Kaspersky SD-WAN en las siguientes guías:

- Guía de implementación del banco de pruebas de Kaspersky SD-WAN para un entorno VMware, parte 1.
- Guía de implementación del banco de pruebas de Kaspersky SD-WAN para un entorno VMware, parte 2.
- Manual del usuario de KESR modelo 1.
- Manual del usuario de KESR modelo 2 (versión 1).
- Manual del usuario de KESR modelo 2 (versión 2).
- Manual del usuario de KESR modelo 3.
- Manual del usuario de KESR modelo 4 (versión 1).
- Manual del usuario de KESR modelo 4 (versión 2).
- Manual del usuario de KESR modelo 5 (versión 1).
- Manual del usuario de KESR modelo 5 (versión 2).
- Reenvío de tráfico SPAN a través del tejido SD-WAN para probar escenarios KICS.

# Glosario

## Administrador de funciones de la red virtual (VNFM)

Administra el ciclo de vida de las funciones de la red virtual mediante SSH, manuales de Ansible, scripts y atributos de inicio en la nube.

## Administrador de infraestructura virtual (VIM)

Administra recursos computacionales, de redes y de almacenamiento dentro de la infraestructura de NFV. Sirve para conectar funciones de red con vínculos virtuales, subredes y puertos.

Se puede implementar en el centro de datos o en un dispositivo uCPE. La implementación del VIM en el centro de datos implica la administración centralizada del ciclo de vida de VNF, mientras que un VIM implementado en un dispositivo uCPE permite enviar VNF a ubicaciones remotas y administrar estos VNF localmente. El VIM implementado debe agregarse en la interfaz web del orquestador.

La plataforma en la nube de OpenStack se utiliza como VIM.

## Controlador

Administra de forma centralizada la red superpuesta:

- Crea la topología de la red.
- Crea servicios de transporte.
- Administra dispositivos CPE mediante el protocolo OpenFlow.
- Equilibra el tráfico entre vínculos.
- Supervisa los vínculos y cambia automáticamente el tráfico a un vínculo de respaldo si el vínculo principal falla.

Para implementar el controlador, debe implementar la función de la red física del controlador, que se encuentra en el archivo de instalación. El orquestador es el encargado de administrar el controlador.

## CPE universal (uCPE)

CPE con compatibilidad adicional para la implementación de funciones de la red virtual. El dispositivo uCPE debe tener suficientes recursos de hardware para proporcionar funciones de la red virtual sin involucrar al centro de datos ni a la nube.

## Equipo local del cliente (CPE)

Equipos de telecomunicaciones, incluidas las máquinas virtuales, ubicados en las instalaciones del cliente. Se utilizan para conectar la ubicación del cliente a la red SD-WAN, establecer vínculos y transferir tráfico entre las ubicaciones del cliente. El tráfico se puede enviar a un centro de datos para proporcionar funciones de red, como protocolos de enrutamiento, prevención de intrusiones o protección antivirus.

## Estrategia de transporte

Un mecanismo de encapsulación del servicio de transporte que incluye el algoritmo para agregar una pila de etiquetas de encabezado de paquetes de tráfico y el tipo de estas etiquetas. Kaspersky SD-WAN admite temporalmente una estrategia de transporte: **Transporte de intercambio de VNI genérico**.

## Función de red física (PNF)

Funciones de red implementadas como hardware especializado o entidades virtuales creadas mediante entornos de virtualización de terceros. El orquestador no administra el ciclo de vida de las funciones de red física.

## Función de red virtual (VNF)

Las funciones de red implementadas como máquinas virtuales en plataformas informáticas comerciales listas para usar (COTS). Un orquestador administra el ciclo de vida de las funciones de la red virtual. Para implementar funciones de la red virtual, necesita la plataforma en la nube de OpenStack.

## Inquilino

Una entidad lógica dentro de la cual se implementa una instancia SD-WAN individual. Los componentes de la solución, como los componentes de servicio de red, los usuarios y los dispositivos CPE, se asignan a un inquilino y, posteriormente, los administradores de inquilinos pueden administrar los componentes asignados. Por ejemplo, puede crear un inquilino independiente para un cliente de su organización.

## Instancia SD-WAN

Una solución de Kaspersky SD-WAN implementada para uno de los inquilinos de su organización. Es una entidad aislada y tiene sus propios servicios de red, dispositivos CPE y parámetros de calidad de servicio.

## Open vSwitch (OVS)

El tipo de interruptor de software que funciona como base del firmware del dispositivo CPE. Esta implementación utiliza procesamiento de paquetes a nivel de kernel y es adecuada para la mayoría de los dispositivos.

## Orquestador

Controla la infraestructura de la solución, funciona como un orquestador de NFV (NFVO) y administra los servicios de red y los administradores de VNF (VNFM) distribuidos. Puede administrar el orquestador a través de la interfaz web o la API REST cuando se utilizan sistemas externos ascendentes.

## Paquete PNF

Un paquete, en formato TAR o ZIP, que contiene los datos necesarios para implementar y administrar el PNF.

## Paquete VNF

Un paquete, en formato TAR o ZIP, que contiene los datos necesarios para implementar y administrar un VNF.

## Plano de control

La parte de control de la red que controla la transmisión de paquetes de tráfico a través de dispositivos CPE. Realiza funciones como el descubrimiento de redes, el cálculo de rutas, la priorización del tráfico y la aplicación de directivas de seguridad. El plano de control permite administrar la red de manera centralizada al proporcionar una vista a gran escala de todas las operaciones realizadas. Consta de un orquestador y un controlador.

## Plano de datos

La parte de la red que procesa y transmite el tráfico entre diferentes ubicaciones y dispositivos. El plano de datos utiliza protocolos y algoritmos de red para enrutar y entregar el tráfico de manera eficiente a través de la red. Consta de dispositivos CPE.

## Puerta de enlace SD-WAN

Dispositivo CPE que tiene la función de puerta de enlace SD-WAN. Las puertas de enlace SD-WAN establecen vínculos con todos los dispositivos de la red, incluidas otras puertas de enlace SD-WAN, lo que proporciona conexión entre todos los dispositivos CPE y el controlador. Puede instalar varias puertas de enlace SD-WAN para la tolerancia a errores.

## Red de área amplia definida por software (SD-WAN)

Enfoque para construir redes definidas por software mediante una red informática global. Las redes de SD-WAN permiten la conexión de redes de área local y usuarios en ubicaciones geográficamente dispersas.

## Redes definidas por software (SDN)

Tecnología para la construcción de redes de comunicación en las que el plano de control está separado del plano de datos y se implementa en el software mediante un controlador SDN centralizado.

## Seguridad de puerto

Esta función mejora la seguridad de la red al nivel de los puertos Ethernet de los conmutadores y evita el acceso no autorizado a la red al limitar la cantidad de direcciones MAC que se pueden asociar con un solo puerto físico. Cuando está habilitada, solo los dispositivos de confianza con direcciones MAC predefinidas pueden conectarse a la red.

## Sistema operativo del conmutador (SWOS)

El tipo de interruptor de software que funciona como base del firmware del dispositivo CPE. Esta es una implementación alternativa con el procesamiento de paquetes basado en DPDK. Puede ofrecer un mayor rendimiento gracias al procesamiento de paquetes que omite el kernel.

## Unidad de implementación virtual (VDU)

Una máquina virtual que actúa como un host VNF y agrega recursos informáticos virtuales, como CPU y memoria, necesarios para ejecutar el software VNF, y también contiene ciertas implementaciones de la función de red, como algoritmos de enrutamiento o lógica de equilibrio de carga.

Se pueden combinar varias VDU en una sola VNF para proporcionar escalabilidad o alta disponibilidad. Las VDU se pueden distribuir en varios servidores físicos; aún puede administrarlos como un solo VNF. Las VDU interactúan entre sí y con otras VNF para realizar sus funciones dentro de un servicio de red.

# Información sobre código de terceros

La información sobre el código de terceros se encuentra en el archivo legal_notices.txt en la carpeta de instalación de la aplicación.

# Avisos de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Active Directory es una marca comercial del grupo de empresas Microsoft.

Ansible, CentOS, Red Hat son marcas comerciales o marcas comerciales registradas de Red Hat, Inc. o sus filiales en los Estados Unidos y otros países.

Arm es una marca comercial registrada de Arm Limited (o sus filiales) en los EE. UU. y otros países.

Atom, Celeron, Intel y Xeon son marcas comerciales de Intel Corporation o sus filiales.

Debian es una marca comercial registrada de Software in the Public Interest, Inc.

Docker y el logotipo de Docker son marcas comerciales o marcas comerciales registradas de Docker, Inc. en los EE. UU. y otros países. Docker, Inc. y otras partes pueden tener derechos sobre las marcas comerciales descritas con otros términos utilizados en este documento.

Firefox es una marca comercial de Mozilla Foundation en EE. UU. y en otros países.

Google Chrome es una marca comercial de Google LLC.

IBM es una marca comercial de International Business Machines Corporation registrada en muchas jurisdicciones de todo el mundo.

Intel y Xeon son marcas comerciales de Intel Corporation o sus filiales.

Kraftway es una marca registrada de AO Kraftway Corporation PLC.

Linux, LTS son marcas registradas de Linus Torvalds en EE. UU. y en otros países.

Microsoft Edge y Windows son marcas comerciales del grupo de empresas de Microsoft.

MIPS es una marca comercial o una marca comercial registrada de MIPS Technologies en los EE. UU. y en otros países.

OpenStack es una marca comercial registrada de OpenStack Foundation en EE. UU. y en otros países.

OpenStreetMap es una marca comercial de OpenStreetMap Foundation. Este producto no está afiliado ni respaldado por la Fundación OpenStreetMap.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Safari es una marca comercial de Apple Inc.

SUSE es una marca comercial de SUSE LLC registrada en los Estados Unidos y en otros lugares.

Ubuntu es una marca comercial registrada de Canonical Ltd.

VMware es una marca comercial registrada o una marca comercial de VMware, Inc. en los Estados Unidos y en otros países.

Zabbix es una marca comercial registrada de Zabbix SIA.