

Configurar y verificar el seguimiento y la reserva de DIA NAT

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Restricciones de NAT DIA Tracker](#)

[Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.10.1a y versiones anteriores](#)

[Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.11.1a](#)

[Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.13.1a](#)

[Interfaces Soportadas para NAT DIA Tracker](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Paso 1. Configurar el rastreador DIA de NAT](#)

[Paso 2. Enlazar el rastreador a la interfaz de transporte](#)

[Paso 3. Activar reserva NAT en política DIA existente](#)

[Verificación](#)

[Rastreador de Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y verificar DIA NAT Tracker y Fallback en los routers Cisco IOS XE® mediante la GUI de Cisco Catalyst Manager.

Prerequisites

Requirements

La política NAT DIA de Cisco SD-WAN se debe configurar en los dispositivos de sucursal. Consulte la sección [Información Relacionada](#) para obtener instrucciones sobre cómo implementar el acceso directo a Internet (DIA) para SD-WAN.

Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

- Cisco Catalyst SD-WAN Manager versión 20.14.1

- Controlador Cisco Catalyst SD-WAN versión 20.14.1
- Cisco Edge Router versión 17.14.01a

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Restricciones de NAT DIA Tracker

Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.10.1a y versiones anteriores

- En Cisco IOS XE Release 17.6.x y versiones anteriores, el rastreador DIA NAT no se soporta en las interfaces de marcador. A partir de Cisco IOS XE Catalyst SD-WAN versión 17.7.1a, las subinterfaces y las interfaces de marcador admiten rastreadores de terminales únicos y duales.
- El extremo de URL DNS no es compatible con los dispositivos Catalyst SD-WAN de Cisco IOS XE.
- Sólo puede aplicar un rastreador o grupo de rastreadores a una interfaz.
- La función de reserva de NAT sólo es compatible con Cisco IOS XE Catalyst SD-WAN versión 17.3.2.
- La dirección IP del túnel con la dirección 169.254.x.x no se admite para realizar un seguimiento del extremo de zScaler en los túneles manuales.
- Debe configurar un mínimo de dos rastreadores de punto final único para configurar un grupo de seguimiento.
- Un grupo de seguimiento sólo puede incorporar un máximo de dos rastreadores de punto final únicos.
- En Cisco IOS XE Release 17.10.1 y versiones anteriores, no puede configurar el rastreador IPv4 en una interfaz IPv6 o viceversa. El rastreador no estará activo.

Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

- El extremo de URL de API solo se admite en el rastreador DIA IPv6 y no en el rastreador DIA IPv4.
- Los rastreadores IPv4 e IPv6 no se pueden utilizar en el mismo grupo de seguimiento.
- Debe configurar el comando allow service all en la interfaz de túnel TLOC para que los rastreadores IPv6 funcionen con una interfaz de túnel TLOC.
- No se admiten varias interfaces DIA NAT66.
- No se admite el repliegue NAT en la política de datos centralizada.

Restricciones de Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

- Los elementos DNS de extremo no se admiten en un grupo de seguimiento.

Nota: Asegúrese de que utiliza una dirección IP de terminal que responde a las

solicitudes HTTP/HTTPS. Por ejemplo, el servidor DNS 8.8.8.8 de Google no se puede utilizar como dirección IP de terminal.

Interfaces Soportadas para NAT DIA Tracker

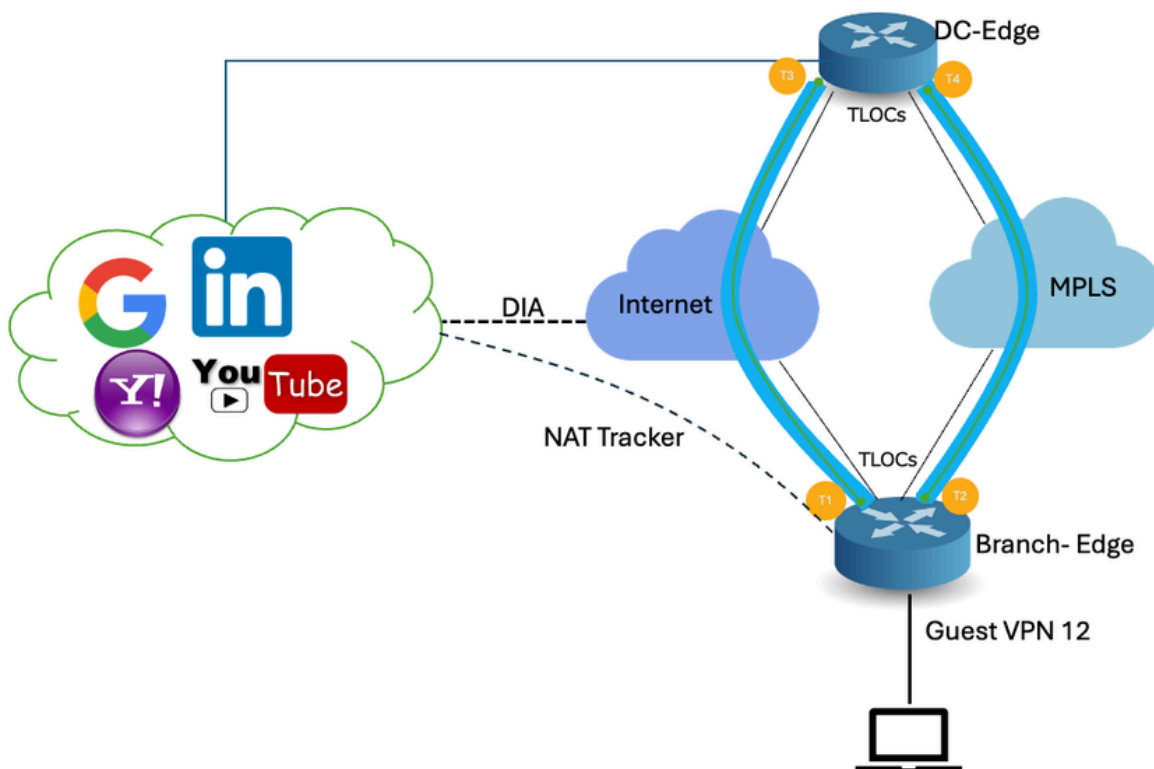
Puede configurar el rastreador DIA NAT para estas interfaces:

- Interfaces celulares
- Interfaces Ethernet
- Interfaces Ethernet (PPPoE)
- Subinterfaces
- Interfaces del marcador DSL (PPPoE y PPPoA)

Nota: El rastreador DIA NAT IPv6 sólo se admite en interfaces físicas y subinterfaces de interfaces Ethernet.

Configurar

Diagrama de la red



Configuraciones

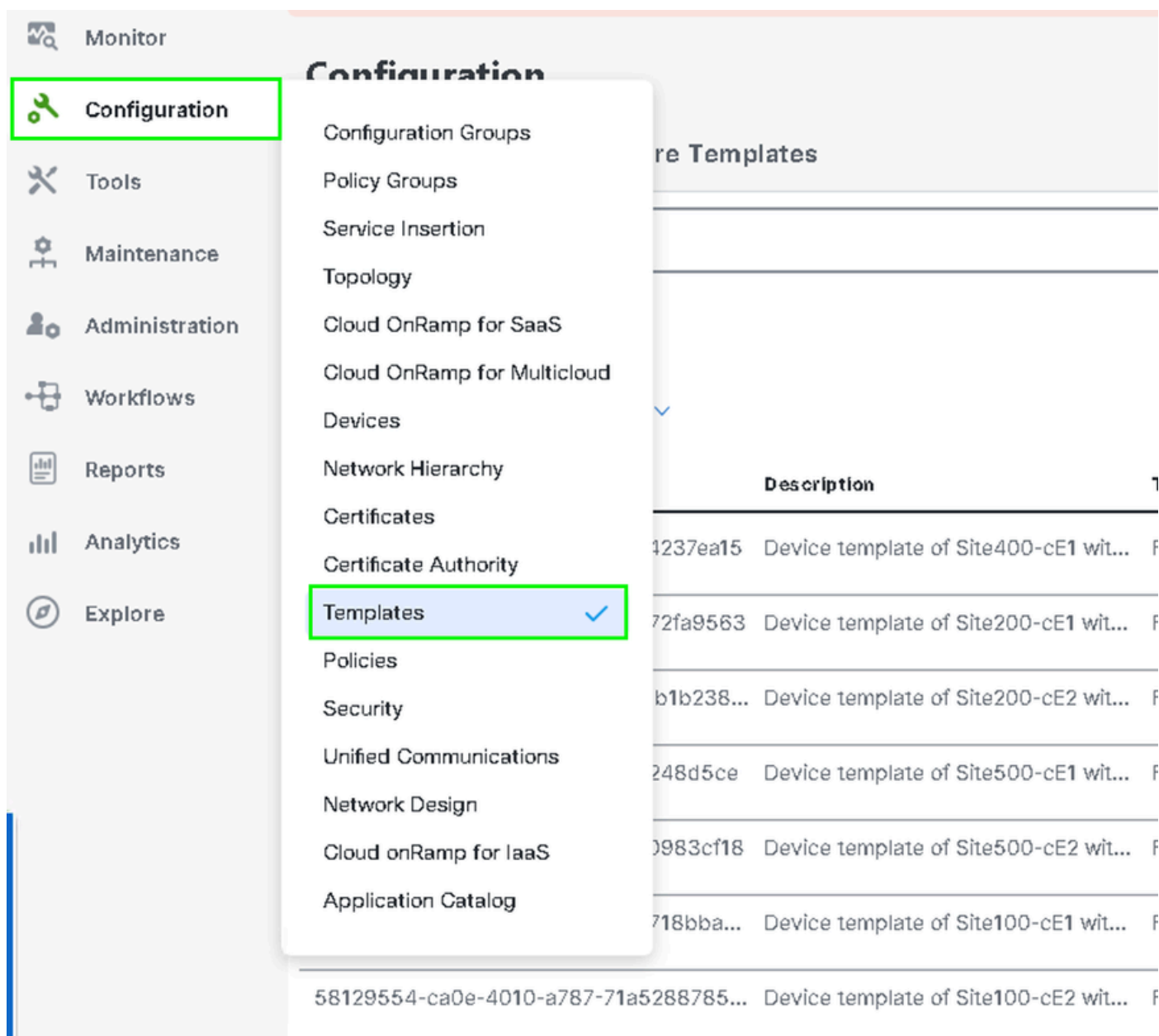
El rastreador DIA ayuda a determinar si Internet o la red externa no están disponibles. La función

NAT DIA Tracking es útil cuando NAT está habilitada en una interfaz de transporte en VPN 0 para permitir que el tráfico de datos del router salga directamente a Internet.

Si Internet o la red externa no están disponibles, el router continúa reenviando el tráfico basado en la ruta NAT en la VPN de servicio. El tráfico que se reenvía a Internet se descarta. Para evitar que se descarte el tráfico de Internet, configure el rastreador DIA en el router de borde para realizar un seguimiento del estado de la interfaz de transporte. El rastreador sondea periódicamente la interfaz para determinar el estado de Internet y devuelve los datos a los puntos de conexión asociados con el rastreador.

Paso 1. Configurar el rastreador DIA de NAT

En el menú Cisco SD-WAN Manager, navegue hasta Configuration > Templates.



The screenshot shows the Cisco SD-WAN Manager interface. On the left, there is a navigation menu with the following items: Monitor, Configuration (highlighted with a green box), Tools, Maintenance, Administration, Workflows, Reports, Analytics, and Explore. The main content area is titled 'Configuration' and shows a list of configuration options: Configuration Groups, Policy Groups, Service Insertion, Topology, Cloud OnRamp for SaaS, Cloud OnRamp for Multicloud, Devices, Network Hierarchy, Certificates, Certificate Authority, Templates (highlighted with a green box and a blue checkmark), Policies, Security, Unified Communications, Network Design, Cloud onRamp for IaaS, and Application Catalog. On the right side, there is a table titled 'Device Templates' with columns for ID, Description, and Status. The table contains several rows of data, including entries for Site400-cE1, Site200-cE1, Site200-cE2, Site500-cE1, Site500-cE2, Site100-cE1, and Site100-cE2.

ID	Description	Status
4237ea15	Device template of Site400-cE1 wit...	F
72fa9563	Device template of Site200-cE1 wit...	F
b1b238...	Device template of Site200-cE2 wit...	F
248d5ce	Device template of Site500-cE1 wit...	F
0983cf18	Device template of Site500-cE2 wit...	F
718bba...	Device template of Site100-cE1 wit...	F
58129554-ca0e-4010-a787-71a5288785...	Device template of Site100-cE2 wit...	F

Haga clic en Plantillas de funciones. Busque la plantilla de función Cisco System en la barra de

búsqueda, haga clic en los tres puntos (...) y haga clic en Edit para modificarla.

Configuration

Device Templates **Feature Templates**

Q 400 x system x Search

Add Template

Template Type Non-Default

Total Rows: 3 of 125

Name	Description	Type	Device Model	Device Templates	Devices Attached	Updated By	Last Updated
ntp_system_21*10*2021_19*3...	Test Drive Template: System ...	Cisco NTP	CSR1000v	8	8	admin	04 Apr 2024 7:19:47 PM GM ...
system_Site400-cE1_400_28...	Test Drive Template: System ...	Cisco System	C8000v	1	1	admin	04 Apr 2024 4:21:19 PM GM ...
system_Site500-cE2_500_14e...	Test Drive Template: System ...	Cisco System	C8000v	1	1	admin	04 Apr 2024 4:27:53 ...

- View
- Edit**
- Change Device Models
- Delete
- Copy

En el equipo de características del sistema, haga clic en Rastreador.

Configuration

Device Templates **Feature Templates**

Feature Template > Cisco System > system_Site400-cE1_400_288e91b4-e59e-4af4-92f8-847b4237ea15_04-04-2024_16-21-17

Device Type C8000v

Template Name* system_Site400-cE1_400_288e91b4-e59e-4af4-

Description* Test Drive Template: System feature of Site400

Basic Configuration GPS **Tracker** Advanced

BASIC CONFIGURATION

Haga clic en New Endpoint Tracker para configurar los parámetros del rastreador.

Tracker

TRACKERS TRACKER GROUPS

New Endpoint Tracker

Optional	Name	Threshold	Interval	Multiplier	Tracker Type
No data available					

Ingrese los parámetros del rastreador y haga clic en Agregar.

Nombre: Nombre del rastreador. El nombre puede tener hasta 128 caracteres alfanuméricos. Puede configurar hasta ocho rastreadores.

Umbral: tiempo que se debe esperar a que la sonda devuelva una respuesta antes de declarar que la interfaz de transporte está inactiva. Intervalo: de 100 a 1000 milisegundos. Predeterminado: 300 milisegundos.

Intervalo: frecuencia con la que se envía una sonda para determinar el estado de la interfaz de transporte. Intervalo: de 20 a 600 segundos. Valor predeterminado: 60 segundos (1 minuto).

Multiplicador: número de veces que se puede volver a enviar una sonda antes de declarar que la interfaz de transporte está inactiva. Intervalo: de 1 a 10. Valor predeterminado: 3.

Tipo de rastreador: Elija Interfaz para configurar el rastreador DIA.

Tipo de terminal: puede seleccionar una dirección IP, un nombre DNS o una URL.

Nombre DNS del punto final: nombre DNS del punto final. Este es el destino en Internet al que el router envía sondas para determinar el estado de la interfaz de transporte.

Haga clic en la lista desplegable y seleccione Global para cambiar cualquier valor predeterminado.

The screenshot shows a configuration window titled "Tracker" with a dropdown menu. Below the title, there are two tabs: "TRACKERS" and "TRACKER GROUPS". A "New Endpoint Tracker" button is visible. The configuration fields are as follows:

- Name:** A text input field containing "tracker1".
- Threshold:** A numeric input field containing "300".
- Interval:** A dropdown menu with "Global" selected. Other options include "Device Specific" and "Default".
- Multiplier:** A numeric input field, currently empty.
- Tracker Type:** A dropdown menu with "Interface" selected.
- Endpoint Type:** Radio buttons for "IP Address", "DNS Name" (selected), and "URL".
- Endpoint DNS Name:** A text input field containing "www.cisco.com".

At the bottom right, there are "Cancel" and "Add" buttons. The "Add" button is highlighted with a green box.

Haga clic en Update (Actualizar).

TRACKERS TRACKER GROUPS

New Endpoint Tracker

Optional	Name	Threshold	Interval	Multiplier	Tracker Type	Action
<input type="checkbox"/>	<input type="text" value="tracker1"/>	<input type="text" value="100"/>	<input type="text" value="30"/>	<input type="text" value="3"/>	<input type="text" value="interface"/>	 

New Object Tracker

Mark as Optional Row ⓘ

Tracker Type

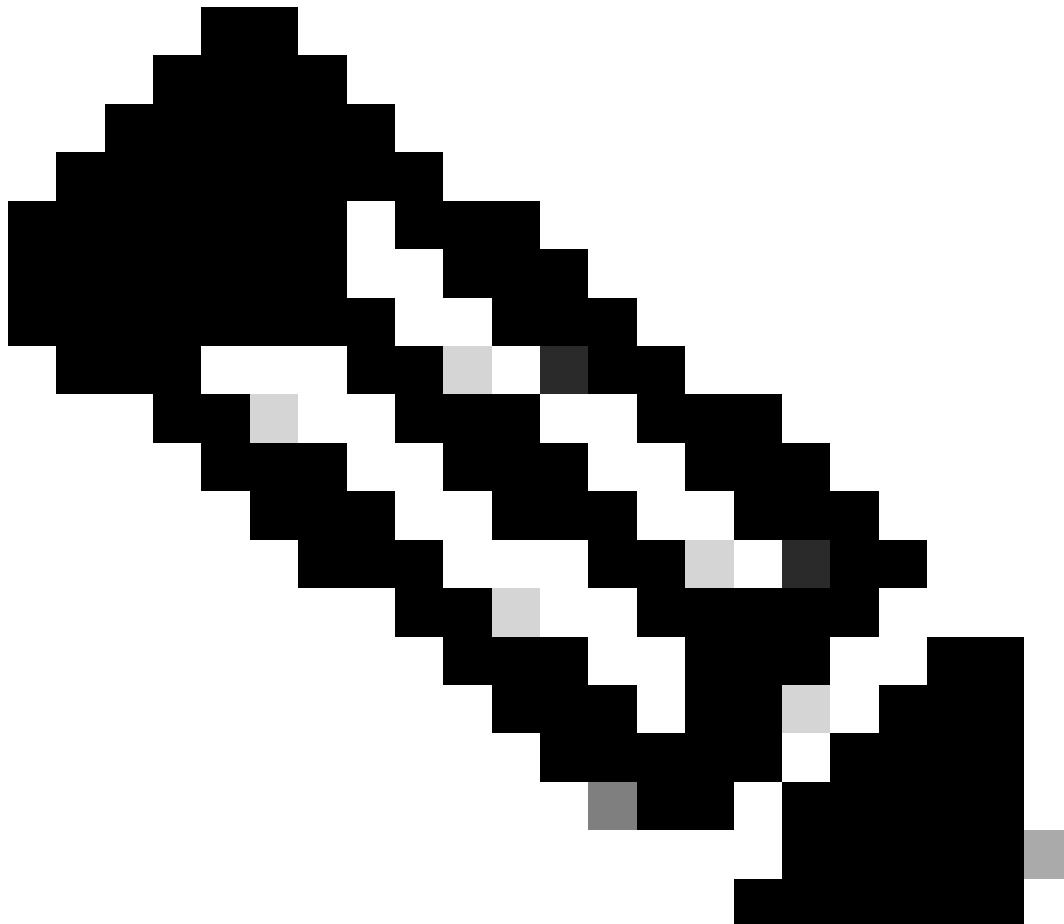
Interface SIG Route

Object ID

Interface

Cancel

Update



Nota: Asegúrese de haber configurado dos rastreadores de punto final único antes de configurar un grupo de seguimiento.

Haga clic en Next (Siguiente).

Device Template | 288e91b4-e59e-4af4-92f8-847b4237ea15

Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Prefix(0.0.0.0/0)	Address(192.168.1.1)	Interface Name(GigabitEthernet8)	IPv4 Address/ prefix-k
✓	C8K-08B43DFE-2350-F2B2-E8E2-F80...		Site400-cE1	0.0.0.0/0		GigabitEthernet8	...

Next Cancel

Haga clic en Devices (Dispositivos) y asegúrese de que la configuración es correcta. Haga clic en Config Diff y Side by Side Diff. Haga clic en Configure Devices.

Device Template | 288e91b4-e59e-4af4-9... | Total: 1

Device list (Total: 1 devices)

Filter/Search

C8K-08B43DFE-2350-F2B2-E8E2-F80F3EDDB887 | Site400-cE1|11.40.1 | Configure Devi...

Config Preview | Config Diff

```
system
ztp-status          in-progress
device-model        vedge-c8000v
gps-location latitude 19.04674
gps-location longitude 72.85223
system-ip
overlay-id          1
site-id             400
no transport-gateway enable
port-offset         0
control-session-pps 300
admin-tech-on-failure
sp-organization-name Viptela-POC-Tool
organization-name   Viptela-POC-Tool
```


333	no crypto ikev2 diagnose error	333	endpoint-tracker tracker1
334	no crypto isakmp diagnose error	334	tracker-type interface
335	no network-clock revertive	335	endpoint-dns-name www.cisco.com
336	snmp-server ifindex persist	336	threshold 100
337	fhrp version vrrp v2	337	interval 30
338	line con 0	338	!
339	speed 115200	339	no crypto ikev2 diagnose error
340	stopbits 1	340	no crypto isakmp diagnose error
341	!	341	no network-clock revertive
342	line vty 0 4	342	snmp-server ifindex persist
343	transport input ssh	343	fhrp version vrrp v2
344	!	344	line con 0
345	line vty 5 80	345	speed 115200
		346	stopbits 1
		347	!
		348	line vty 0 4
		349	transport input ssh
		350	!
		351	line vty 5 80

Back Configure Devices Cancel

vManage configuró correctamente la plantilla del dispositivo con la configuración del rastreador.

Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success : 1

Device Group (1)

Q Search Table

Status	Message	Chassis Number
● Success	Template successfully attac...	

View Logs

Host: Site400-cE1()

Site ID: 400

Device: C8000v

Model:

[29-Jul-2024 7:50:20 PDT] Configuring device with feature template:

[29-Jul-2024 7:50:21 PDT] Checking and creating device in Manager

[29-Jul-2024 7:50:22 PDT] Generating configuration from template

[29-Jul-2024 7:50:29 PDT] Device is online

[29-Jul-2024 7:50:29 PDT] Updating device configuration in Manager

[29-Jul-2024 7:50:29 PDT] Sending configuration to device

[29-Jul-2024 7:50:36 PDT] Successfully notified device to pull configuration

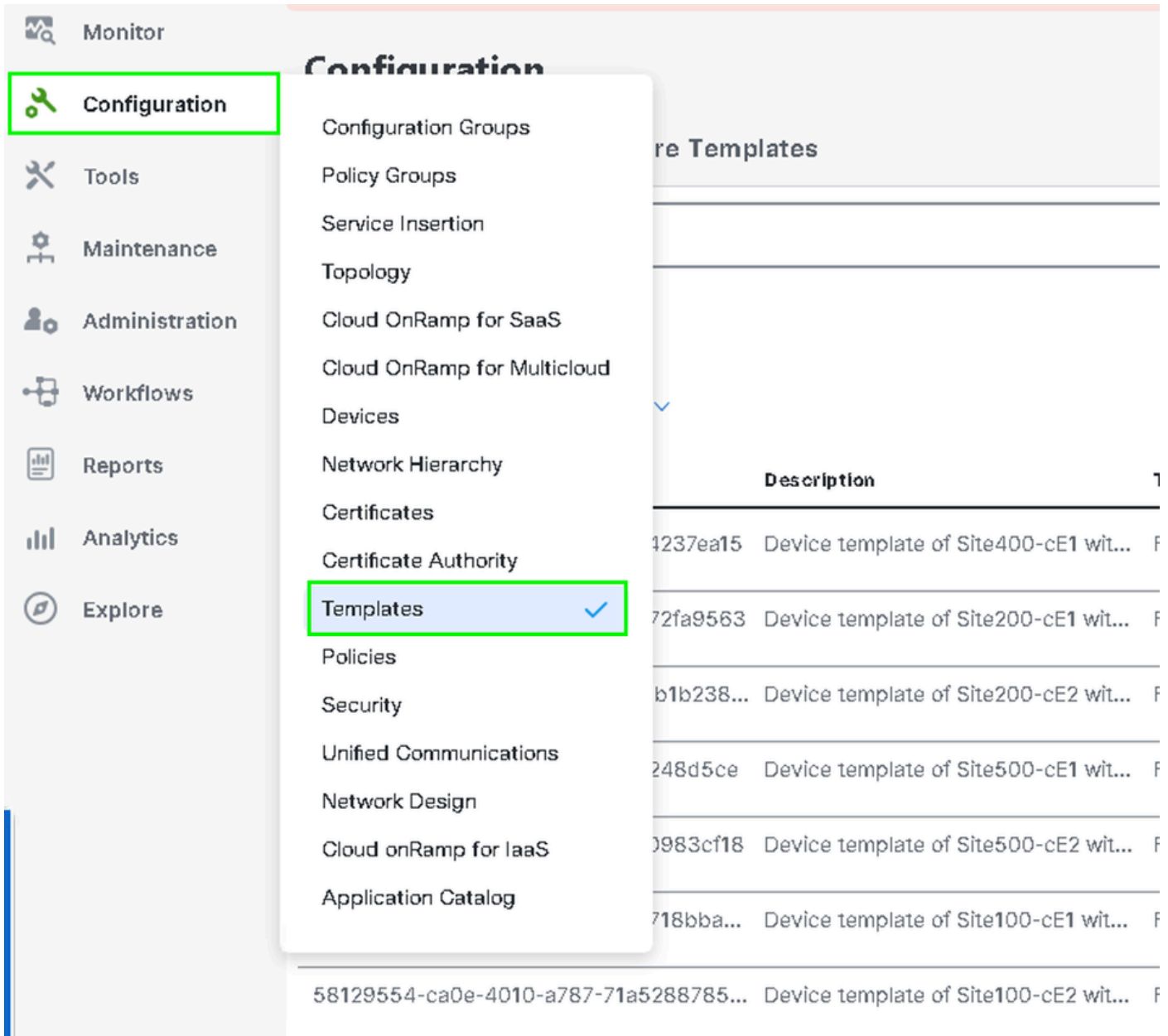
[29-Jul-2024 7:50:36 PDT] Device has pulled the configuration

[29-Jul-2024 7:50:39 PDT] Device: Config applied successfully

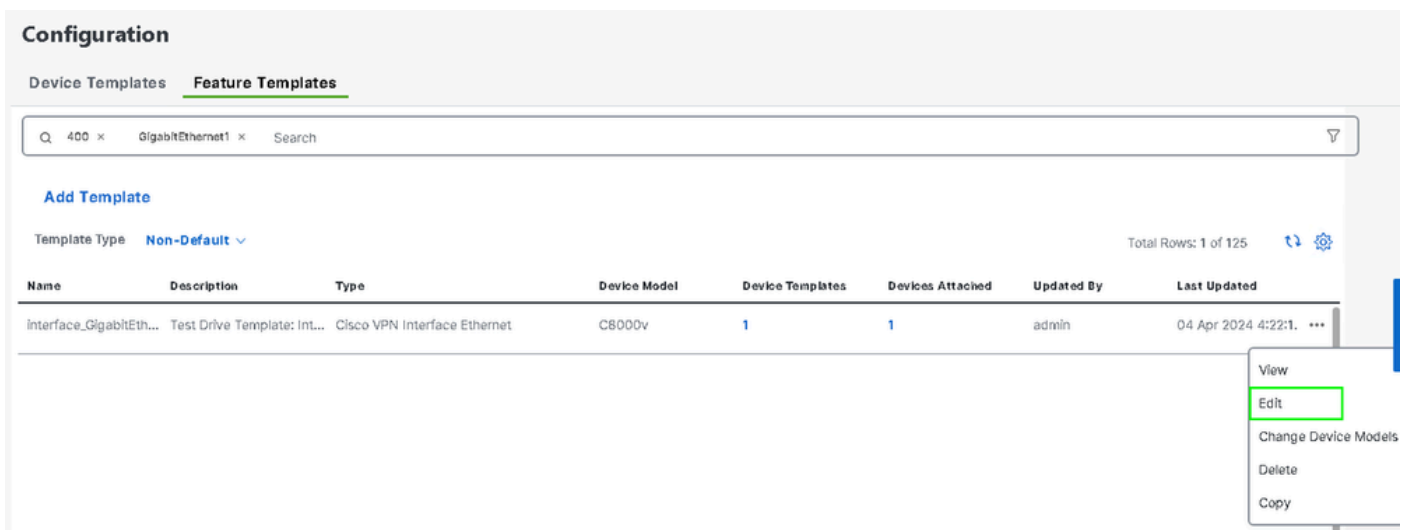
[29-Jul-2024 7:50:39 PDT] Template successfully attached to device

Paso 2. Enlazar el rastreador a la interfaz de transporte

En el menú Cisco SD-WAN Manager, navegue hasta Configuration > Templates.



Busque la plantilla de la función Interfaz de transporte NAT en la barra de búsqueda, haga clic en los tres puntos (...) y haga clic en Editar para modificar.



Haga clic en la ficha Advanced (Opciones avanzadas).

Configuration

Device Templates **Feature Templates**

Feature Template > Cisco VPN Interface Ethernet > interface_GigabitEthernet1_04-04-2024_16-21-18

Device Type: C8000v

Template Name*: interface_GigabitEthernet1_04-04-2024_16-21-18

Description*: Test Drive Template: Interface GigabitEthernet1 fe

Basic Configuration Tunnel NAT VRRP ACL/QoS ARP TrustSec **Advanced**

Para agregar el nombre del rastreador en el Rastreador, seleccione Global en el menú desplegable.

Tracker

ICMP/ICMPv6 Redirect Disable

GRE tunnel source IP

Global (selected)
Device Specific >
Default

Ingrese el nombre del rastreador que creó en la plantilla del sistema y haga clic en Update.

Tracker: tracker1

ICMP/ICMPv6 Redirect Disable: On

GRE tunnel source IP

Xconnect

Cancel Update

Haga clic en Next (Siguiete).

Device Template | 288e91b4-e59e-4af4-92f8-847b4237ea15

Q Search

Total Rows: 1

S...	Chassis Number	System IP	Hostname	Prefix(0.0.0.0/0)	Address(192.168.1.1)	Interface Name(GigabitEthernet8)	IPv4 Address/ prefix-k
✓	C8K08B43DFE-2350-F2B2-E8E2-F80...		Site400-cE1	0.0.0.0/0		GigabitEthernet8	...

Next Cancel

Haga clic en Devices (Dispositivos) y asegúrese de que la configuración es correcta. Haga clic en Config Diff y Side by Side Diff. Haga clic en Configure Devices.

Device Template
288e91b4-e59e-4af4-9...

Device list (Total: 1 devices)

Filter/Search

C8K-08B43DFE-2350-F2B2-E8E2-F80F3EDDB887
Site400-cE1|1.1.40.1

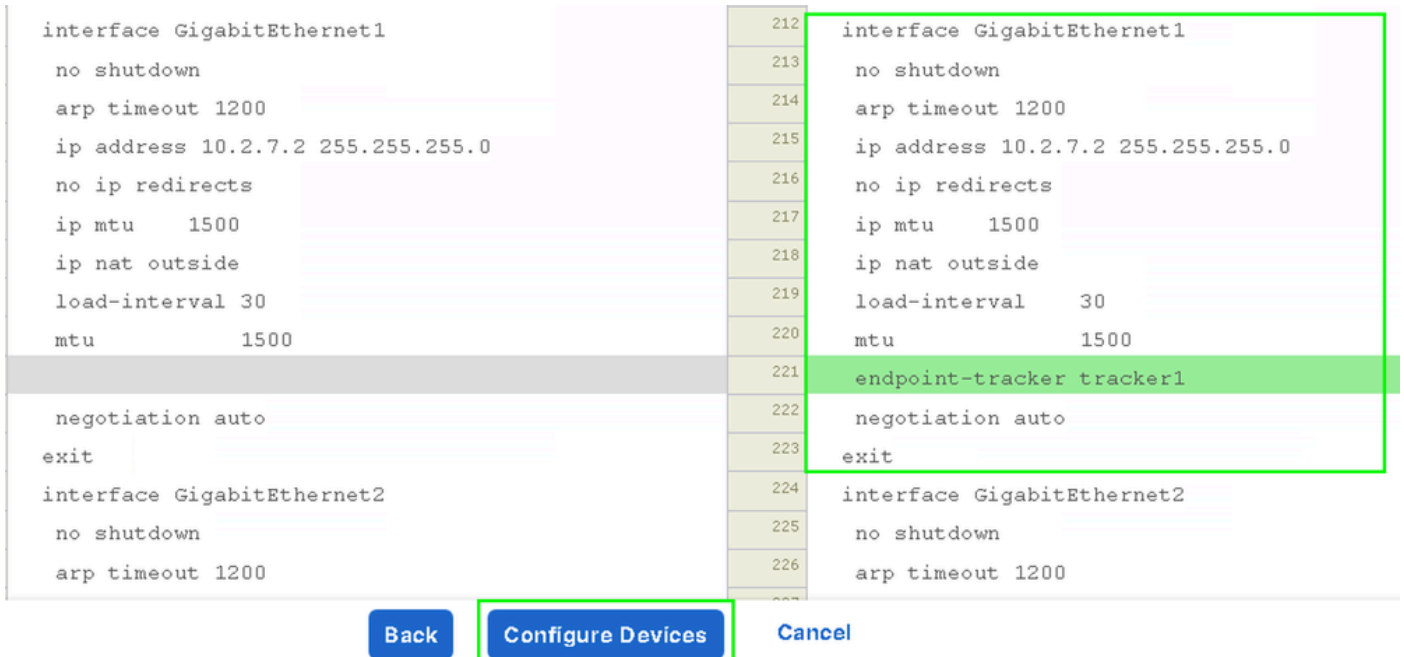
Configure Devi...

Total
1

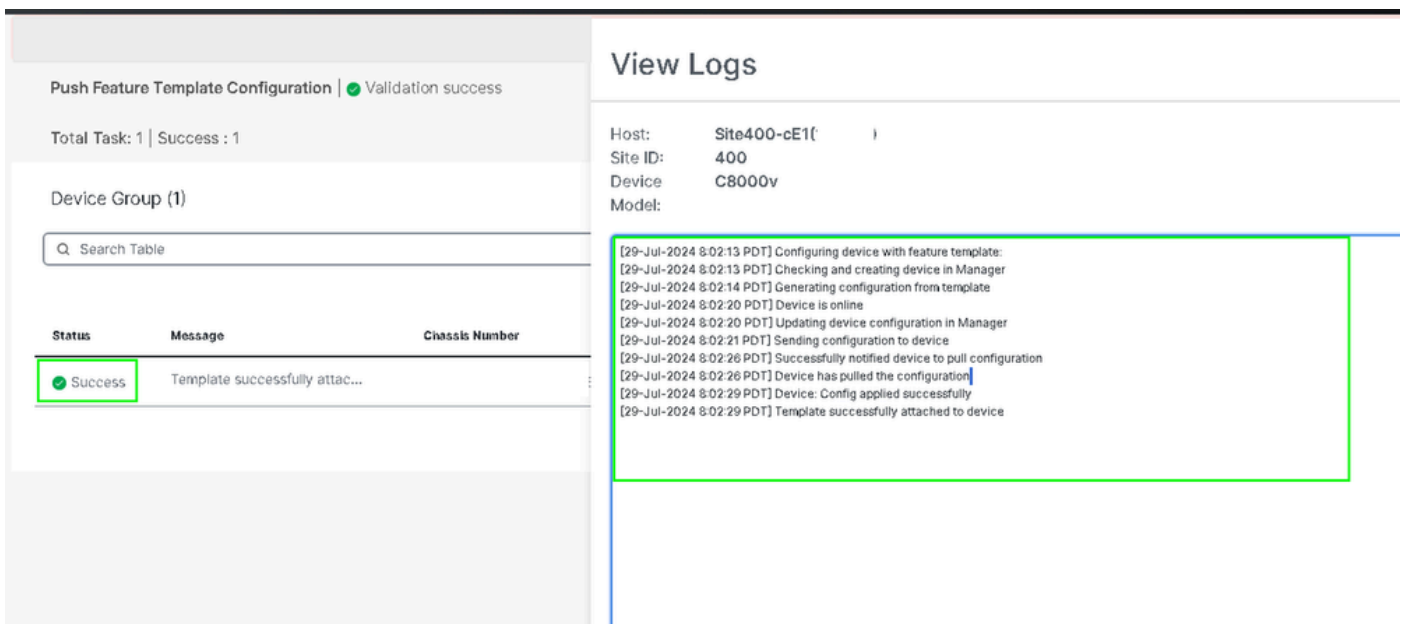
Config Preview
Config Diff

```

system
 ztp-status          in-progress
 device-model        vedge-C8000V
 gps-location latitude 19.04674
 gps-location longitude 72.85223
 system-ip
 overlay-id          1
 site-id             400
 no transport-gateway enable
 port-offset         0
 control-session-pps 300
 admin-tech-on-failure
 sp-organization-name Viptela-POC-Tool
 organization-name   Viptela-POC-Tool
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate   115200
 no on-demand enable
 on-demand idle-timeout 10
          
```



vManage ha configurado correctamente la plantilla de dispositivo.



Paso 3. Activar reserva NAT en política DIA existente

Los dispositivos Cisco IOS XE Catalyst SD-WAN admiten la función de reserva NAT para el acceso directo a Internet (DIA). La función de reserva de NAT permite que el tráfico utilice una trayectoria alternativa si falla la trayectoria de NAT primaria. Esto garantiza una conectividad continua incluso si hay problemas con la configuración de NAT primaria.

Para habilitar la reserva de NAT mediante el Administrador de SD-WAN de Cisco:

En el menú Cisco SD-WAN Manager, vaya a Configuration > Policy.



Monitor



Configuration



Tools



Maintenance



Administration



Workflows



Reports



Analytics



Explore

Configuration Groups

Policy Groups

Service Insertion

Topology

Cloud OnRamp for SaaS

Cloud OnRamp for Multicloud

Devices

Network Hierarchy

Certificates

Certificate Authority

Templates

Policies ✓

Security

Unified Communications

Network Design

Cloud onRamp for IaaS

Application Catalog

VIP10_DC_Preference

VIP16_QoS_Classify_SIP

```
interface GigabitEthernet1
ip address 10.2.7.2 255.255.255.0
no ip redirects
ip nat outside
load-interval 30
negotiation auto
```

```
endpoint-tracker tracker1
```

```
arp timeout 1200
end
```

```
Site400-cE1#show sdwan running-config | sec endpoint
endpoint-tracker tracker1
tracker-type interface
endpoint-dns-name www.cisco.com
threshold 100
interval 30
```

El resultado muestra cómo verificar el estado del rastreador mediante los comandos show endpoint-tracker y show endpoint-tracker GigabitEthernet1.

```
Site400-cE1#show endpoint-tracker
```

Interface	Record Name	Status	Address Family	RTT in msec	Probe ID	Next Hop
GigabitEthernet1	tracker1	Up	IPv4	8	6	10.2.7.1

```
Site400-cE1#show endpoint-tracker interface GigabitEthernet1
```

Interface	Record Name	Status	Address Family	RTT in msec	Probe ID	Next Hop
GigabitEthernet1	tracker1	Up	IPv4	8	6	10.2.7.1

El resultado muestra información relacionada con el temporizador sobre el rastreador para ayudar a depurar los problemas relacionados con el rastreador, si los hubiera:

```
Site400-cE1#show endpoint-tracker records
```

Record Name	Endpoint	EndPoint Type	Threshold(ms)	Multiplier	Interval(s)	Tracker-Type
tracker1	www.cisco.com	DNS_NAME	100	3	30	interface

El resultado del comando show ip sla summary.

```
Site400-cE1#show ip sla summary
```

```
IPSLAs Latest Operation Summary
```

```
Codes: * active, ^ inactive, ~ pending
```

All Stats are in milliseconds. Stats with u are in microseconds

ID	Type	Destination	Stats	Return Code	Last Run
*5	dns	8.8.8.8	RTT=16	OK	16 seconds ago
*6	http	x.x.x.x	RTT=15	OK	3 seconds ago

Verifique la configuración de reserva aplicada en el dispositivo mediante el comando `show sdwan policy from-vsmart`.

<#root>

```
Site400-cE1#show sdwan policy from-vsmart
from-vsmart data-policy _VPN12_VPN12_DIA
direction from-service
vpn-list VPN12
sequence 1
match
source-data-prefix-list Site400_AllVPN_Prefixes
action accept
nat use-vpn 0

nat fallback

no nat bypass
default-action drop
```

Rastreador de Troubleshooting

Active estas depuraciones en el dispositivo de borde para verificar cómo el router envía sondas para determinar el estado de la interfaz de transporte.

- Para monitorear cómo el router envía sondeos y determina el estado de las interfaces de transporte, utilice el comando `debug platform software sdwan tracker` que se soporta hasta la versión 17.12.x.
- A partir de 17.13.x en adelante, para monitorear los registros de sondeos, habilite estas depuraciones.
 - `set platform software trace ios R0 sdwanrp-tracker debug`
 - `set platform software trace ios R0 sdwanrp-cfg debug`
- Para verificar los registros relacionados con el seguimiento y error de operaciones de IP SLA, habilite estos debugs. Estos registros muestran si las operaciones de IP SLA están fallando.
 - `debug ip sla trace`
 - `debug ip sla error`

Ejecute estos comandos `show` y `monitor` para verificar los registros de depuración:

- show logging profile sdwan internal
- monitor logging profile sdwan internal

Site400-cE1#show logging profile sdwan internal

Logging display requested on 2024/08/13 08:10:45 (PDT) for Hostname: [Site400-cE1], Model: [C8000V], Ve

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds

executing cmd on chassis local ...

Unified Decoder Library Init .. DONE

Found 1 UTF Streams

```
2024/08/13 08:02:28.408998337 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 s
2024/08/13 08:02:28.409061529 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.409086404 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409160541 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE: Sla sync
2024/08/13 08:02:28.409182208 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 St
2024/08/13 08:02:28.409197024 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.409215496 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 DN
2024/08/13 08:02:28.409242243 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409274690 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 De
2024/08/13 08:02:28.409298157 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 So
2024/08/13 08:02:28.409377223 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Ne
2024/08/13 08:02:28.409391034 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.409434969 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 ac
2024/08/13 08:02:28.409525831 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Pr
2024/08/13 08:02:28.426966448 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Qu
2024/08/13 08:02:28.427004143 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 Re
2024/08/13 08:02:28.427029754 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 RT
2024/08/13 08:02:28.427161550 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427177727 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427188035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427199147 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427208941 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:10 IP
2024/08/13 08:02:28.427219960 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427238042 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427301952 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427316275 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427326235 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): Received IPSLA sta
2024/08/13 08:02:28.427328425 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS status callbac
2024/08/13 08:02:28.427341452 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS query valid TR
2024/08/13 08:02:28.427343152 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS resolved addre
2024/08/13 08:02:28.427344332 {iosrp_R0-0}{255}: [sdwanrp-tracker] [17432]: (debug): DNS probe handler
2024/08/13 08:02:28.427349194 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427359268 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427370416 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427555382 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427565670 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427577691 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427588947 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427600567 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427611465 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:28.427620724 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:28.427645035 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:10 S
2024/08/13 08:02:55.599896668 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 sI
2024/08/13 08:02:55.599966240 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 St
2024/08/13 08:02:55.599981173 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sta
2024/08/13 08:02:55.600045761 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Nex
2024/08/13 08:02:55.600111585 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 DNS
2024/08/13 08:02:55.600330868 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 sla
```

```
2024/08/13 08:02:55.610693565 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.610717011 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.610777327 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Sen
2024/08/13 08:02:55.610788233 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Wai
2024/08/13 08:02:55.618534651 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 Soc
2024/08/13 08:02:55.618685838 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 HTT
2024/08/13 08:02:55.618697389 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618706090 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618714316 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618723915 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-INFRA_TRACE:OPER:3 Sc
2024/08/13 08:02:55.618732815 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE:OPER:3 IPS
2024/08/13 08:02:55.618821650 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618833396 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
2024/08/13 08:02:55.618857012 {iosrp_R0-0}{255}: [buginf] [17432]: (debug): IPSLA-OPER_TRACE: Common St
```

Información Relacionada

[Implementación de acceso directo a Internet \(DIA\) para SD-WAN](#)

[Guía de configuración de NAT de Cisco Catalyst SD-WAN](#)

[Reserva NAT en dispositivos Catalyst SD-WAN de Cisco IOS XE](#)

[Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).