

Configurar e verificar o DIA NAT Tracker e Fallback

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Restrições para o NAT DIA Tracker](#)

[Restrições para Cisco IOS XE Catalyst SD-WAN versão 17.10.1a e versões anteriores](#)

[Restrições para o Cisco IOS XE Catalyst SD-WAN versão 17.11.1a](#)

[Restrições para o Cisco IOS XE Catalyst SD-WAN versão 17.13.1a](#)

[Interfaces suportadas para o NAT DIA Tracker](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Etapa 1. Configurar o NAT DIA Tracker](#)

[Etapa 2. Vincular o rastreador à interface de transporte](#)

[Etapa 3. Habilitar Fallback de NAT na Política de DIA Existente](#)

[Verificar](#)

[Rastreador de solução de problemas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e verificar o DIA NAT Tracker e Fallback em roteadores IOS XE® usando a GUI do Cisco Catalyst Manager.

Pré-requisitos

Requisitos

A política do Cisco SD-WAN NAT DIA deve ser configurada nos dispositivos da filial. Consulte a seção [Informações Relacionadas](#) para obter instruções sobre como Implementar Acesso Direto à Internet (DIA) para SD-WAN.

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

- Cisco Catalyst SD-WAN Manager versão 20.14.1

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Restrições para o NAT DIA Tracker

Restrições para Cisco IOS XE Catalyst SD-WAN versão 17.10.1a e versões anteriores

- No Cisco IOS XE versão 17.6.x e anterior, o NAT DIA Tracker não é suportado nas interfaces do discador. A partir do Cisco IOS XE Catalyst SD-WAN Versão 17.7.1a, as subinterfaces e as interfaces do discador suportam rastreadores de endpoint único e de endpoint duplo.
- Não há suporte para o ponto de extremidade de URL DNS em dispositivos Cisco IOS XE Catalyst SD-WAN.
- Você só pode aplicar um rastreador ou grupo de rastreadores a uma interface.
- O recurso de fallback de NAT é suportado somente no Cisco IOS XE Catalyst SD-WAN Versão 17.3.2.
- O endereço IP do túnel com endereço 169.254.x.x não é suportado para rastrear o ponto de extremidade do zScaler em túneis manuais.
- Você deve configurar no mínimo dois rastreadores de endpoint únicos para configurar um grupo de rastreadores.
- Um grupo de rastreadores pode incorporar apenas um máximo de dois rastreadores de endpoint únicos.
- No Cisco IOS XE Release 17.10.1 e em versões anteriores, não é possível configurar o rastreador IPv4 em uma interface IPv6 ou vice-versa. O rastreador não estará ativo.

Restrições para Cisco IOS XE Catalyst SD-WAN Versão 17.11.1a

- O ponto de extremidade da URL da API é suportado apenas no rastreador DIA IPv6 e não no rastreador DIA IPv4.
- Os rastreadores IPv4 e IPv6 não podem ser usados no mesmo grupo de rastreadores.
- Você deve configurar o comando `allow service all` na interface de túnel TLOC para que os rastreadores IPv6 funcionem com uma interface de túnel TLOC.
- Não há suporte para várias interfaces NAT66 DIA.
- Não há suporte para fallback de NAT na política de dados centralizada.

Restrições para Cisco IOS XE Catalyst SD-WAN Versão 17.13.1a

- Não há suporte para elementos DNS de ponto de extremidade em um grupo de rastreadores.
-
-

Observação: certifique-se de usar um endereço IP de ponto final que responda às solicitações HTTP/HTTPS. Por exemplo, o servidor DNS 8.8.8.8 do Google não pode ser usado como um endereço IP de endpoint.

Interfaces suportadas para o NAT DIA Tracker

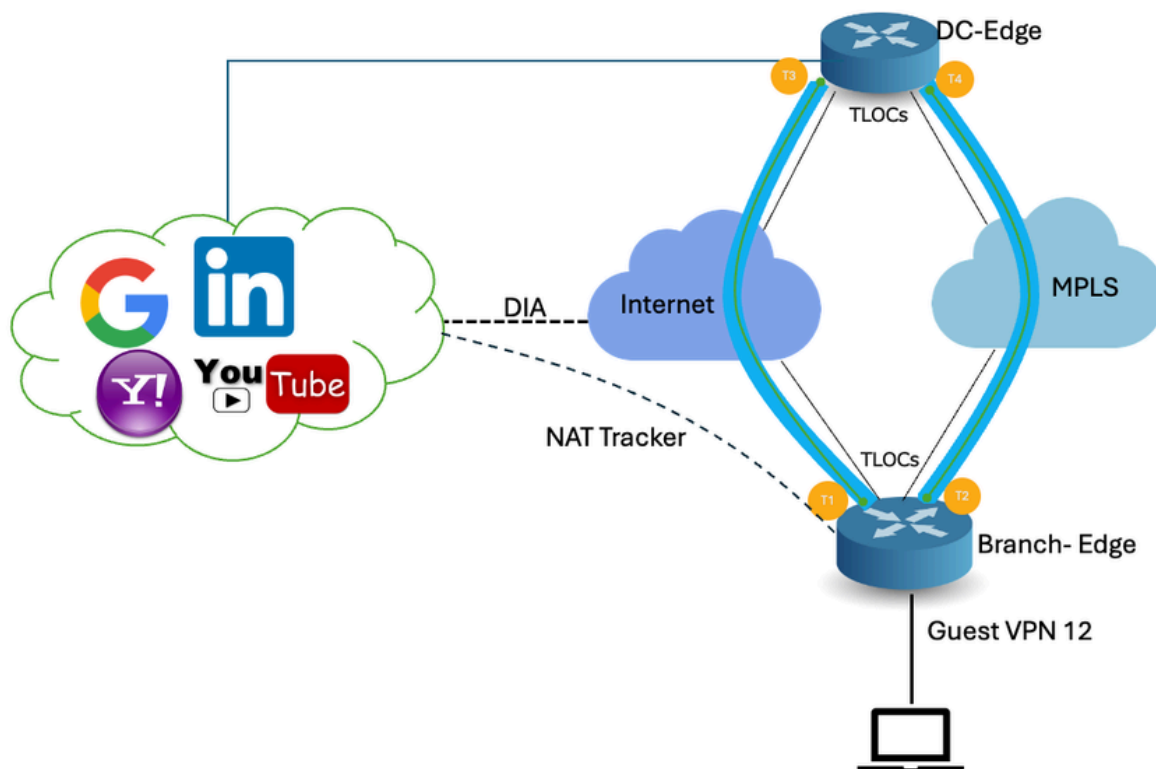
Você pode configurar o NAT DIA Tracker para as seguintes interfaces:

- Interfaces de celular
 - Interfaces de Ethernet
 - Interfaces Ethernet (PPPoE)
 - Subinterfaces
 - Interfaces do discador DSL (PPPoE e PPPoA)
-

Observação: o rastreador NAT DIA IPv6 é suportado apenas em interfaces físicas e subinterfaces de interfaces Ethernet.

Configurar

Diagrama de Rede



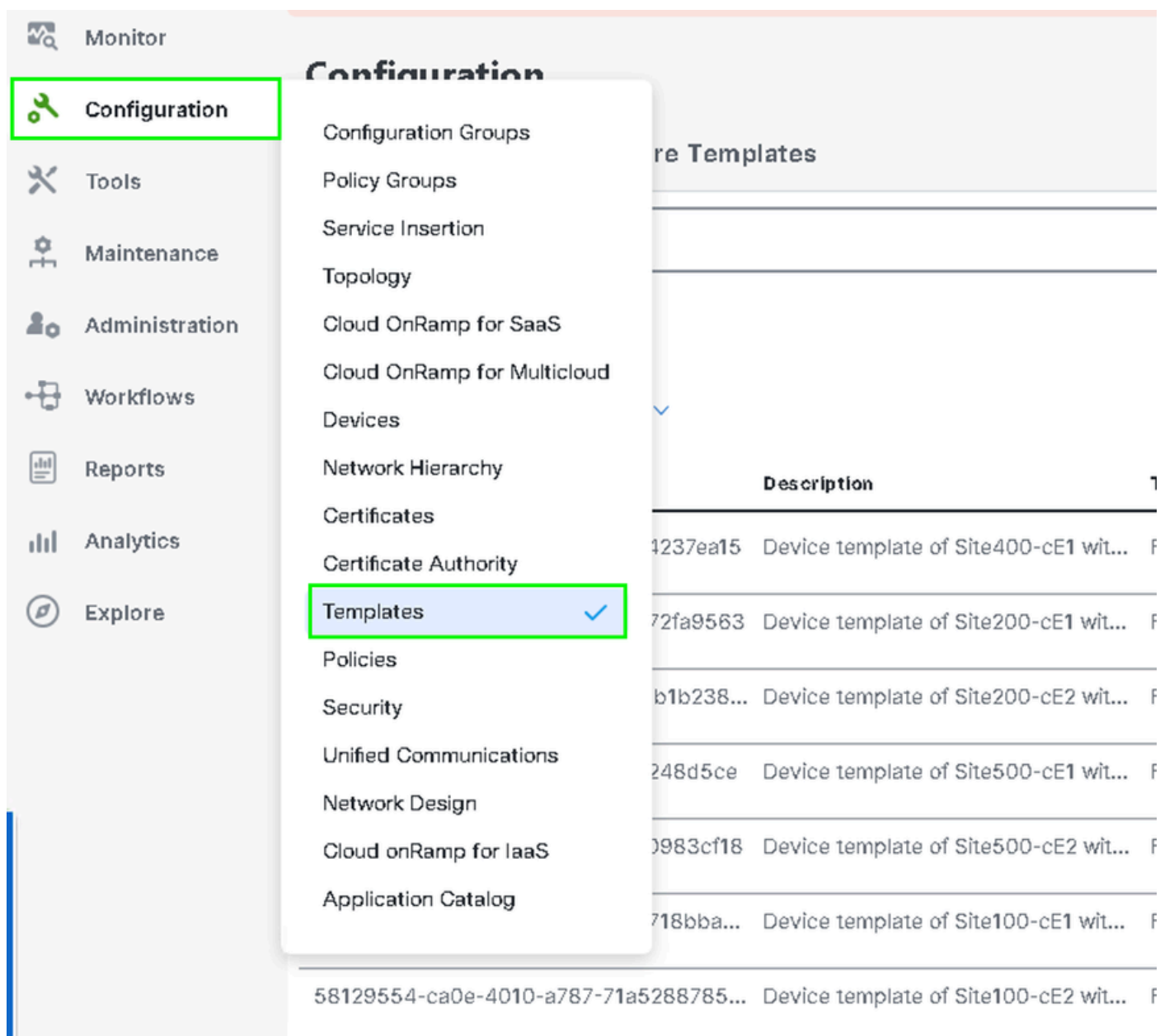
Configurações

O rastreador DIA ajuda a determinar se a Internet ou a rede externa se tornou indisponível. O recurso NAT DIA Tracking é útil quando o NAT está habilitado em uma interface de transporte na VPN 0 para permitir que o tráfego de dados do roteador saia diretamente para a Internet.

Se a Internet ou a rede externa ficar indisponível, o roteador continuará a encaminhar o tráfego com base na rota NAT no serviço VPN. O tráfego encaminhado para a Internet é descartado. Para evitar que o tráfego de destino da Internet seja descartado, configure o rastreador DIA no roteador de borda para rastrear o status da interface de transporte. O rastreador investiga periodicamente a interface para determinar o status da Internet e retorna os dados aos pontos de conexão associados ao rastreador.

Etapa 1. Configurar o NAT DIA Tracker

No menu Cisco SD-WAN Manager, navegue para 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 displays a list of configuration options. The "Templates" option is highlighted with a blue box and a checkmark. Below the configuration options, there is a table with the following columns: ID, Description, and Status. The table contains several rows of device templates.

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

Clique em Modelos de recurso. Procure o modelo de recurso Cisco System na barra de pesquisa, clique nos três pontos (...) e clique em Editar para modificar.

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

No exemplo de recurso Sistema, clique em 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 Site40C

Basic Configuration GPS **Tracker** Advanced

BASIC CONFIGURATION

Clique em New Endpoint Tracker para configurar os parâmetros do rastreador.

Tracker

TRACKERS **TRACKER GROUPS**

New Endpoint Tracker

Optional	Name	Threshold	Interval	Multiplier	Tracker Type
No data available					

Insira os parâmetros do rastreador e clique em Adicionar.

Nome: Nome do rastreador. O nome pode ter até 128 caracteres alfanuméricos. Você pode configurar até oito rastreadores.

Limite: A duração a aguardar para que o probe retorne uma resposta antes de declarar que a interface de transporte está inativa. Intervalo: 100 a 1000 milissegundos. Padrão: 300 milissegundos.

Intervalo: frequência na qual um teste é enviado para determinar o status da interface de transporte. Intervalo: 20 a 600 segundos. Padrão: 60 segundos (1 minuto).

Multiplicador: Número de vezes que um teste pode ser reenviado antes de declarar que a interface de transporte está inativa. Faixa: 1 a 10. Padrão: 3.

Tipo de rastreador: escolha Interface para configurar o rastreador DIA.

Tipo de ponto final: você pode selecionar o endereço IP ou o nome DNS ou o URL.

Nome DNS do ponto final: nome DNS do ponto final. Esse é o destino na Internet para o qual o roteador envia testes para determinar o status da interface de transporte.

Clique na lista suspensa e selecione Global para alterar qualquer valor padrão.

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.
- 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.

Clique em Update.

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

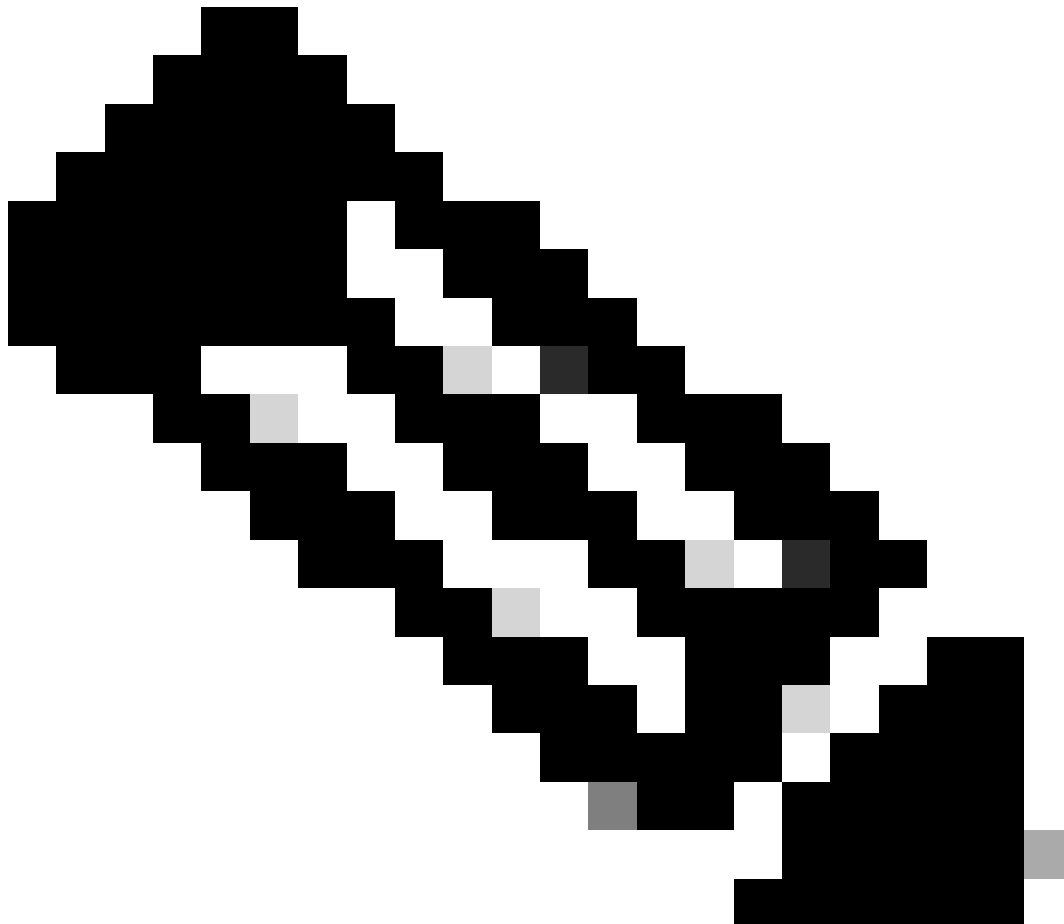
Interface SIG Route

Object ID

Interface

Cancel

Update



Observação: verifique se você configurou dois rastreadores de endpoint únicos antes de configurar um grupo de rastreadores.

Clique em Next.

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

Clique em dispositivos e verifique se a configuração está correta. Clique em Config Diff e Side by Side Diff. Clique em 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

O vManage configurou com êxito o modelo de dispositivo com a configuração do 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

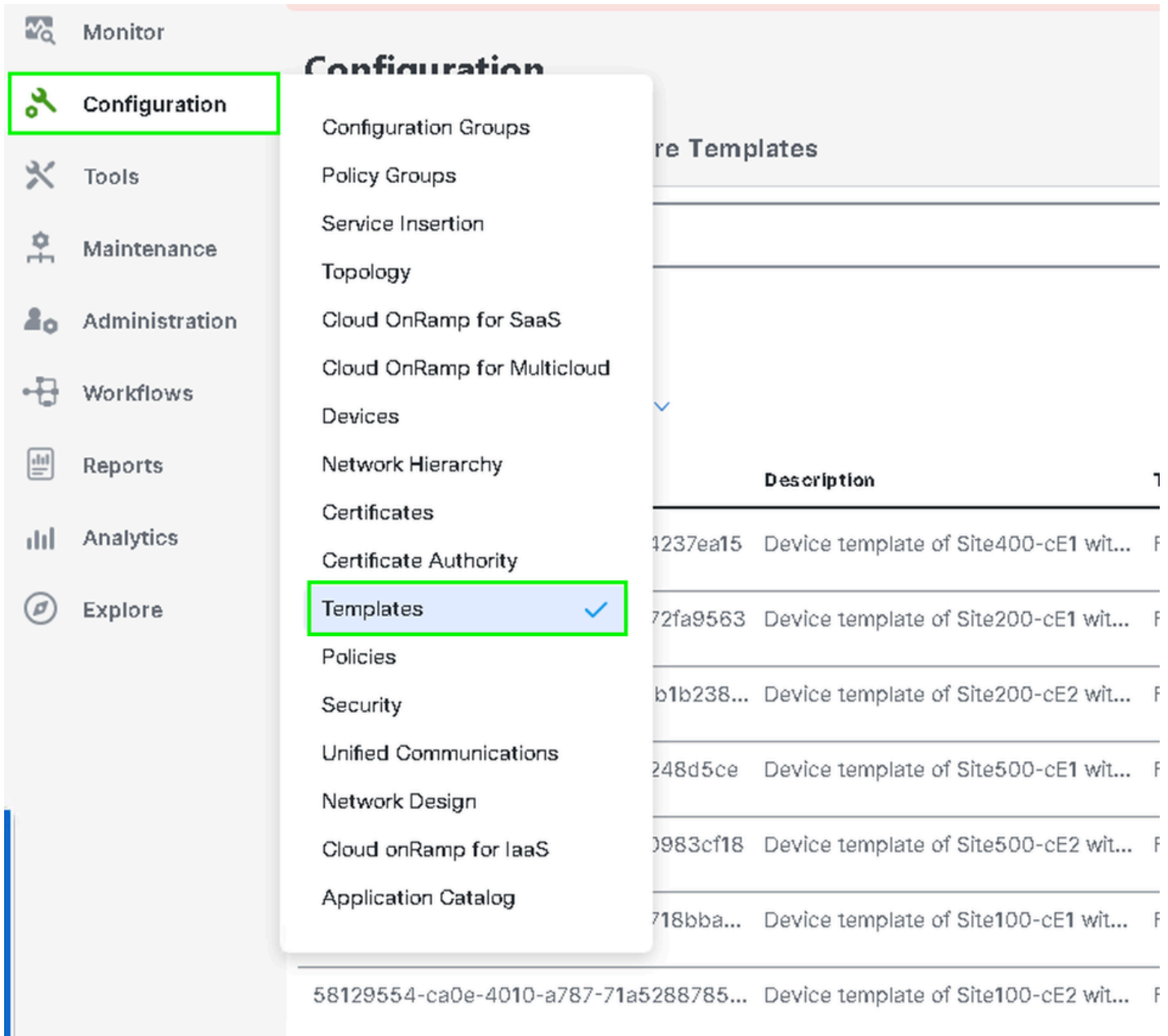
[29-Jul-2024 7:50:36 PDT] Device has pulled the configuration

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

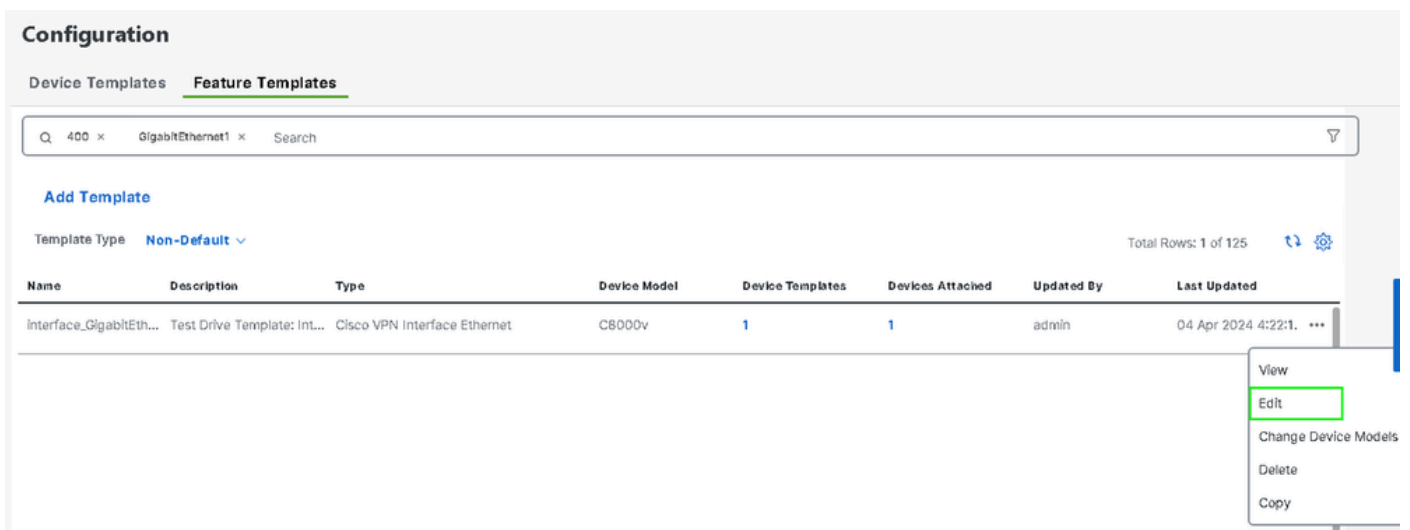
[29-Jul-2024 7:50:39 PDT] Template successfully attached to device

Etapa 2. Vincular o rastreador à interface de transporte

No menu Cisco SD-WAN Manager, navegue para Configuration > Templates.



Procure o modelo de recurso NAT Transport Interface na barra de pesquisa, clique nos três pontos (...) e clique em Edit para modificar.



Clique na guia Advanced.

Configuration

Device Templates **Feature Templates**

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

Device Type: CB000v

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 adicionar o nome do rastreador no rastreador, selecione Global no menu suspenso.

Tracker

ICMP/ICMPv6 Redirect Disable

GRE tunnel source IP

Global

Device Specific >

Default

Insira o nome do rastreador que você criou no modelo do sistema e clique em Atualizar.

Tracker

ICMP/ICMPv6 Redirect Disable

GRE tunnel source IP

Xconnect

tracker1

On Off

Cancel **Update**

Clique em Next.

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

Clique em dispositivos e verifique se a configuração está correta. Clique em Config Diff e Side by Side Diff. Clique em Configure Devices.

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

Device list (Total: 1 devices)

Filter/Search

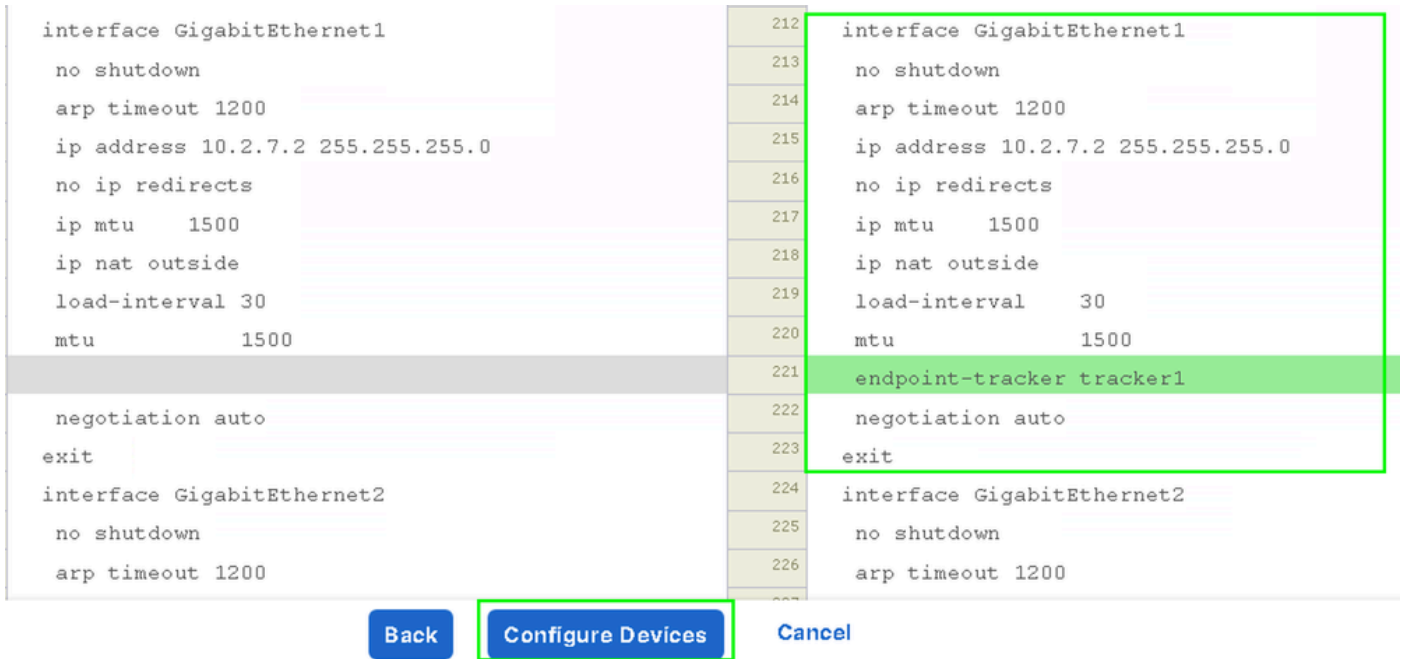
C8K-08B43DFE-2350-F2B2-E8E2-F80F3EDDB887
 Site400-cE1|1.140.1

Configure Devi...

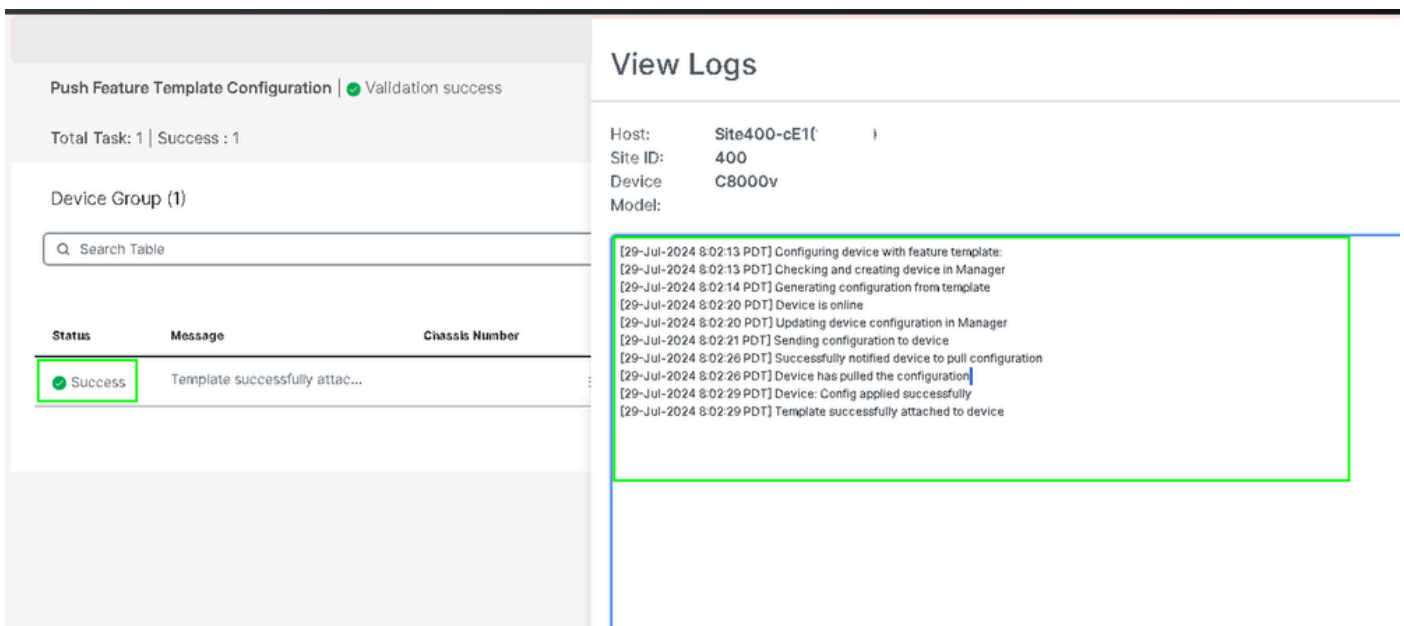
Config Preview
Config Diff

```

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
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate   115200
 no on-demand enable
 on-demand idle-timeout 10
          
```



O vManage configurou com êxito o modelo de dispositivo.



Etapa 3. Habilitar Fallback de NAT na Política de DIA Existente

Os dispositivos Cisco IOS XE Catalyst SD-WAN suportam o recurso de recuo NAT para acesso direto à Internet (DIA). O recurso de recuo de NAT permite que o tráfego use um caminho alternativo se o caminho principal de NAT falhar. Isso garante a conectividade contínua mesmo se houver problemas com a configuração de NAT principal.

Para ativar o fallback de NAT usando o Cisco SD-WAN Manager:

No menu Cisco SD-WAN Manager, navegue para 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

```

A saída mostra como verificar o status do rastreador usando os comandos show endpoint-tracker e 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

```

A saída mostra informações relacionadas ao temporizador sobre o rastreador para ajudar a depurar problemas relacionados ao rastreador, se houver:

```

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

```

A saída do 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 a configuração de fallback aplicada no dispositivo usando o 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 solução de problemas

Ative essas depurações no dispositivo de borda para verificar como o roteador envia testes para determinar o status da interface de transporte.

- Para monitorar como o roteador envia testes e determina o status das interfaces de transporte, use o comando `debug platform software sdwan tracker`, que é suportado até a versão 17.12.x.
- A partir de 17.13.x, para monitorar os logs de teste, ative essas depurações.
 - `set platform software trace ios R0 sdwanrp-tracker debug`
 - `set platform software trace ios R0 sdwanrp-cfg debug`
- Para verificar os logs relacionados ao erro e ao rastreamento das operações IP SLA, habilite essas depurações. Esses registros mostram se as operações IP SLA estão falhando.
 - `debug ip sla trace`
 - `debug ip sla error`

Execute estes comandos `show` e `monitor` para verificar os logs de depuração:

- `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
```

Informações Relacionadas

[Implementar acesso direto à Internet \(DIA\) para SD-WAN](#)

[Guia de configuração do Cisco Catalyst SD-WAN NAT](#)

[Fallback de NAT em dispositivos Cisco IOS XE Catalyst SD-WAN](#)

[Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.