

Configurazione e verifica di DIA NAT Tracker e Fallback

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Restrizioni per NAT DIA Tracker](#)

[Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.10.1a e release precedenti](#)

[Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.11.1a](#)

[Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.13.1a](#)

[Interfacce supportate per NAT DIA Tracker](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Passaggio 1. Configurazione di NAT DIA Tracker](#)

[Passaggio 2. Associa l'interfaccia da Tracker a Transport](#)

[Passaggio 3. Abilita NAT Fallback su criteri DIA esistenti](#)

[Verifica](#)

[Tracker della risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare DIA NAT Tracker e Fallback sui router Cisco IOS XE® con l'interfaccia utente di Cisco Catalyst Manager.

Prerequisiti

Requisiti

Il criterio Cisco SD-WAN NAT DIA deve essere configurato sui dispositivi della filiale. Consultare la sezione [Informazioni correlate](#) per istruzioni su come implementare Direct Internet Access (DIA) per SD-WAN.

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

- Cisco Catalyst SD-WAN Manager versione 20.14.1

- Cisco Catalyst SD-WAN Controller versione 20.14.1
- Cisco Edge Router versione 17.14.01a

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Restrizioni per NAT DIA Tracker

Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.10.1a e release precedenti

- In Cisco IOS XE versione 17.6.x e precedenti, NAT DIA tracker non è supportato sulle interfacce dialer. A partire dalla versione Cisco IOS XE Catalyst SD-WAN 17.7.1a, le sottointerfacce e le interfacce dialer supportano i tracker a endpoint singolo e doppio.
- L'endpoint URL DNS non è supportato sui dispositivi SD-WAN Cisco IOS XE Catalyst.
- È possibile applicare un solo tracciatore o gruppo di tracciatori a un'interfaccia.
- La funzione di fallback NAT è supportata solo da Cisco IOS XE Catalyst SD-WAN release 17.3.2.
- L'indirizzo IP del tunnel con indirizzo 169.254.x.x non è supportato per tenere traccia dell'endpoint zScaler sui tunnel manuali.
- È necessario configurare almeno due rilevatori di endpoint singoli per configurare un gruppo di rilevatori.
- Un gruppo di tracciatori può incorporare solo un massimo di due tracciatori di endpoint singoli.
- In Cisco IOS XE versione 17.10.1 e versioni precedenti, non è possibile configurare il tracker IPv4 su un'interfaccia IPv6 o viceversa. Il tracciatore non sarà attivo.

Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.11.1a

- L'endpoint dell'URL dell'API è supportato solo da DIA tracker IPv6 e non da DIA tracker IPv4.
- Non è possibile utilizzare i tracciatori IPv4 e IPv6 nello stesso gruppo di tracciatori.
- È necessario configurare il comando allow service all nell'interfaccia del tunnel TLOC per consentire ai tracciatori IPv6 di funzionare con un'interfaccia del tunnel TLOC.
- Non sono supportate più interfacce DIA NAT66.
- Il fallback NAT su criteri dati centralizzati non è supportato.

Restrizioni per Cisco IOS XE Catalyst SD-WAN release 17.13.1a

- Gli elementi DNS degli endpoint non sono supportati in un gruppo di individuazione.

Nota: assicurarsi di utilizzare un indirizzo IP di endpoint che risponda alle richieste HTTP/HTTPS. Ad esempio, il server DNS Google 8.8.8.8 non può essere utilizzato come indirizzo IP dell'endpoint.

Interfacce supportate per NAT DIA Tracker

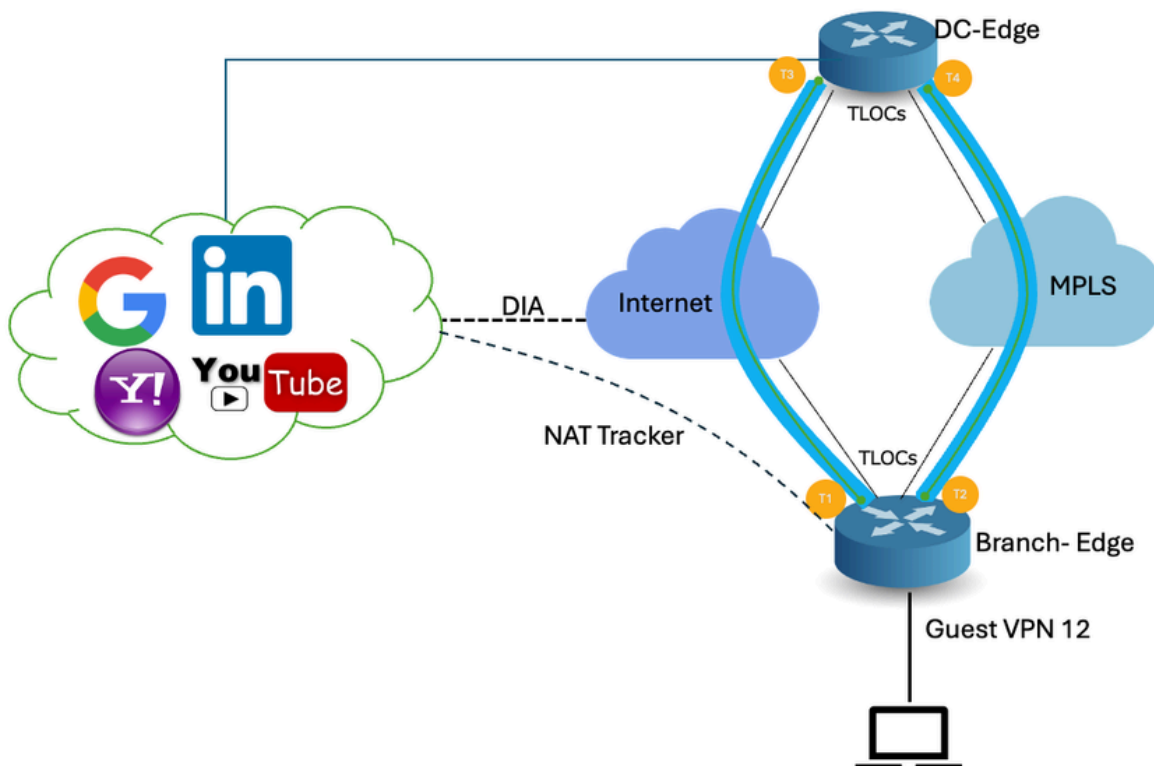
È possibile configurare NAT DIA tracker per le seguenti interfacce:

- Interfacce cellulari
- Interfacce Ethernet
- Interfacce Ethernet (PPPoE)
- Sottointerfacce
- Interfacce dialer DSL (PPPoE e PPPoA)

Nota: IPv6 NAT DIA tracker è supportato solo sulle interfacce fisiche e secondarie delle interfacce Ethernet.

Configurazione

Esempio di rete



Configurazioni

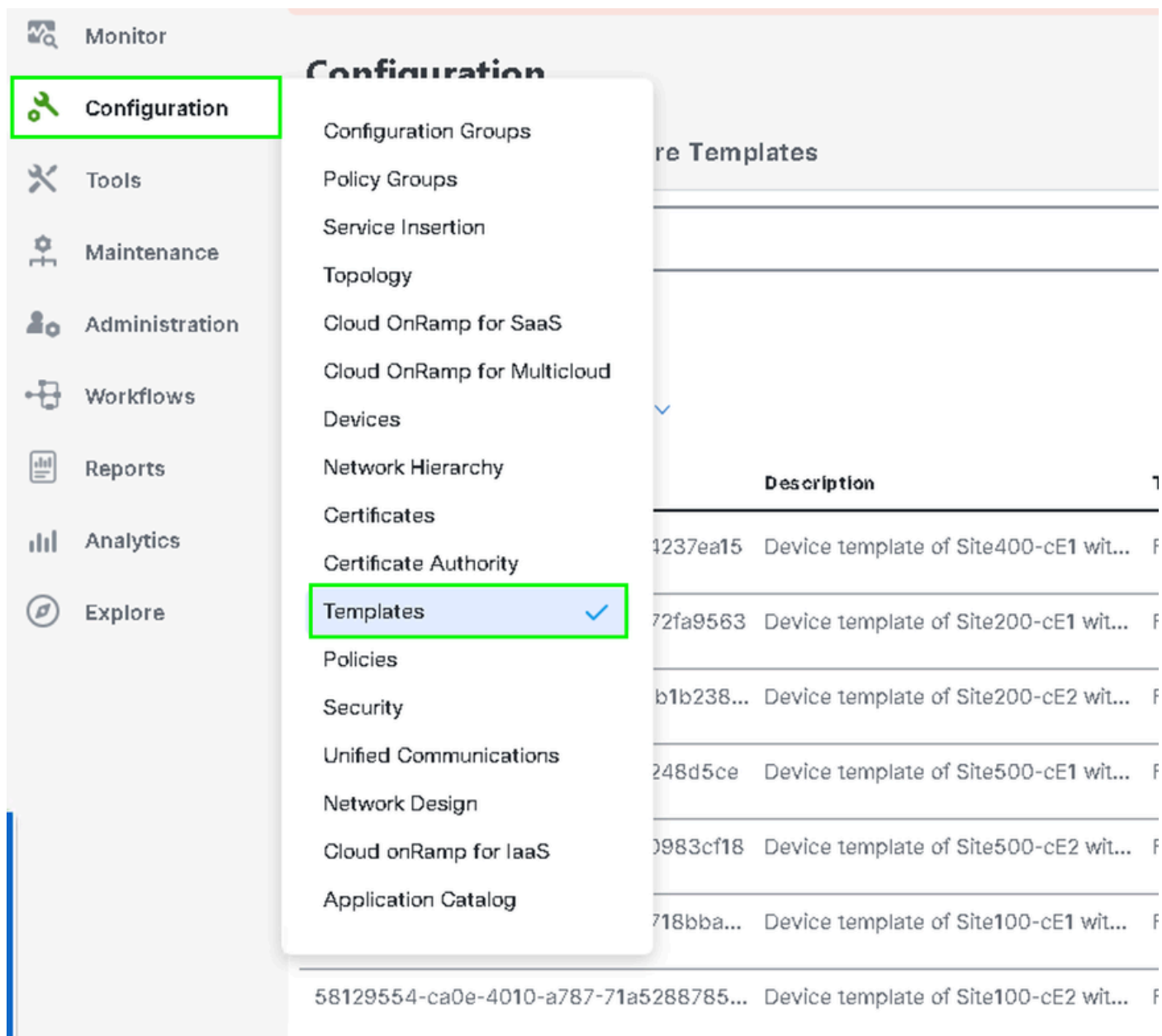
Il tracciatore DIA consente di determinare se Internet o la rete esterna non sono più disponibili. La funzione NAT DIA Tracking è utile quando NAT è abilitato su un'interfaccia di trasporto nella VPN 0 per consentire al traffico di dati dal router di uscire direttamente a Internet.

Se Internet o la rete esterna non è più disponibile, il router continua a inoltrare il traffico in base al percorso NAT nella VPN del servizio. Il traffico che viene inoltrato a Internet viene scartato. Per

evitare che il traffico Internet venga interrotto, configurare DIA tracker sul router perimetrale in modo che tenga traccia dello stato dell'interfaccia di trasporto. Il tracker effettua periodicamente delle verifiche sull'interfaccia per determinare lo stato di Internet e restituire i dati ai punti di collegamento associati al tracker.

Passaggio 1. Configurazione di NAT DIA Tracker

Dal menu Cisco SD-WAN Manager, selezionare Configurazione > Modelli.



Fate clic su Modelli feature (Feature Templates). Cercare il modello della funzionalità di Cisco System nella barra di ricerca, fare clic sui tre punti (...), quindi fare clic su Modifica per apportare le modifiche desiderate.

Configuration

Device Templates **Feature Templates**

Q 400 × system × 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

Nell'esempio delle funzionalità di sistema, fare clic su Tracker.

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

Fare clic su New Endpoint Tracker per configurare i parametri di rilevamento.

Tracker

TRACKERS TRACKER GROUPS

New Endpoint Tracker

Optional	Name	Threshold	Interval	Multiplier	Tracker Type
No data available					

Immettere i parametri di rilevamento e fare clic su Aggiungi.

Nome: il nome del tracciatore. Il nome può contenere un massimo di 128 caratteri alfanumerici. È

possibile configurare fino a otto tracker.

Soglia: periodo di attesa della risposta della sonda prima che venga dichiarato che l'interfaccia di trasporto è inattiva. Intervallo: da 100 a 1000 millisecondi. Impostazione predefinita: 300 millisecondi.

Intervallo: frequenza di invio di una sonda per determinare lo stato dell'interfaccia di trasporto. Intervallo: da 20 a 600 secondi. Impostazione predefinita: 60 secondi (1 minuto).

Moltiplicatore: numero di volte in cui è possibile inviare nuovamente una sonda prima di dichiarare che l'interfaccia di trasporto è inattiva. Range: da 1 a 10. Predefinito: 3.

Tipo di tracciatore: scegliere Interfaccia per configurare il tracciatore DIA.

Tipo di endpoint: è possibile selezionare un indirizzo IP, un nome DNS o un URL.

Nome DNS endpoint: nome DNS dell'endpoint. Questa è la destinazione nell'Internet a cui il router invia le richieste per determinare lo stato dell'interfaccia di trasporto.

Fare clic sull'elenco a discesa e selezionare Globale per modificare qualsiasi valore predefinito.

The screenshot shows a configuration window titled "Tracker". At the top, there are tabs for "TRACKERS" and "TRACKER GROUPS", with a "New Endpoint Tracker" button. The form contains the following fields:

- Name:** A text input field containing "tracker1".
- Threshold:** A numeric input field containing "300".
- Interval:** A dropdown menu with "Global" selected. A sub-menu is open showing "Global", "Device Specific >", and "Default".
- Multiplier:** A dropdown menu with "Default" selected.
- 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 border.

Fare clic su Aggiorna.

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

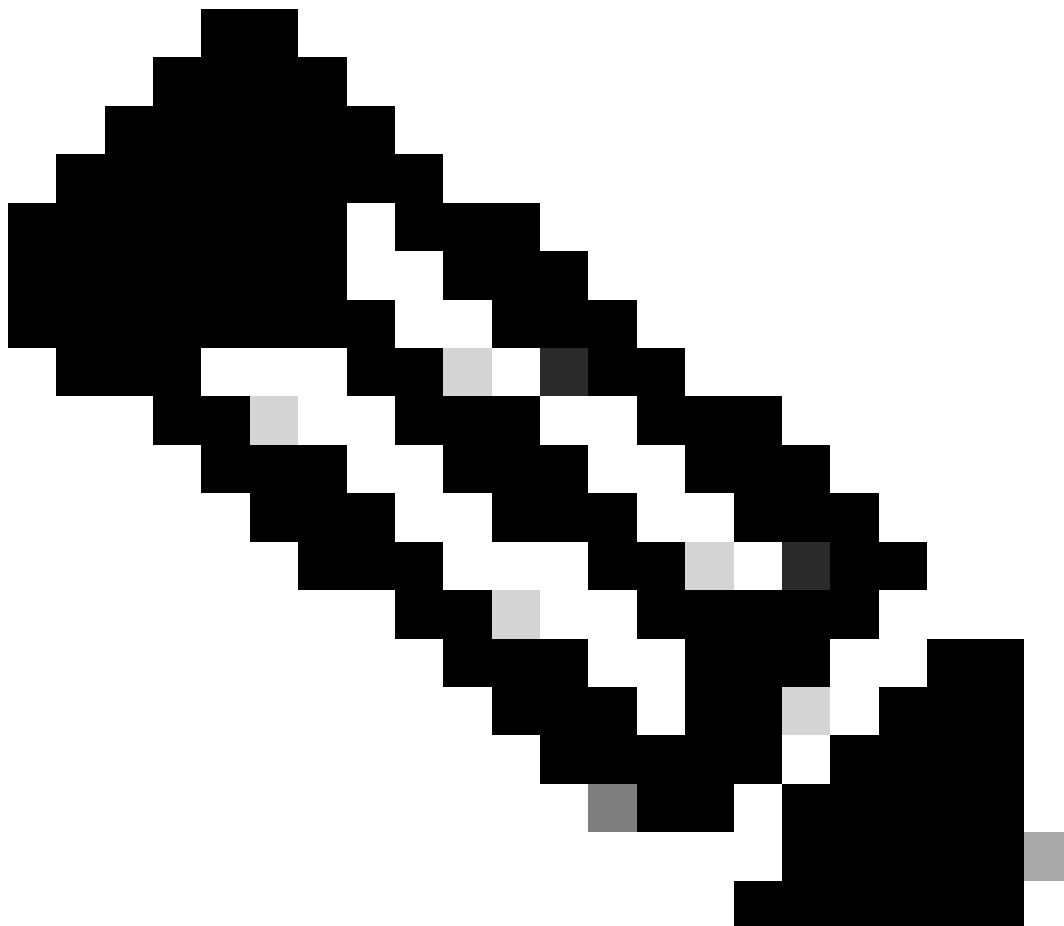
Interface SIG Route

Object ID

Interface

Cancel

Update



Nota: prima di configurare un gruppo di tracciatori, accertarsi di aver configurato due rilevatori di endpoint singoli.

Fare clic su Next (Avanti).

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

Fare clic su devices (Dispositivi), quindi verificare che la configurazione sia corretta. Fare clic su Config Diff e su Side by Side Diff. Fare clic su 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|1.1.40.1

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

Back
Configure Devices
Cancel

vManage: configurazione del modello di dispositivo con la configurazione del tracker completata.

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

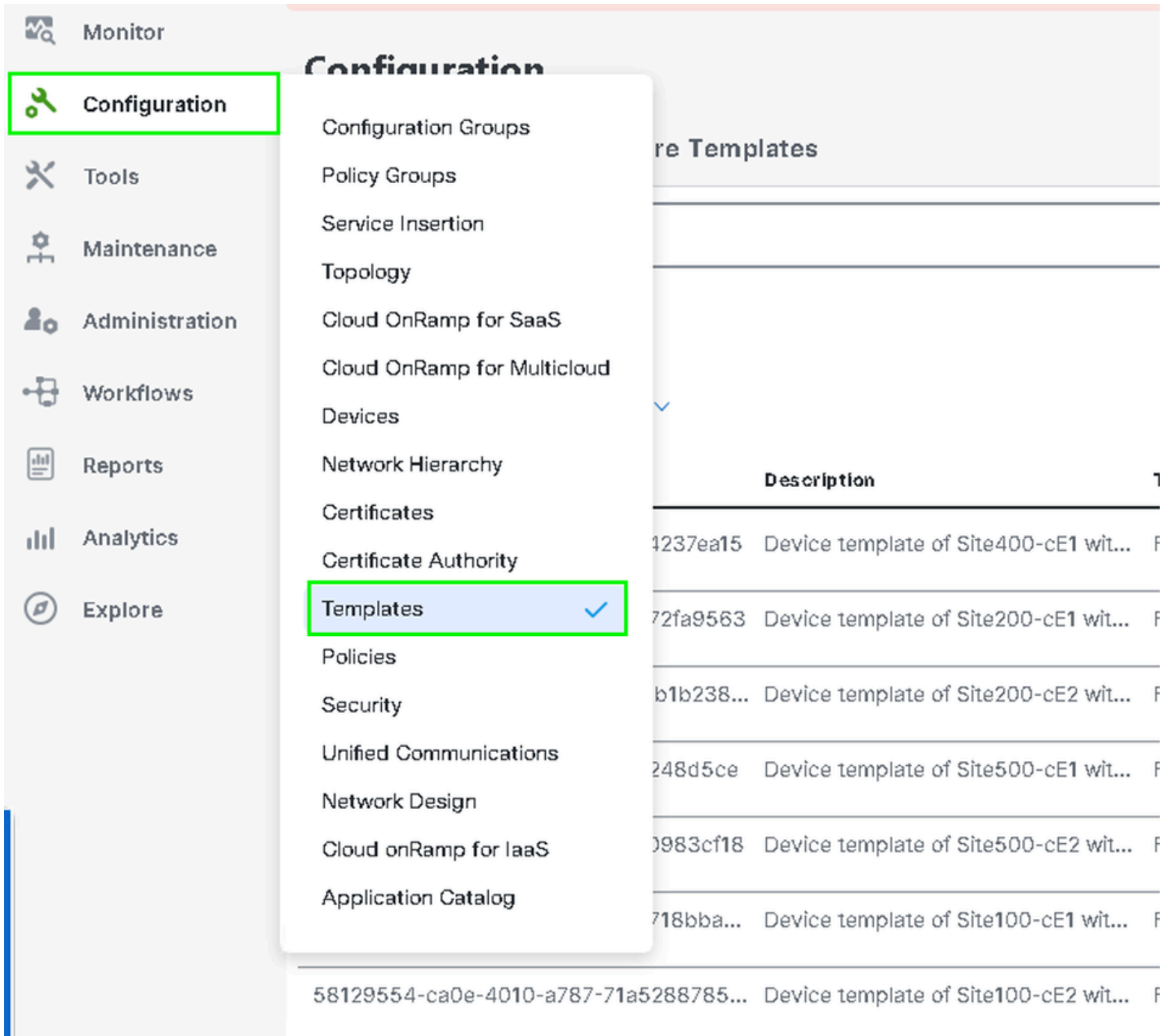
Device: C8000v

Model:

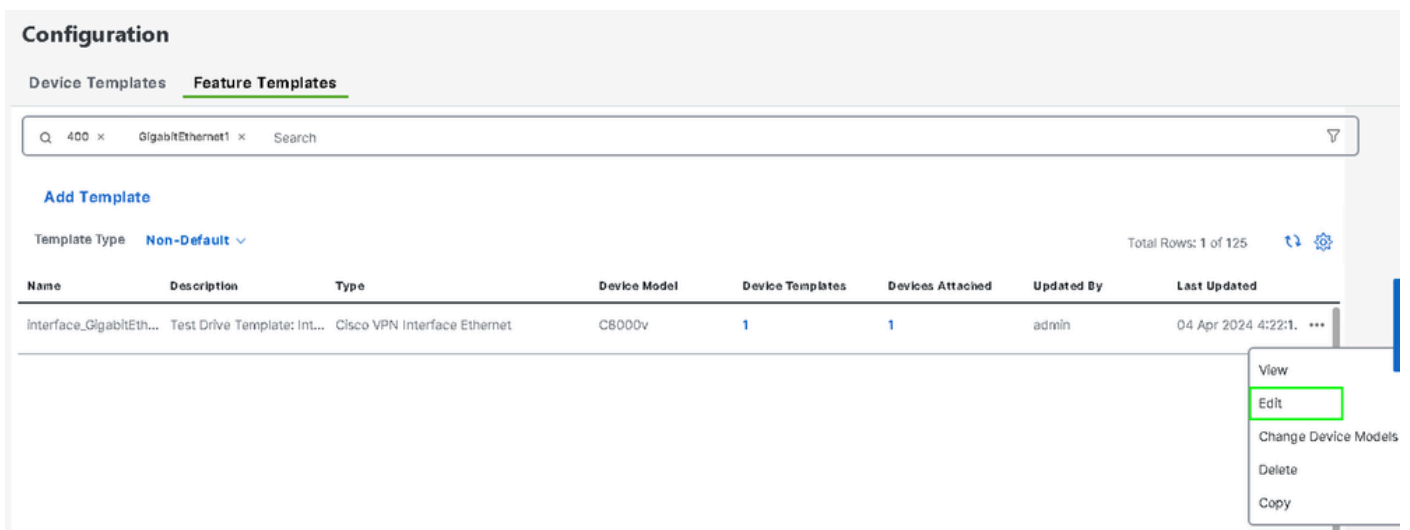
[29-Jul-2024 7:50:20 PDT] Configuring device with feature template:
 [29-Jul-2024 7:50:21 PDT] Checking and creating device in Manager
 [29-Jul-2024 7:50:22 PDT] Generating configuration from template
 [29-Jul-2024 7:50:29 PDT] Device is online
 [29-Jul-2024 7:50:29 PDT] Updating device configuration 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

Passaggio 2. Associa l'interfaccia da Tracker a Transport

Nel menu Cisco SD-WAN Manager, selezionare Configuration > Templates (Configurazione > Modelli).



Cercare il modello della funzionalità Interfaccia trasporto NAT nella barra di ricerca, fare clic sui tre punti (...) e fare clic su Modifica per apportare le modifiche desiderate.



Fare clic sulla scheda Avanzate.

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**

Per aggiungere il nome del tracciatore nel Tracker, selezionare Globale dal menu a discesa.

Tracker

ICMP/ICMPv6 Redirect Disable

GRE tunnel source IP

Global

Device Specific >

Default

Immettere il nome del tracciatore creato nel modello di sistema e fare clic su Aggiorna.

Tracker: tracker1

ICMP/ICMPv6 Redirect Disable: On

GRE tunnel source IP

Xconnect

Cancel **Update**

Fare clic su Next (Avanti).

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

Fare clic su devices (Dispositivi), quindi verificare che la configurazione sia corretta. Fare clic su Config Diff e su Side by Side Diff. Fare clic su 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...

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
          
```

interface GigabitEthernet1	212	interface GigabitEthernet1
no shutdown	213	no shutdown
arp timeout 1200	214	arp timeout 1200
ip address 10.2.7.2 255.255.255.0	215	ip address 10.2.7.2 255.255.255.0
no ip redirects	216	no ip redirects
ip mtu 1500	217	ip mtu 1500
ip nat outside	218	ip nat outside
load-interval 30	219	load-interval 30
mtu 1500	220	mtu 1500
	221	endpoint-tracker tracker1
negotiation auto	222	negotiation auto
exit	223	exit
interface GigabitEthernet2	224	interface GigabitEthernet2
no shutdown	225	no shutdown
arp timeout 1200	226	arp timeout 1200

Back
Configure Devices
Cancel

vManage: configurazione del modello di dispositivo completata.

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 8:02:13 PDT] Configuring device with feature template:

[29-Jul-2024 8:02:13 PDT] Checking and creating device in Manager

[29-Jul-2024 8:02:14 PDT] Generating configuration from template

[29-Jul-2024 8:02:20 PDT] Device is online

[29-Jul-2024 8:02:20 PDT] Updating device configuration in Manager

[29-Jul-2024 8:02:21 PDT] Sending configuration to device

[29-Jul-2024 8:02:26 PDT] Successfully notified device to pull configuration

[29-Jul-2024 8:02:26 PDT] Device has pulled the configuration

[29-Jul-2024 8:02:29 PDT] Device: Config applied successfully

[29-Jul-2024 8:02:29 PDT] Template successfully attached to device

Passaggio 3. Abilita NAT Fallback su criteri DIA esistenti

I dispositivi Cisco IOS XE Catalyst SD-WAN supportano la funzione di fallback NAT per Direct Internet Access (DIA). La funzionalità di fallback NAT consente al traffico di utilizzare un percorso alternativo se il percorso NAT primario ha esito negativo. Ciò assicura una connettività continua anche in caso di problemi con la configurazione NAT principale.

Per abilitare il fallback NAT utilizzando Cisco SD-WAN Manager:

Dal menu Cisco SD-WAN Manager, selezionare Configuration > Policy (Configurazione > Criteri).



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

```

L'output mostra come verificare lo stato del tracciatore utilizzando i comandi show endpoint-tracker e show endpoint-tracker Gigabit Ethernet1.

```

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

```

L'output mostra le informazioni relative al timer sul tracker per facilitare il debug di eventuali problemi correlati al tracker:

```

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

```

L'output 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

Verificare la configurazione di fallback applicata al dispositivo utilizzando il 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
```

Tracker della risoluzione dei problemi

Abilitare questi debug sul dispositivo perimetrale per controllare come il router invia le richieste per determinare lo stato dell'interfaccia di trasporto.

- Per monitorare il modo in cui il router invia le richieste e determina lo stato delle interfacce di trasporto, usare il comando `debug platform software sdwan tracker` che è supportato fino alla versione 17.12.x.
- A partire dalla versione 17.13.x, per monitorare i registri delle richieste, abilitare i debug.
 - `set platform software trace ios R0 sdwanrp-tracker debug`
 - `set platform software trace ios R0 sdwanrp-cfg debug`
- Per controllare i log relativi agli errori e alla traccia delle operazioni del contratto di servizio IP, abilitare questi debug. Questi registri mostrano se le operazioni dello SLA IP hanno esito negativo.
 - `traccia debug ip sla`
 - `errore debug ip sla`

Eseguire i seguenti comandi `show and monitor` per controllare i log di debug:

- `show logging profile sdwan internal`

- profilo di registrazione monitor 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
```

Informazioni correlate

[Implementazione dell'accesso diretto a Internet \(DIA\) per SD-WAN](#)

[Guida alla configurazione di Cisco Catalyst SD-WAN NAT](#)

[Fallback NAT sui dispositivi Cisco IOS XE Catalyst SD-WAN](#)

[Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).