Configurazione di ThousandEyes Agent-to-Server SD-WAN Service-Side con contrassegno DSCP

Sommario

Introduzione

Questo documento descrive la configurazione di ThousandEyes Agent-to-Server SD-WAN con contrassegno DSCP per il monitoraggio del traffico in una sovrapposizione Cisco SD-WAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- Panoramica generale su SD-WAN
- Modelli
- Migliaia di occhi

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Cisco Manager versione 20.15.3
- Cisco Validator versione 20.15.3

- Cisco Controller versione 20.15.3
- ISR (Integrated Service Router)4331/K9 versione 17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

Configurazioni preliminari

- Configura DNS: Il router può risolvere il DNS e accedere a Internet sulla VPN 0.
- Configurare NAT DIA: La configurazione DIA deve essere presente sul router.

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.

Test da agente a server

Per eseguire un test da agente a server, è necessario configurare l'agente ThousandEyes sulla VPN del servizio. In questo scenario, il server è l'indirizzo IP TLOC monitorato. In genere, un test da agente a server viene utilizzato per monitorare un server; tuttavia, in questo caso, viene utilizzato per monitorare un'interfaccia TLOC situata in un sito diverso da quello in cui è ospitato l'agente.

Se sono presenti più interfacce TLOC, utilizzare l'accesso diretto a Internet (DIA) NAT e un criterio dati per reindirizzare il traffico all'interfaccia TLOC VPN 0 desiderata. Impostare i criteri di corrispondenza in base al valore DSCP configurato sul lato agente in ThousandEyes da reindirizzare verso e attraverso la VPN 0, eseguendo contemporaneamente il demarking per evitare che l'ISP venga sovraccaricato con il proprio contrassegno DSCP.

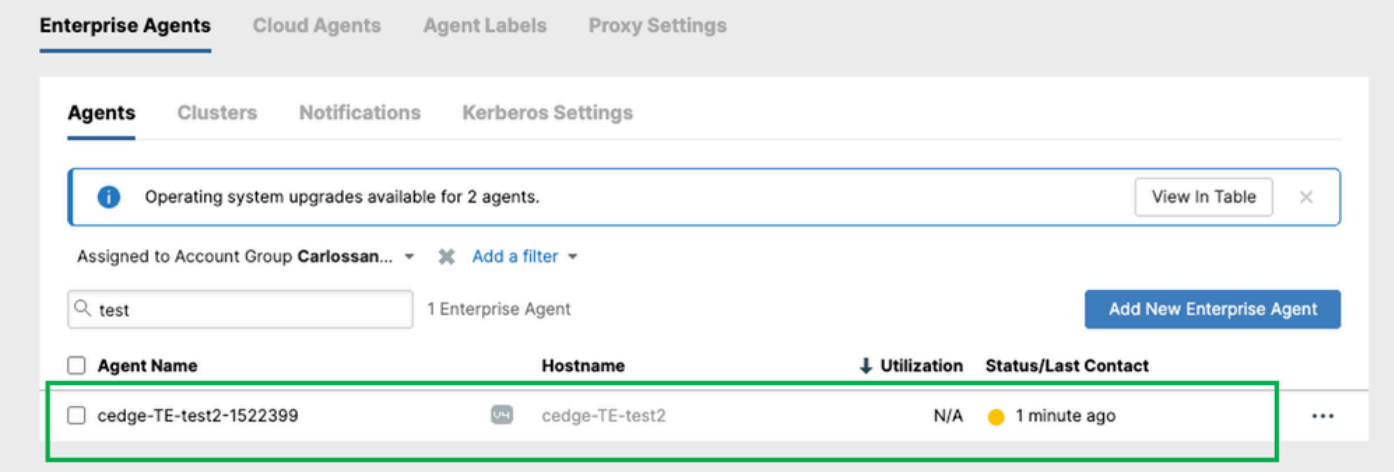
Configurazione

Configurazione di ThousandEyes Test e DSCP

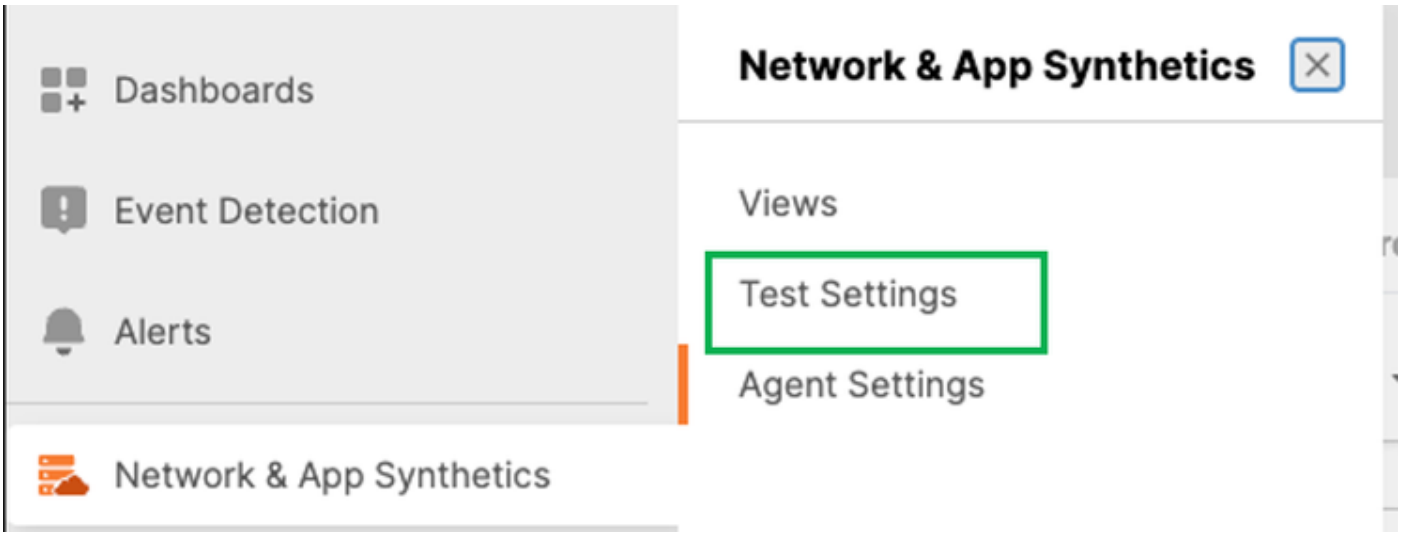
Per configurare DSCP (Differentiated Services Code Point):

1. Accedere all'account ThousandEyes dalla pagina Cisco ThousandEyes Agentpage.

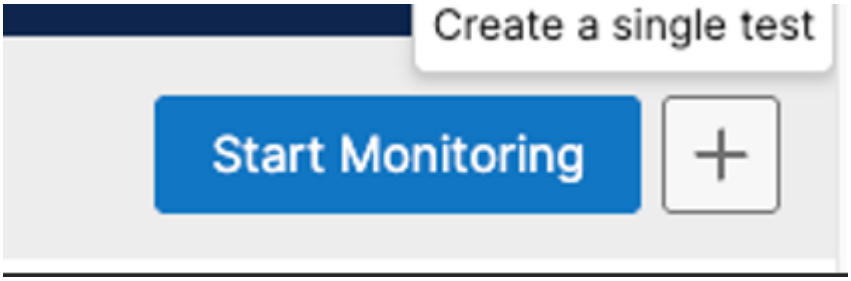
Verificare che l'agente installato nel router comunichi con ThousandEyes Cloud.



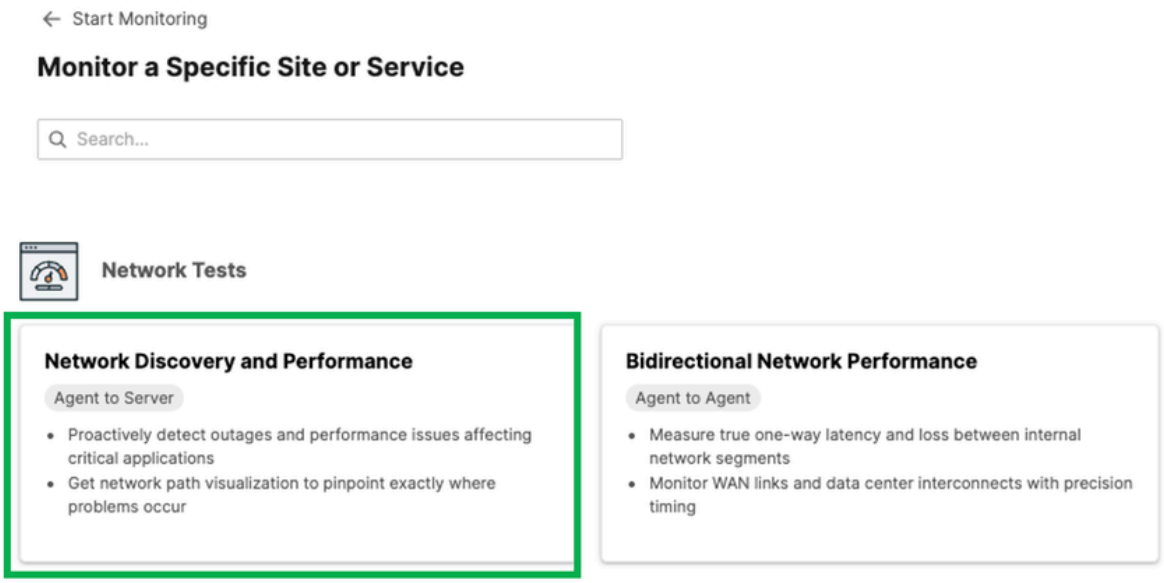
Una volta installato l'agente sul dispositivo e confermata la comunicazione con ThousandEyes Cloud, creare un test. Per creare un test, spostarsi in Network & App Synthetics > Test Settings.



Nella schermata in alto a destra, fare clic sull'icona +.

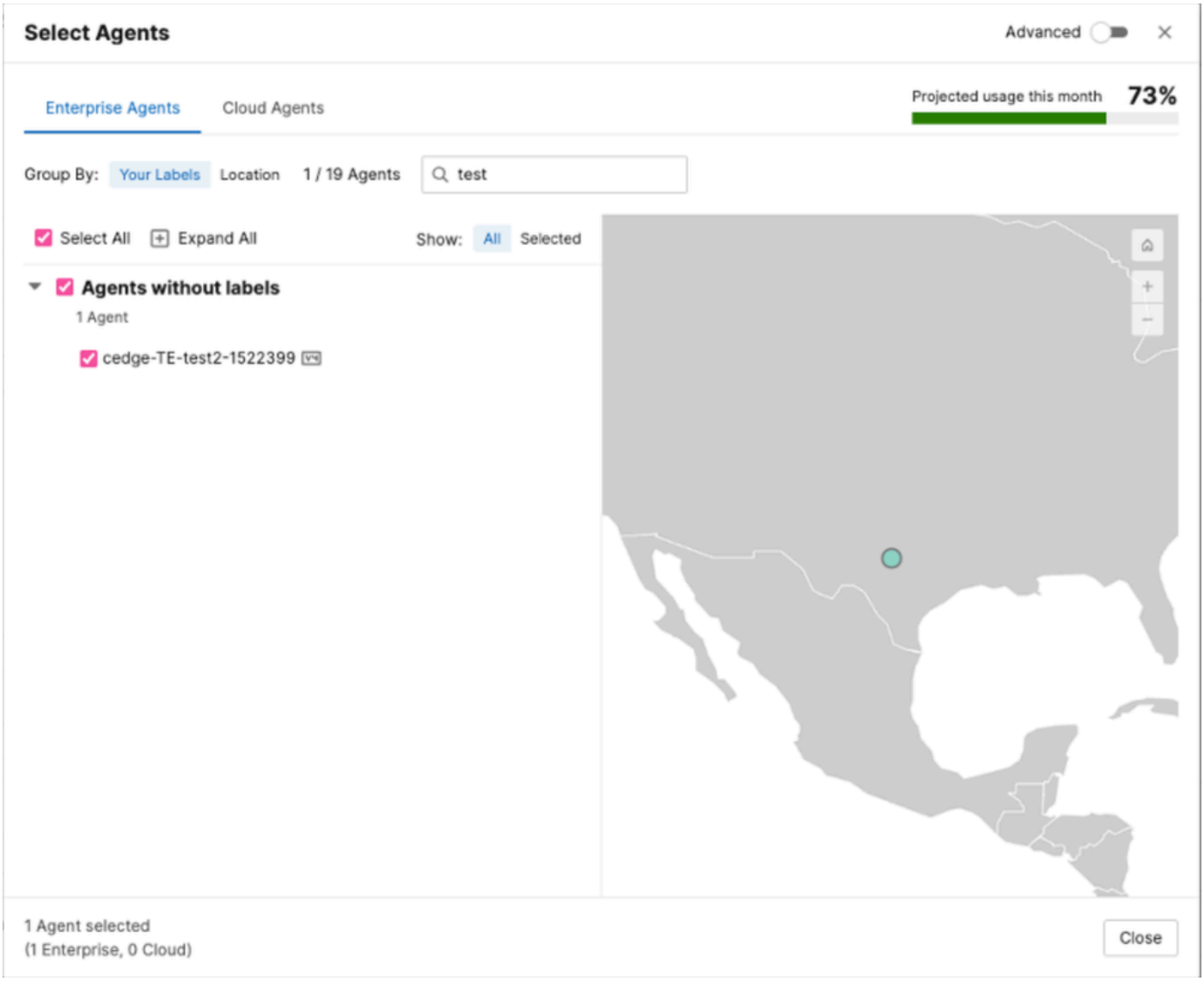


Nel nuovo dashboard selezionare Test da agente a server.



Nella sezione "Destinazione", selezionare l'indirizzo IP da utilizzare per il test. Nell'esempio, viene usato 192.168.1.47, che è l'indirizzo IP di un altro TLOC su un router diverso all'interno della stessa subnet.

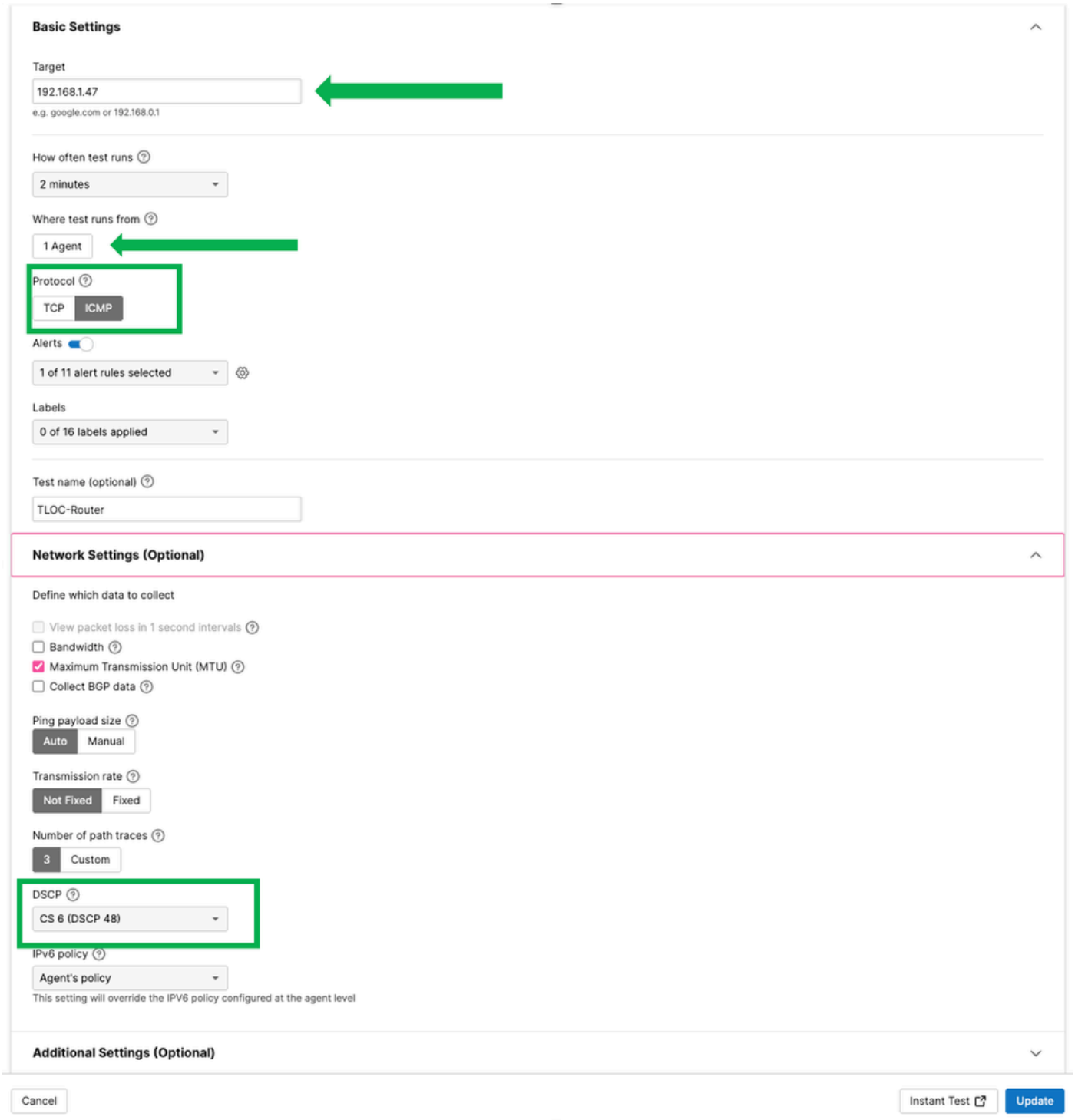
In "Where test running From", selezionare l'agente creato per il router (contenente il nome host del router) come mostrato di seguito:



Seleziona protocollo ICMP

Nella sezione Impostazioni di rete (facoltative), selezionare DSCP e fare clic su Aggiorna.

Nella stessa sezione fare clic su Test immediato.



Configurazione di SD-WAN

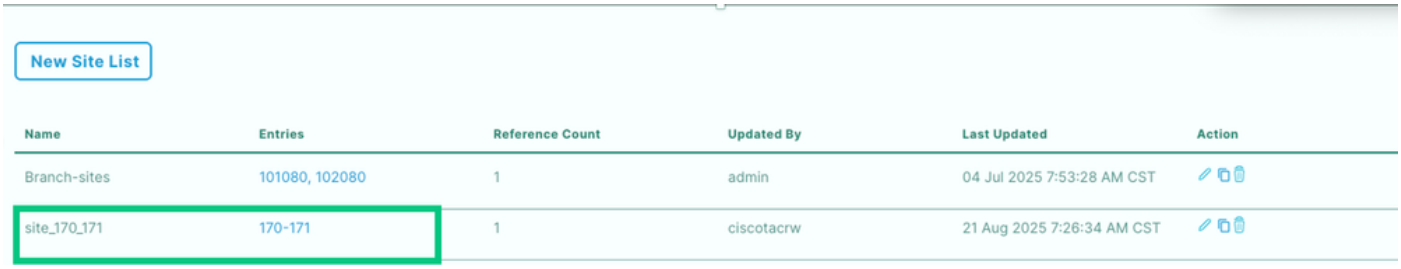
Utilizzare il documento di riferimento per configurare Thousand Eyes Agent sul router perimetrale [Configurare ThousandEyes sui dispositivi SD-WAN]

Una volta installato l'agente ThousandEyes sul router, il modello ThousandEyes visualizza le informazioni seguenti:

Configurare DSCP

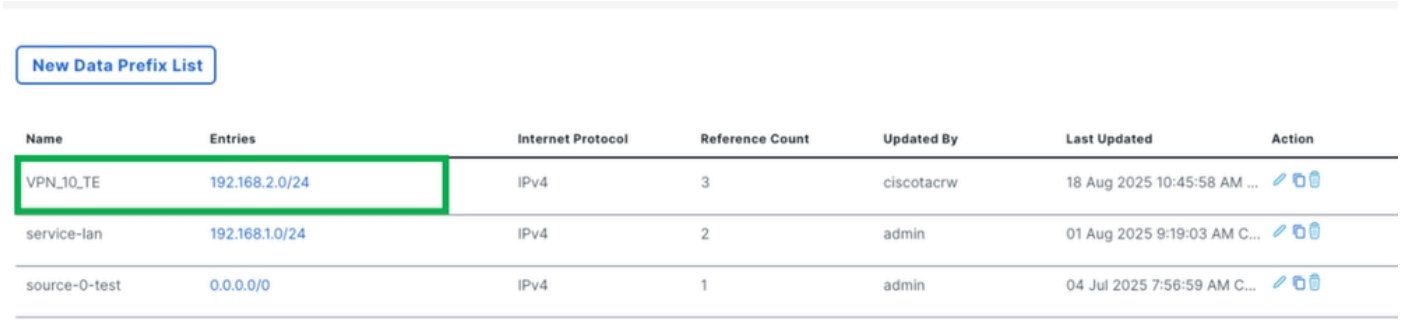
Selezionare Configuration > Policies >Centralized Policy > Click on Add policy. Al momento della creazione del gruppo di interesse, aggiungere Sito, VPN e Prefisso dati.

Sito (sito in cui è stato installato l'agente ThousandEyes)



VPN (Service VPN)

Prefisso dati (include la subnet configurata nel modello ThousandEyes) in questo esempio è stata utilizzata la subnet 192.168.2.0/24.



Fare clic su Avanti > Avanti, nella sezione Configurazione regole traffico selezionare Dati traffico, quindi fare clic su Aggiungi criterio.

Selezionare DSCP, in questo esempio utilizzato 48

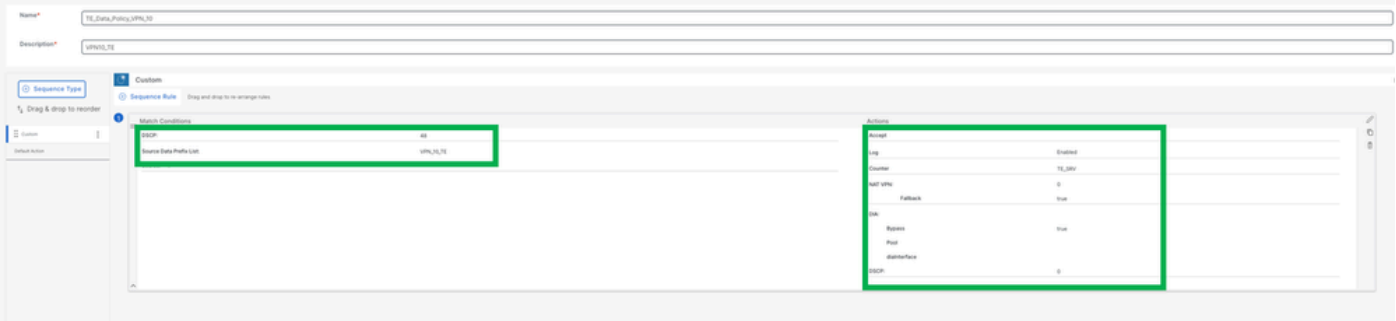
Scegliere l'opzione "Elenco prefissi dati di origine". Utilizzare "VPN_10_TE" (come documentato in precedenza), ossia la rete utilizzata per la configurazione ThousandEyes sul router.

Sezione Azioni:

Seleziona VPN NAT

Fallback

In questo esempio, DSCP configurato è 0



Azione predefinita abilitata.

Fare clic su Avanti, aggiungere Nome criterio e Descrizione criterio. Nella sezione Traffic Data (Dati sul traffico), fare clic su New Site/WAN Region List (Nuovo elenco siti/aree WAN) and VPN List (Elenco VPN), salvare la policy e attivarla,

Dopo aver attivato il criterio, verificare nel router il criterio applicato:

Eseguire il comando show sdwan policy from-vsmart

```
cedge-TE-test2#show sdwan  policy from-vsmart
from-vsmart data-policy _VPN_10_TE_Data_Policy_VPN_10
 direction from-service
 vpn-list VPN_10
  sequence 1
   match
    source-data-prefix-list VPN_10_TE
    dscp                    48
   action accept
    count TE_SRV_1549695060
    nat use-vpn 0
    nat fallback
    log
    set
     dscp 0

  default-action accept
from-vsmart lists vpn-list VPN_10
 vpn 10
from-vsmart lists data-prefix-list VPN_10_TE
 ip-prefix 192.168.2.0/24
```

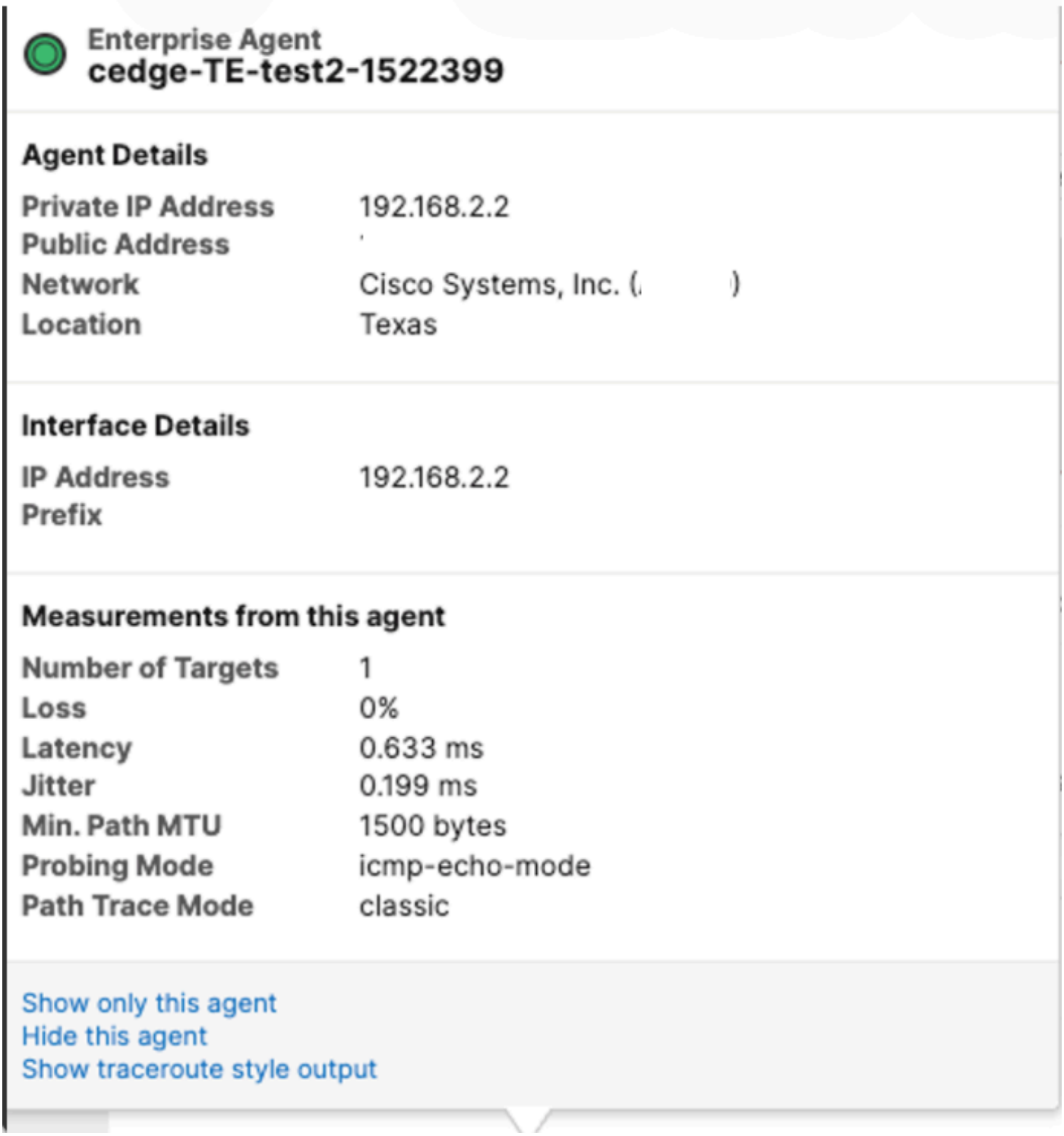
Verifica

Per eseguire un test, fare clic su Installa test e aprire una nuova finestra.

Una volta completato il test, è possibile vedere il percorso che ha richiesto per raggiungere il 192.168.1.47

Agent192.168.2.2 >>>>>DG TE 192.168.2.1 >>>>>Test 192.168.1.47

Dove è stato contrassegnato come dscp48 prima di andare per la base e dopo andare sopra la base è contrassegnare come 0.



Configurare una traccia FIA sul router perimetrale:

```
debug platform condition ipv4 <ip address> both

debug platform packet-trace packet 2048 circular fia-trace data-size 4096

debug platform packet-trace copy packet both size 128 L2
```

Aprire un pacchetto:

<#root>

```
cedge-TE-test2#show platform  packet-trace  packet 0 decode
Packet: 0           CBUG ID: 3480
Summary
  Input     : VirtualPortGroup4
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 149091925690917 ns (08/19/2025 19:30:43.807639 UTC)
    Stop    : 149091925874126 ns (08/19/2025 19:30:43.807822 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : VirtualPortGroup4
    Output      : <unknown>
    Source      : 192.168.2.2
    Destination : 192.168.1.47
    Protocol    : 1 (ICMP)
  <Omitted output>
  Feature: NBAR
    Packet number in flow: N/A
    Classification state: Final
    Classification name: ping
    Classification ID: 1404 [CANA-L7:479]
    Candidate classification sources:
      DPI: ping [1404]
    Early cls priority: 0
    Permit apps list id: 0
    Sdavc Early prioirty as app: 0
    Classification visibility name: ping
    Classification visibility ID: 1404 [CANA-L7:479]
    Number of matched sub-classifications: 0
    Number of extracted fields: 0
    Is PA (split) packet: False
    Is FIF (first in flow) packet: False
    TPH-MQC bitmask value: 0x0
    Source MAC address: 52:54:DD:82:B5:F8
    Destination MAC address: 00:27:90:64:D6:D0
    Traffic Categories: N/A
  Feature: IPV4_INPUT_STILE_LEGACY
    Entry       : Input - 0x8142ecc0
    Input       : VirtualPortGroup4
    Output      : <unknown>
    Lapsed time : 23615 ns
 <Omitted output>
  Feature: SDWAN Data Policy IN
    VPN ID      : 10
    VRF         : 2
    Policy Name  :

_VPN_10_DP_VPN10_TLOC-VPN_10 (CG:5)

 <<<<<<<<<<<
    Seq         : 1
    DNS Flags   : (0x0) NONE
    Policy Flags : 0x80210018
    Policy Flags2: 0x0
    Action      : POL_LOG
    Action      :

SET_DSCP default(0)

   <<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

```
Action       : REDIRECT_NAT
Action       : NAT_FALLBACK
```

Informazioni correlate

- Configurazione di ThousandEyes sui dispositivi 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).