使用DSCP標籤配置ThousandEyes Agent-to-Server SD-WAN服務端

目錄

簡介

本文檔介紹如何使用DSCP標籤配置ThousandEyes Agent-to-Server SD-WAN，以便在Cisco SD-WAN重疊中監控流量。

必要條件

需求

思科建議您瞭解這些主題。

- SD-WAN概述
- 模板
- 千隻眼

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- 思科管理員版本20.15.3
- 思科驗證器版本20.15.3
- 思科控制器版本20.15.3
- 整合服務路由器(ISR)4331/K9版本17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

初步配置

- 配置DNS:路由器可以在VPN 0上解析DNS並訪問網際網路。
- 配置NAT DIA:路由器上需要存在DIA配置。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

代理與伺服器測試

要運行「代理到伺服器」測試，必須在服務VPN上配置ThousandEyes代理。在此案例中，伺服器是受監控的TLOC IP位址。通常，代理與伺服器測試用於監控伺服器；但是，在這種情況下，它用於監視與代理所在站點不同站點上的TLOC介面。

如果存在多個TLOC介面，請使用NAT直接網際網路訪問(DIA)和資料策略將流量重定向到所需的VPN 0 TLOC介面。根據ThousandEyes中代理端配置的DSCP值設定匹配條件，以重定向到VPN 0，並同時執行標籤，以避免ISP使用它們自己的DSCP標籤可能具有的任何超越。

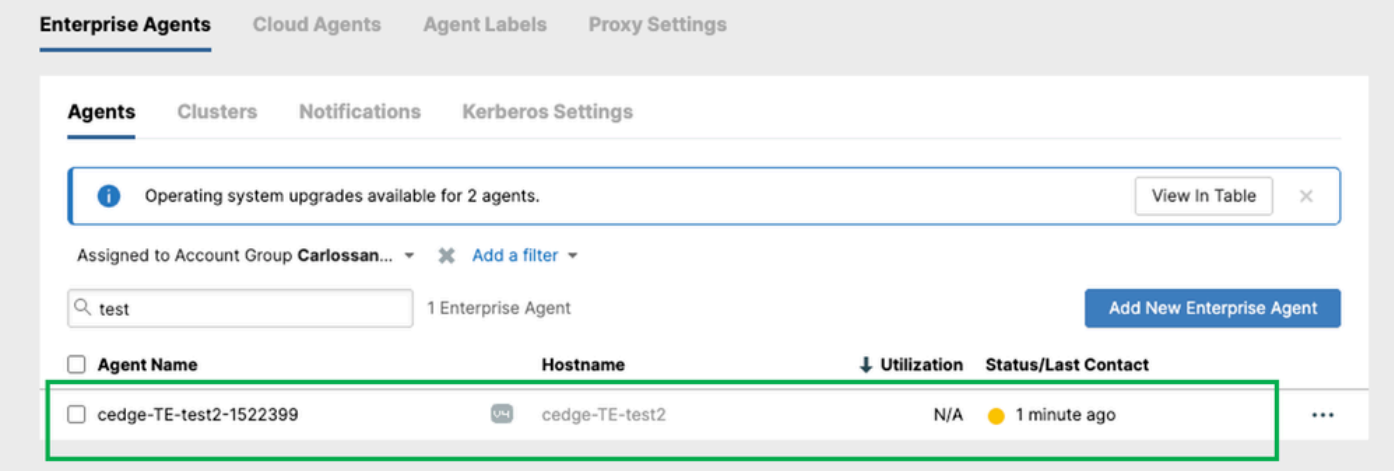
設定

配置ThousandEyes Test和DSCP

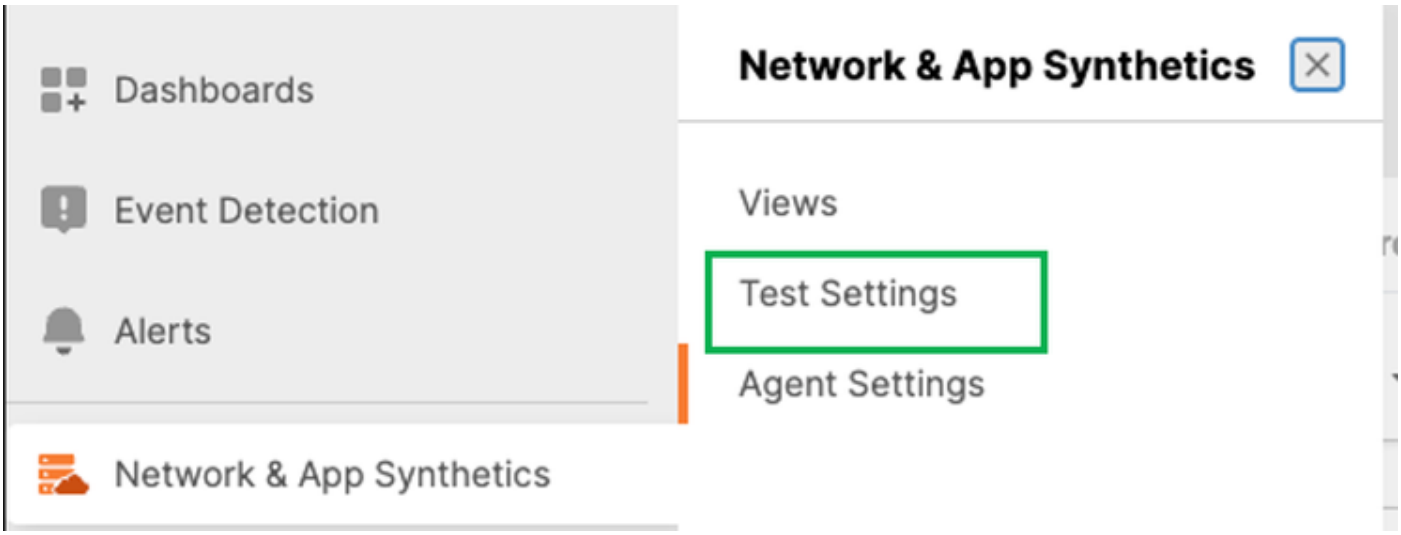
要配置區別服務代碼點(DSCP)，請執行以下操作：

1. 從Cisco ThosandEyes Agent頁登入ThousandEyes帳戶。

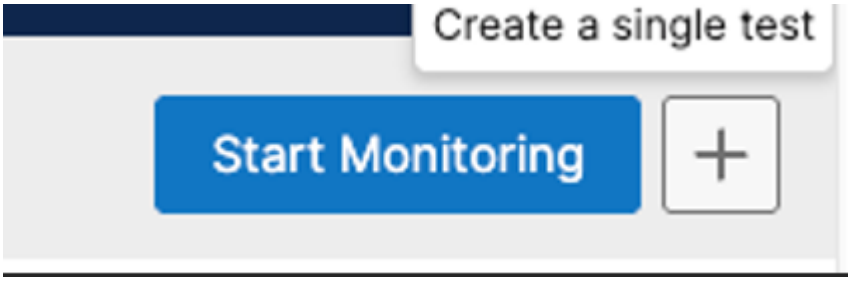
驗證路由器中安裝的代理是否與ThousandEyes Cloud通訊。



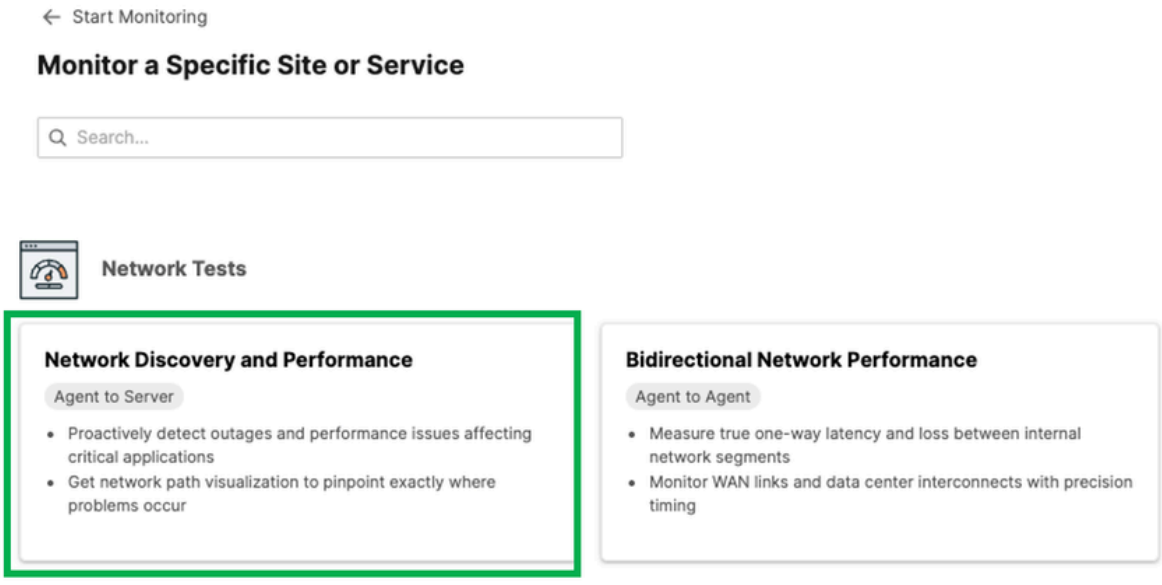
在裝置上安裝代理並確認與ThousandEyes Cloud的通訊後，建立測試。要建立測試，請導航網路與應用合成 >測試設定。



在右上角螢幕中，按一下+圖示。

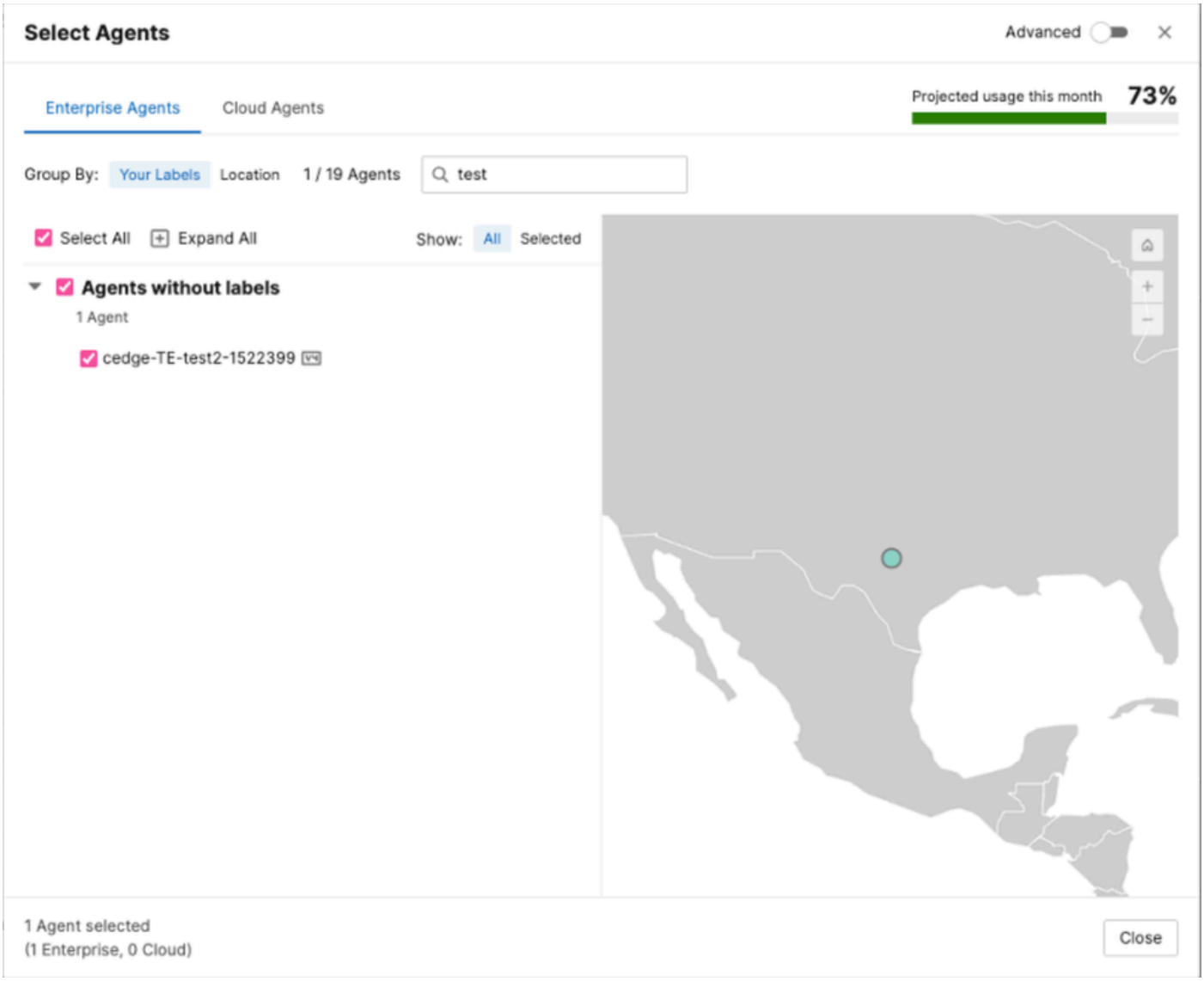


在新儀表板中，選擇Agent to Server Test。



在「目標」部分，選擇測試所需的IP地址。在本示例中，使用了192.168.1.47，這是同一子網內不同路由器上另一個TLOC的IP地址。

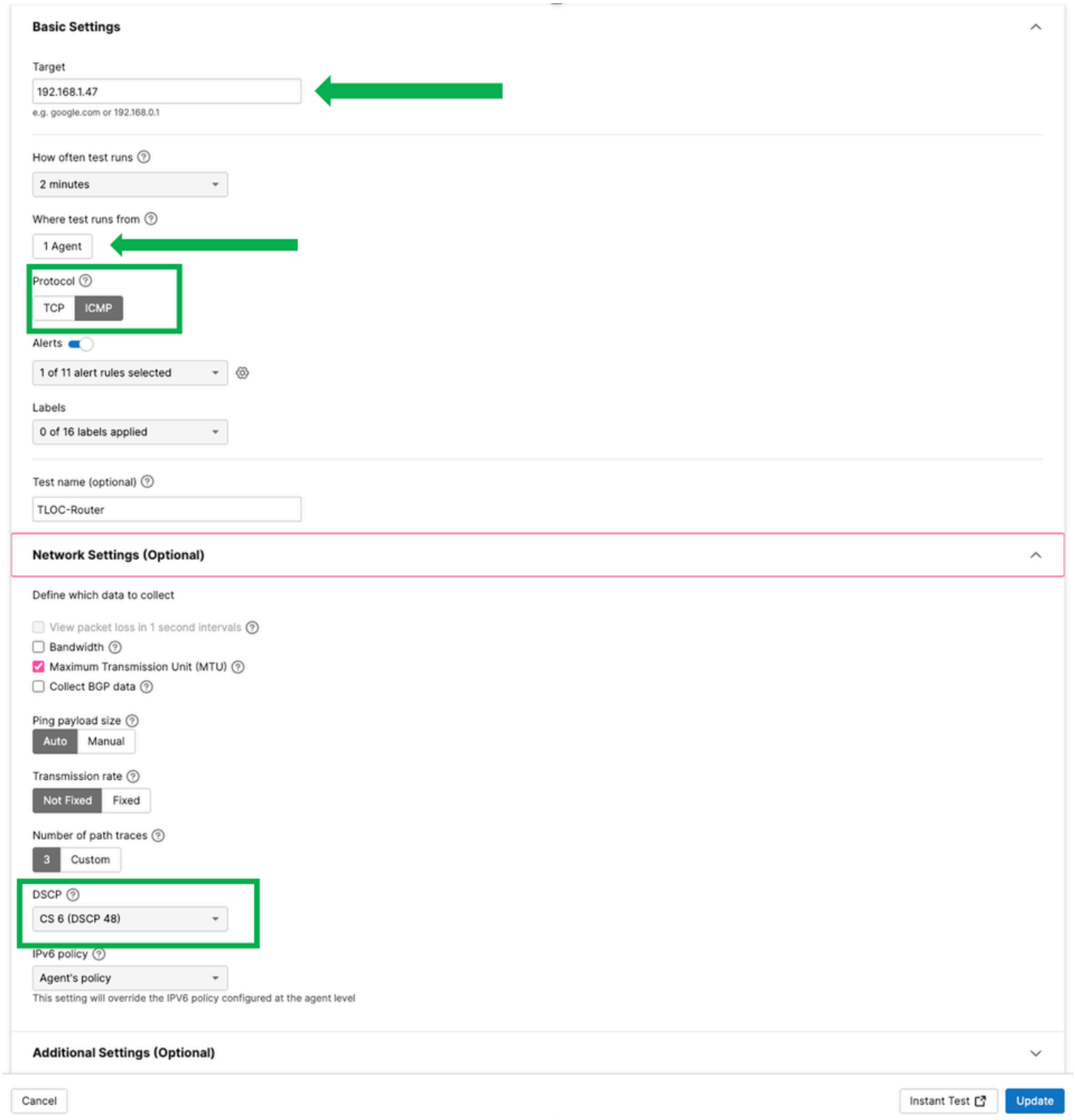
在Where test runs From中，選擇為路由器建立的代理（包含路由器的主機名），如下所示：



選擇ICMP協定

在網路設定（可選）部分，選擇DSCP並按一下更新。

在同一部分中按一下Instant Test(即時測試)。



配置SD-WAN

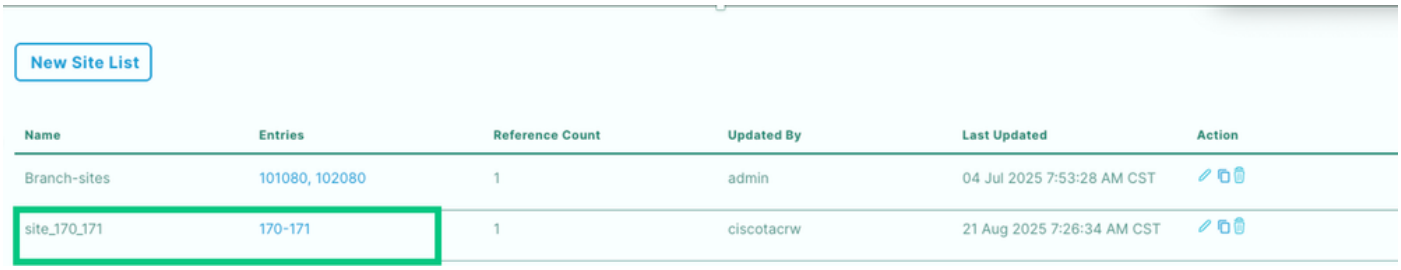
使用參考文檔在邊緣路由器上配置Thousand Eyes Agent[在SD-WAN裝置上配置ThousandEyes]

在路由器上安裝ThousandEyes Agent後，ThousandEyes模板將顯示以下資訊：

配置DSCP

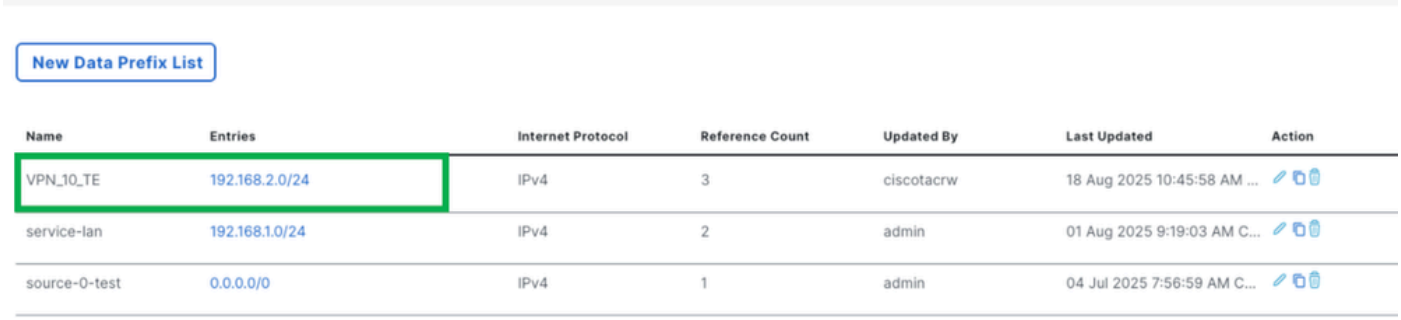
導航到Configuration > Policies >Centralized Policy > Click Add policy。在建立興趣組時，新增站點、VPN和資料字首。

站點（安裝ThousandEyes Agent的站點）



VPN（服務VPN）

在此示例中，資料字首（包括在ThousandEyes Template上配置的子網）使用子網192.168.2.0/24。



按一下Next > Next，在Configure Traffic Rules部分，選擇Traffic Data，然後按一下Add Policy。

選擇DSCP，在此示例中使用48

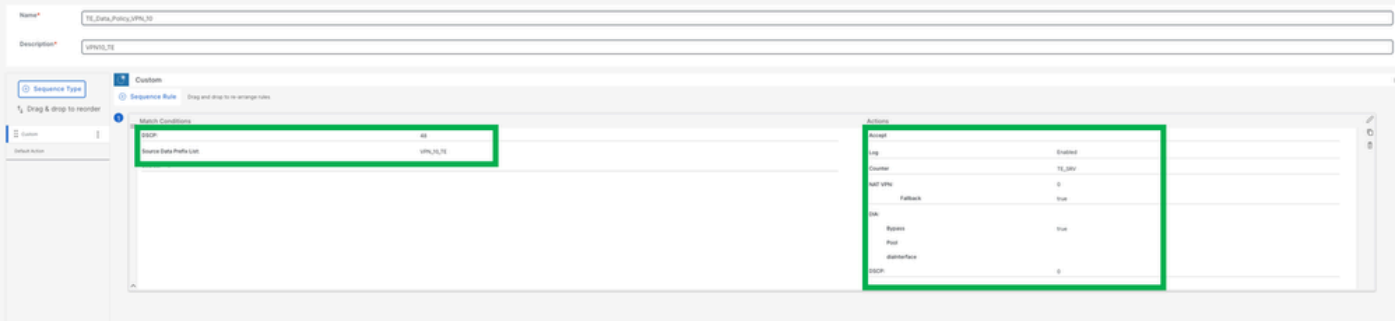
選擇「源資料字首清單」選項。使用"VPN_10_TE"（如前所述），該網路用於路由器上的ThousandEyes配置。

在操作部分：

選擇NAT VPN

後援

DSCP在此示例中，配置的DSCP為0



預設操作已啟用。

按一下Next，新增Policy name和Policy Description。在Traffic Data部分，點選New Site/WAN Region List and VPN List，儲存策略並啟用它，

啟用策略後，在路由器中驗證應用了策略：

運行show sdwan policy from-vsmart命令

```
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
```

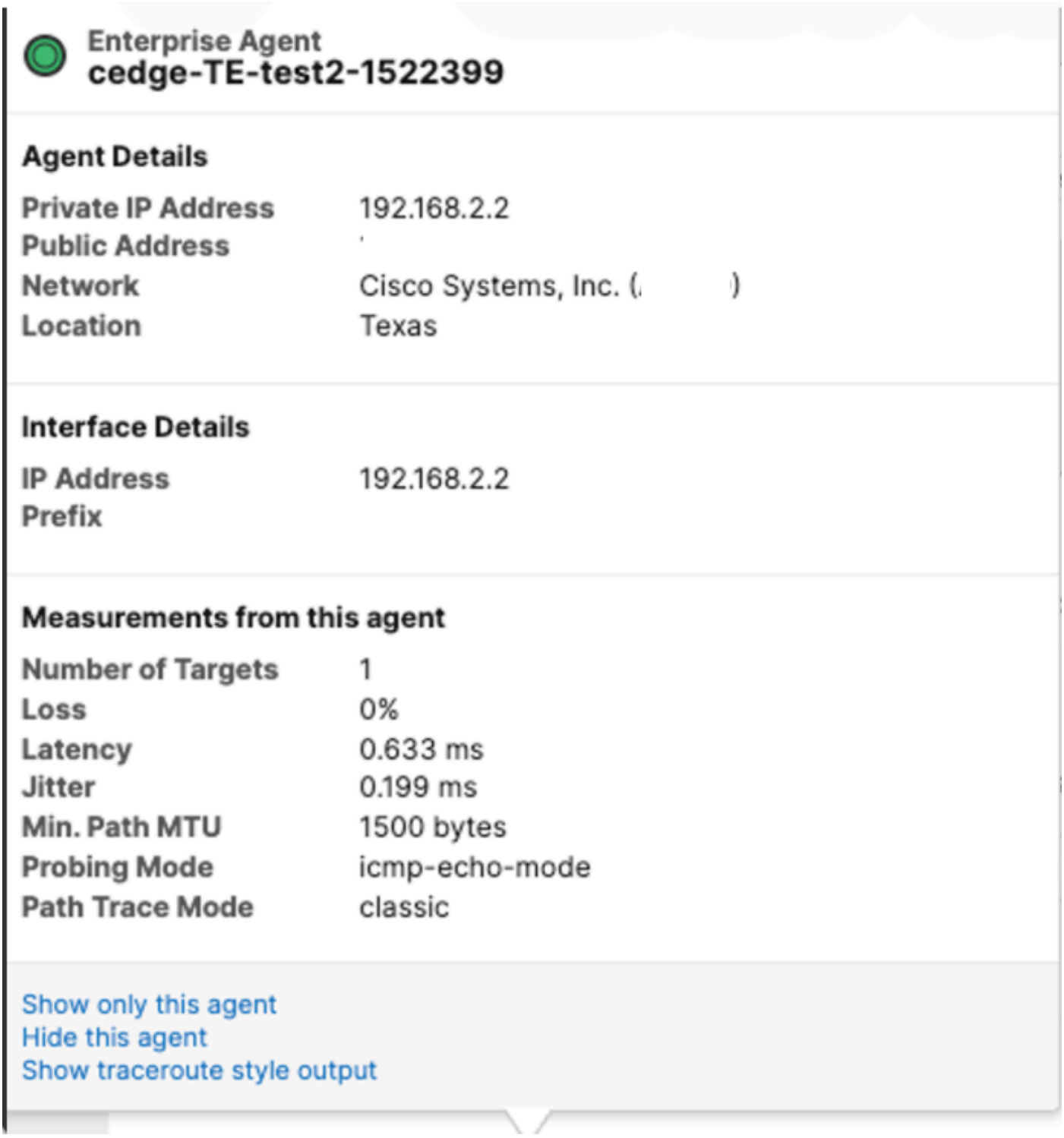
驗證

要運行測試，請按一下安裝測試並開啟一個新視窗。

測試完成後，您可以看到到達192.168.1.47所用的路徑

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

其中，在去襯底之前被標籤為dscp48，在去襯底之後被標籤為0。



在邊緣路由器上配置FIA跟蹤：

```
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
```

開啟封包：

<#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
```

相關資訊

- 在SD-WAN裝置上配置ThousandEyes
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。