DSCPマーキングによるThousandEyesのエージェントとサーバ間のSD-WANサービス側の設定

内容

はじめに

このドキュメントでは、Cisco SD-WANオーバーレイでのトラフィックモニタリング用にDSCPマーキングを使用したThousandEyes Agent-to-Server SD-WANの設定について説明します。

前提条件

要件

次のトピックに関する知識を身に付けておくことをお勧めします。

- SD-WANの概要
- テンプレート
- 千目

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Managerバージョン20.15.3
- Cisco Validatorバージョン20.15.3
- Ciscoコントローラバージョン20.15.3
- サービス統合型ルータ(ISR)4331/K9バージョン17.12.3a

- thousandeyes-enterprise-agent-5.5.1.cisco（登録ユーザ専用）

事前設定

- DNSの設定：ルータはDNSを解決して、VPN 0上のインターネットにアクセスできます。
- NAT DIAの設定：DIA設定はルータ上に存在している必要があります。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

エージェントからサーバへのテスト

エージェントからサーバへのテストを実行するには、サービスVPN上でThousandEyesエージェントを設定する必要があります。このシナリオでは、サーバはモニタされるTLOC IPアドレスです。通常、エージェントからサーバへのテストはサーバの監視に使用されますが、この場合は、エージェントがホストされているサイトとは別のサイトにあるTLOCインターフェイスの監視に使用されます。

複数のTLOCインターフェイスがある場合、NATダイレクトインターネットアクセス(DIA)とデータポリシーを使用して、トラフィックを目的のVPN 0 TLOCインターフェイスにリダイレクトします。 ThousandEyesのエージェント側で設定されたDSCP値に基づいて一致基準を設定し、それと同時にVPN 0を経由してリダイレクトされます。これにより、ISPが独自のDSCPマーキングで行う可能性のあるオーバーステッピングを回避できます。

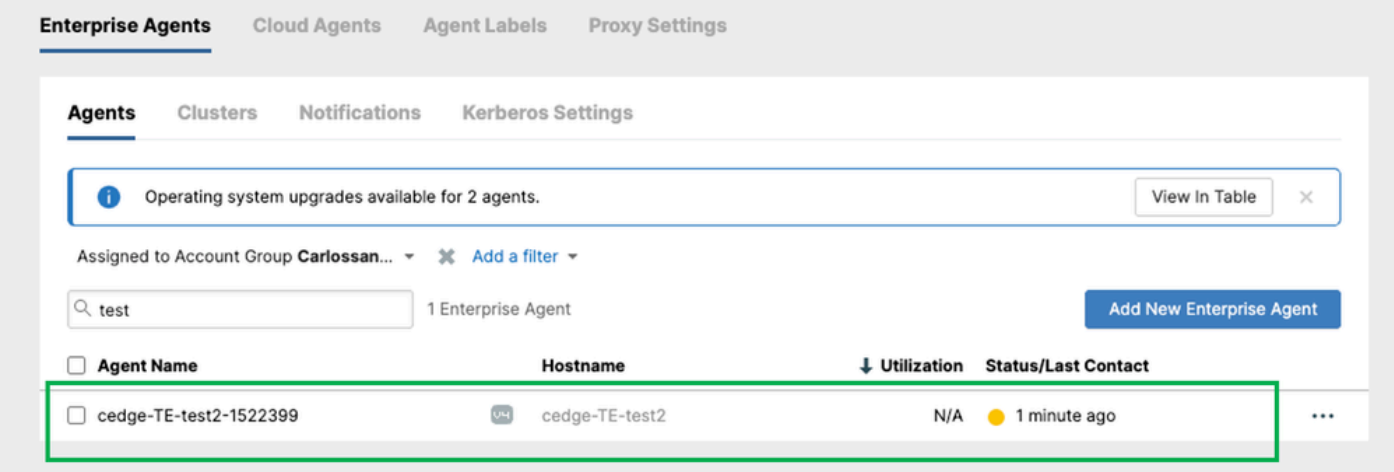
設定

ThousandEyes TestおよびDSCPの設定

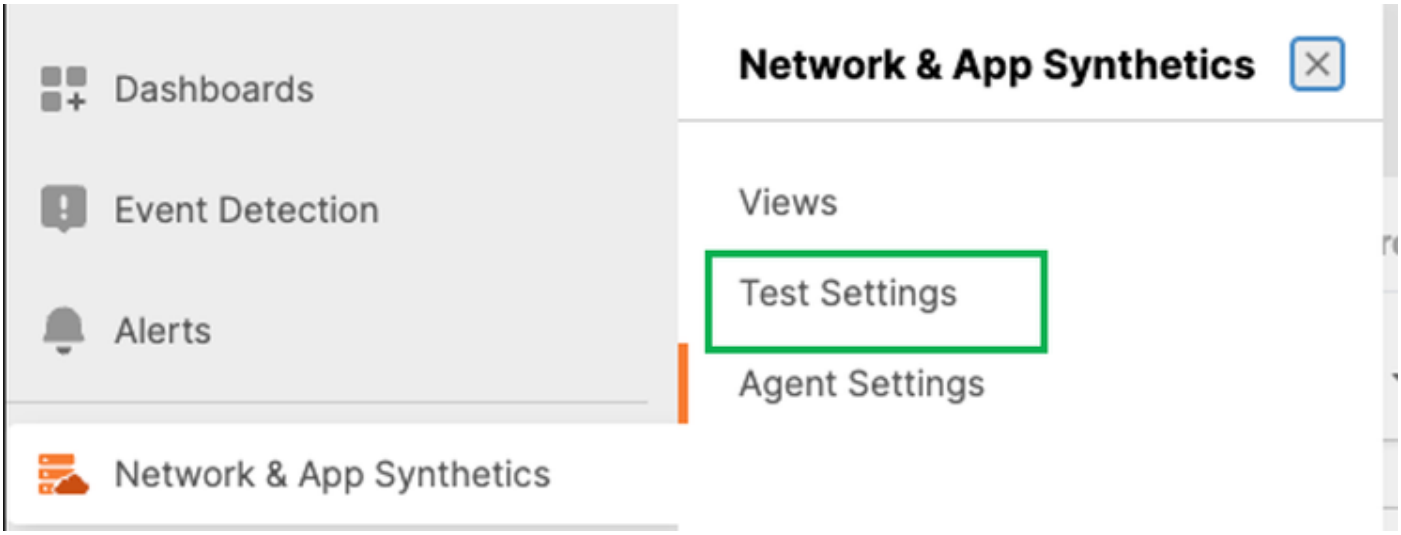
Differentiated Services Code Point(DSCP)を設定するには、次の手順に従います。

1. Cisco ThosandEyesエージェントページからThousandEyesアカウントにログインします。

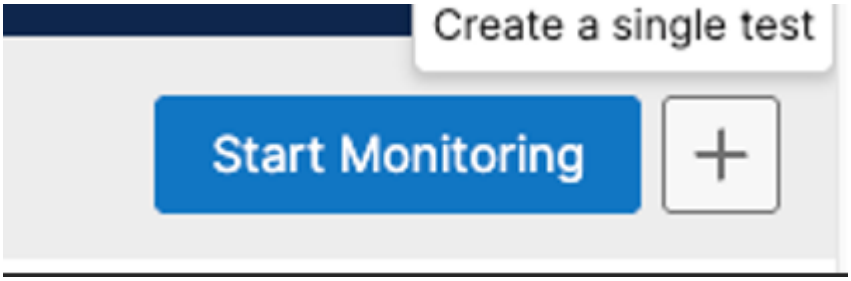
ルータにインストールされているエージェントがThousandEyes Cloudと通信できることを確認します。



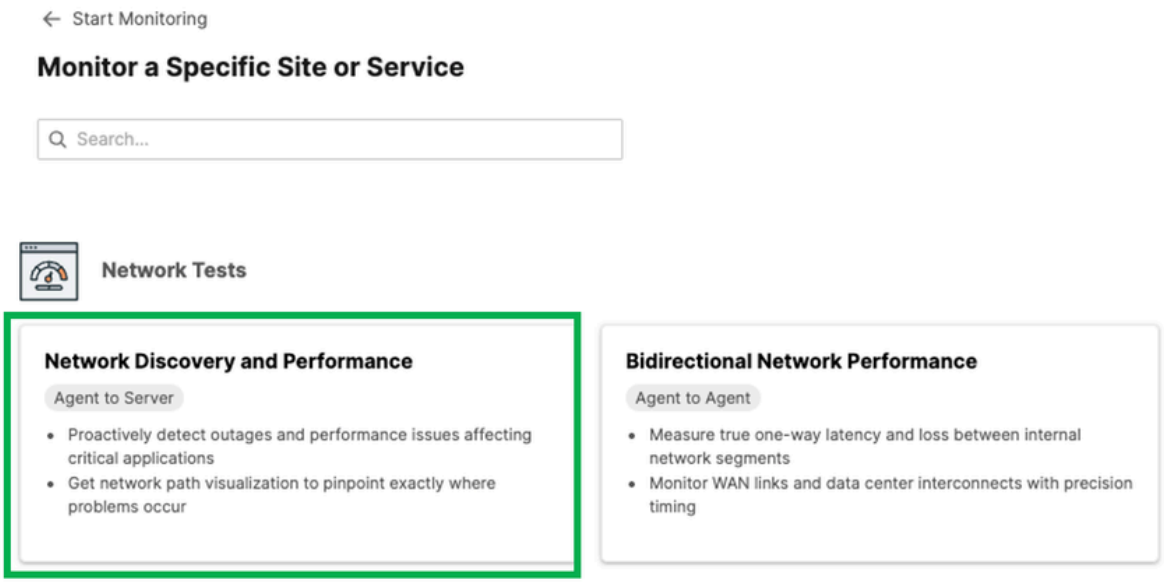
エージェントがデバイスにインストールされ、ThousandEyes Cloudとの通信が確認されたら、テストを作成します。テストを作成するには、Network & App Synthetics > Test Settingsの順に選択します。



右上の画面で+アイコンをクリックします。

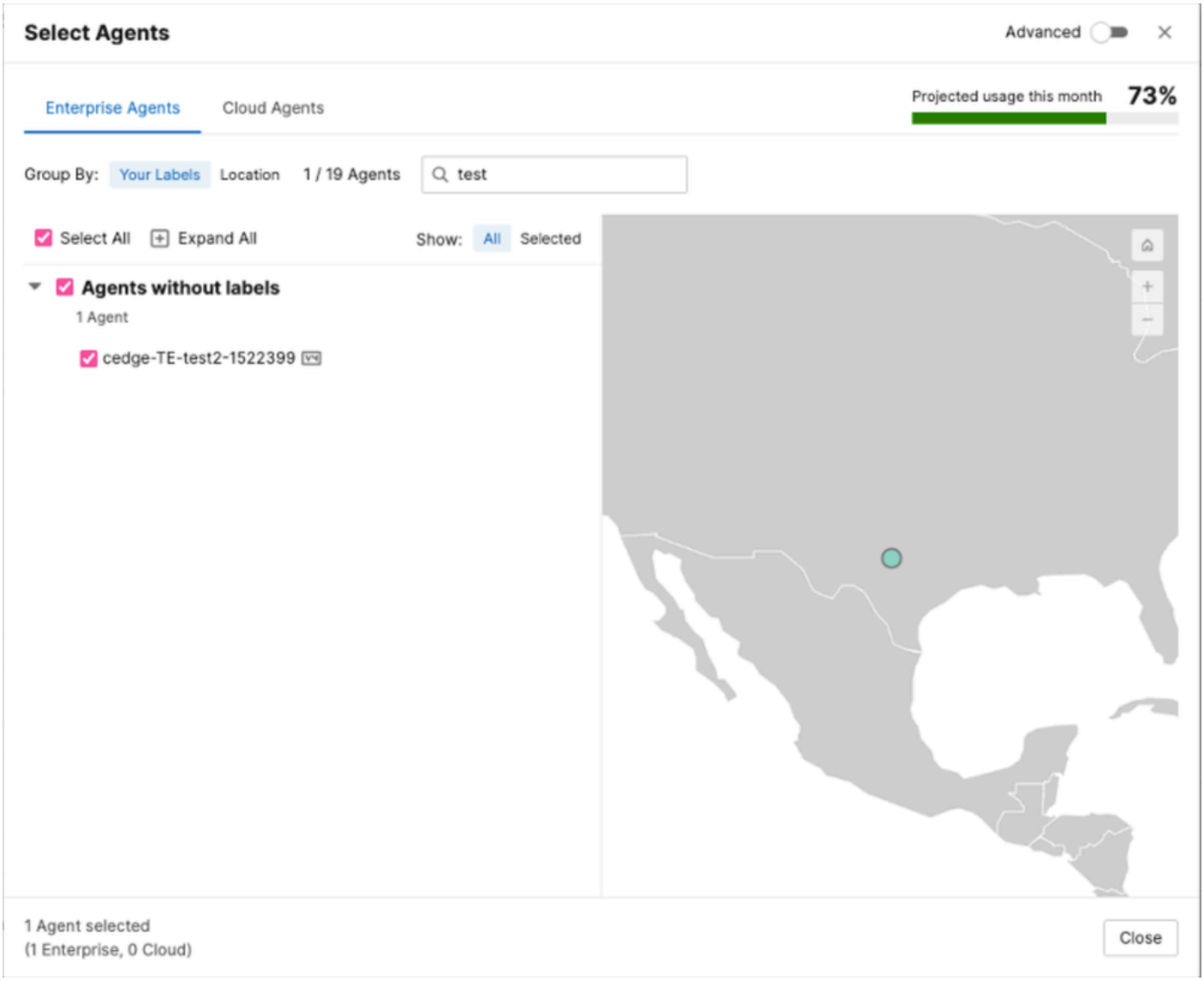


新しいダッシュボードでAgent to Server Testの順に選択します。



「Target」セクションで、テストに使用するIPアドレスを選択します。この例では、192.168.1.47を使用しています。これは、同じサブネット内の別のルータにある別のTLOCのIPアドレスです。

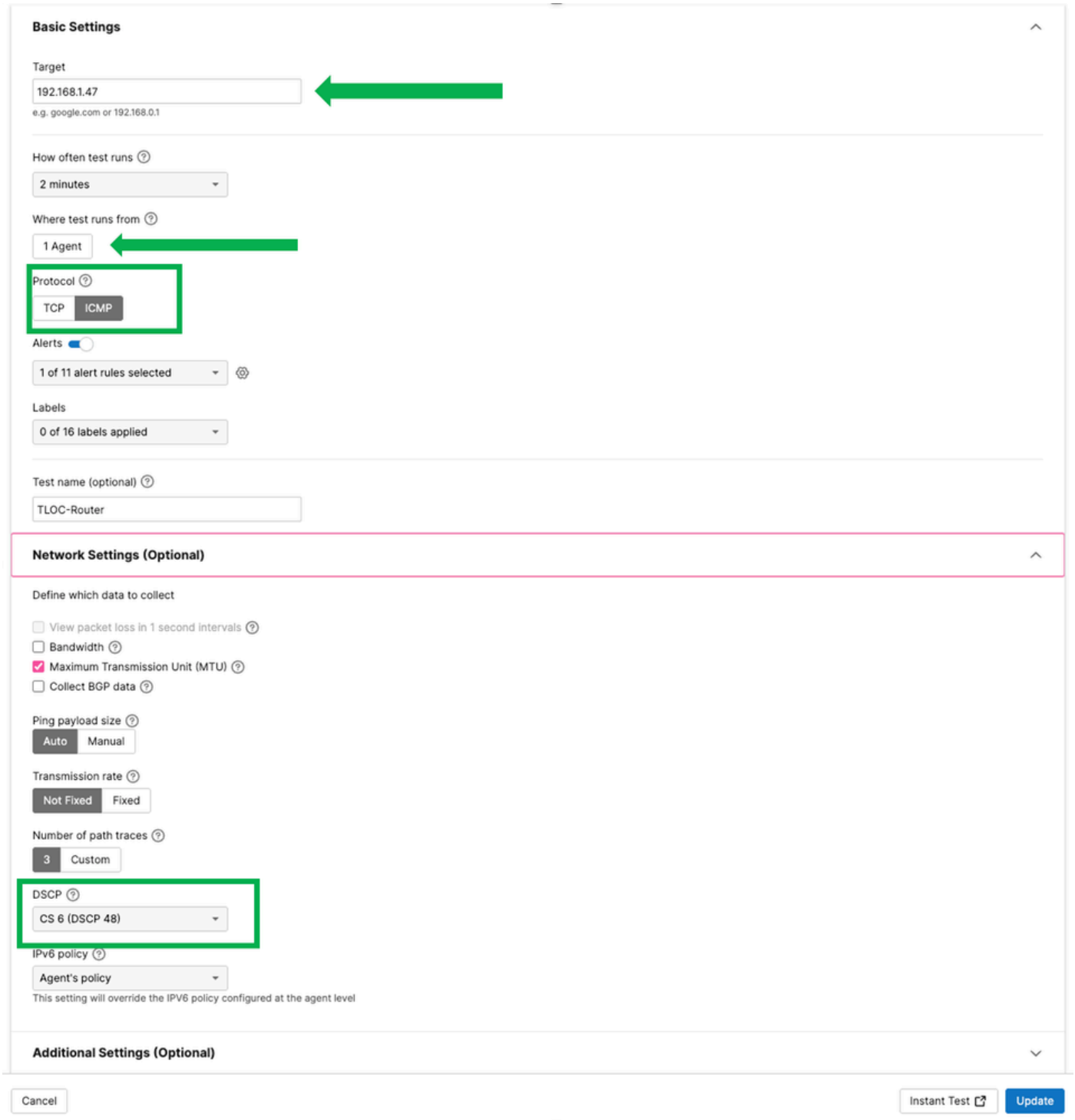
「Where test runs From」で、次のように、ルータ用に作成されたエージェント（ルータのホスト名を含む）を選択します。



ICMPプロトコルの選択

[ネットワークの設定（オプション）]セクションで、DSCPを選択し、[更新]をクリックします。

同じセクションでInstant Testをクリックします。



SD-WANの設定

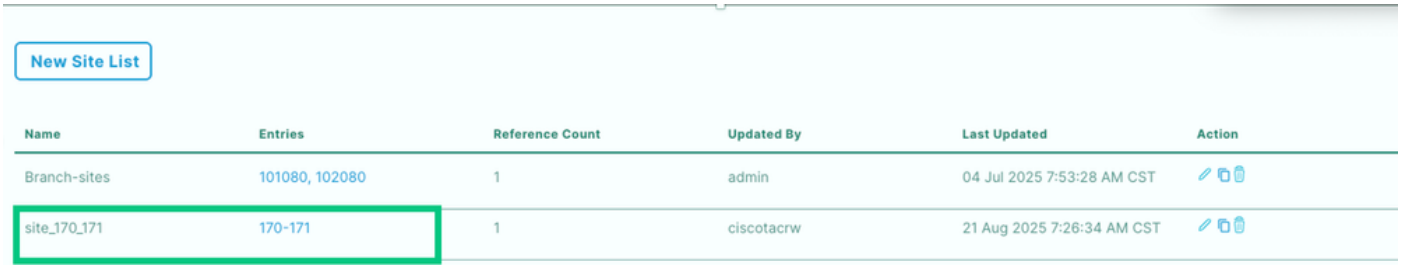
参照ドキュメントを使用してエッジルータ上でThousand Eyesエージェントを設定するSD-WANデバイス上でThousandEyesを設定する

ThousandEyes Agentがルータにインストールされると、ThousandEyesテンプレートに次の情報が表示されます。

DSCPの設定

Configuration > Policies >Centralized Policyの順に移動し、Add policyをクリックします。対象のグループを作成するときに、サイト、VPN、およびデータプレフィックスを追加します。

サイト（ThousandEyes Agentがインストールされているサイト）



VPN（サービスVPN）

この例のデータプレフィクス（ThousandEyesテンプレートで設定されているサブネットを含む）では、サブネット192.168.2.0/24が使用されています。

Next > Nextの順にクリックし、Configure Traffic RulesセクションでTraffic Dataを選択して、Add Policyをクリックします。

DSCPを選択します。この例では48を使用します。

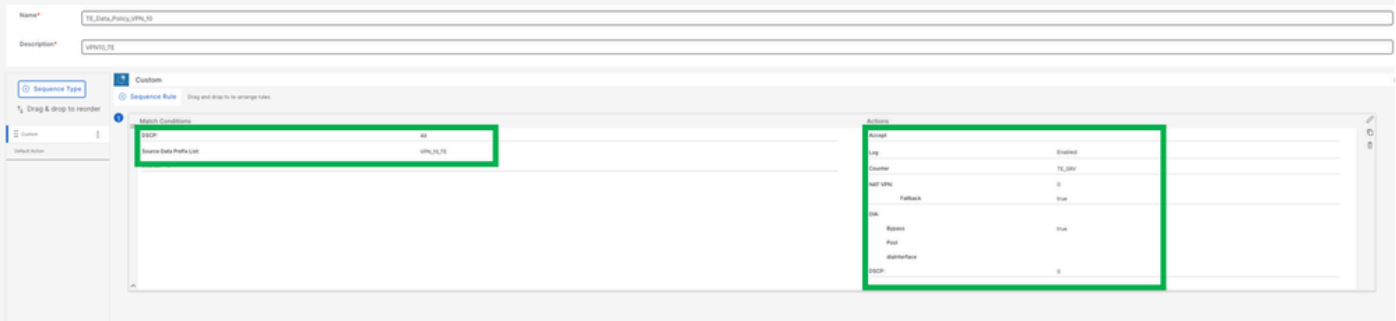
「Source Data Prefix List」オプションを選択します。（前に説明したように）「VPN_10_TE」を使用します。これは、ルータのThousandEye設定に使用するネットワークです。

アクション・セクション：

NAT VPNの選択

フォールバック

この例で設定されているDSCPは0です。



デフォルトのアクションは有効です。

Next, add Policy nameおよびPolicy Descriptionをクリックします。Traffic Dataセクションで、New Site/WAN Region List and VPN Listをクリックし、ポリシーを保存してアクティブにします。

ポリシーがアクティブになったら、ルータでポリシーが適用されていることを確認します。

show sdwan policy from-vsmartコマンドを実行します。

```
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
```

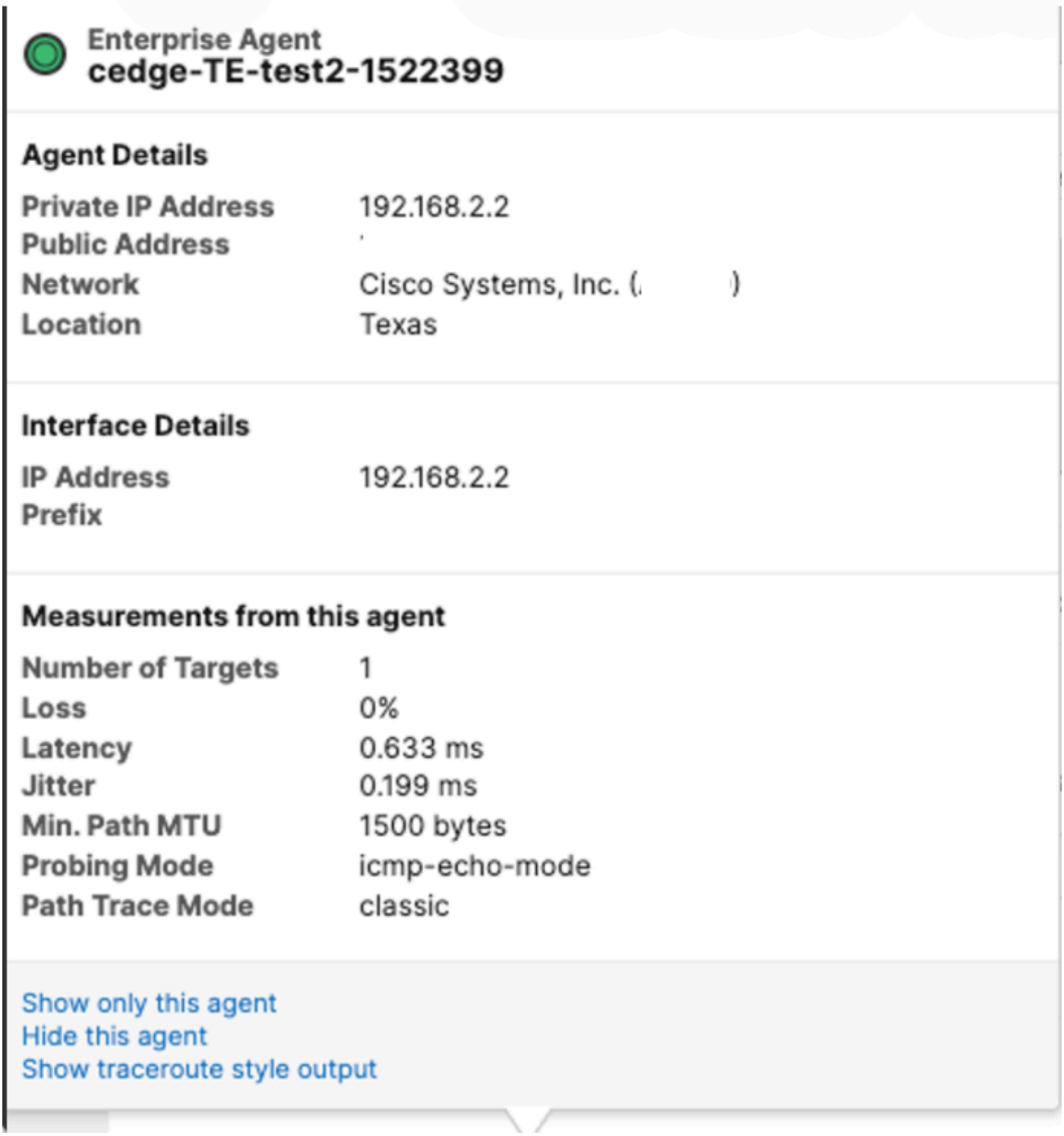
確認

テストを実行するには、Instat Testをクリックして新しいウィンドウを開きます。

テストが終了すると、192.168.1.47に到達するまでにかかったパスが表示されます

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

がアンダーレイに対して移動する前にdscp48とマークされ、アンダーレイに対して移動した後は0とマークされます。



エッジルータでFIAトレースを設定します。

```
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
```

パケットを開きます。

<#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
```

関連情報

- SD-WANデバイスでのThousandEyesの設定
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。