Configuration côté service SD-WAN agent-serveur de ThousandEyes avec marquage DSCP

Table des matières

Introduction

Ce document décrit la configuration de ThousandEyes Agent-to-Server SD-WAN avec marquage DSCP pour la surveillance du trafic dans une superposition Cisco SD-WAN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes .

- Présentation générale du SD-WAN
- Modèles
- Mille Yeux

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Cisco Manager Version 20.15.3
- Cisco Validator version 20.15.3
- Contrôleur Cisco version 20.15.3

- Routeurs à services intégrés (ISR)4331/K9 version 17.12.3a
- thousandeyes-enterprise-agent-5.5.1.cisco

Configurations préliminaires

- Configurer DNS : Le routeur peut résoudre le DNS et accéder à Internet sur le VPN 0.
- Configurez NAT DIA : La configuration DIA doit être présente sur le routeur.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Test agent-serveur

Pour exécuter un test Agent to Server, l'agent ThousandEyes doit être configuré sur le VPN de service. Dans ce scénario, le serveur est l'adresse IP TLOC qui est surveillée. En général, un test Agent à serveur est utilisé pour surveiller un serveur ; toutefois, dans ce cas, il est utilisé pour surveiller une interface TLOC située sur un site différent de celui où l'agent est hébergé.

S'il existe plusieurs interfaces TLOC, utilisez NAT Direct Internet Access (DIA) et une stratégie de données pour rediriger le trafic vers l'interface TLOC VPN 0 souhaitée. Définissez les critères de correspondance en fonction de la valeur DSCP configurée côté agent dans ThousandEyes pour être redirigée vers et via le VPN 0 tout en effectuant le démarquage afin d'éviter tout dépassement de la valeur DSCP que le FAI pourrait avoir avec son propre marquage DSCP.

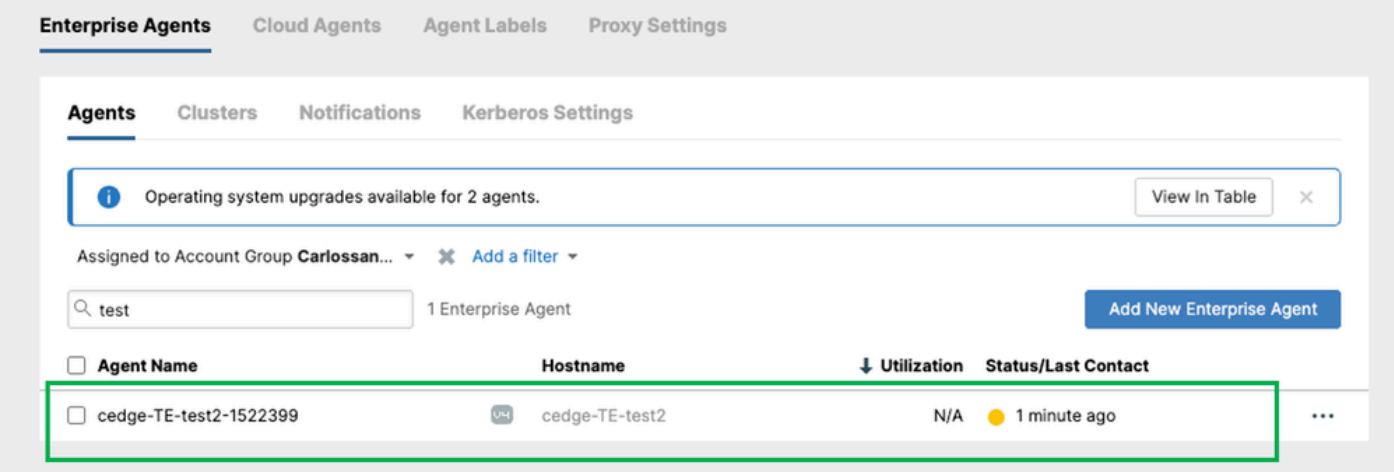
Configurer

Configurer le test ThousandEyes et le DSCP

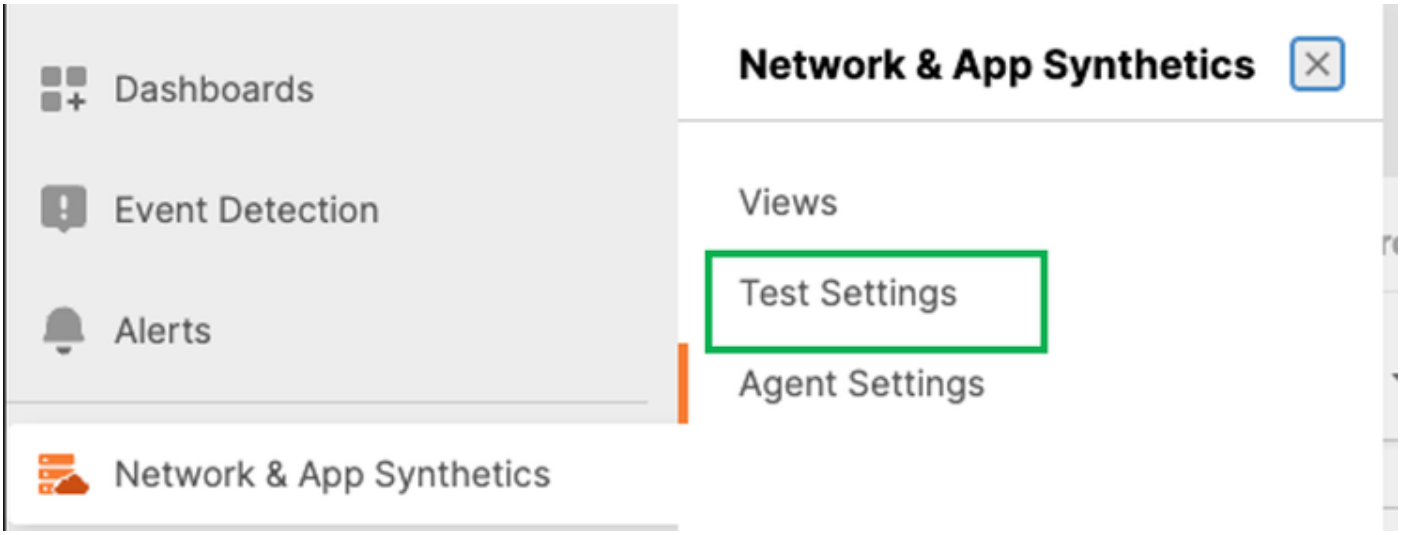
Pour configurer le DSCP (Differentiated Services Code Point) :

1. Connectez-vous au compte ThousandEyes depuis la page Cisco ThousandEyes Agent.

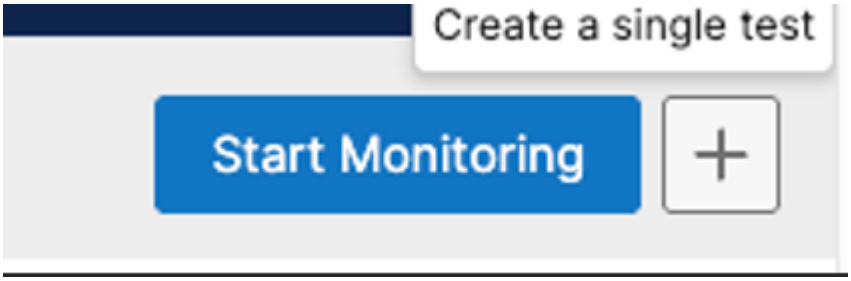
Vérifiez que l'agent installé sur le routeur communique avec le cloud ThousandEyes.



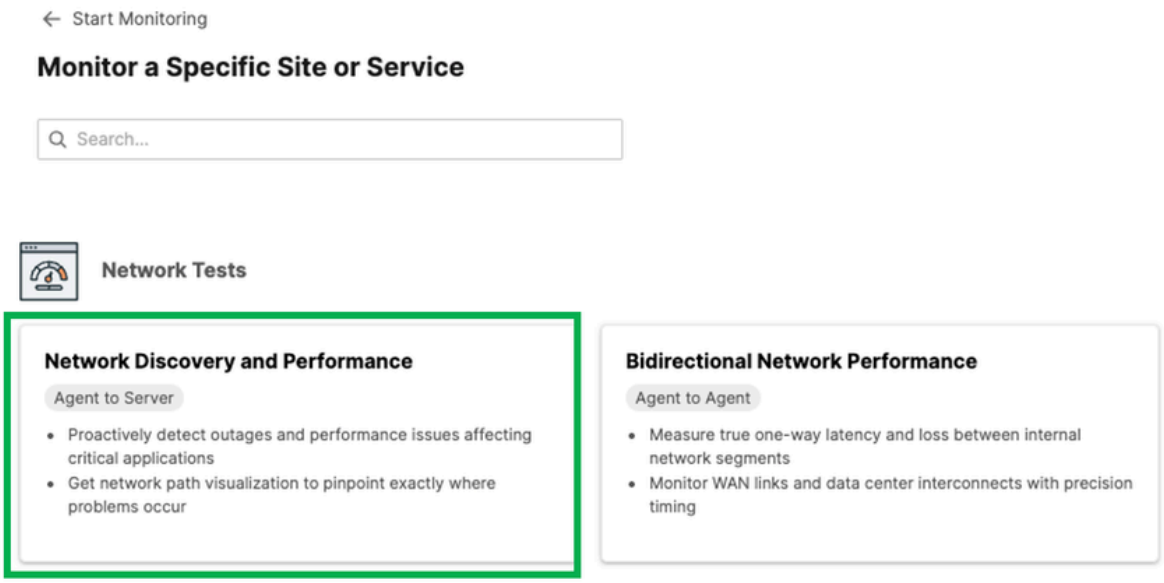
Une fois que l'agent est installé sur le périphérique et que la communication avec le cloud ThousandEyes est confirmée, créez un test. Pour créer un test, naviguez dans Network & App Synthetics > Paramètres de test.



Dans l'écran supérieur droit, cliquez sur l'icône +.

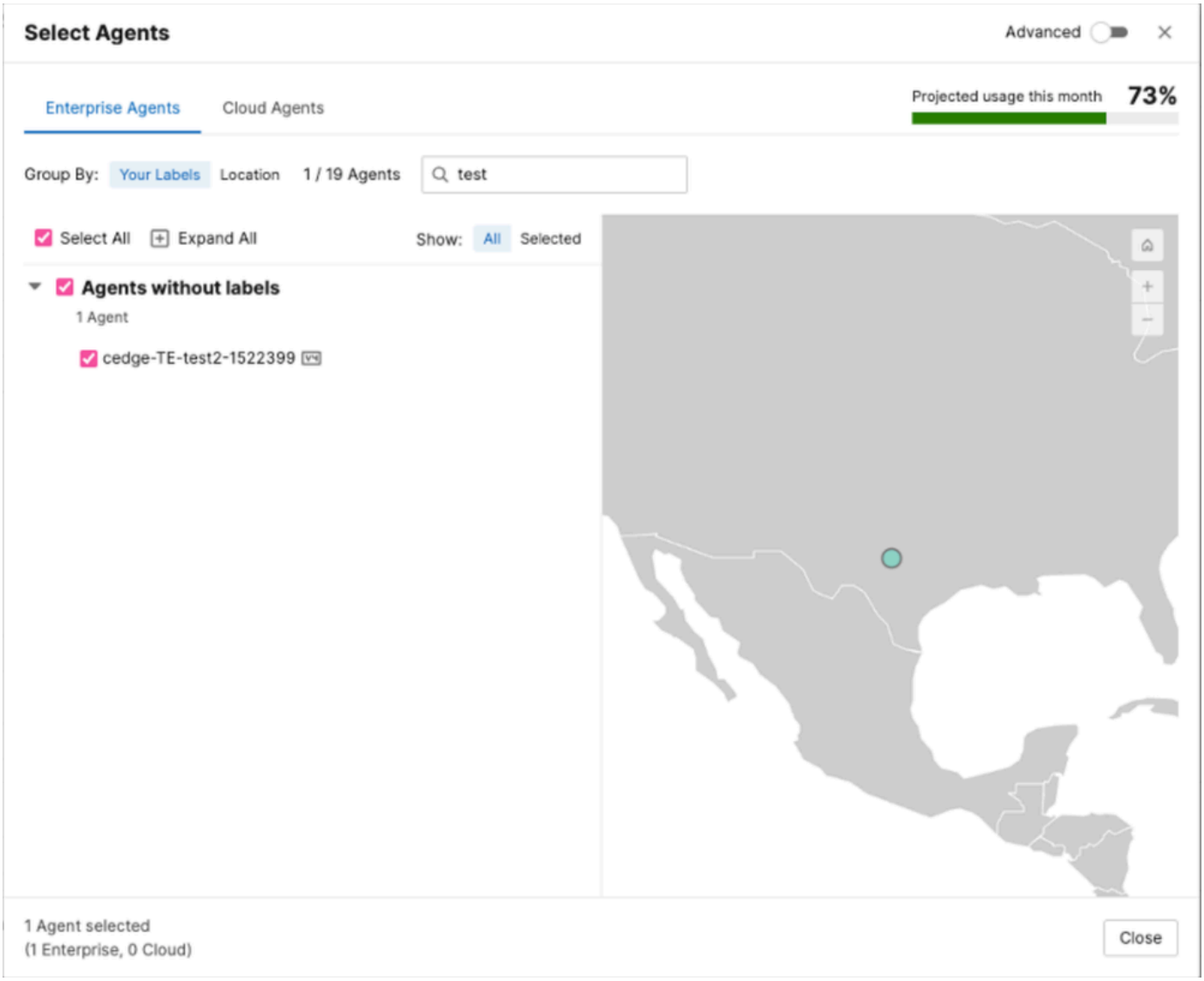


Dans le nouveau tableau de bord, sélectionnez Test agent-serveur.



Dans la section "Cible", sélectionnez l'adresse IP à utiliser pour le test. Dans cet exemple, nous avons utilisé 192.168.1.47, qui est l'adresse IP d'un autre TLOC sur un autre routeur du même sous-réseau.

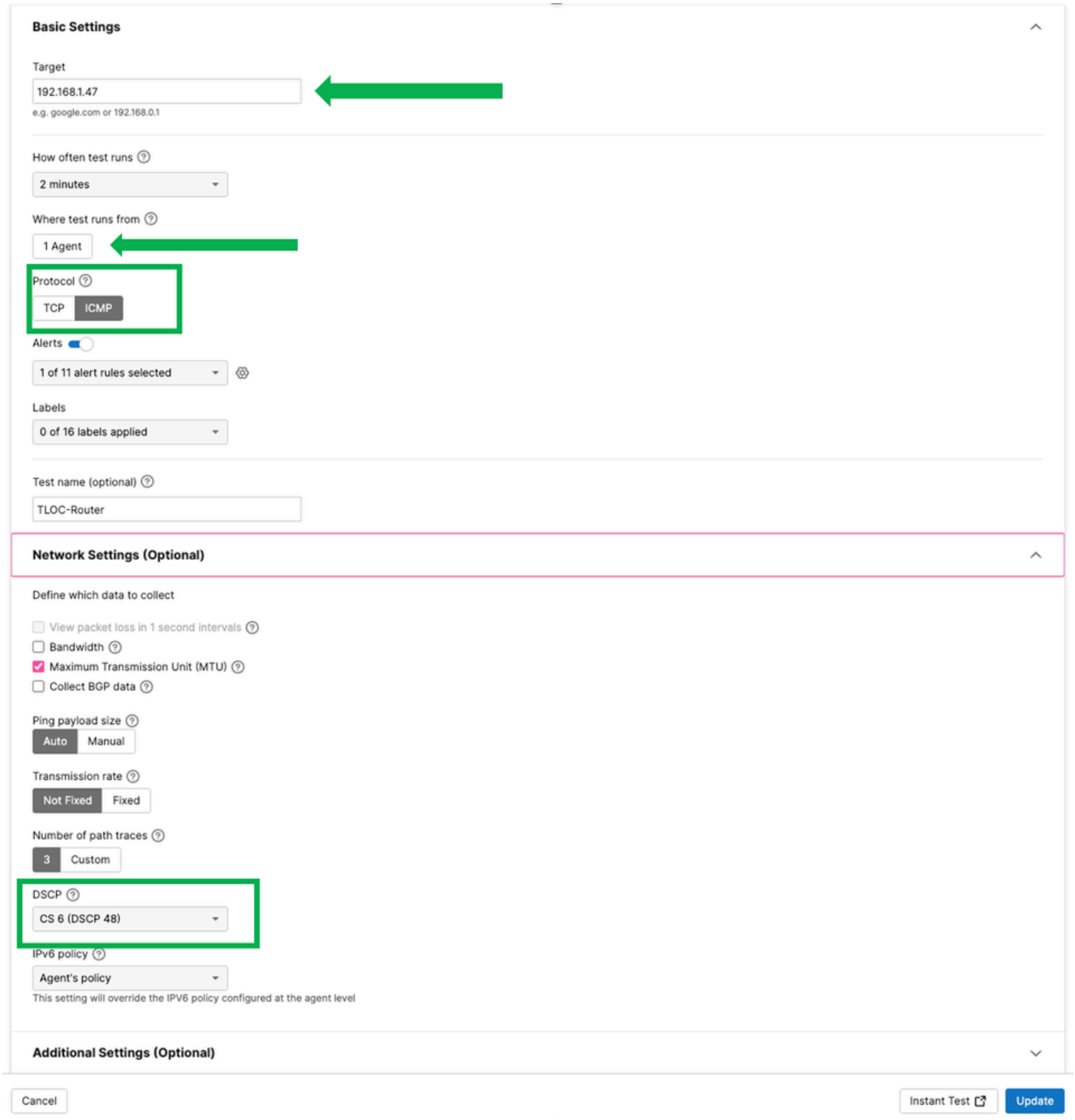
Dans "Where test runs From", sélectionnez l'agent créé pour votre routeur (contient le nom d'hôte de votre routeur) comme indiqué ci-dessous :



Sélectionner le protocole ICMP

Dans la section Paramètres réseau (facultatif), sélectionnez le DSCP et cliquez sur Mettre à jour.

Dans la même section, cliquez sur Instant Test.



Configuration de SD-WAN

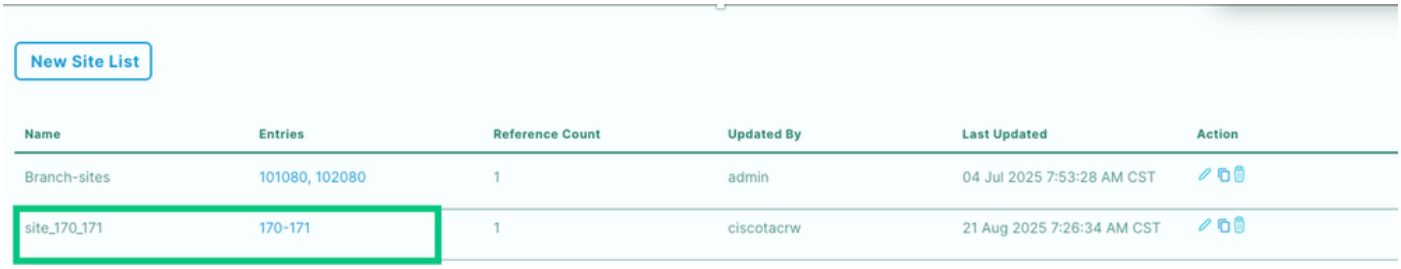
Utilisez le document de référence pour configurer l'agent Thousand Eyes sur le routeur de périphérie [Configurer Thousand Eyes sur les périphériques SD-WAN]

Une fois l'agent ThousandEyes installé sur le routeur, le modèle ThousandEyes affiche les informations suivantes :

Configurer DSCP

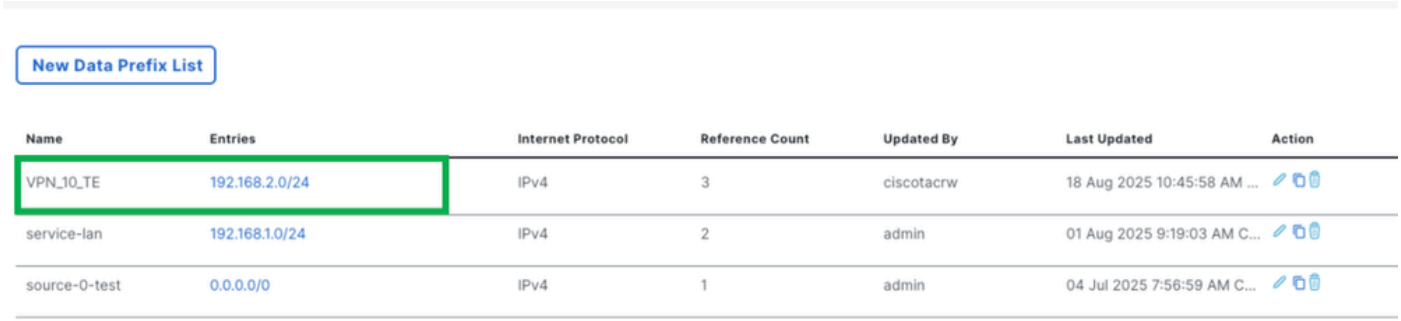
Accédez à Configuration > Policies >Centralized Policy > Cliquez sur Add policy. Lors de la création du groupe d'intérêt, ajoutez Site, VPN et Data Prefix.

Site (site où l'agent ThousandEyes a été installé)



VPN (Service VPN)

Le préfixe de données (inclure le sous-réseau configuré sur le modèle ThousandEyes) dans cet exemple a utilisé le sous-réseau 192.168.2.0/24.



Cliquez sur Next > Next, Dans la section Configure Traffic Rules, sélectionnez Traffic Data et cliquez sur Add Policy.

Sélectionnez DSCP, dans cet exemple utilisé 48

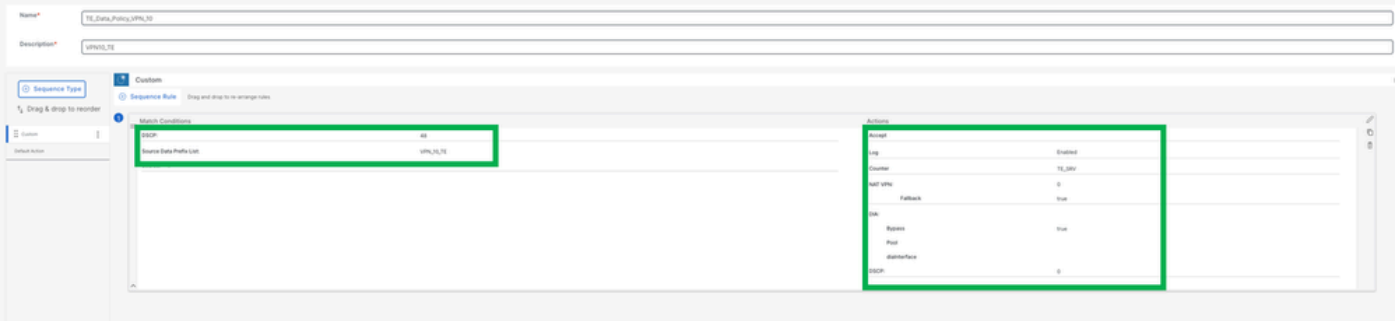
Sélectionnez l'option "Liste de préfixes de données source". Utilisez "VPN_10_TE" (comme décrit précédemment), qui est le réseau utilisé pour la configuration ThousandEyes sur le routeur.

Section Sur les actions :

Sélectionnez NAT VPN

De Secours

DSCP dans cet exemple, le DSCP configuré est 0



Action par défaut activée.

Cliquez sur Next, add Policy name and Policy Description. Dans la section Traffic Data, cliquez sur New Site/WAN Region List and VPN List, enregistrez la stratégie et activez-la,

Une fois la stratégie activée, vérifiez sur le routeur la stratégie appliquée :

Exécutez la commande 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
```

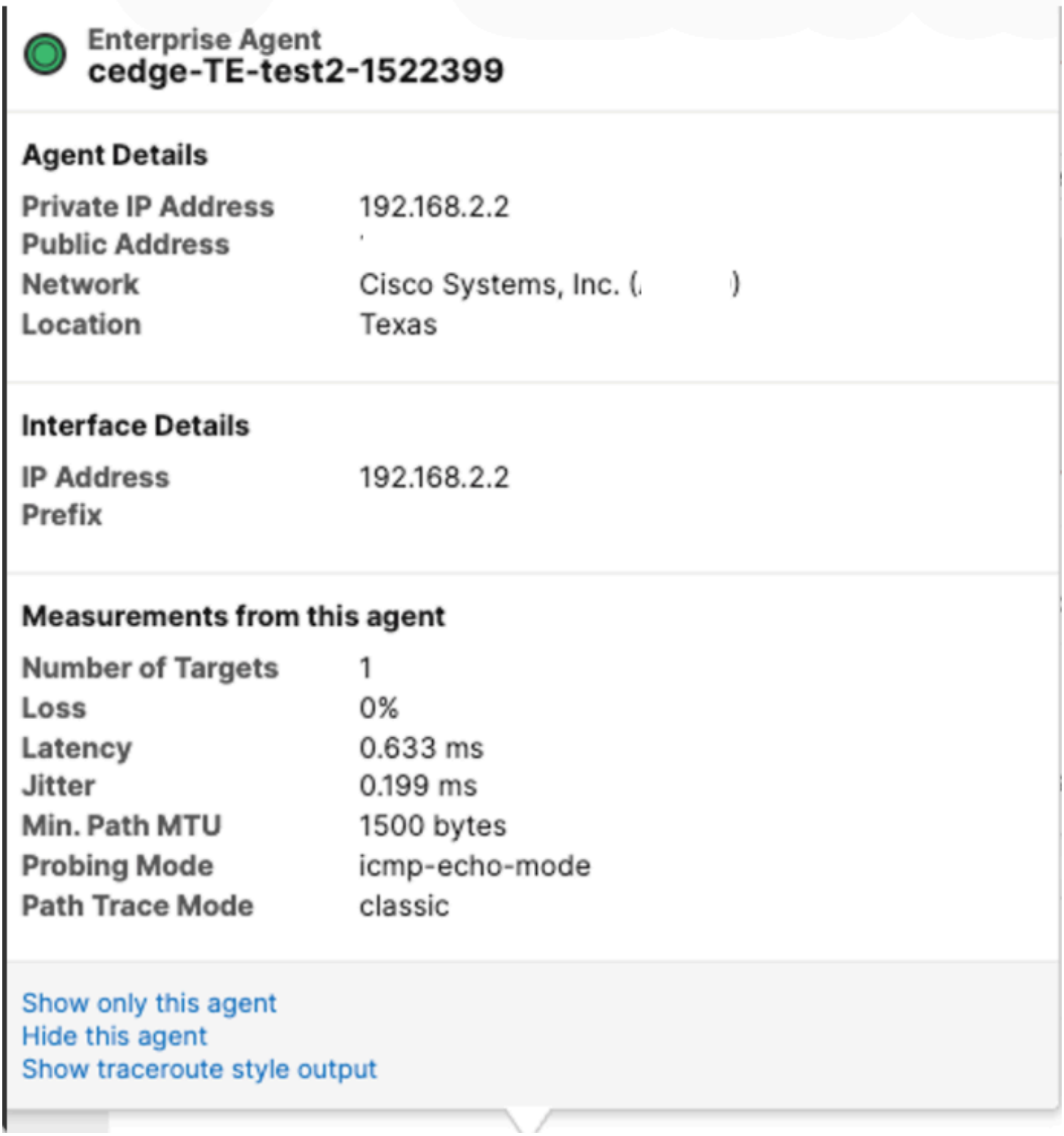
Vérifier

Pour exécuter un test, cliquez sur Instat Test et ouvrez une nouvelle fenêtre.

Une fois le test terminé, vous pouvez voir le chemin emprunté pour atteindre l'adresse 192.168.1.47

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

Où a été marqué comme dscp48 avant d'aller pour la couche sous-jacente et après aller sur la couche sous-jacente est marqué comme 0.



Configurez une trace FIA sur le routeur de périphérie :

```
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
```

Ouvrez un paquet :

<#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
```

Informations connexes

- Configurer ThousandEyes sur les périphériques SD-WAN
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.