# تكوين جانب خدمة SD-WAN من برنامج آلافEyes من وكيل إلى خادم باستخدام تمييز DSCP

## المحتويات



## المقدمة

يصف هذا المستند تكوين شبكة SD-WAN من نوع آلافEyes من عميل إلى خادم باستخدام تمييز DSCP لمراقبة حركة المرور في تغشية Cisco SD-WAN.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية.

- نظرة عامة على شبكة WAN الخاصة بتقنية SD
- قوالب
- ألف عين

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية.

- Cisco Manager، الإصدار 20.15.3
- Cisco Validator، الإصدار 20.15.3
- وحدة التحكم من Cisco، الإصدار 20.15.3

- موجهات الخدمة المتكاملة (ISR)4331/K9، الإصدار 17.12.3a
- آلاف من عم-enterprise-agent-5.5.1.cisco

التكوينات الأولية

- تكوين DNS: يمكن للموجه حل DNS والوصول إلى الإنترنت على VPN 0.
- تكوين NAT DIA: يلزم وجود تكوين DIA على الموجه.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

# إختبار الوكيل إلى الخادم

لتشغيل إختبار "عميل إلى خادم"، يجب تكوين عميل 0Eyes على شبكة VPN الخاصة بالخدمة. في هذا السيناريو، يكون الخادم هو عنوان IP الخاص بوحدة التحكم في الوصول (TLOC) الذي يتم رصده. في العادة، يتم إستخدام إختبار "وكيل إلى خادم" لمراقبة الخادم؛ ومع ذلك، في هذه الحالة، يتم إستخدامها لمراقبة واجهة TLOC الموجودة في موقع مختلف من حيث يتم إستضافة الوكيل.

في حالة وجود العديد من واجهات TLOC، أستخدم NAT Direct Internet Access (DIA) وسياسة بيانات لإعادة توجيه حركة المرور إلى واجهة VPN 0 TLOC المطلوبة. قم بتعيين معايير المطابقة استنادا إلى قيمة DSCP التي تم تكوينها على جانب الوكيل في آلافEyes لإعادة توجيهها إلى الشبكة الخاصة الظاهرية (VPN) 0 من خلالها، مع القيام في الوقت نفسه بإجراء العلامة لتجنب أي تجاوز لمعايير ISP يمكن أن يكون لديه علامة DSCP خاصة به.

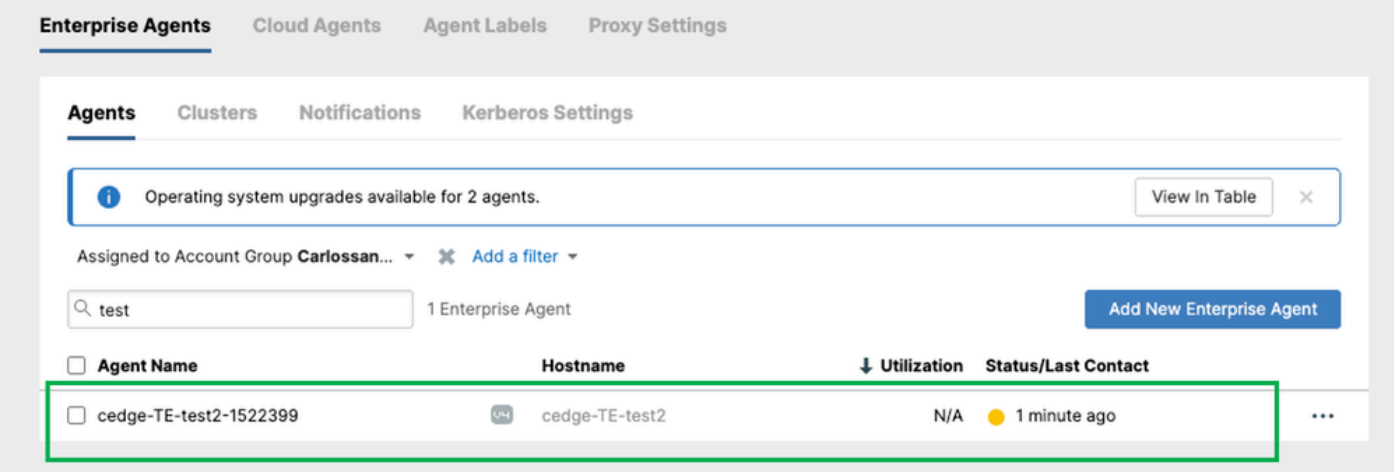
# التكوين

## تكوين إختبار آلافEyes و DSCP

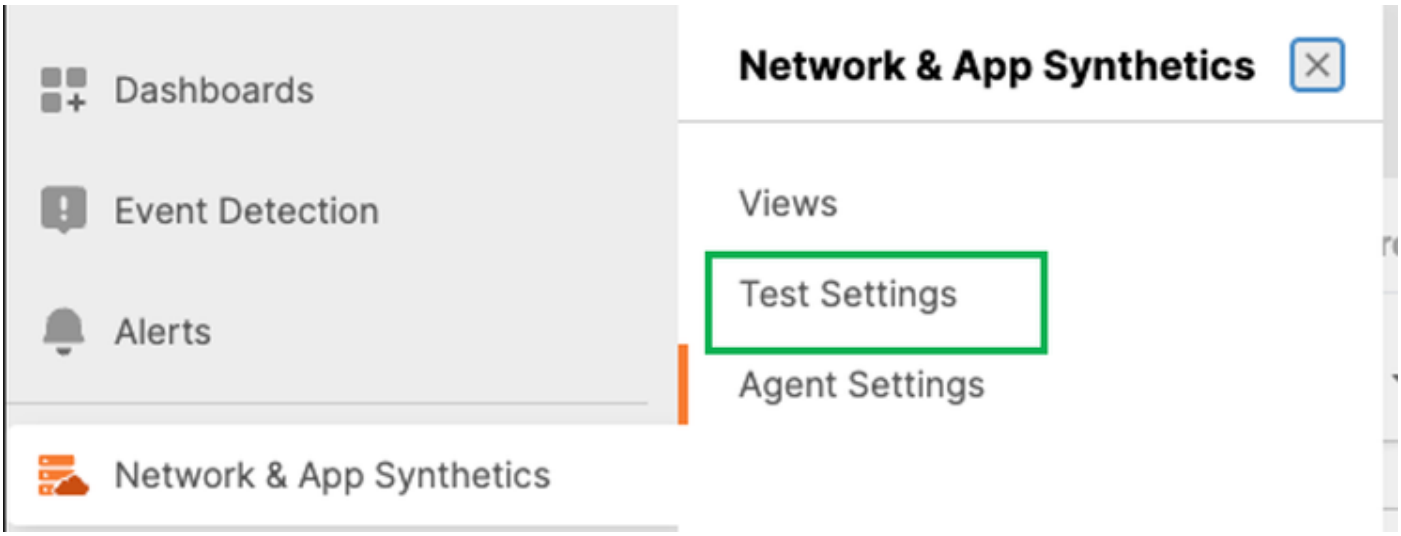
لتكوين نقطة كود الخدمات المميزة (DSCP):

1. تسجيل الدخول إلى حساب ThousandEyes من صفحة بيانات Cisco ThosandEyes.

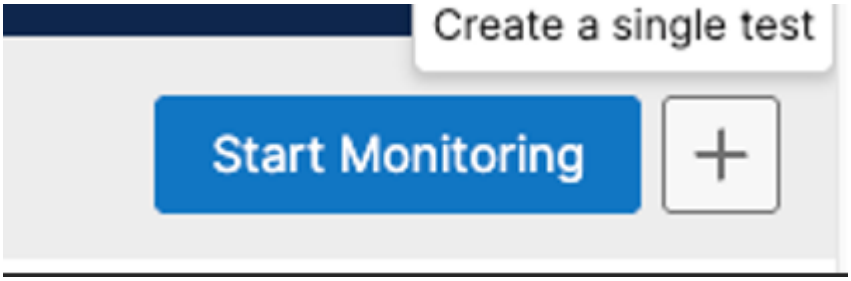
تحقق من أن "العميل" المثبت في الموجه لديه اتصال بسحابة ThousandEyes.



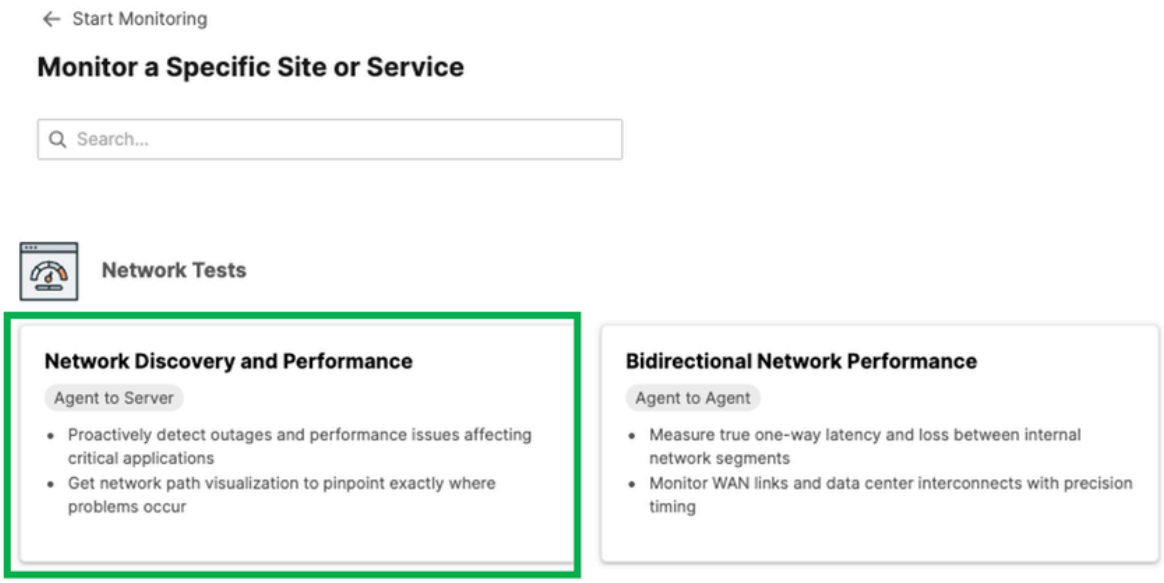

بعد تثبيت العميل على الجهاز وتأكيد الاتصال بسحابة ThousandEyes، قم بإنشاء إختبار. لإنشاء إختبار تنقل على الشبكة والتطبيق >إعدادات الاختبار.




في الشاشة العلوية اليمنى، انقر على + أيقونة.

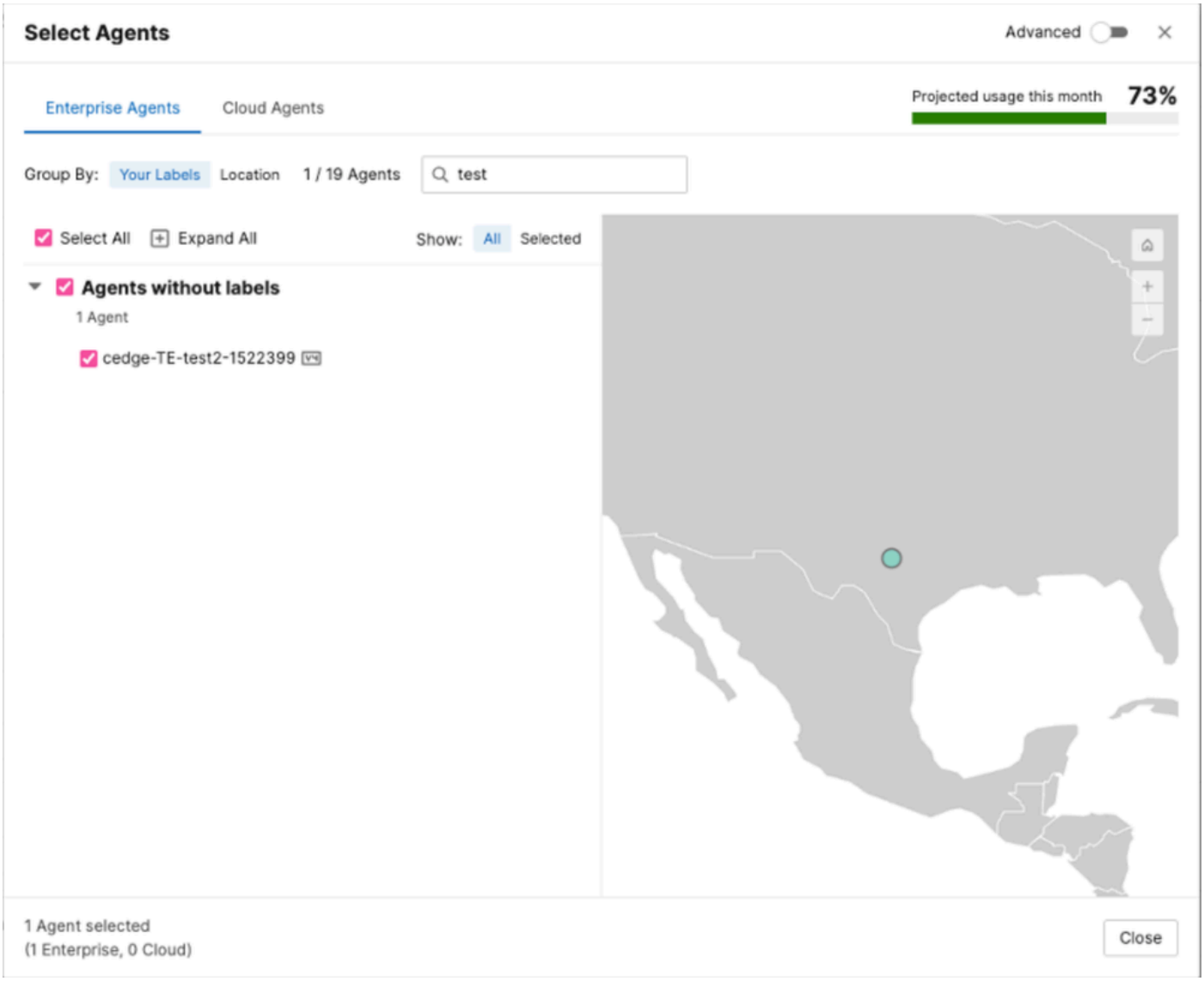



في إختبار لوحة المعلومات الجديدة، قم بتحديد وكيل إلى الخادم.




في قسم "الهدف"، حدد عنوان IP المطلوب إستخدامه للاختبار. في هذا المثال، تم إستخدام 192.168.1.47، وهو عنوان IP الخاص ب TLOC آخر على موجه مختلف داخل الشبكة الفرعية نفسها.

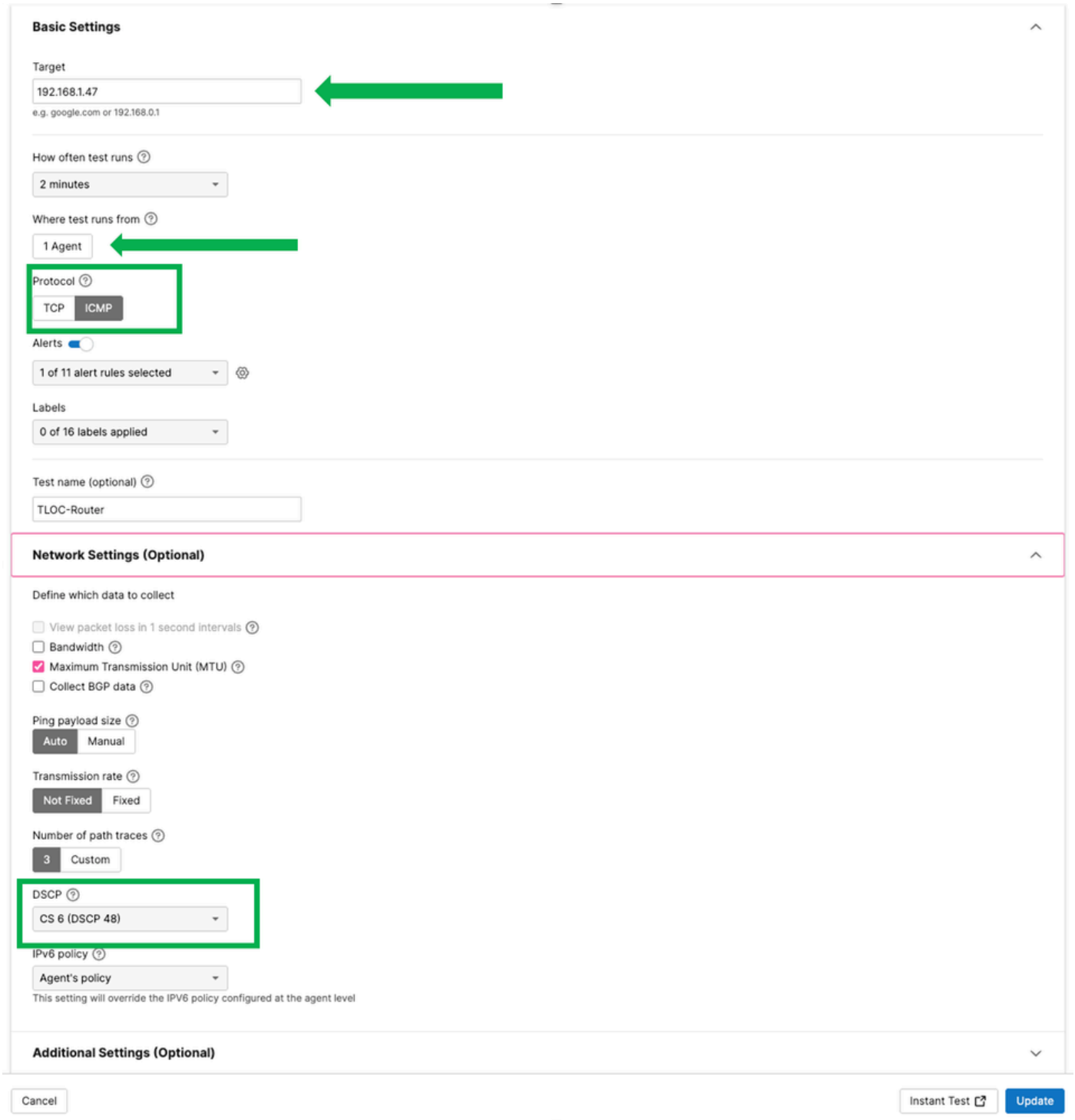
في "من حيث يعمل الاختبار"، حدد الوكيل الذي تم إنشاؤه للموجه الخاص بك (يحتوي على اسم المضيف للموجه الخاص بك) كما هو موضح أدناه:




## تحديد بروتوكول ICMP

في قسم إعدادات الشبكة (إختياري)، حدد DSCP وانقر تحديث.

في نفس القسم، انقر فوق الاختبار الفوري.




# تكوين SD-WAN

أستخدم المستند المرجعي لتكوين عميل ألف عين على موجه الحافة، قم بتكوين ThousandsEyes على أجهزة SD-WAN

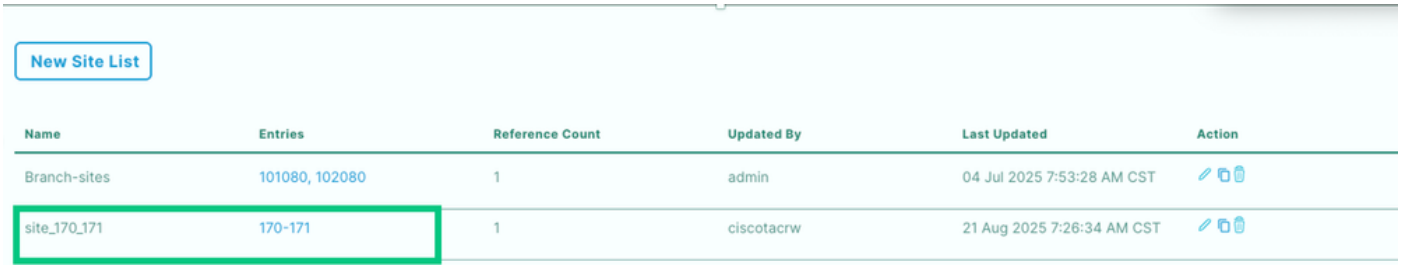
بمجرد تثبيت عميل ألفEyes على الموجه، يعرض قالب ألفEyes المعلومات:

## تكوين DSCP

انتقل إلى التكوين > السياسات >سياسة مركزية > انقر فوق إضافة سياسة. في إنشاء

مجموعة من المواقع الهامة، قم بإضافة الموقع والشبكة الخاصة الظاهرية وبادئة البيانات.

الموقع (الموقع الذي تم فيه تثبيت عميل ThousandEyes)




VPN (خدمة VPN)


قامت بادئة البيانات (بتضمين الشبكة الفرعية التي تم تكوينها على قالب ThousandEyes) في هذا المثال باستخدام الشبكة الفرعية 192.168.2.0/24.


طقطقت بعد ذلك>بعد ذلك، على شكل حركة مرور قاعدة قسم، حركة مرور بيانات وطقطقة يضيف سياسة.

تحديد DSCP، في هذا المثال المستخدم 48

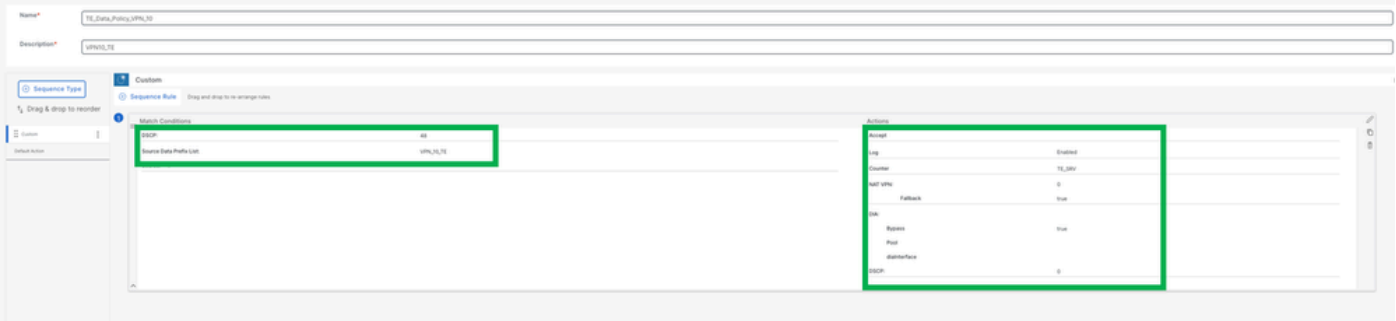
أختر خيار "قائمة بادئات البيانات المصدر". أستخدم "VPN_10_TE" (كما هو موثق مسبقا)، وهي الشبكة المستخدمة لتكوين آلافEyes على الموجه.

في قسم الإجراءات:

تحديد NAT VPN

إحتياطي

بروتوكول DSCP في هذا المثال يكون بروتوكول DSCP الذي تم تكوينه هو 0



تم تمكين الإجراء الافتراضي.

انقر فوق التالي، ثم أضف اسم النهج ووصف النهج. في قسم بيانات حركة المرور، انقر فوق قائمة منطقة الموقع/شبكة WAN الجديدة وقائمة شبكات VPN الجديدة، احفظ النهج وقم بتنشيطه،

بمجرد تنشيط النهج، تحقق في الموجه من تطبيق النهج:

قم بتشغيل الأمر 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
```

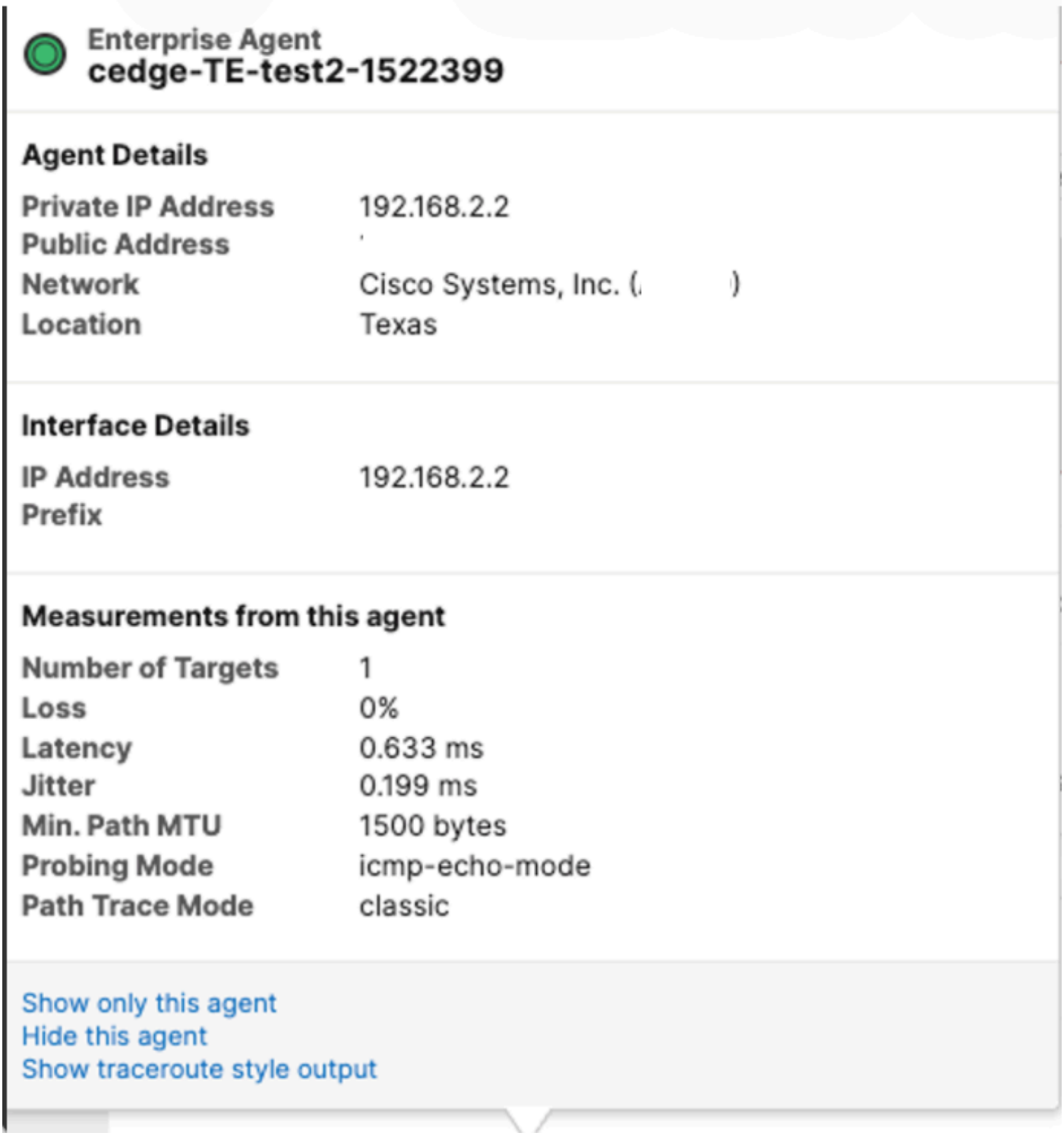
# التحقق من الصحة

لتشغيل إختبار، انقر فوق Instat Test وافتح نوافذ جديدة.

بمجرد أن ينتهي الاختبار، يمكنك أن ترى المسار الذي أخذ للوصول إلى 192.168.1.47

العميل 192.168.2.2>>>DG TE 192.168.2.1>>الاختبار 192.168.1.47

تم وضع علامة DSCP48 قبل الانتقال إلى الجزء السفلي وبعد الانتقال إلى الجزء السفلي، علامة 0.




تكوين تتبع FIA على موجه Edge:

```
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
```

فتح حزمة:

<#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
```

## معلومات ذات صلة

- تكوين آلافEyes على أجهزة SD-WAN
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).