Amélioration du débit sur Catalyst 8000V dans Azure

Table des matières

Introduction

Ce document explique comment améliorer les performances des commutateurs Cisco Catalyst 8000V déployés dans Azure.

Amélioration du débit Catalyst 8000V dans Azure

Avec Cisco Cloud OnRamp for Multicloud, les utilisateurs peuvent déployer des routeurs virtuels Cisco Catalyst 8000V dans NVA dans Azure directement avec SD-WAN Manager (interface utilisateur ou API).

L'automatisation Cloud OnRamp permet aux utilisateurs de créer et de découvrir en toute transparence des WAN virtuels, des concentrateurs virtuels et de créer des connexions aux réseaux virtuels dans Azure.

Une fois les commutateurs Cisco Catalyst 8000V déployés dans Azure, les appliances virtuelles peuvent être surveillées et gérées à partir du gestionnaire SD-WAN.

Ce document explique comment améliorer les performances dans Azure sous trois angles :

- l'installation de la licence HSEC ;
- limitations de débit sur le port TCP 12346 dans Azure ;
- vitesse négociée automatiquement sur l'interface de transport.

Installation de la licence HSEC

Les périphériques qui utilisent la stratégie Smart Licensing Using et qui doivent prendre en charge un débit de trafic chiffré de 250 Mbits/s ou plus nécessitent une licence HSEC.

C'est une exigence de la réglementation américaine sur le contrôle des exportations. Vous pouvez utiliser Cisco SD-WAN Manager pour installer des licences HSEC.

Cisco SD-WAN Manager contacte Cisco Smart Software Manager (SSM), qui fournit un code d'autorisation de licence Smart (SLAC) à charger sur un périphérique.

Le chargement de la SLAC sur un périphérique active une licence HSEC.

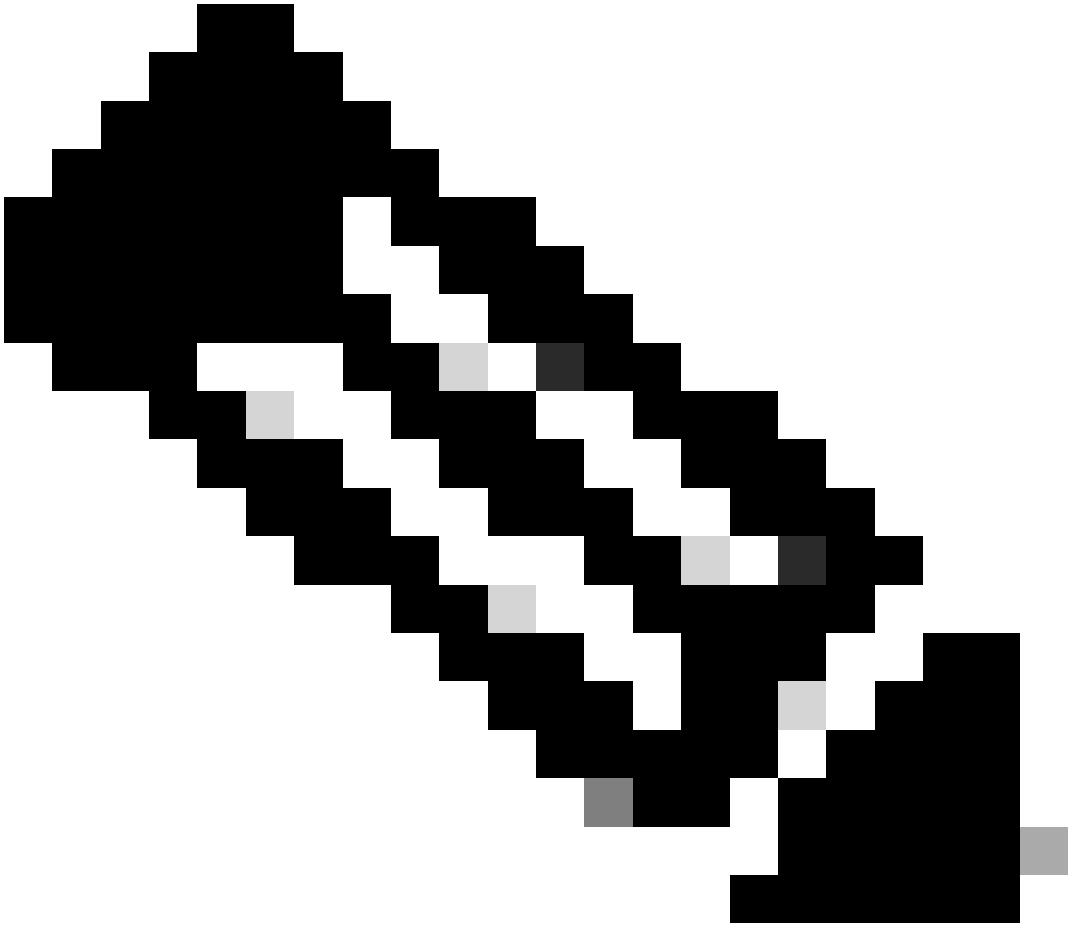
Référez-vous à Gestion des licences HSEC dans Cisco Catalyst SD-WAN pour plus de détails sur l'installation et la gestion des licences.

Limitations de débit sur le port TCP 12346 dans Azure

Actuellement, l'automatisation déploie C8000V avec une interface de transport (GigabitEthernet1) et une interface de service (GigabitEthernet2).

En raison des limitations de trafic entrant Azure sur le port SD-WAN TCP 12346, le débit peut être limité par interface de transport lorsque le trafic entre dans l'infrastructure Azure.

La limite entrante de 200 000 PPS est imposée par l'infrastructure Azure et les utilisateurs ne peuvent donc pas atteindre plus de ~1 Gbit/s par instance NVA C8000V (une hypothèse d'exemple : une taille de paquet de 600 Go, calcul : 600 B * 8 = 4800 bits ; 4800b * 200 Kpps = 960 Mbits/s).

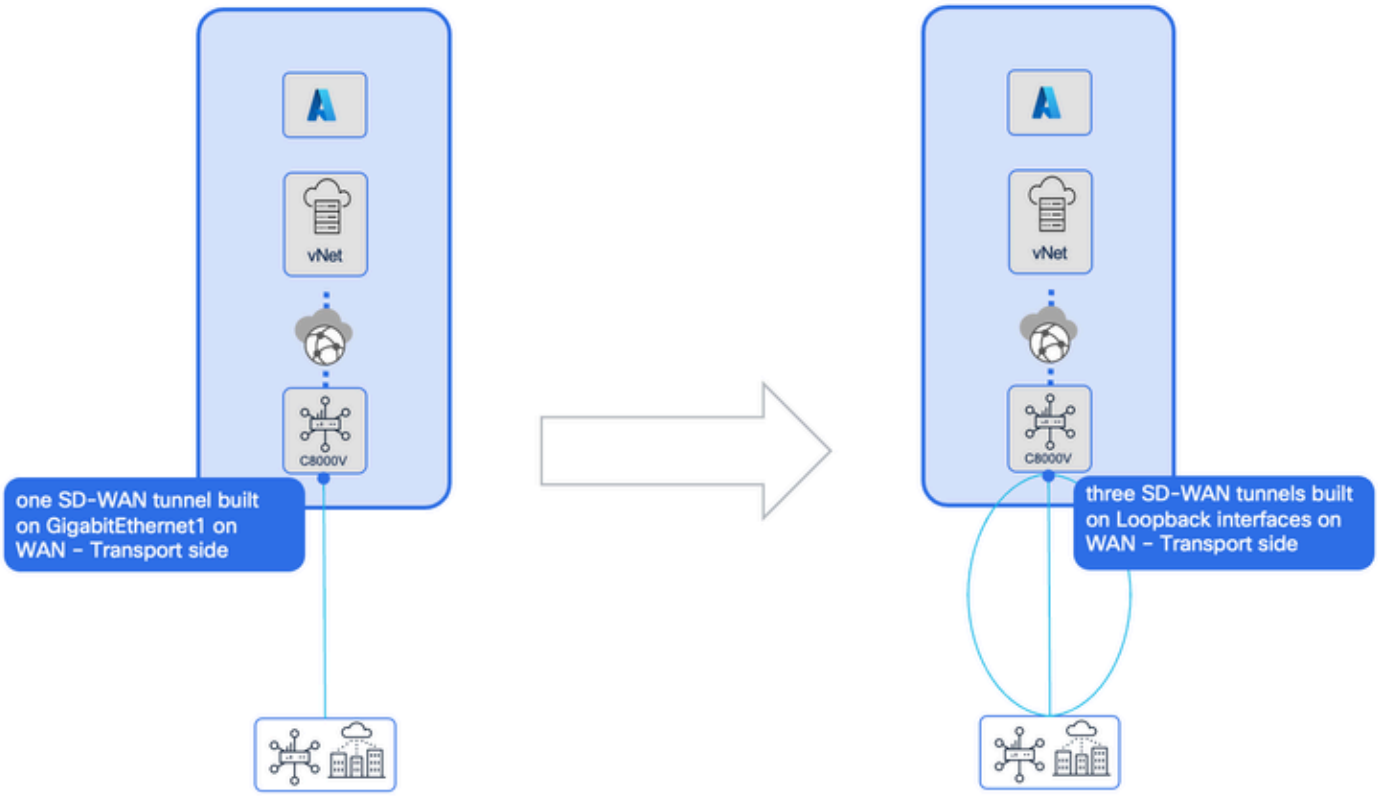


Remarque : Azure peut augmenter la limite de trafic entrant à 400 000 PPS par cas (ticket). Les clients doivent contacter Azure directement et demander l'augmentation.

Pour surmonter cette limitation, Cisco a collaboré avec Azure pour permettre aux filiales SD-WAN de créer plusieurs tunnels SD-WAN vers chaque instance NVA.

Pour effectuer cette modification de configuration, l'administrateur doit suivre ces étapes :

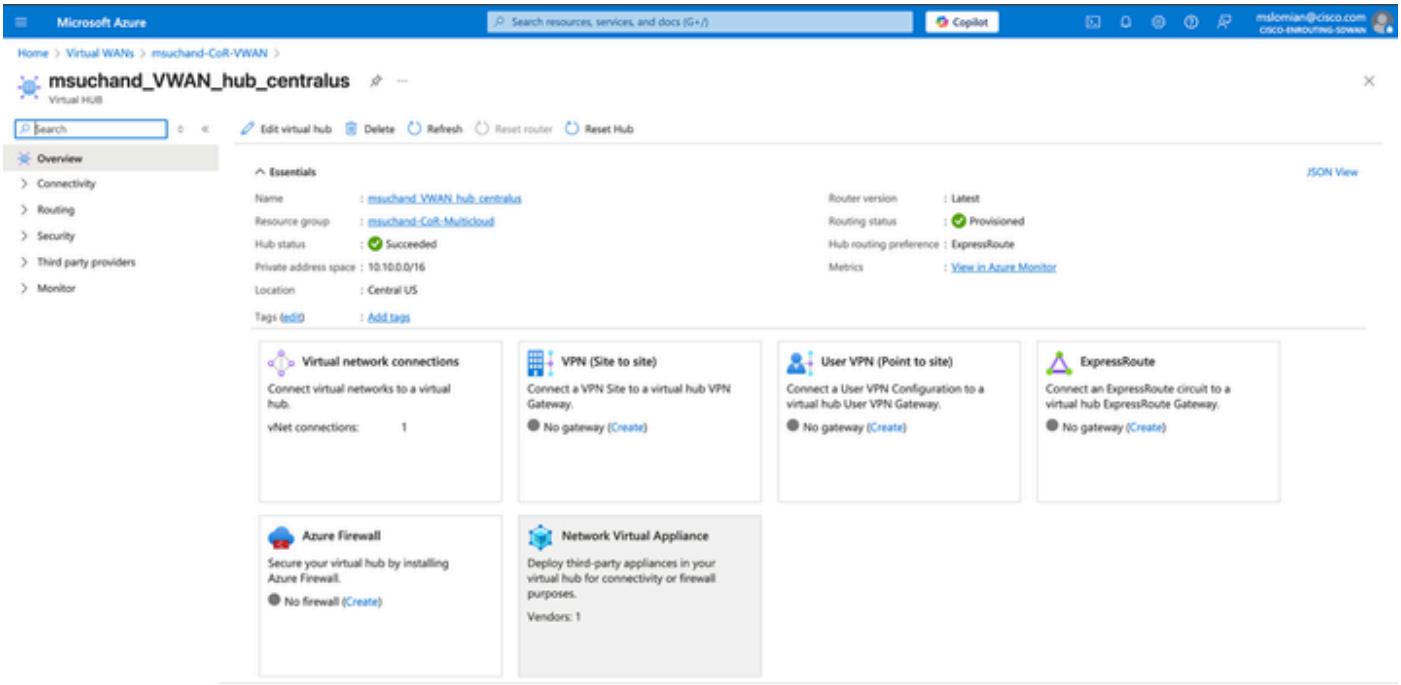
1. Dans SD-WAN Manager, déployez la passerelle cloud avec C8000V dans Azure en utilisant l'automatisation Cloud OnRamp.
2. Dans le portail Azure, modifiez les paramètres IP pour NVA dans le concentrateur virtuel.
3. Dans SD-WAN Manager, créez et diffusez un nouveau groupe de configuration à l'aide des paramètres du portail cloud.



Étape 1 :

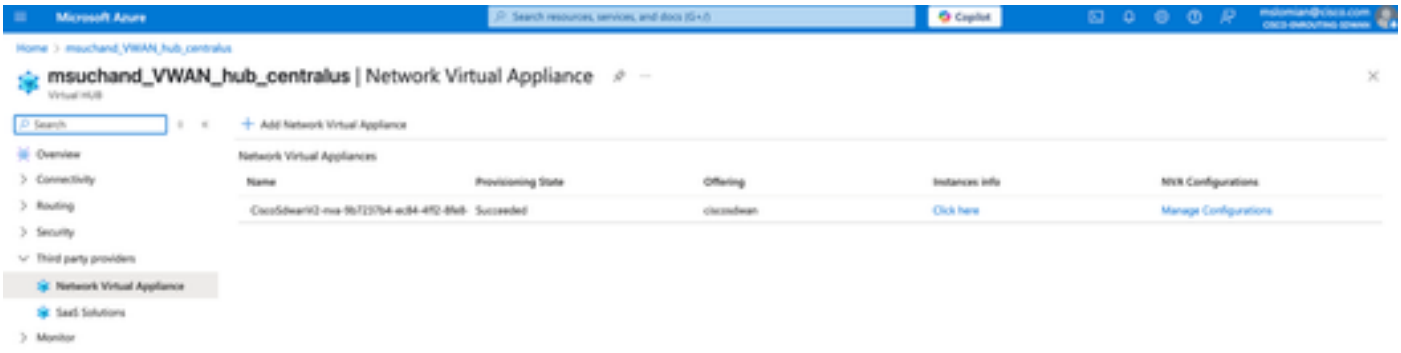
Déployez Cisco Catalyst 8000V dans Azure à l'aide de la procédure disponible ici sur cette chaîne Youtube ou dans les Notes de version.

Étape 2 :
Pour modifier les paramètres IP, accédez à Azure Portal > Virtual WANs > selected virtual WAN > virtual hub > NVA dans virtual hub.



Dans la vue Virtual Hub sur NVA, naviguez jusqu'à Third Party Providers > Manage

Configurations.



Dans la configuration NVA, accédez à Interface IP Configurations et Add Configurations. L'attribution d'adresses IP peut prendre jusqu'à 30 minutes,

Étape 3 :

Une fois les adresses attribuées, notez-les et accédez à SD-WAN Manager. Tous les C8000V ont besoin de cette mise à jour de configuration.

Il peut être fait par l'ajout CLI (il ajoute tout ce qui est dans les modèles / profils de configuration). Reportez-vous à cet exemple de configuration :

```
interface Loopback 1000
    ip address 10.0.0.244 255.255.255.255
    no shut
exit
interface Loopback 2000
    ip address 10.0.0.246 255.255.255.255
    no shut
exit
interface Loopback 3000
    ip address 10.0.0.247 255.255.255.255
    no shut
exit
interface GigabitEthernet1
    speed 10000
    no ip dhcp client default-router distance 1
    no ip address dhcp client-id GigabitEthernet1
    ip unnumbered Loopback1000
exit
interface GigabitEthernet2
    speed 10000
```

```
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.241 → 10.0.0.241 IP is Loopback 1000 IP -3
ip route 10.0.0.241 255.255.255.255 GigabitEthernet1 → 10.0.0.241 IP is Loopback 1000 IP -3
interface Tunnel1
    no shutdown
    ip unnumbered Loopback1000
    ipv6 unnumbered Loopback1000
    tunnel source Loopback1000
    tunnel mode sdwan
interface Tunnel2
    no shutdown
    ip unnumbered Loopback2000
    ipv6 unnumbered Loopback2000
    tunnel source Loopback2000
    tunnel mode sdwan
interface Tunnel3
    no shutdown
    ip unnumbered Loopback3000
    ipv6 unnumbered Loopback3000
    tunnel source Loopback3000
    tunnel mode sdwan
sdwan
 interface Loopback1000
   tunnel-interface
    encapsulation ipsec weight 1
    no border
    color biz-internet
    no last-resort-circuit
    no low-bandwidth-link
    no vbond-as-stun-server
    vmanage-connection-preference 5
    port-hop
    carrier                       default
    nat-refresh-interval          5
    hello-interval                1000
    hello-tolerance               12
    no allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    no allow-service snmp
    no allow-service bfd
  exit
 exit
 interface Loopback2000
   tunnel-interface
    encapsulation ipsec weight 1
    no border
    color public-internet
    no last-resort-circuit
    no low-bandwidth-link
    no vbond-as-stun-server
    vmanage-connection-preference 4
    port-hop
    carrier                       default
```

```
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   no allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 interface Loopback3000
   tunnel-interface
    encapsulation ipsec weight 1
    no border
    color custom1
    no last-resort-circuit
    no low-bandwidth-link
    no vbond-as-stun-server
    vmanage-connection-preference 3
    port-hop
    carrier                       default
    nat-refresh-interval          5
    hello-interval                1000
    hello-tolerance               12
    no allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    no allow-service snmp
    no allow-service bfd
  exit
 exit
 interface GigabitEthernet1
  no tunnel-interface
  exit
 exit
```

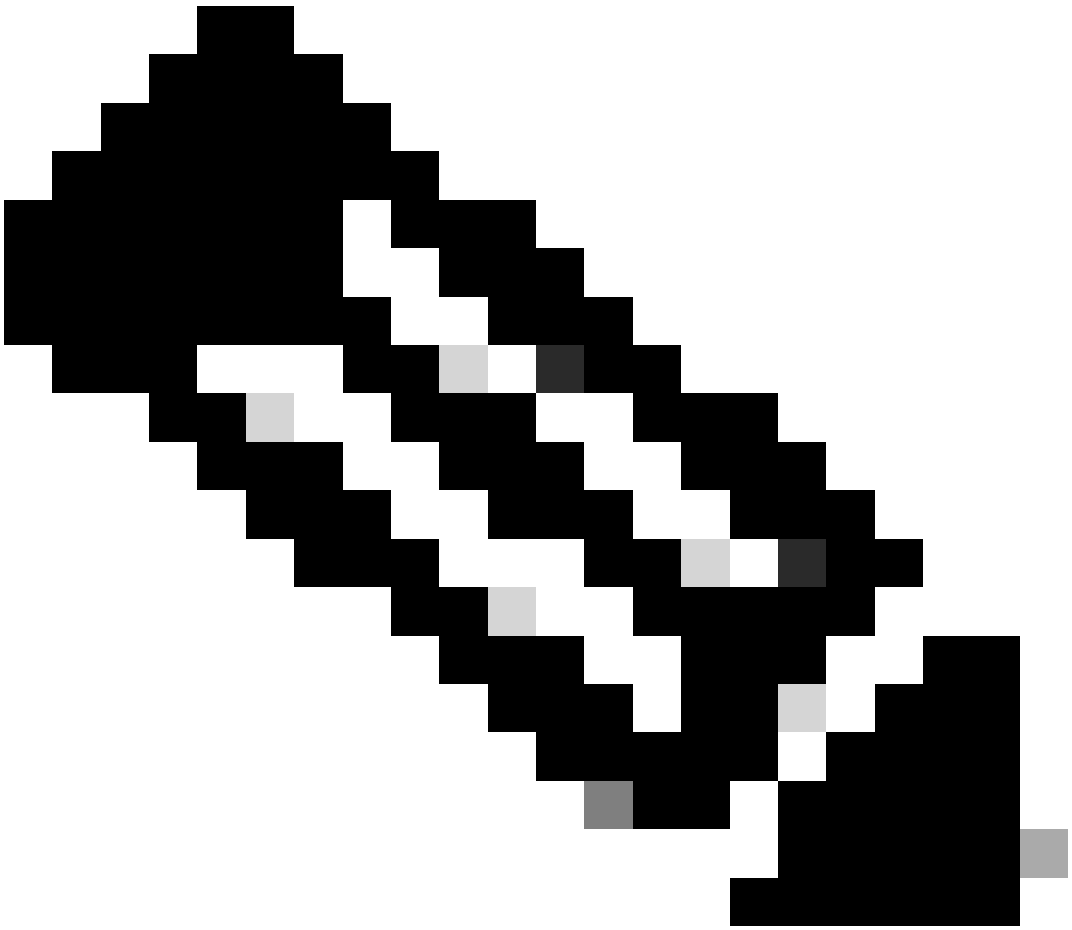
Vitesse négociée automatiquement sur l'interface de transport

L'interface de transport Cisco sur Cisco Catalyst 8000V, qui est utilisée dans les modèles par défaut ou les groupes de configuration générés automatiquement (GigabitEthernet1), est configurée avec l'option de négociation automatique pour s'assurer que la connexion est établie.

Afin d'obtenir de meilleures performances (supérieures à 1 Go), il est recommandé de définir la vitesse sur les interfaces à 10 Go. Cela s'applique également à l'interface de service (GigabitEthernet2). Pour vérifier la vitesse négociée, exécutez ces commandes :

```
azure-central-us-1#sh int gi1
GigabitEthernet1 is up, line protocol is up
  Hardware is vNIC, address is 000d.3a92.e2ff (bia 000d.3a92.e2ff)
  Internet address is 10.48.0.244/28
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,

…
azure-central-us-1#sh int gi2
GigabitEthernet2 is up, line protocol is up
  Hardware is vNIC, address is 000d.3a92.ea8a (bia 000d.3a92.ea8a)
  Internet address is 10.48.0.229/28
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```



Remarque : Bien que cet article porte sur le déploiement C8000V dans Azure avec l'automatisation Cloud OnRamp (NVA), la vitesse négociée automatiquement s'applique également aux déploiements Azure dans les déploiements VNets, AWS et Google.

Afin de changer cela, faites des changements dans le modèle (Configuration > Templates > Feature Template > Cisco VPN Interface Ethernet) / groupe de configuration (voir le guide). Les administrateurs peuvent également modifier ce paramètre dans l'interface de ligne de commande, si le périphérique est géré par cette interface.

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.