提高Azure中Catalyst 8000V的吞吐量

目錄

簡介

本文檔介紹如何提高在Azure中部署的Cisco Catalyst 8000Vs的效能。

Azure中的Catalyst 8000V吞吐量改進

藉助適用於多雲的Cisco Cloud OnRamp，使用者可以直接使用SD-WAN管理器（UI或API）在Azure中的NVA中部署Cisco Catalyst 8000V虛擬路由器。

Cloud OnRamp自動化允許使用者無縫建立和發現虛擬WAN、虛擬集線器，並建立到Azure中虛擬網路的連線。

在Azure中部署Cisco Catalyst 8000Vs後，可以通過SD-WAN管理器監控和管理虛擬裝置。

本文檔從三個角度說明了如何提高Azure的效能：

- 安裝HSEC許可證；
- Azure中TCP連線埠12346吞吐量限制；
- 傳輸介面上的自動交涉速度。

安裝HSEC許可證

使用使用策略的智慧許可且必須支援250 Mbps或更高的加密流量吞吐量的裝置需要HSEC許可證。

這是美國出口管製法規的一項要求。您可以使用Cisco SD-WAN Manager安裝HSEC許可證。

Cisco SD-WAN Manager會聯絡Cisco Smart Software Manager(SSM)，後者提供載入到裝置的智慧許可證授權代碼(SLAC)。

在裝置上載入SLAC將啟用HSEC許可證。

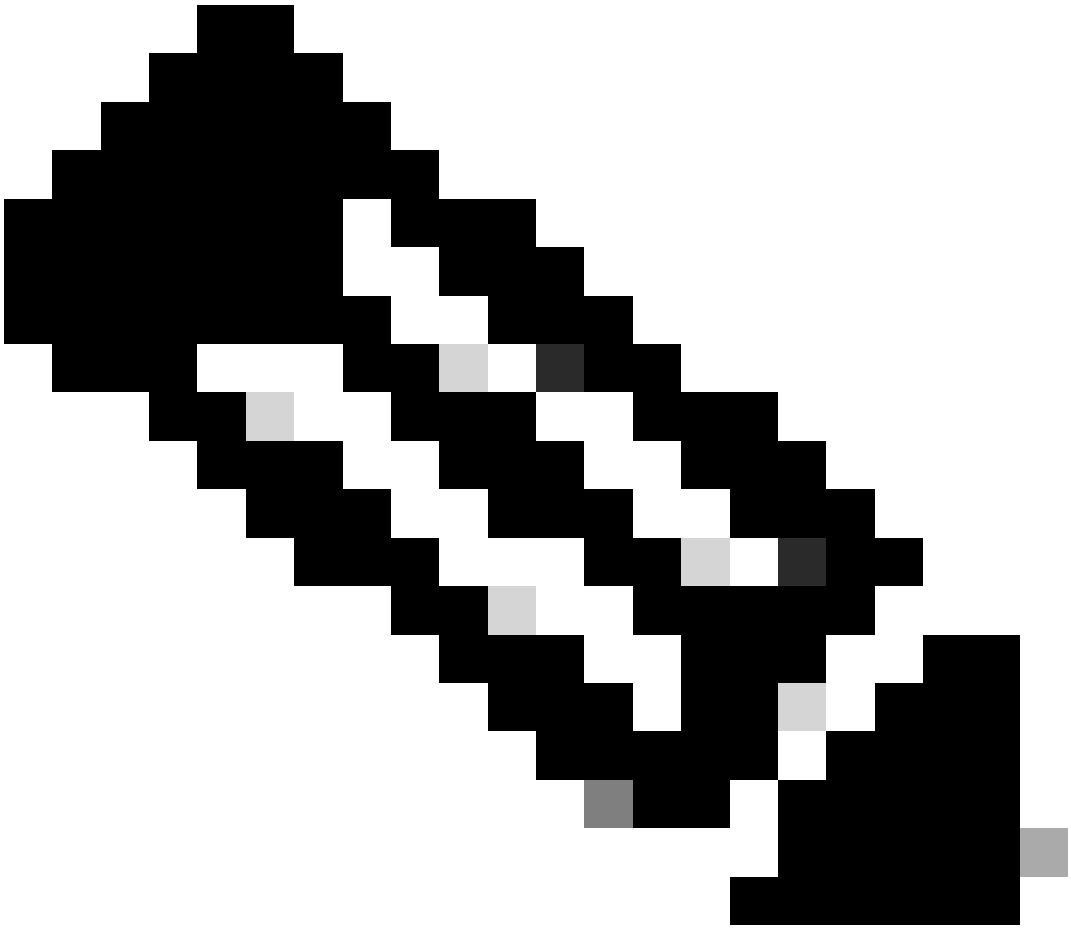
有關安裝和管理許可證的詳細資訊，請參閱在Cisco Catalyst SD-WAN中管理HSEC許可證。

Azure中TCP UDP埠12346吞吐量限制

目前，該自動化裝置部署帶有一個傳輸介面(GigabitEtherent1)和一個服務介面(GigabitEtherent2)的C8000V。

由於SD-WAN埠TCP 12346上的Azure入站限制，當流量進入Azure基礎設施時，吞吐量可能會基於每個傳輸介面受到限制。

200K PPS的入站限制由Azure基礎設施強制實施，因此使用者每個C8000V NVA例項不能達到超過~1Gbps(示例假設：封包大小為600B，計算：600B * 8 = 4800位；4800b * 200Kpps = 960 Mbps)。

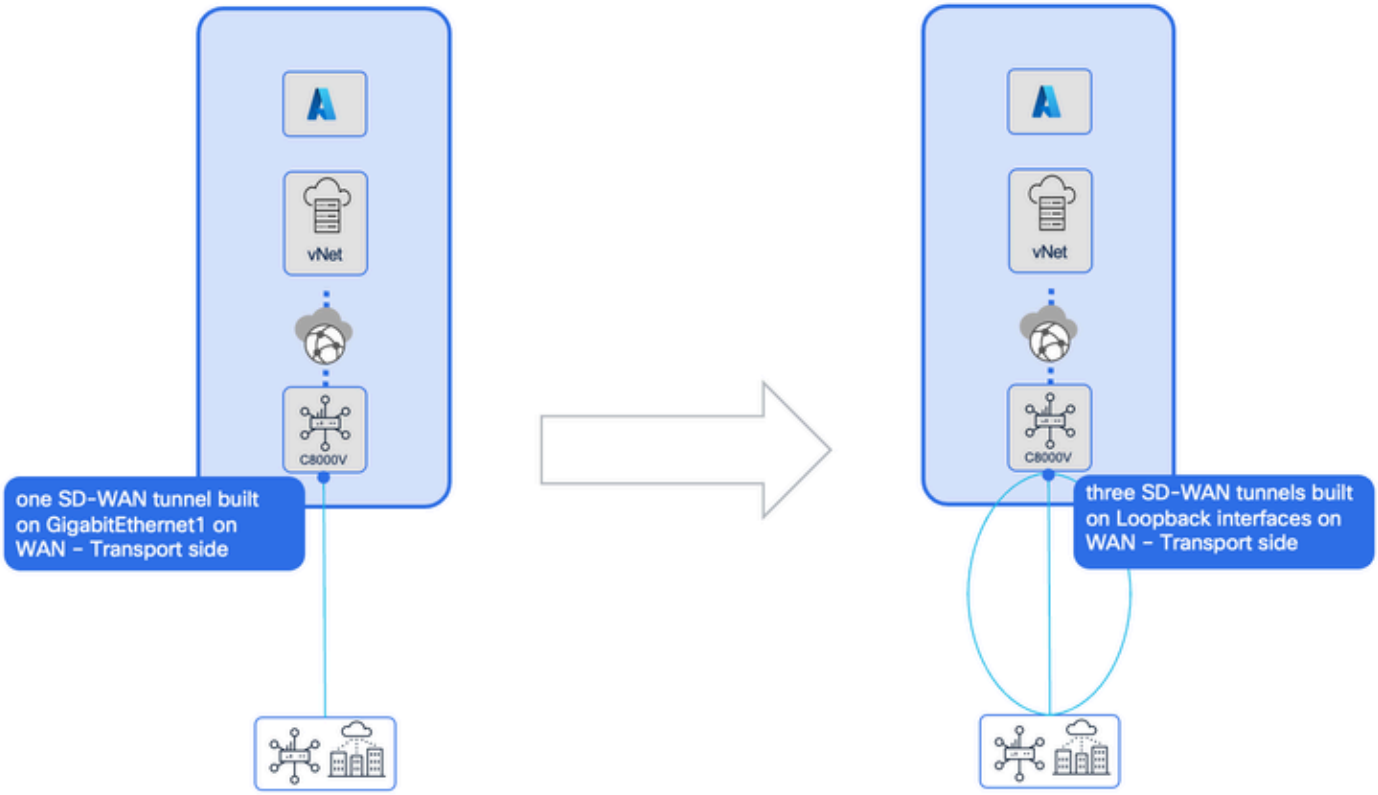


附註：Azure可以將入站限制提高到每個案例（票證）的400K PPS。客戶需要直接聯絡Azure並請求增加。

為了克服這一限制，思科與Azure合作，允許SD-WAN分支機構為每個NVA例項構建多個SD-WAN隧道。

要進行此配置更改，管理員必須執行以下步驟:

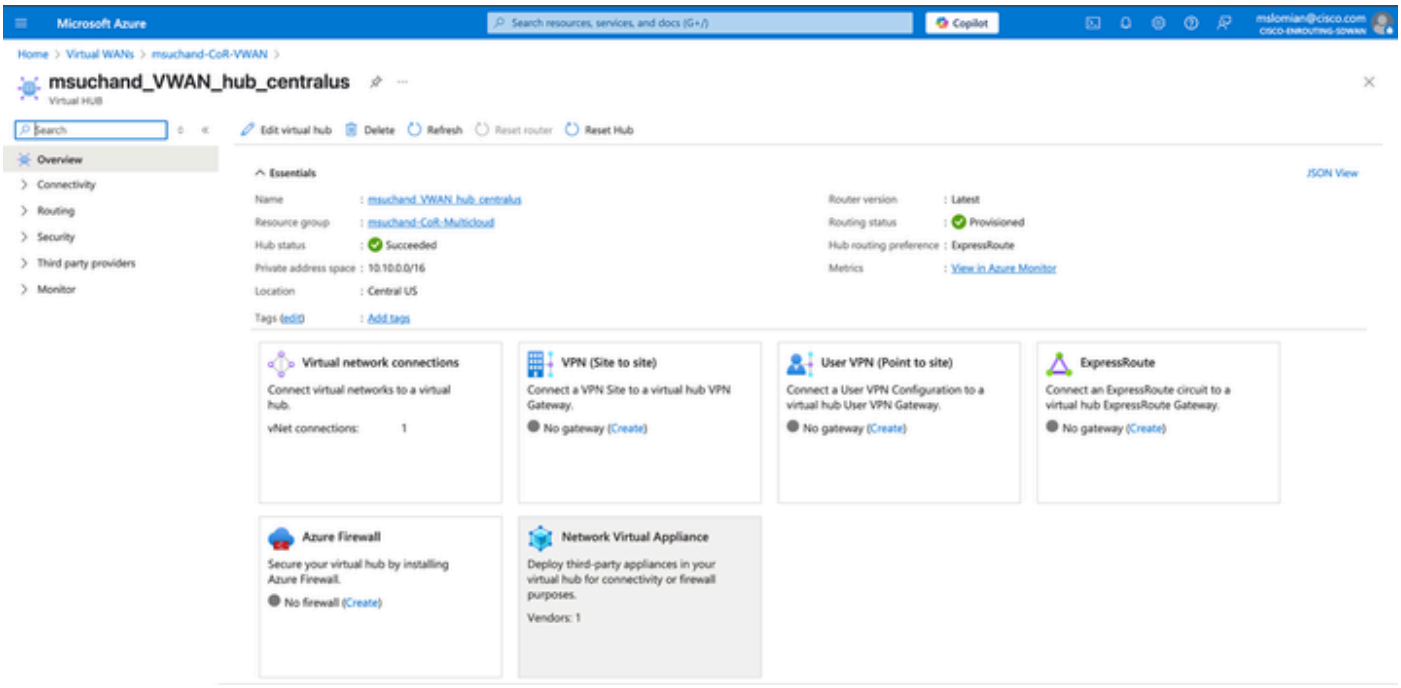
1. 在SD-WAN Manager中，使用Cloud OnRamp自動化在Azure中部署C8000V雲網關。
2. 在Azure門戶中，更改虛擬中心中NVA的IP設定。
3. 在SD-WAN Manager中，使用雲門戶中的設定建立和推送新的配置組。



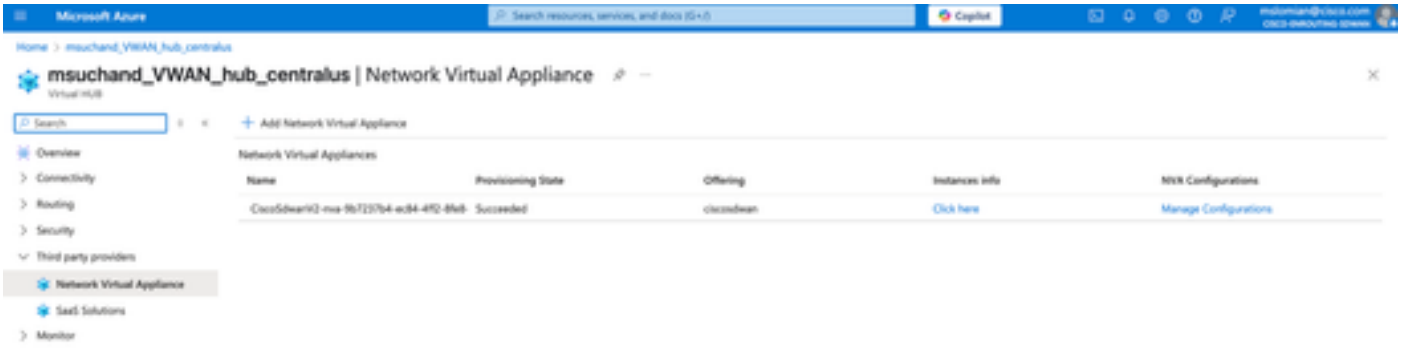
步驟 1:

使用此Youtube channel或發行說明中此處找到的步驟在Azure中部署Cisco Catalyst 8000V。

步驟 2:
要更改IP設定，請導航到Azure porta > Virtual WANs > selected virtual WAN > virtual hub > NVA in virtual hub。



在NVA上的虛擬中心檢視中，導航到第三方提供程式>管理配置。



在NVA配置中，導航到介面IP配置和新增配置。分配IP地址最多需要30分鐘，

步驟 3:

分配地址後，記下這些地址並轉至SD-WAN Manager。所有C8000V都需要此配置更新。

它可以通過CLI外掛完成（它會附加模板/配置檔案中的任何內容）。 請參閱以下範例組態：

```
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
```

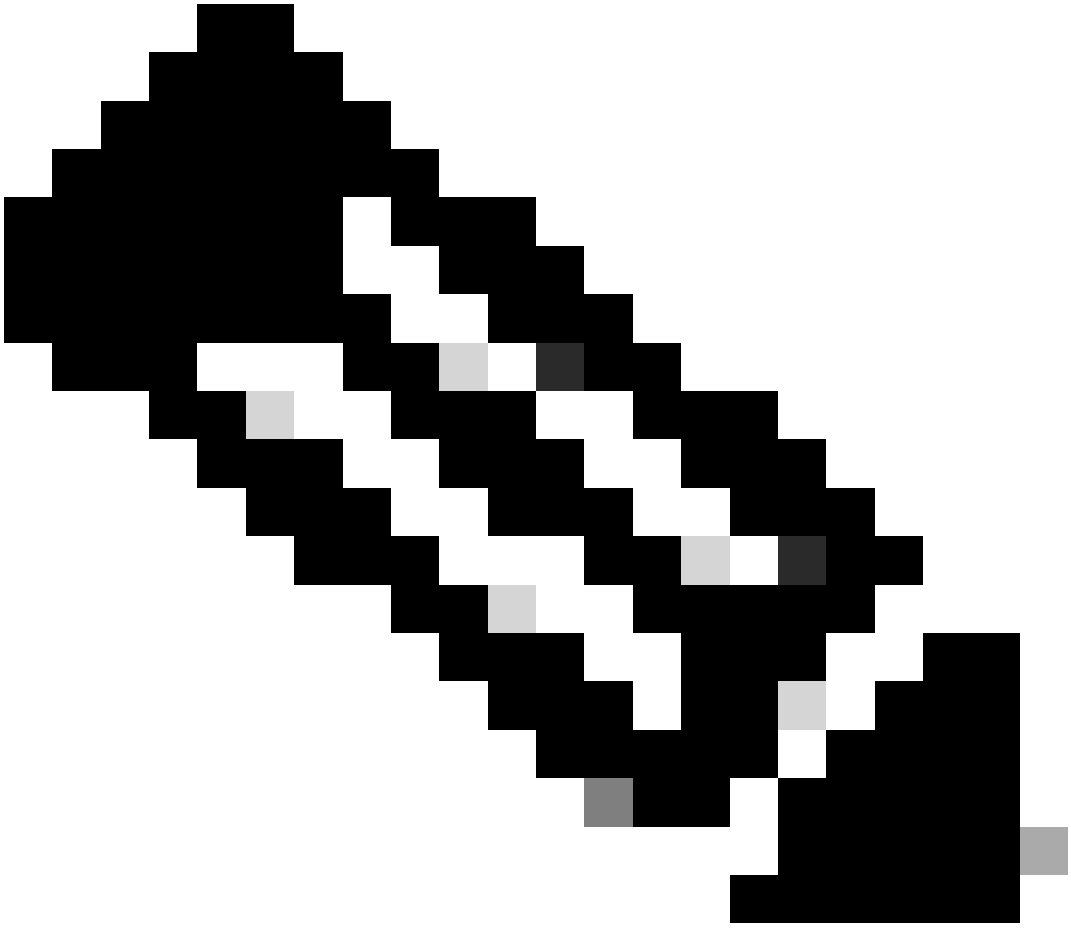
傳輸介面上的自動交涉速度

Cisco Catalyst 8000V上的思科傳輸介面(用於預設範本或自動產生的組態組(GigabitEthernet1))設定為自動交涉，以確保已建立連線。

為了獲得更好的效能（高於1Gb），建議將介面速度設定為10Gb。這也適用於服務介面(GigabitEthernet2)。 要驗證協商速度，請運行以下命令：

```
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,
```



附註：雖然本文重點介紹使用Cloud OnRamp automation(NVA)在Azure中部署C8000V，但自動協商速度也適用於VNet、AWS和Google部署中的Azure部署。

要更改此設定，請更改模板(Confusation > Templates > Feature Template > Cisco VPN Interface Ethernet)/配置組(請參閱指南)。 或者，如果裝置由CLI管理，管理員也可以在CLI中編輯此資訊。

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）。