

配置和驗證適用於多雲的雲OnRamp - AWS

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[步驟 1.將AWS裝置模板連線到兩個C8000v裝置](#)

[步驟 2.配置SD-WAN與AWS的整合](#)

[步驟 3.如何刪除雲網關](#)

[驗證](#)

[相關資訊](#)

簡介

本文檔介紹如何配置和驗證Cisco SD-WAN Cloud OnRamp，以實現與Amazon Web Services (AWS)的多雲整合。

必要條件

確保您擁有以下內容：

- AWS雲帳戶詳細資訊。
- 訂購AWS Marketplace。
- Cisco SD-WAN Manager必須有兩個可用的Catalyst 8000V OTP令牌才能在其證書頁籤中建立雲網關。

需求

思科建議您瞭解以下主題：

- 思科軟體定義廣域網路(SD-WAN)
- AWS

採用元件

本檔案根據這些軟體和硬體版本：

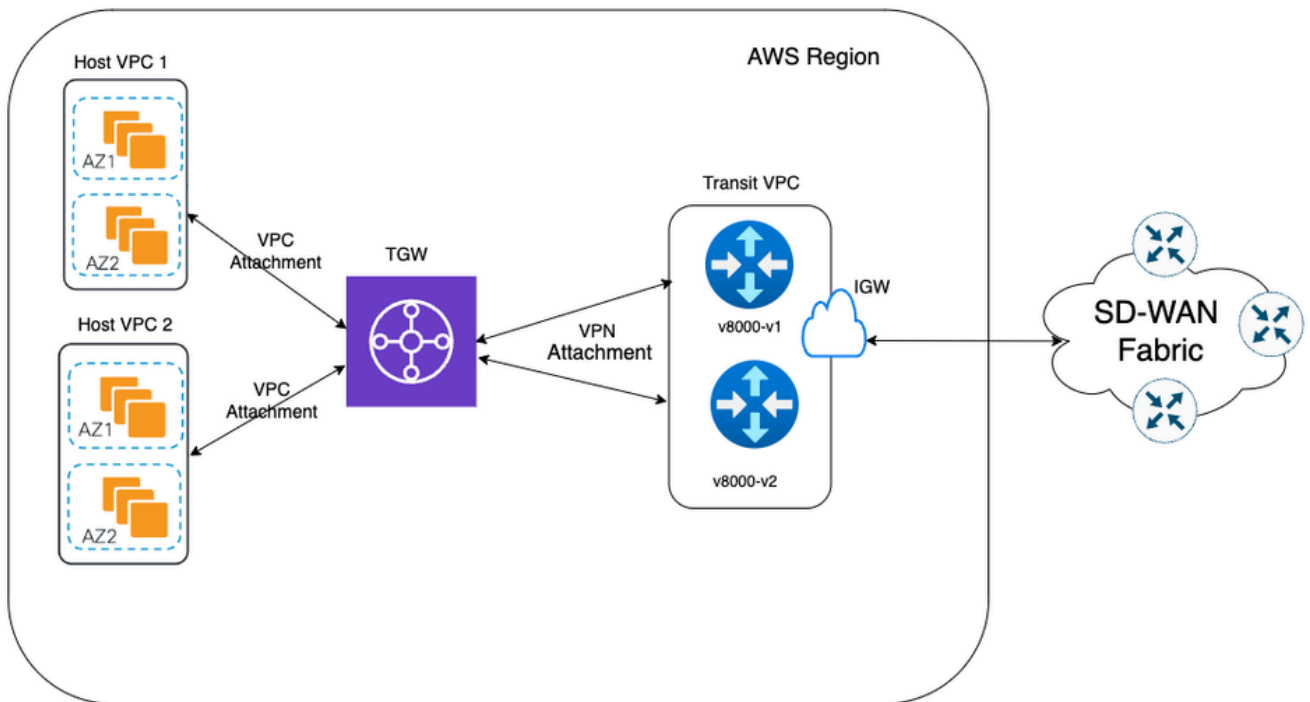
- Cisco Catalyst SD-WAN Manager版本20.9.4.1

- Cisco Catalyst SD-WAN控制器版本20.9.4
- 思科邊緣路由器版本17.9.04a

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

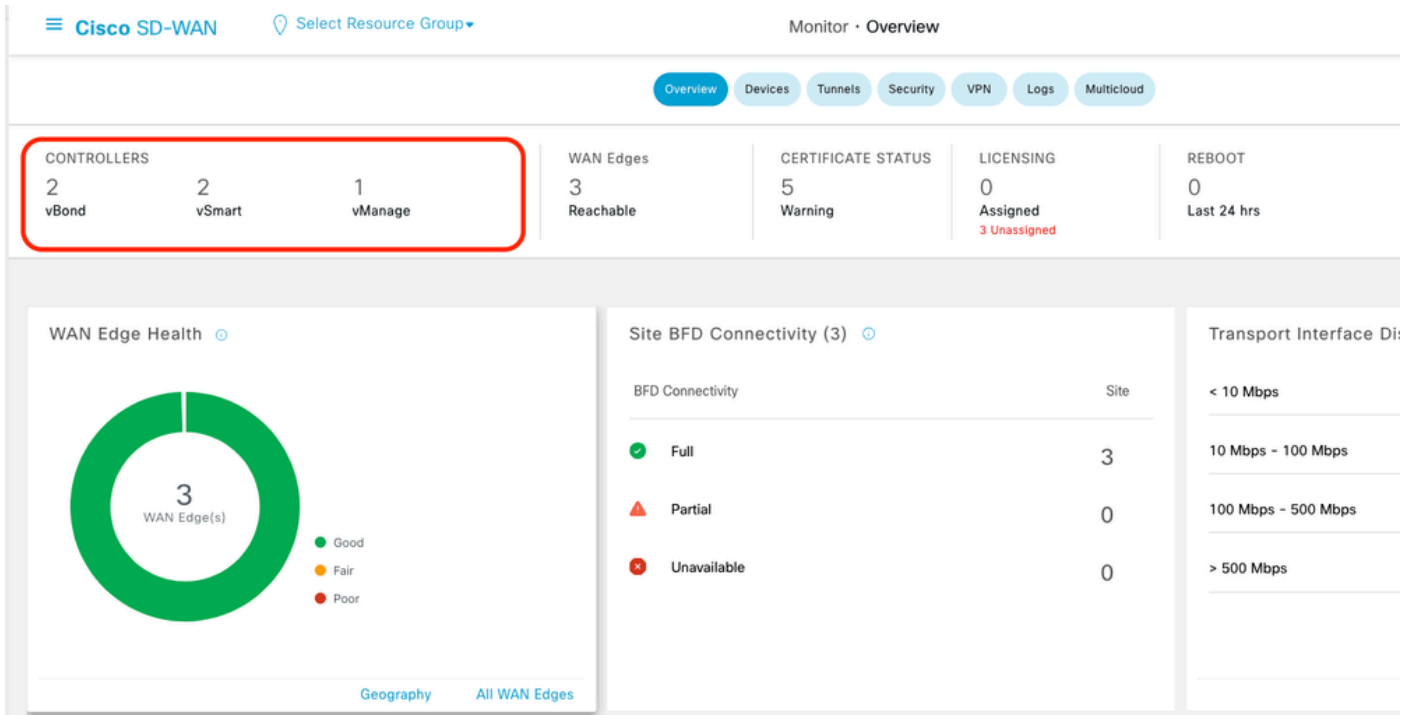
設定

網路圖表



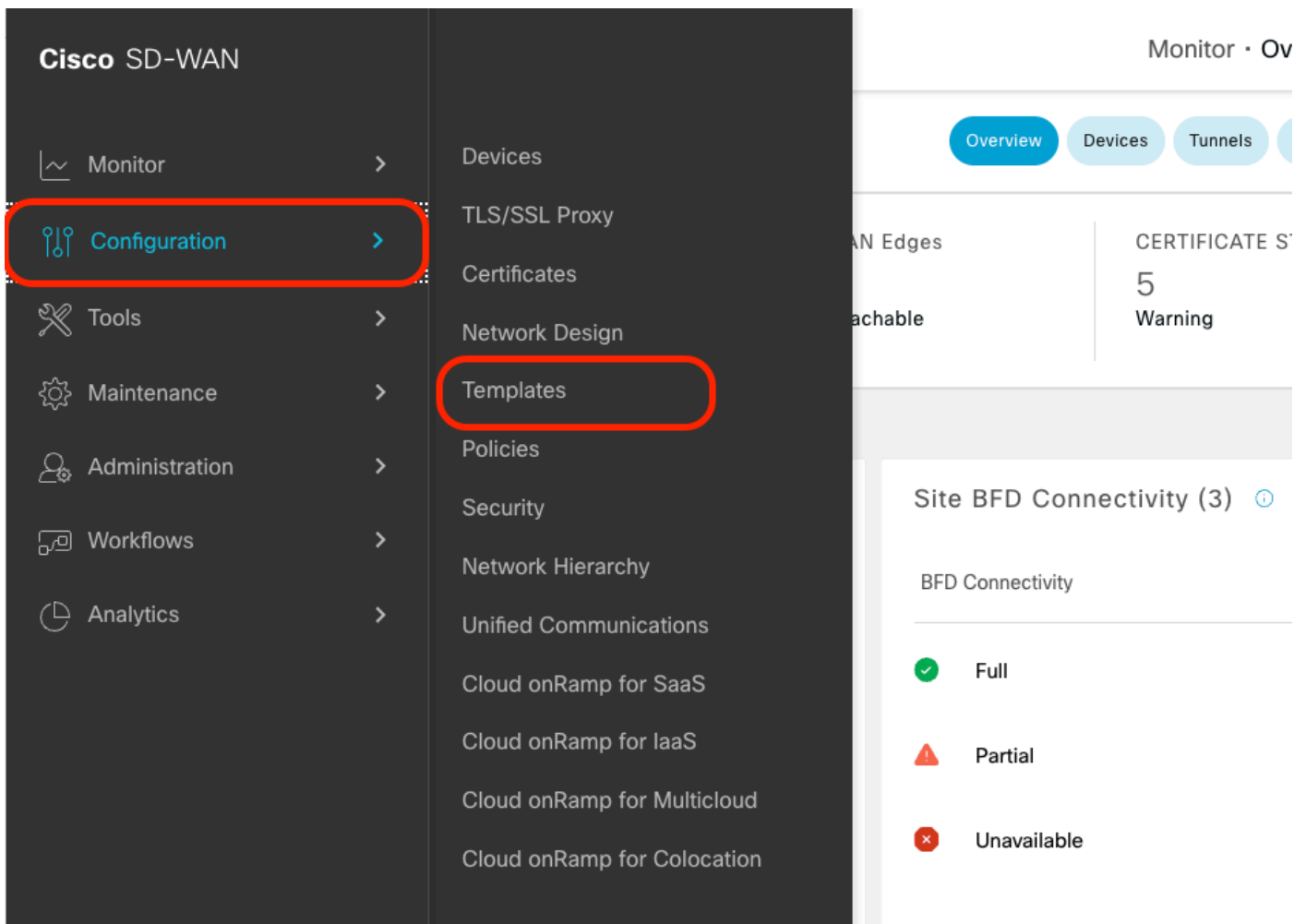
組態

登入Catalyst SD-WAN Manager GUI，驗證所有控制器均已啟用。



第1步：將AWS裝置模板連線到兩個C8000v裝置

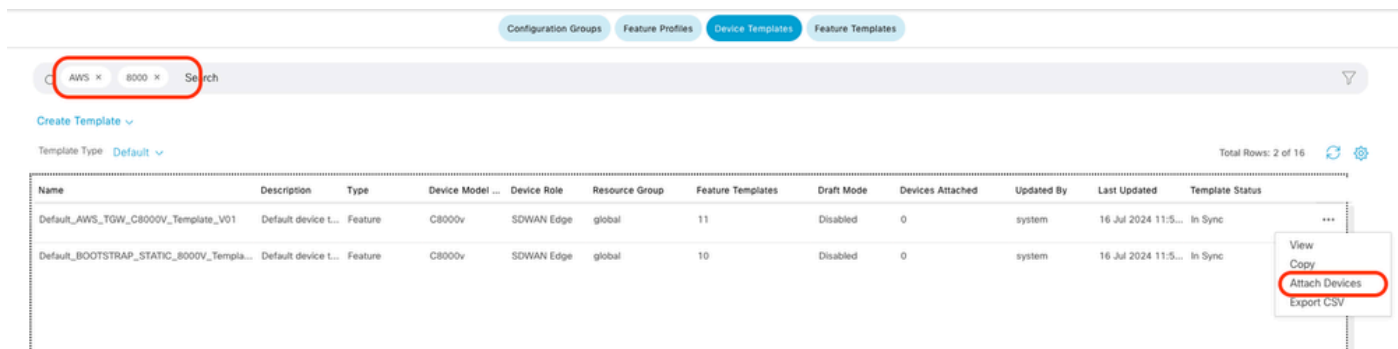
在Cisco SD-WAN Manager選單上，導航到Configuration > Templates。



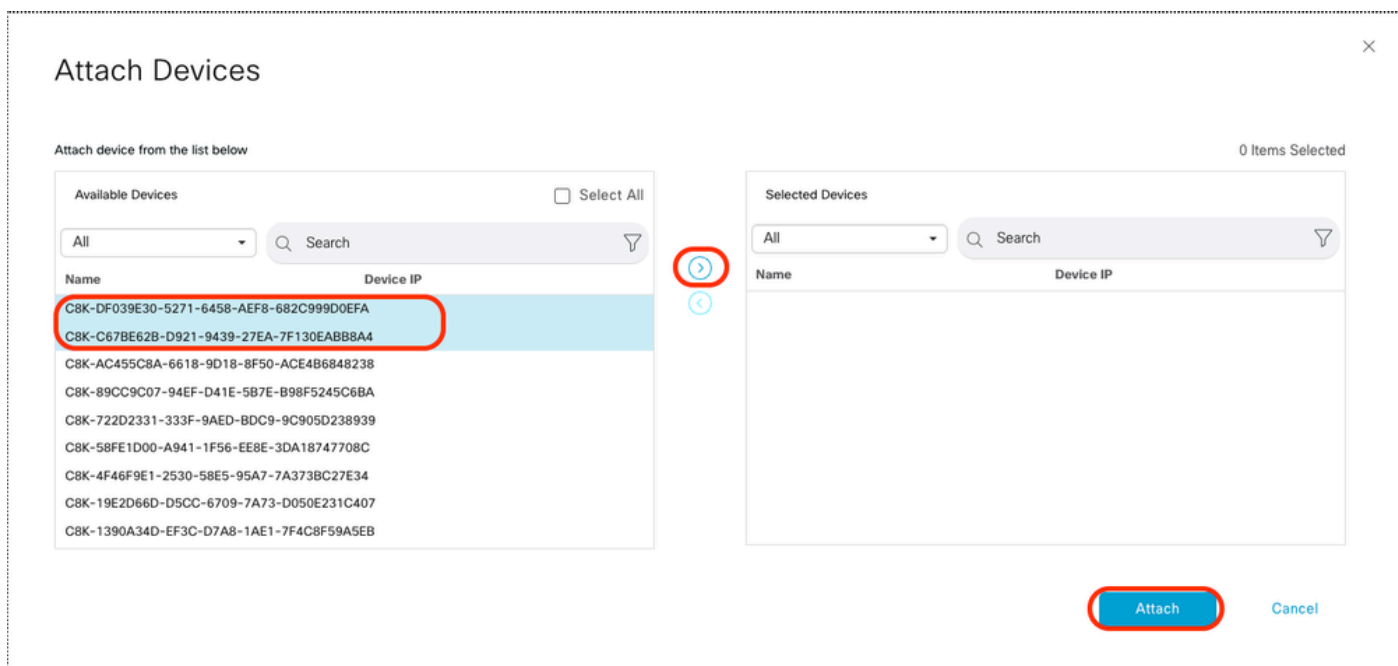
按一下Device Templates > From Template。鍵入下拉選單並選擇Default。



在搜尋欄中，鍵入AWS和C8000v。然後，點選Default_AWS_TGW_C8000V_Template_V01模板旁邊的3點(...)。在下拉選單中選擇Attach Devices。



選擇兩台C8000v裝置。按一下向右箭頭，然後按一下「附加」。



點選裝置上的3個點(...)並導航至編輯裝置模板。



按一下下拉選單並選擇Color，輸入Hostname、System IP、Site ID。輸入這些詳細資訊後，按一下Update。

輸入每個獨立裝置的值，然後按一下Update。

範例：

<#root>

On

Device 1

Color: Select biz-internet from Dropdown

Hostname: C8kv1-aws

System IP: 10.2.2.1

Site: ID 2

<#root>

On

Device 2

Color: biz-internet Color: biz-internet

Hostname: C8kv2-aws

System IP: 10.2.2.2

Site: ID 2

Update Device Template

Variable List (Hover over each field for more information)

Status	in_complete
Chassis Number	C8K-1390A34D-EF3C-D7A8-1AE1-7F4C8F59A5EB
System IP	-
Hostname	-
Color(vpn_if_tunnel_color_value)	<input type="text" value="biz-internet"/>
Hostname(host-name)	<input type="text" value="C8kv1-aws"/>
System IP(system-ip)	<input type="text" value="2.2.2.1"/>
Site ID(site-id)	<input type="text" value="2"/>

完成這兩個裝置的操作後，按一下Next。

Total Rows: 2

Status	Chassis Number	System IP	Hostname	Color(vpn_if_tunnel_color_value)	Hostname(host-name)	System IP(system-ip)	Site ID(site-id)	
✓	C8K-C67BE62B-D921-9439-27EA-7F13...	-	-	<input type="text" value="biz-internet"/>	C8kv1-aws	2.2.2.1	2	...
✓	C8K-DF039E30-5271-6458-AEF8-682C9...	-	-	<input type="text" value="biz-internet"/>	C8kv2-aws	2.2.2.2	2	...

按一下其中一個裝置，並確保配置正確。按一下Configure Devices。

Device Template: Default_AWS_TGW_C8... Total: 1

Device list (Total: 2 devices)

Filter/Search

C8K-C67BE62B-D921-9439-27EA-7F130EAB88A4
-|-

C8K-DF039E30-5271-6458-AEF8-682C999D0EFA
-|-

Configure Device Rollback Timer

Config Preview

```
system
ztp-status          in-progress
device-model        vedge-C8000V
system-ip           2.2.2.1
overlay-id          1
site-id             2
no transport-gateway enable
port-offset         1
control-session-pps 300
admin-tech-on-failure
sp-organization-name
organization-name
port-hop
track-transport
track-default-gateway
console-baud-rate   19200
no on-demand enable
on-demand idle-timeout 10
vbond
logging
disk
  enable
!
!
!
bfd color lte
hello-interval 1000
no pmtu-discovery
multiplier 1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
ipsec
  rekey          86400
  replay-window  512
  authentication-type ah-shal-hmac shal-hmac
  integrity-type  ip-udp-esp esp
```

Back Configure Devices Cancel

在彈出窗口中，點選2個裝置上的確認配置更改覈取方塊，然後點選確定。

Configure Devices

Committing these changes affect the configuration on 2 devices. Are you sure you want to proceed?

Confirm configuration changes on 2 devices.

OK Cancel

確認已排定將範本附加到裝置。

Total Rows: 2

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID	vManage IP
Done - Scheduled	<pre>[18-Jul-2024 16:10:13 UTC] Configuring device with feature template: Default_AWS_TGW_C8000V_Template_V01 [18-Jul-2024 16:10:13 UTC] Checking and creating device in vManage [18-Jul-2024 16:10:14 UTC] Generating configuration from template [18-Jul-2024 16:10:17 UTC] Device is offline [18-Jul-2024 16:10:17 UTC] Updating device configuration in vManage [18-Jul-2024 16:10:18 UTC] Configuration template Default_AWS_TGW_C8000V_Template_V01 scheduled to be attached when device comes onLine. To check the synced state, click Configuration > Devices > Device Options</pre>	C8000v					

步驟 2. 配置SD-WAN與AWS的整合

您可以透過Cisco Catalyst SD-WAN Manager為多雲環境配置和管理Cloud onRamp。

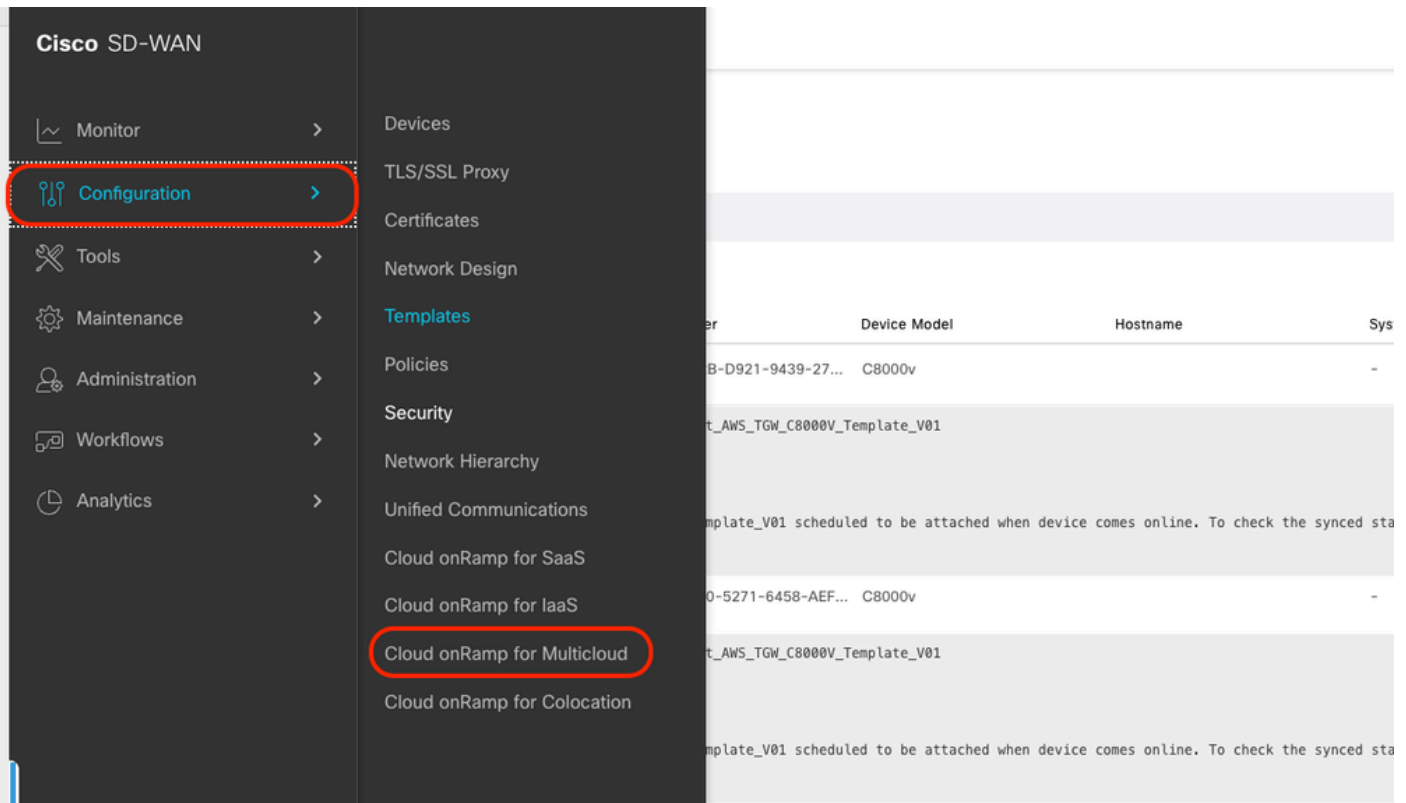
Cisco Catalyst SD-WAN Manager中的配置嚮導可自動將中轉網關轉到您的公共雲帳戶，並自動在重疊網路中的分支機構中連線公共雲應用和這些應用使用者。此功能可與思科雲路由器上的AWS虛擬私有雲(VPC)配合使用。

中轉網關是可用於將VPC和本地網路互連的網路中轉中心。您可以將VPC或VPN連線連線到傳輸網關。它充當在VPC和VPN連線之間傳輸流量的虛擬路由器。

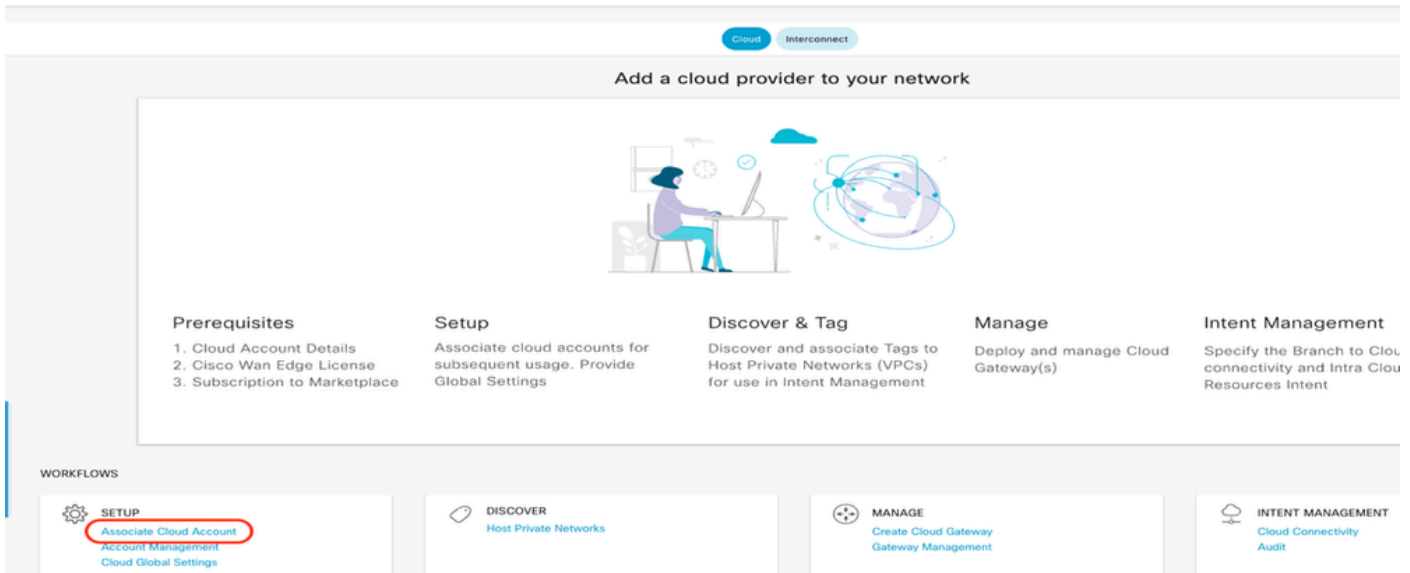
適用於多雲的雲OnRamp支援與多個AWS帳戶的整合。

建立AWS雲帳戶

導航到配置>多雲的雲onRamp。



點選 workflow>設定中的關聯雲帳戶。



- 在Cloud Provider欄位中，從下拉選單中選擇Amazon Web Services。
- 在雲帳戶名稱欄位中輸入帳戶名稱。
- 選擇Yes建立雲網關。
- 在Log in to AWS With欄位中選擇要使用的身份驗證模式。
 - 主要
 - IAM角色

如果您選擇金鑰型號，則請在相應欄位中提供API Key和Secret Key。

Cloud OnRamp For Multicloud > Cloud Account Management > Associate Cloud Account

Provide Cloud Account Details

Cloud Provider:

Cloud Account Name:

Description (optional):

Use for Cloud Gateway: Yes No

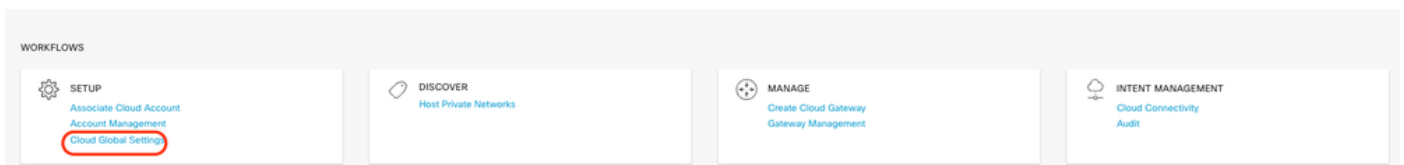
Login in to AWS with: Key IAM Role

API Key:

Secret Key:

Cancel

配置雲全局設定。點選Workflows > Setup > Cloud Global Settings。



依次按一下Add、Cloud Gateway Solution下拉選單，然後選擇Transit Gateway - VPN Base (使用TVPC)。

Cloud Global Settings Interconnect Global Settings

Cloud OnRamp For Multicloud > Cloud Global Settings

Cloud Global Settings - View

Add

Cloud Provider:

Cloud Gateway Solution:

Reference Account Name:

Reference Region:

Enable Periodic Audit: Enabled Disabled

Enable Auto Correct: Enabled Disabled

Cloud Global Settings Interconnect Global Settings

Cloud OnRamp For Multicloud > Cloud Global Settings

Cloud Global Settings - Create

Cloud Provider:

Cloud Gateway Solution:

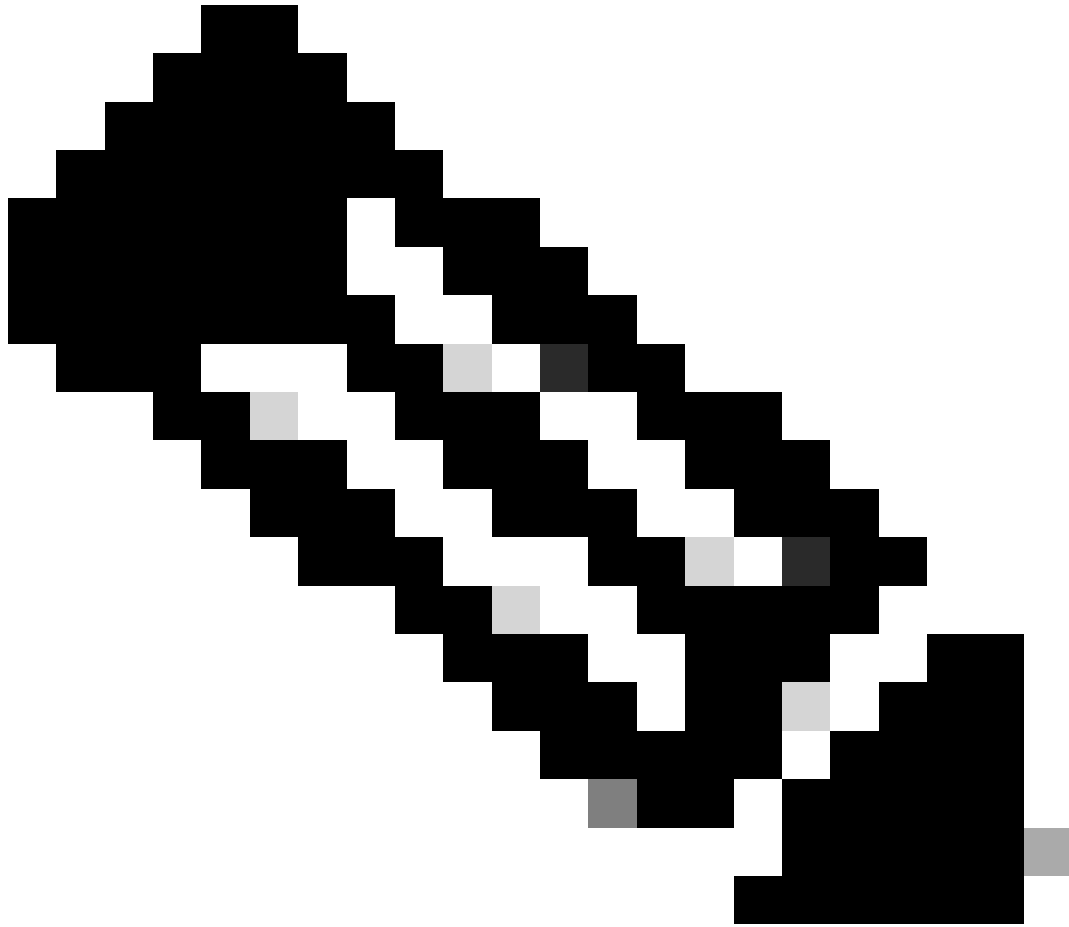
Reference Account Name:

Reference Region:

Enable Periodic Audit: Enabled Disabled

Enable Auto Correct: Enabled Disabled

- 按一下Reference Account Name的下拉選單，然後選擇帳戶。
- 按一下「參照區域」的下拉式功能表，然後從下拉式功能表中選取任何區域。
- 在軟體映像欄位中：
 - a. 點選BYOL使用自帶許可證軟體映像，或點選PAYG使用隨用隨付軟體映像。
 - b. 從下拉選單中選擇software image。
- 點選Instance Size下拉選單，然後為在傳輸VPC中運行的例項選擇大小C5n.large(2 CPU)。
- 輸入IP subnet pool x.x.x.x/24。



注意：當幾個雲網關已在使用池時，無法修改池。不允許子網重疊。

-
- 輸入Cloud Gateway BGP ASN Offset 68520。



附註：可接受的起始位移範圍是64520到65500。它必須是10的倍數。

-
- 按一下Site-to-Site Tunnel Capsulation。鍵入下拉選單，然後選擇IPSEC。
 - 您保留為預設值的其餘單選按鈕（已啟用）。

Reference Account Name

Reference Region

Software Image BYOL PAYG

Instance Size

IP Subnet Pool

Cloud Gateway BGP ASN Offset

Intra Tag Communication Enabled Disabled

Program Default Route in VPCs towards TGW Enabled Disabled

Full Mesh of Transit VPCs Enabled Disabled

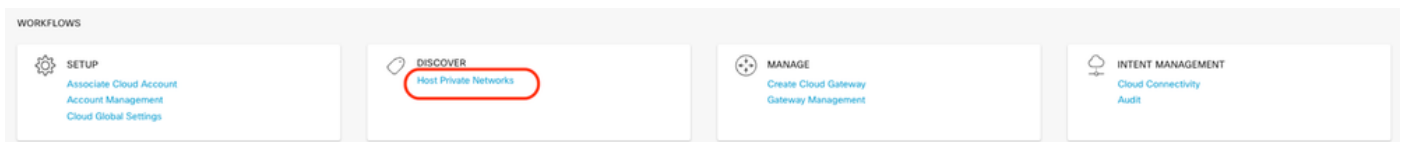
Site-to-Site Tunnel Encapsulation Type

Enable Periodic Audit Enabled Disabled

Enable Auto Correct Enabled Disabled

Cancel

接下來，您需要透過返回Cloud OnRamp For Multicloud主控制台中的Discover(發現)點選Host Private Networks (主機專用網路) 來配置主機VPC。



- 選擇連線到傳輸網關的主機VPC或VPC。
- 點選區域下拉選單根據特定區域選擇VPC。
- 按一下Tag動作以執行動作：

Add Tag -將所選VPC歸組並將它們標籤在一起。

編輯標籤- 將選定VPC從一個標籤遷移到另一個標籤。

刪除標籤- 刪除所選VPC的標籤。

多個主機VPC可以分組在一個標籤下。同一標籤下的所有VPC都被視為單一單元。標籤可確保連線，對於在意圖管理中檢視VPC至關重要。

Cloud Provider aws Amazon Web Services

Available host private networks have been discovered

Search

1 Rows Selected

Tag Actions

- Add Tag
- Edit Tag
- Delete Tag

Cloud Region	Host VPC Name	Host VPC Tag	Interconnect Enabled
<input type="checkbox"/> eu-west-2	-	-	-
<input type="checkbox"/> ap-northeast-1	-	-	-
<input checked="" type="checkbox"/> us-west-2	rtp-infrastructure	-	-
<input type="checkbox"/> ap-southeast-1	-	-	-

輸入Tag Name (標籤名稱可以是任何名稱) , 然後按一下Add。

Add New Tag

Tag Name

Region

Selected VPCs

Enable for SDCI partner Interconnect Connections (NOTE: this cannot be edited once enabled)

Cancel

VPC標籤已成功完成。


Status	Chassis Number	Message	Start Time	System IP
Success	System	Tagging HostVpc with tag: Host-VPC is completed.	18 Jul 2024 2:59:15 PM CDT	-

```
[18-Jul-2024 19:59:15 UTC] Started the tagging of HostVpc with tag: Host-VPC
[18-Jul-2024 19:59:16 UTC] Done tagging HostVpc with tag: Host-VPC. Checking if mapping is required...
[18-Jul-2024 19:59:16 UTC] Tagging HostVpc with tag: Host-VPC is completed.
```

返回到Cloud onRamp for Multicloud , 在MANAGE下按一下Create Cloud Gateway。

Cloud Interconnect Navigati

Add a cloud provider to your network



Prerequisites	Setup	Discover & Tag	Manage	Intent Management
<ol style="list-style-type: none">1. Cloud Account Details2. Cisco Wan Edge License3. Subscription to Marketplace	Associate cloud accounts for subsequent usage. Provide Global Settings	Discover and associate Tags to Host Private Networks (VPCs) for use in Intent Management	Deploy and manage Cloud Gateway(s)	Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent

WORKFLOWS

SETUP	DISCOVER	MANAGE	INTENT MANAGEMENT
Associate Cloud Account Account Management Cloud Global Settings	Host Private Networks	Create Cloud Gateway Gateway Management	Cloud Connectivity Audit

- 點選雲提供商的下拉選單，然後選擇AWS。
- 輸入雲網關名稱。
- 點選Account Name下拉選單，其中包含以前填寫的帳戶資訊。
- 點選Region下拉選單並選擇對主機VPC進行標籤的region。
- 軟體映像、例項大小和IP子網池均從之前填滿的全局雲網關中自動填充。
- 按一下UUID下拉選單。將顯示先前在裝置模板中附加的C8000v的兩個UUID。選擇這些選項，然後按一下Add。

Manage Cloud Gateway - Create

Cloud Provider: aws Amazon Web Services

Cloud Gateway Name:

Description (optional):

Account Name:

Region: us-west-2

SSH Key (optional): Choose SSH Key

Settings ⓘ

Note: * represents the settings fields that have been customized.

Software Image ⓘ BYOL PAYG

Instance Size ⓘ

IP Subnet Pool ⓘ

UUID (specify 2) ⓘ

-
-

Cancel

Add

現在雲網關開始建立，然後等待雲網關的部署成功。

Multicloud - Create Gateway

Initiated By: admin From: 72.163.2

Total Task: 1 | Success: 1

Search

Total Rows: 1

Status	Chassis Number	Message	Start Time	System IP
Success	System	Successfully created CGW: CoR-AWS	18 Jul 2024 3:06:38 PM CDT	-

```
[18-Jul-2024 20:06:38 UTC] Creating Multicloud Gateway: CoR-AWS
[18-Jul-2024 20:06:38 UTC] Creating TGW: CoR-AWS in the cloud
[18-Jul-2024 20:06:53 UTC] TGW: CoR-AWS with id: tpe-469518d85cfc68592 created successfully in the cloud
[18-Jul-2024 20:06:53 UTC] Creating VPC: CoR-AWS in the cloud
[18-Jul-2024 20:07:09 UTC] VPC vpc-08a48517790bc562b Created
[18-Jul-2024 20:07:09 UTC] Creating CSRs---this will take several minutes...
```




注意：廣域網邊緣需要幾分鐘時間才能在處理完成後到達這些邊緣。

Cloud Interconnect Navigation

Network Snapshot

Search

Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Health ...	Devices	Tunnel to Transit Gateway	VPNs ...	Tags	Host Private Networks	Cloud Provider Management Reference	Last Mapping Result
AWS	us-west-2		CoR-AWS	✓	2 reachable	--	0	0	0	NA	Successful

可以訪問AWS中部署的兩台C8000v裝置。現在，按一下Cloud Connectivity。

Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Health ...	Devices	Tunnel to Transit Gateway	VPNs ...	Tags	Host Private Networks	Cloud Provider Management Reference	Last Map	Total R
AWS	us-west-2	CALO	CoR-AWS	✔	2 reachable	--	0	0	0	NA	Success	

WORKFLOWS

- SETUP
 - Associate Cloud Account
 - Account Management
 - Cloud Global Settings
- DISCOVER
 - Host Private Networks
- MANAGE
 - Create Cloud Gateway
 - Gateway Management
- INTENT MANAGEMENT
 - Cloud Connectivity
 - Audit

按一下Edit執行VPN對映，並選擇VPN 1，然後按一下Save。

Mapping Interconnect Connectivity

Cloud OnRamp For Multicloud > Intent Management - Connectivity

Cloud Provider: AWS Amazon Web Services

Intent Management - Connectivity

Legend: Intent Not Defined, System Defined, Intent Defined, Intent Realized, Intent Realized With Errors

Filter Sort

SOURCE: DESTINATION Multi-VPN

VPN1

Host-VPN

Cancel Save

Multicloud - Connectivity Mapping

Total Task: 1 | Success: 1

Initiated By: admin

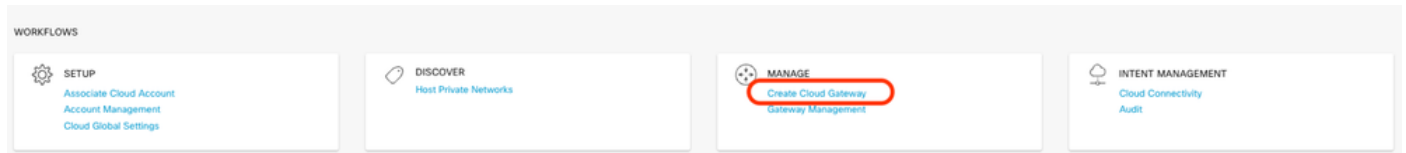
Search

Status	Chassis Number	Message	Start Time	System IP
Success	System	Mapping successful in the cloud	18 Jul 2024 3:57:42 PM CDT	-

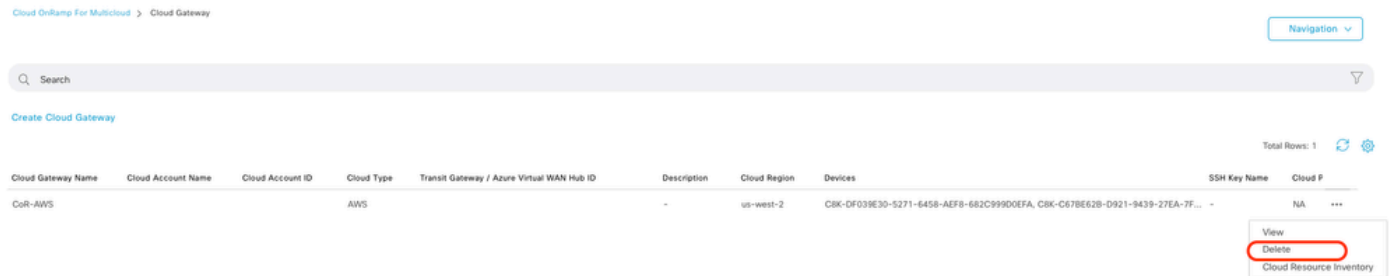
```
[18-Jul-2024 20:57:42 UTC] Started MultiCloud Connectivity Mapping for AWS
[18-Jul-2024 20:57:42 UTC] Mapping started in the cloud
[18-Jul-2024 20:57:43 UTC] Request Basic Validation Complete
[18-Jul-2024 20:57:43 UTC] Cloud State Read
[18-Jul-2024 20:57:43 UTC] Mapping Changes Identified
[18-Jul-2024 20:57:43 UTC] Applying these changes will take several minutes...
```

步驟3.如何刪除雲網關

要刪除雲網關，請在Manage下選擇Gateway Management。



然後，按一下所需雲網關上的3點(...)並按一下刪除。



驗證

本節介紹用於驗證的結果。

對映後，驗證AWS中的兩個C8000v上是否都存在VPN 1服務VPN (VRF)。

<#root>

C8kv1-aws#show ip vrf

Name	Default RD	Interfaces
1	1:1	Tu100001
		Tu100002
65528	<not set>	Lo65528
65529	<not set>	Lo65529
Mgmt-intf	1:512	Gi1

C8kv2-aws#show ip vrf

Name	Default RD	Interfaces
1	1:1	Tu100001
		Tu100002
65528	<not set>	Lo65528
65529	<not set>	Lo65529
Mgmt-intf	1:512	Gi1

您還可以看到從本地分支路由器獲取的OMP路由，以及從主機VPC獲取的BGP路由。

```
C8kv1-aws#show ip route vrf 1
```

```
Routing Table: 1
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
m 10.1.50.64/26 [251/0] via 10.1.1.231, 02:55:52, Sdwan-system-intf
B 10.2.0.0/16 [20/100] via 169.254.0.17, 02:55:22
[20/100] via 169.254.0.13, 02:55:22
m 10.2.112.192/26 [251/0] via 10.1.1.221, 02:55:52, Sdwan-system-intf
m 10.2.193.0/26 [251/0] via 10.1.1.101, 02:55:52, Sdwan-system-intf
169.254.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 169.254.0.12/30 is directly connected, Tunnel100001
L 169.254.0.14/32 is directly connected, Tunnel100001
C 169.254.0.16/30 is directly connected, Tunnel100002
L 169.254.0.18/32 is directly connected, Tunnel100002
B 172.31.0.0/16 [20/100] via 169.254.0.17, 02:55:22
[20/100] via 169.254.0.13, 02:55:22
```

```
C8kv2-aws#show ip route vrf 1
```

```
Routing Table: 1
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
m 10.1.50.64/26 [251/0] via 10.1.1.231, 02:57:17, Sdwan-system-intf
B 10.2.0.0/16 [20/100] via 169.254.0.9, 02:57:08
[20/100] via 169.254.0.5, 02:57:08
m 10.2.112.192/26 [251/0] via 10.1.1.221, 02:57:17, Sdwan-system-intf
m 10.2.193.0/26 [251/0] via 10.1.1.101, 02:57:17, Sdwan-system-intf
169.254.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 169.254.0.4/30 is directly connected, Tunnel100001
```

```
L      169.254.0.6/32 is directly connected, Tunnel100001
C      169.254.0.8/30 is directly connected, Tunnel100002
L      169.254.0.10/32 is directly connected, Tunnel100002
B      172.31.0.0/16 [20/100] via 169.254.0.9, 02:57:08
        [20/100] via 169.254.0.5, 02:57:08
```

相關資訊

[SD-WAN雲OnRamp配置指南](#)

[技術支援與文件 - Cisco Systems](#)

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）。