

# Konfiguration und Überprüfung von Cloud OnRamp für Multicloud - AWS

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Schritt 1: Anhängen der AWS-Gerätevorlage an zwei C8000v-Geräte](#)

[Schritt 2: Konfiguration der SD-WAN-Integration in AWS](#)

[Schritt 3: So entfernen Sie Cloud Gateway](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration und Überprüfung von Cisco SD-WAN Cloud OnRamp für die Multicloud-Integration mit Amazon Web Services (AWS) beschrieben.

## Voraussetzungen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- AWS Cloud-Kontodetails
- Abonnement für AWS Marketplace.
- Der Cisco SD-WAN Manager muss über zwei verfügbare Catalyst 8000V OTP-Token verfügen, um die Cloud Gateways auf der Registerkarte "Zertifikate" erstellen zu können.

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-defined Wide Area Network (SD-WAN)
- AWS

## Verwendete Komponenten

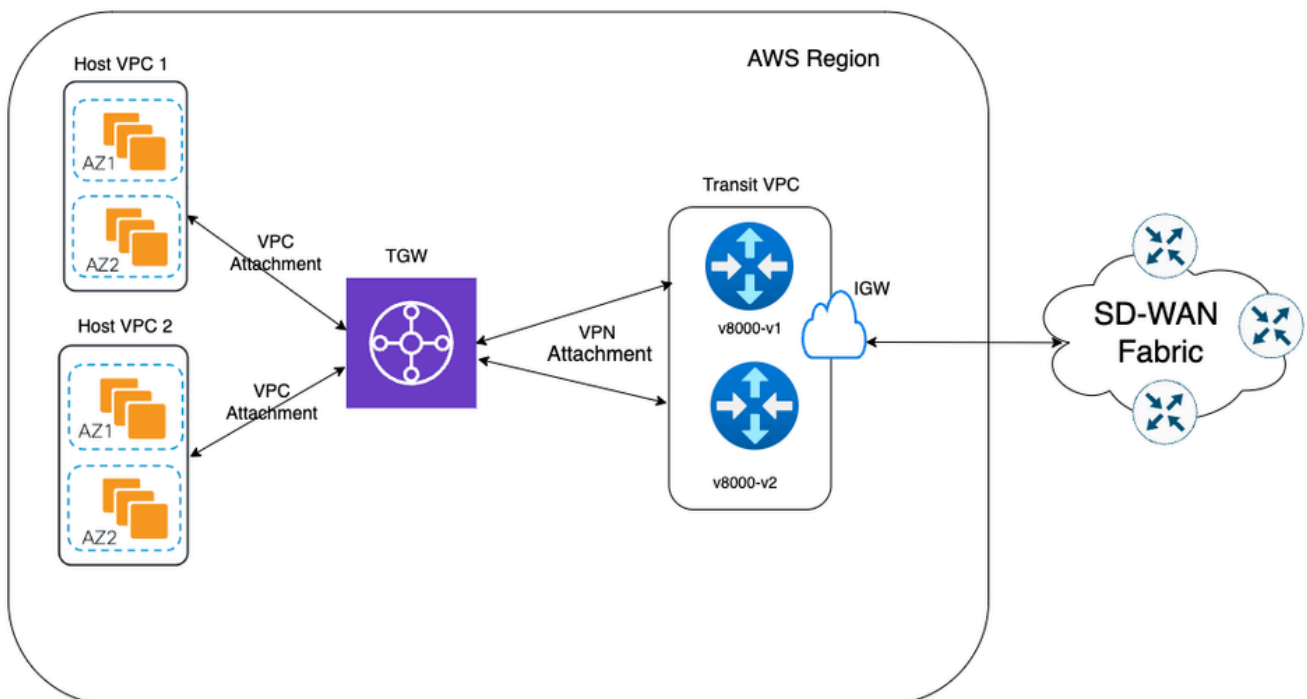
Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst SD-WAN Manager Version 20.9.4.1
- Cisco Catalyst SD-WAN Controller Version 20.9.4
- Cisco Edge Router Version 17.9.04a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

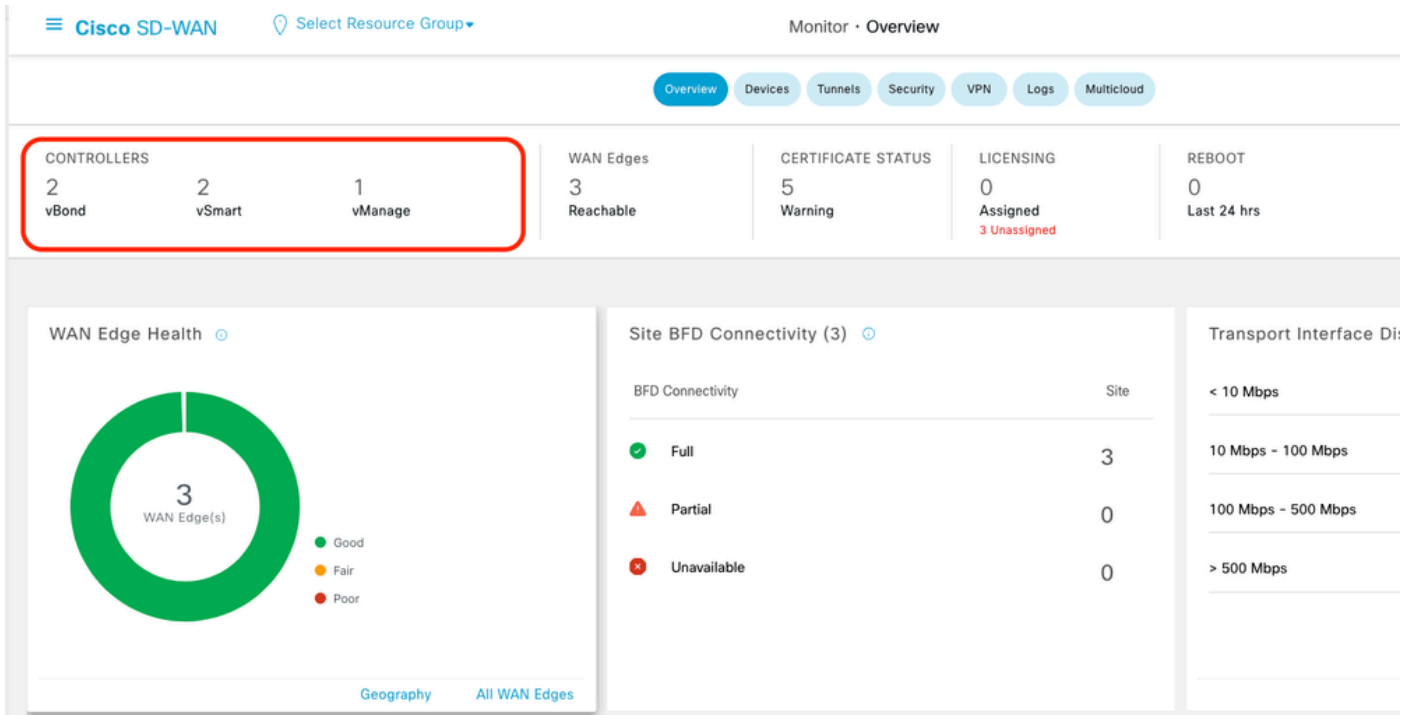
## Konfigurieren

### Netzwerkdiagramm



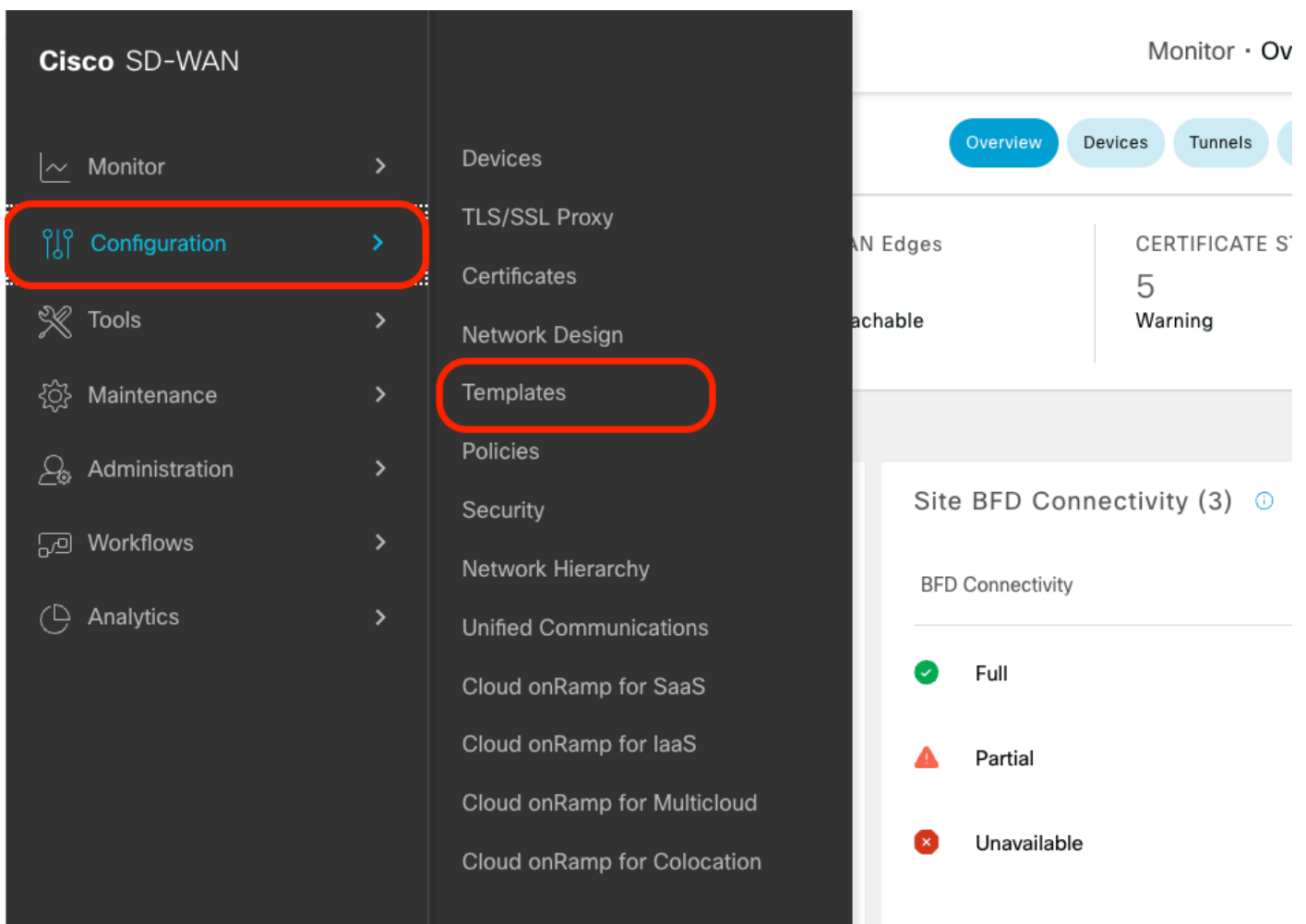
### Konfigurationen

Melden Sie sich bei der Catalyst SD-WAN Manager-GUI an, und stellen Sie sicher, dass alle Controller aktiv sind.

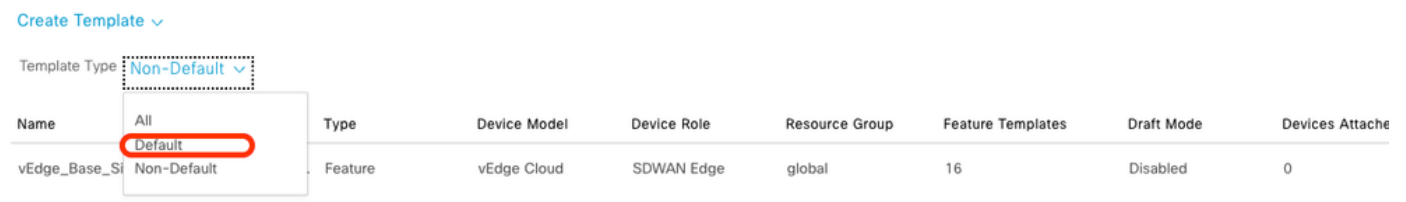


## Schritt 1: Anhängen der AWS-Gerätevorlage an zwei C8000v-Geräte

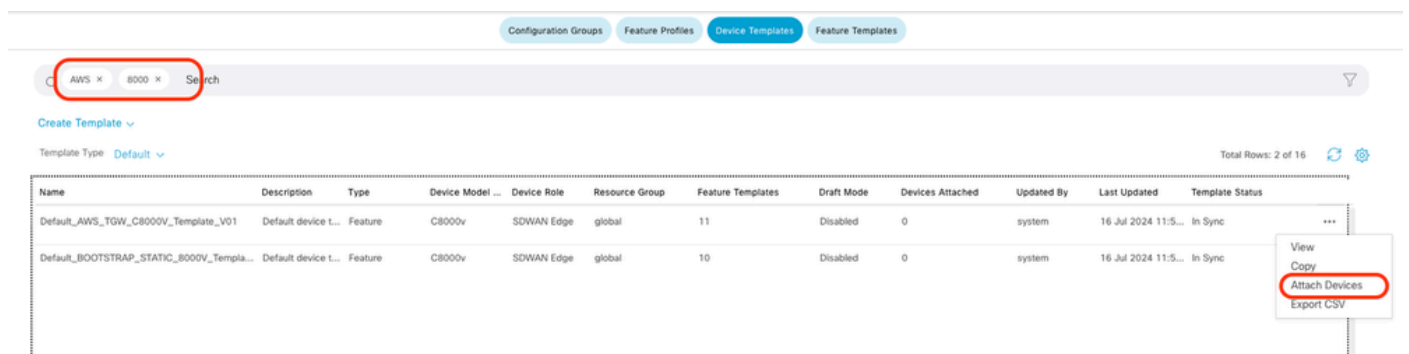
Navigieren Sie im Menü Cisco SD-WAN Manager zu Configuration > Templates (Konfiguration > Vorlagen).



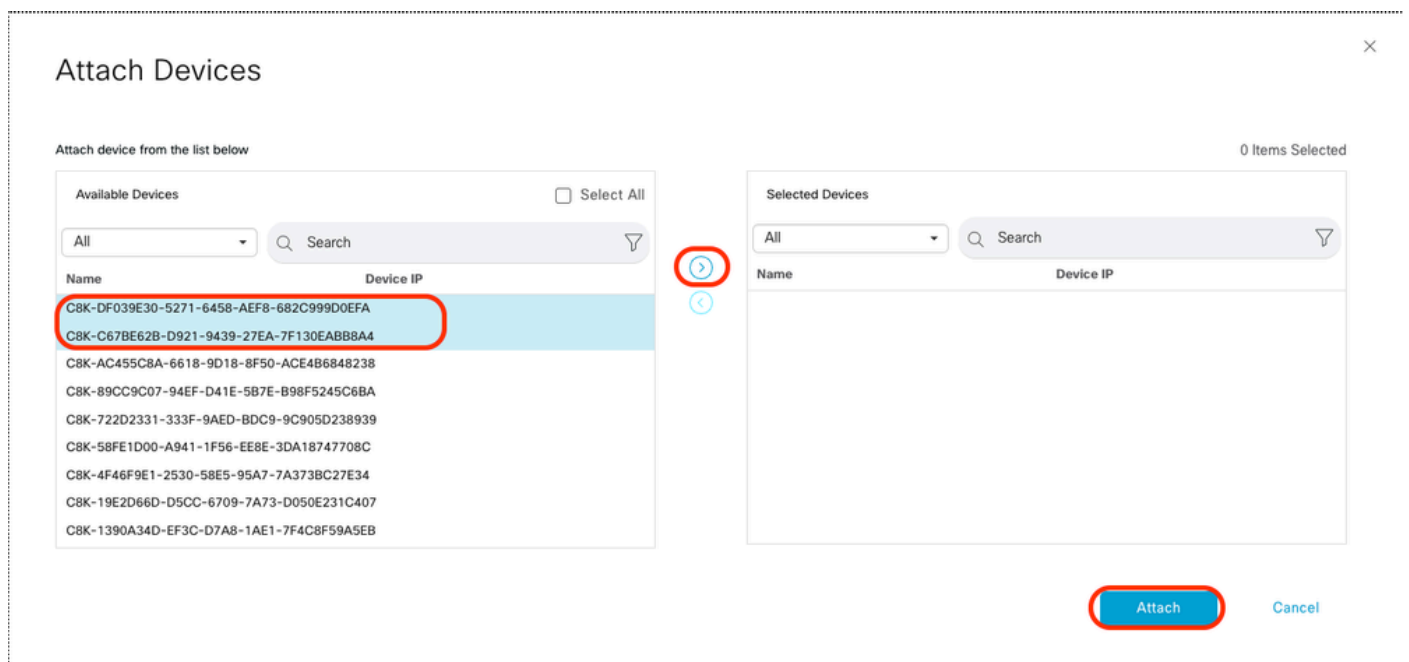
Klicken Sie auf Device Templates > From Template. Geben Sie das Dropdown-Menü ein, und wählen Sie Standard aus.



Geben Sie in die Suchleiste AWS und C8000v ein. Klicken Sie dann auf die 3 Punkte (...) neben der Vorlage Default\_AWS\_TGW\_C8000V\_Template\_V01. Wählen Sie im Dropdown-Menü die Option Geräte anhängen aus.



Wählen Sie zwei der C8000v-Geräte aus. Klicken Sie auf den nach rechts zeigenden Pfeil, und klicken Sie dann auf Anfügen.



Klicken Sie auf den Geräten auf 3 Punkte (...), und navigieren Sie zu Gerätevorlage bearbeiten.



Klicken Sie auf das Dropdown-Menü, und wählen Sie Farbe, geben Sie Hostname, System-IP und Standort-ID ein. Klicken Sie nach Eingabe dieser Details auf Aktualisieren.

Geben Sie die Werte für die einzelnen Geräte ein, und klicken Sie dann auf Aktualisieren.

Beispiel:

<#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"/>

Wenn Sie beide Geräte beendet haben, klicken Sie auf Weiter.

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

Klicken Sie auf eines der Geräte, und stellen Sie sicher, dass die Konfiguration korrekt ist. Klicken Sie auf Geräte konfigurieren.

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-sha1-hmac sha1-hmac
integrity-type ip-udp-esp esp
```

Back Configure Devices Cancel

Aktivieren Sie im Pop-up-Fenster das Kontrollkästchen Konfigurationsänderungen auf zwei Geräten bestätigen, und klicken Sie dann auf OK.

## 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

Bestätigen Sie, dass die Vorlagen für das Anschließen an die Geräte geplant wurden.

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_TGM_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_TGM_C8000V_Template_V01 scheduled to be attached when device comes online. To check the synced state, click Configuration &gt; Devices &gt; Device Options </pre>	C8000v	C8000v		-	-	

## Schritt 2: Konfiguration der SD-WAN-Integration in AWS

Sie können Cloud onRamp für Umgebungen mit mehreren Clouds über den Cisco Catalyst SD-WAN Manager konfigurieren und verwalten.

Ein Konfigurationsassistent im Cisco Catalyst SD-WAN Manager automatisiert das Hochfahren des Transit-Gateways zu Ihrem Public Cloud-Konto und die Verbindungen zwischen Public Cloud-Anwendungen und den Benutzern dieser Anwendungen in Zweigstellen im Overlay-Netzwerk. Diese Funktion ist mit AWS Virtual Private Clouds (VPCs) auf Cisco Cloud-Routern kompatibel.

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, über den Sie Ihre VPC und Ihre lokalen Netzwerke miteinander verbinden können. Sie können eine vPC- oder eine VPN-Verbindung mit einem Transit-Gateway verbinden. Er fungiert als virtueller Router für den Datenverkehr, der zwischen Ihren VPC- und VPN-Verbindungen übertragen wird.

Cloud OnRamp für Multicloud unterstützt die Integration mit mehreren AWS-Konten.

AWS Cloud-Konto erstellen

Navigieren Sie zu Configuration > Cloud onRamp for Multicloud.



Cisco SD-WAN

- Monitor >
- Configuration >**
- Tools >
- Maintenance >
- Administration >
- Workflows >
- Analytics >

- Devices
- TLS/SSL Proxy
- Certificates
- Network Design
- Templates**
- Policies
- Security**
- Network Hierarchy
- Unified Communications
- Cloud onRamp for SaaS
- Cloud onRamp for IaaS
- Cloud onRamp for Multicloud**
- Cloud onRamp for Colocation

Device Model	Hostname	Sys
B-D921-9439-27...		-
t_AWS_TGW_C8000V_Template_V01		
0-5271-6458-AEF...		-
t_AWS_TGW_C8000V_Template_V01		

Klicken Sie unter Workflows > Setup auf Associate Cloud Account.

Cloud Interconnect

### Add a cloud provider to your network

**Prerequisites**

- Cloud Account Details
- Cisco Wan Edge License
- Subscription to Marketplace

**Setup**  
Associate cloud accounts for subsequent usage. Provide Global Settings

**Discover & Tag**  
Discover and associate Tags to Host Private Networks (VPCs) for use in Intent Management

**Manage**  
Deploy and manage Cloud Gateway(s)

**Intent Management**  
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent

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

- Wählen Sie im Feld "Cloud Provider" in der Dropdown-Liste die Option Amazon Web Services aus.
- Geben Sie den Kontonamen in das Feld Cloud-Kontoname ein.
- Wählen Sie Ja aus, um Cloud Gateway zu erstellen.
- Wählen Sie das Authentifizierungsmodell aus, das Sie im Feld Bei AWS anmelden mit verwenden möchten.
  - Wichtigste
  - IAM-Rolle

Wenn Sie das Schlüsselmodell auswählen, geben Sie API-Schlüssel und geheimen Schlüssel in

den entsprechenden Feldern ein.

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

Add

Globale Cloud-Einstellungen konfigurieren Klicken Sie auf Workflows > Setup > Cloud Global Settings.

WORKFLOWS

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

Klicken Sie auf Hinzufügen, klicken Sie auf das Dropdown-Menü für Cloud Gateway Solution, und wählen Sie dann Transit Gateway - VPN Base (über TVPC) aus.

Cloud Global Settings

Interconnect Global Settings

Cloud OnRamp For Multicloud > Cloud Global Settings

#### Cloud Global Settings - View

Cloud Provider

Cloud Gateway Solution

Reference Account Name

Reference Region

Enable Periodic Audit  Enabled  Disabled

Enable Auto Correct  Enabled  Disabled

Add

Cloud OnRamp For Multicloud &gt; 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

- Klicken Sie auf das Dropdown-Menü für Referenzkontoname, und wählen Sie das Konto aus.
- Klicken Sie auf das Dropdown-Menü für Referenzregion, und wählen Sie eine Region aus dem Dropdown-Menü aus.
- Im Software-Imagefeld:
  - a. Klicken Sie auf BYOL, um ein eigenes Lizenz-Software-Image zu verwenden, oder auf PAYG, um ein nutzungsabhängiges Software-Image zu verwenden.
  - b. Wählen Sie aus der Dropdown-Liste ein Software-Image aus.
- Klicken Sie auf das Dropdown-Menü Instance Size (Instanzgröße), und wählen Sie dann die Größe C5n.large (2 CPU) für die Instanzen aus, die in Transit VPC ausgeführt werden.
- Geben Sie den IP-Subnetz-Pool x.x.x.x/24 ein.



Hinweis: Sie können den Pool nicht ändern, wenn dieser bereits von einigen wenigen Cloud-Gateways genutzt wird. Das Überlappen von Subnetzen ist nicht zulässig.

- 
- Geben Sie den Cloud Gateway BGP ASN Offset 68520 ein.



Hinweis: Der zulässige Startoffset liegt zwischen 64520 und 65500. Es muss ein Vielfaches von 10 sein.

- 
- Klicken Sie auf Site-to-Site Tunnel Encapsulation. Geben Sie Dropdown-Menü ein, und wählen Sie dann IPSEC aus.
  - Die übrigen Optionsfelder, die Sie als Standard beibehalten, sind aktiviert.

Reference Account Name

Reference Region

Software Image  BYDL  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

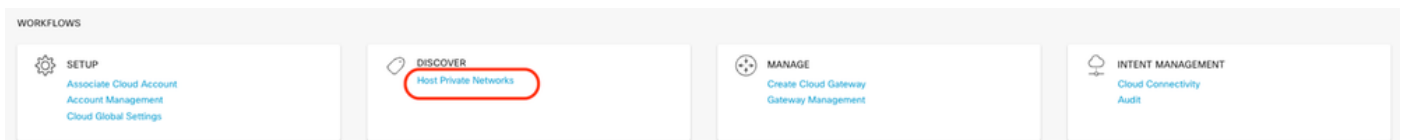
Site-to-Site Tunnel Encapsulation Type

Enable Periodic Audit  Enabled  Disabled

Enable Auto Correct  Enabled  Disabled

Cancel

Als Nächstes müssen Sie Host-VPCs konfigurieren, indem Sie zum Haupt-Dashboard Cloud OnRamp For Multicloud zurückkehren und unter Erkennen auf Host Private Networks klicken.



- Wählen Sie die Host-VPCs oder VPCs aus, die an das Transit-Gateway angeschlossen werden sollen.
- Klicken Sie auf die Dropdown-Liste Region, um die vPCs basierend auf der jeweiligen Region auszuwählen.
- Klicken Sie auf Tag-Aktionen, um folgende Aktionen auszuführen:

Tag hinzufügen: Gruppieren Sie die ausgewählten vPCs, und markieren Sie sie.

Tag bearbeiten: Migration der ausgewählten vPCs von einem Tag zu einem anderen.

Tag löschen: Der Tag für die ausgewählten VPCs wird entfernt.

Mehrere Host-VPCs können unter einem Tag gruppiert werden. Alle vPCs mit demselben Tag gelten als eine Einheit. Ein Tag stellt die Verbindung sicher und ist für die Anzeige der vPCs in Intent Management erforderlich.

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	-	-	-

Geben Sie einen Tag-Namen ein (der Tag-Name kann beliebig sein), und klicken Sie dann auf Hinzufügen.

Add New Tag

Tag Name

Region

Selected VPCs

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

Cancel

VPC-Tagging erfolgreich abgeschlossen.

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.
```

Kehren Sie zu Cloud onRamp for Multicloud zurück, und klicken Sie unter MANAGE auf Create Cloud Gateway (Cloud-Gateway erstellen).

Cloud Interconnect Navigation

### Add a cloud provider to your network

Prerequisites	Setup	Discover & Tag	Manage	Intent Management
1. Cloud Account Details 2. Cisco Wan Edge License 3. 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**

- Associate Cloud Account
- Account Management
- Cloud Global Settings

**DISCOVER**

- Host Private Networks

**MANAGE**

- Create Cloud Gateway
- Gateway Management

**INTENT MANAGEMENT**

- Cloud Connectivity
- Audit

- Klicken Sie auf das Dropdown-Menü für Cloud Provider, und wählen Sie AWS aus.
- Geben Sie einen Namen für das Cloud-Gateway ein.
- Klicken Sie auf das Dropdown-Menü Kontoname. Es enthält die zuvor eingegebenen Konteninformationen.
- Klicken Sie auf das Dropdown-Menü Region, und wählen Sie die Region aus, in der die Host-VPCs markiert wurden.
- Software-Image, Instanzgröße und IP-Subnetz-Pool werden automatisch aus dem zuvor gefüllten Global Cloud Gateway übernommen.
- Klicken Sie auf das Dropdown-Menü UUID (UUID). Es werden die beiden UUIDs für den C8000v angezeigt, die zuvor mit der Gerätevorlage verknüpft waren. Wählen Sie sie aus, und klicken Sie dann auf Hinzufügen.



### 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

Nun beginnen die Cloud-Gateways mit der Erstellung und warten, bis die Bereitstellung des Cloud Gateway erfolgreich abgeschlossen wurde.

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 TOM: CoR-AWS in the cloud
[18-Jul-2024 20:06:53 UTC] TOM: CoR-AWS with id: tpu=8695186856cf68592 created successfully in the cloud
[18-Jul-2024 20:06:53 UTC] Creating TVPC: CoR-AWS in the cloud
[18-Jul-2024 20:07:09 UTC] VPC vpc-88a485177940c562b Created
[18-Jul-2024 20:07:09 UTC] Creating CGW--this will take several minutes...
... ..
```



Hinweis: WAN-Edges sind nach Abschluss des Vorgangs in wenigen Minuten erreichbar.

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		ColR-AWS	✓	2 reachable	--	0	0	0	NA	Successful

Zwei in AWS bereitgestellte C8000v-Geräte sind erreichbar. Klicken Sie nun auf 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
AWS	us-west-2	CALO	Cor-AWS	<span style="color: green;">✔</span>	<span style="color: green;">✔</span> 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

Klicken Sie auf Bearbeiten, um die VPN-Zuordnung durchzuführen, und wählen Sie VPN 1 aus, und klicken Sie dann auf Speichern.

Mapping Interconnect Connectivity

Cloud OnRamp For Multicloud > Intent Management - Connectivity Navigation ▾

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: EXTENSION Hub-VPC

VPN1: 1

Host-VPC: -

Cancel Save

Multicloud - Connectivity Mapping Initiated By: admin

Total Task: 1 | Success: 1

Search

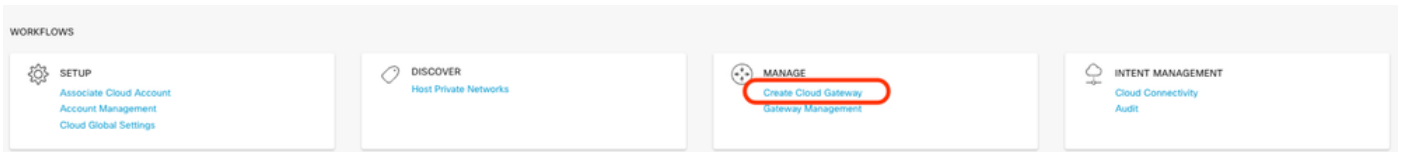
Status	Chassis Number	Message	Start Time	System IP
<span style="color: green;">✔</span> Success	System	Mapping successful in the cloud	18 Jul 2024 3:57:42 PM CDT	-

```

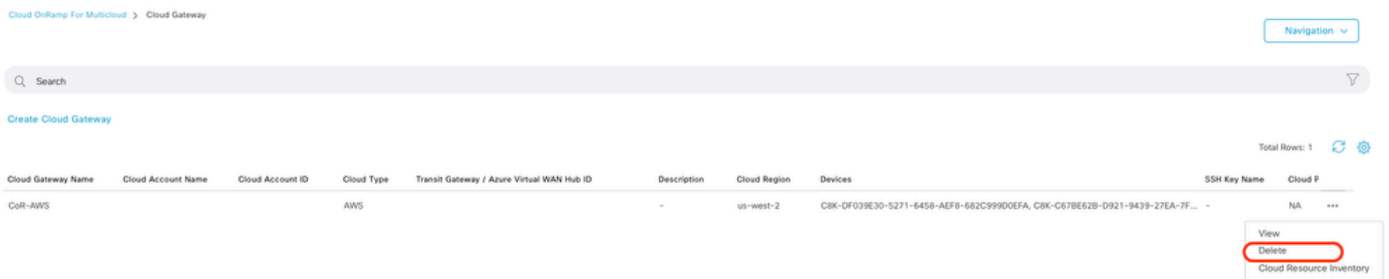
[18-Jul-2024 20:57:42 UTC] Started MultiCloud Connectivity Mapping for AWS
[18-Jul-2024 20:57:42 UTC] Mapping started in the cloud
[18-Jul-2024 20:57:43 UTC] Request Basic Validation Complete
[18-Jul-2024 20:57:43 UTC] Cloud State Read
[18-Jul-2024 20:57:43 UTC] Mapping Changes Identified
[18-Jul-2024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

## Schritt 3: Entfernen des Cloud Gateway

Um das Cloud Gateway zu löschen, wählen Sie unter Verwalten die Option Gateway-Verwaltung aus.



Klicken Sie dann auf die 3 Punkte (...) auf dem gewünschten Cloud-Gateway und klicken Sie auf Löschen.



## Überprüfung

In diesem Abschnitt werden die Ergebnisse für Überprüfungszwecke beschrieben.

Überprüfen Sie nach der Zuordnung, ob das VPN 1-Service-VPN (VRF) auf beiden C8000v in AWS vorhanden ist.

<#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

65528	<not set>	Lo65528
65529	<not set>	Lo65529
Mgmt-intf	1:512	Gi1

Außerdem werden die vom Router in der Zweigstelle vor Ort übernommenen OMP-Routen sowie die BGP-Routen von den Host-VPCs angezeigt.

```
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
```

## Zugehörige Informationen

[SD-WAN Cloud OnRamp - Konfigurationsleitfaden](#)

[Technischer Support und Dokumentation für Cisco Systeme](#)

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.