CSR1000v HA Version 3 auf AWS, Azure und GCP konfigurieren

Inhalt

Einführung

Dieses Dokument beschreibt die Schritte zur Konfiguration von CSR1000v-Routern für HAv3 (High Availability Version 3) auf Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP).

Voraussetzungen

Anforderungen

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

- AWS-, Azure- oder GCP-Clouds.
- CSR1000v-Router.
- Cisco IOS®-XE

In diesem Artikel wird davon ausgegangen, dass die zugrunde liegende Netzwerkkonfiguration bereits abgeschlossen wurde und sich auf die HAv3-Konfiguration konzentriert.

Die vollständigen Konfigurationsdetails finden Sie im Cisco CSR 1000v- und Cisco ISRv-Software-Konfigurationsleitfaden.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Ein AWS-, Azure- oder GCP-Konto.
- 2 CSR1000v-Router.
- Mindestens Cisco IOS®-XE Polaris 16.11.1s

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 potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco empfiehlt, dass Sie über Kenntnisse der verschiedenen verfügbaren HA-Versionen verfügen:

- HAv1: Die HA-Konfiguration wird als IOS-Befehle durchgeführt und beruht auf BFD als Mechanismus zur Fehlererkennung.
- HAv2/HAv3: Die Implementierung wurde als Python-Skripte in den guestshell-Container verschoben. BFD ist optional, und benutzerdefinierte Skripts können geschrieben werden, um Fehler zu erkennen und ein Failover auszulösen. Die Azure HAv2-Konfiguration ähnelt weitgehend der HAv3-Konfiguration, wobei geringfügige Unterschiede bei den Pip-Installationspaketen und der IOS-Redundanzkonfiguration bestehen.
- HAv3: Die HA-Implementierung wurde größtenteils aus dem Cisco IOS®-XE-Code entfernt und wird im guestshell-Container ausgeführt.

HAv3 ist von Cisco IOS®-XE Polaris 16.11.1s erhältlich und bietet eine Reihe neuer Funktionen:

- **Cloud-unabhängig:** Diese Version der Hochverfügbarkeit funktioniert auf CSR 1000v-Routern aller Cloud-Service-Provider. Die Cloud-Terminologie und -Parameter unterscheiden sich in der Regel, aber die Funktionen und Skripte zur Konfiguration, Kontrolle und Darstellung der Hochverfügbarkeitsfunktionen sind bei den verschiedenen Cloud-Service-Providern üblich. Die hochverfügbare Version 3 (HAv3) wird von CSR 1000v-Routern auf AWS, Azure und GCP unterstützt. Unterstützung für den GCP-Anbieter wurde in 16.11.1 hinzugefügt. Wenden Sie sich an Cisco, um aktuelle Informationen zur Hochverfügbarkeit in den Clouds der einzelnen Anbieter zu erhalten.
- **Aktiv/Aktiv Betrieb:** Sie können beide Cisco CSR 1000v-Router so konfigurieren, dass sie gleichzeitig aktiv sind, was eine Lastverteilung ermöglicht. In diesem Betriebsmodus hat jede Route in einer Routing-Tabelle einen der beiden Router, der als primärer Router und der andere Router als sekundärer Router dient. Um die Lastverteilung zu aktivieren, trennen Sie alle Routen von den beiden Cisco CSR 1000v-Routern. Beachten Sie, dass diese Funktion für AWS-basierte Clouds neu ist.
- **Umleitung auf primären CSR nach Fehlerwiederherstellung:** Sie können einen Cisco CSR 1000v als primären Router für eine bestimmte Route festlegen. Dieser Cisco CSR 1000v ist aktiv. es ist der nächste Hop für die Route. Wenn dieser Cisco CSR 1000v ausfällt, übernimmt der Peer-Cisco CSR 1000v den nächsten Hop für die Route, wobei die Netzwerkverbindung erhalten bleibt. Wenn der ursprüngliche Router nach dem Ausfall wiederhergestellt wird, übernimmt er den Besitz der Route und ist der nächste Hop-Router. Diese Funktion ist auch für AWS-basierte Clouds neu.

- **Vom Benutzer bereitgestellte Skripts:** Die guestshell ist ein Container, in dem Sie eigene Skripte bereitstellen können. HAv3 macht eine Programmierschnittstelle für vom Benutzer bereitgestellte Skripts verfügbar. Dies bedeutet, dass Sie nun Skripts schreiben können, die sowohl Failover- als auch Reversion-Ereignisse auslösen können. Sie können auch eigene Algorithmen und Trigger entwickeln, um zu steuern, welcher Cisco CSR 1000v die Weiterleitungsservices für eine bestimmte Route bereitstellt. Diese Funktion ist neu für AWS-basierte Clouds.
- **Neue Konfigurations- und Bereitstellungsmechanismen:** Die Implementierung von HA wurde aus dem Cisco IOS®-XE-Code entfernt. Der Hochverfügbarkeitscode wird nun im guestshell-Container ausgeführt. Weitere Informationen zu guestshell finden Sie im Abschnitt "Guest Shell" im Konfigurationsleitfaden zur Programmierbarkeit. In HAv3 wird die Konfiguration von Redundanzknoten in der Gästeschale durchgeführt, die eine Reihe von Python-Skripts verwendet. Diese Funktion wurde nun für AWS-basierte Clouds eingeführt.

  Hinweis: Für Ressourcen, die in AWS, Azure oder GCP bereitgestellt werden, können in diesem Dokument Kosten anfallen.

Topologie

Vor Beginn der Konfiguration ist es wichtig, die Topologie und das Design vollständig zu verstehen. So können potenzielle Probleme später behoben werden.

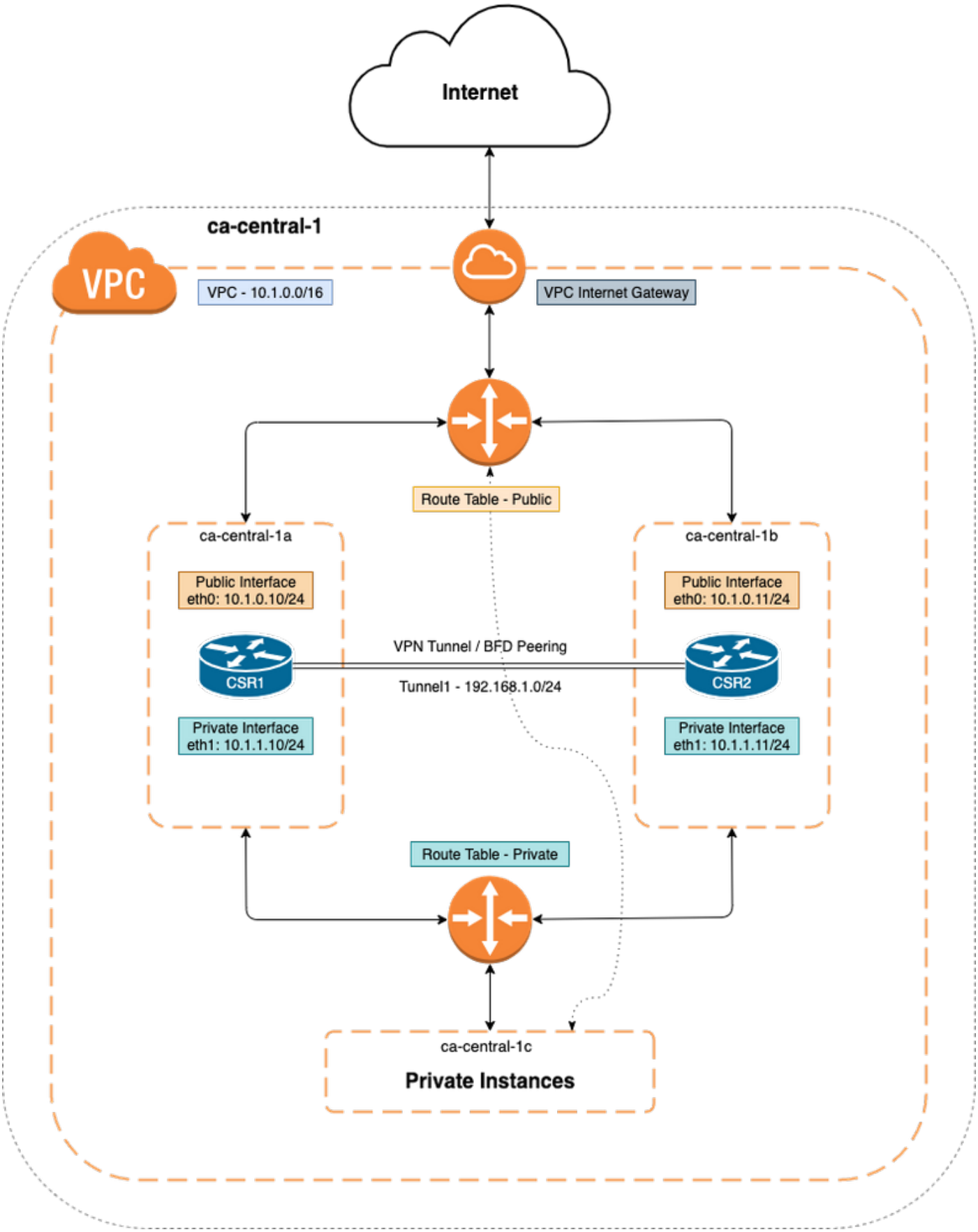
Obwohl das Netzwerktopologiediagramm auf AWS basiert, ist die zugrunde liegende Netzwerkbereitstellung zwischen Clouds relativ ähnlich. Die Netzwerktopologie ist auch unabhängig von der verwendeten HA-Version, egal ob es sich um HAv1, HAv2 oder HAv3 handelt.

Für dieses Topologiemanagement wird die HA-Redundanz mit den folgenden Einstellungen in AWS konfiguriert:

- 1x - Region
- 1x - VPC
- 3x - Verfügbarkeitszonen
- 4x - Netzwerkschnittstellen/Subnetze (2x öffentliche/2x private Ausrichtung)
- 2x - Routentabellen (öffentlich und privat)
- 2x - CSR1000v-Router (Cisco IOS®-XE 17.01.01)

Es gibt zwei CSR1000v-Router in einem HA-Paar in zwei verschiedenen Verfügbarkeitszonen. Die dritte Zone ist eine private Instanz, die ein Gerät in einem privaten Rechenzentrum simuliert. Im Allgemeinen muss der gesamte normale Datenverkehr die private (oder interne) Routing-Tabelle durchlaufen.

Netzwerkdiagramm



Netzwerkdiagramm

CSR1000v-Router konfigurieren

Cloud-unabhängige Konfiguration

Schritt 1: Konfigurieren von IOX-Anwendungshosting und guestshell, um die IP-Erreichbarkeit in guestshell zu ermöglichen Dieser Schritt kann standardmäßig automatisch konfiguriert werden, wenn CSR1000v bereitgestellt wird.

vrf definition GS ! iox app-hosting appid guestshell app-vnic gateway1 virtualportgroup 0 guest-interface 0 guest-ipaddress 192.168.35.102 netmask 255.255.255.0 app-default-gateway 192.168.35.101 guest-interface 0 name-server0 8.8.8.8 ! interface VirtualPortGroup0 vrf forwarding GS ip address 192.168.35.101 255.255.255.0 ip nat inside ! interface GigabitEthernet1 ip nat outside ! ip access-list standard GS_NAT_ACL permit 192.168.35.0 0.0.0.255 ! ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 vrf GS overload ! ! The static route points to the G1 ip address's gateway ip route vrf GS 0.0.0.0 0.0.0.0 GigabitEthernet1 10.1.0.1 global

Schritt 2: Aktivieren und Anmelden bei guestshell

```
Device#guestshell enable
Interface will be selected if configured in app-hosting
Please wait for completion
guestshell installed successfully
Current state is: DEPLOYED
guestshell activated successfully
Current state is: ACTIVATED
guestshell started successfully
Current state is: RUNNING
Guestshell enabled successfully

Device#guestshell
[guestshell@guestshell ~]$
```

> **Hinweis:** Weitere Informationen zu guestshell finden Sie unter - Konfigurationsleitfaden zur Programmierbarkeit

Schritt 3: Bestätigen Sie, dass Guestshell mit dem Internet kommunizieren kann.

```
[guestshell@guestshell ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=109 time=1.74 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=109 time=2.19 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=109 time=2.49 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=109 time=1.41 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=109 time=3.04 ms
```

Schritt 4: (Optional) Aktivieren Sie BFD (Bi-directional Forwarding Detection) und ein Routing-Protokoll als EIGRP (Enhanced Interior Gateway Routing Protocol) oder Border Gateway Protocol (BGP) für den Tunnel, um Fehler zu erkennen. Konfigurieren Sie entweder einen VxLAN- oder IPsec-Tunnel zwischen den Cisco CSR 1000v-Routern.

- IPsec-Tunnel zwischen den Cisco CSR 1000v-Routern.

crypto isakmp policy 1 encr aes 256 authentication pre-share crypto isakmp key cisco address crypto ipsec transform-set uni-perf esp-aes 256 esp-sha-hmac mode tunnel crypto ipsec profile vti-1 set security-association lifetime kilobytes disable set security-association lifetime seconds 86400 set transform-set uni-perf set pfs group2 interface Tunnel1 ip address 192.168.1.1 255.255.255.0 bfd interval 500 min_rx 500 multiplier 3 tunnel source GigabitEthernet1 tunnel destination redundancy cloud-ha bfd peer Example - #CSR1 ! interface Tunnel1 ip address 192.168.1.1 255.255.255.0 bfd interval 500 min_rx 500 multiplier 3 tunnel source GigabitEthernet1 tunnel destination 10.1.0.11 ! redundancy cloud-ha bfd peer 192.168.1.2 #CSR2 ! interface Tunnel1 ip address 192.168.1.2 255.255.255.0 bfd interval 500 min_rx 500 multiplier 3 tunnel source GigabitEthernet1 tunnel destination 10.1.0.10 ! redundancy cloud-ha bfd peer 192.168.1.1

- VxLAN-Tunnel zwischen den Cisco CSR 1000v-Routern.

Example: interface Tunnel100 ip address 192.168.1.1 255.255.255.0 bfd interval 500 min_rx 500 multiplier 3 tunnel source GigabitEthernet1 tunnel mode vxlan-gpe ipv4 tunnel destination tunnel vxlan vni 10000 redundancy cloud-ha bfd peer

Schritt 4.1: (Optional) Konfigurieren Sie EIGRP über Tunnelschnittstellen.

router eigrp 1 bfd interface Tunnel1 network 192.168.1.0 0.0.0.255

- Benutzerdefinierte Skripts können zum Auslösen von Failover verwendet werden, z. B.:

event manager applet Interface_GigabitEthernet2 event syslog pattern “Interface GigabitEthernet2, changed state to administratively down” action 1 cli command “enable” action 2 cli command “guestshell run node_event.py -i 10 -e peerFail” exit exit

AWS-spezifische Konfiguration

- AWS HA-Parameter

Parameter	Switch	Description
Node Index	-i	Index that is used to uniquely identify this node. Valid values: 1-1023.
Region Name	-rg	Name of the region that contains the route table. For example, us-west-2.
Route Table Name	-t	Name of the route table to be updated. The name of the route table must begin with the substring rtb-. For example, rtb-001333c29ef2aec5f
Route	-r	If a route is unspecified, then the redundancy node is considered to apply to all routes in the routing table. The CSR cannot change routes which are of type local or gateway.
Next Hop Interface	-n	Name of the interface to which packets should be forwarded in order to reach the destination route. The name of the interface must begin with the substring eni-. For example, eni-07160c7e740ac8ef4.
Mode	-m	Indicates whether this router is the primary or secondary router for servicing this route. Valid values are primary or secondary. This is an optional parameter. The default value is secondary.

Schritt 1: Konfigurieren Sie die Authentifizierung mit IAM.

Damit der CSR1000v-Router eine Routing-Tabelle im AWS-Netzwerk aktualisieren kann, muss der Router authentifiziert werden. In AWS müssen Sie eine Richtlinie erstellen, die dem CSR 1000v-Router den Zugriff auf die Routing-Tabelle ermöglicht. Anschließend wird eine IAM-Rolle erstellt, die diese Richtlinie verwendet und auf die EC2-Ressource angewendet wird.

Nachdem die CSR 1000v EC2-Instanzen erstellt wurden, muss die erstellte IAM-Rolle jedem Router zugewiesen werden.

Die in der neuen IAM-Rolle verwendete Richtlinie lautet:

{ "Version": "2012-10-17", "Statement": [{ "Sid": "VisualEditor0", "Effect": "Allow", "Action": ["logs:CreateLogStream", "cloudwatch:", "s3:", "ec2:AssociateRouteTable", "ec2:CreateRoute", "ec2:CreateRouteTable", "ec2:DeleteRoute", "ec2:DeleteRouteTable", "ec2:DescribeRouteTables", "ec2:DescribeVpcs", "ec2:ReplaceRoute", "ec2:DescribeRegions", "ec2:DescribeNetworkInterfaces", "ec2:DisassociateRouteTable", "ec2:ReplaceRouteTableAssociation", "logs:CreateLogGroup", "logs:PutLogEvents"], "Resource": "*" }] }

Hinweis: Detaillierte Schritte finden Sie unter IAM-Rolle mit einer Richtlinie und ordnen sie dem VPC zu.

Schritt 2: Installieren Sie das HA python-Paket.

```
[guestshell@guestshell ~]$ pip install csr_aws_ha --user
[guestshell@guestshell ~]$ source ~/.bashrc
```

Schritt 3: Konfigurieren Sie die HA-Parameter auf dem primären Router.

```
[guestshell@guestshell ~]$ create_node.py -i 10 -t rtb-01c5b0633a3422575 -rg ca-central-1 -n eni-0bc1912748614df2a -r 0.0.0.0/0 -m primary
```

Schritt 4: Konfigurieren Sie die HA-Parameter auf dem sekundären Router.

```
[guestshell@guestshell ~]$ create_node.py -i 10 -t rtb-01c5b0633a3422575 -rg ca-central-1 -n eni-0e351ab1b8f416728 -r 0.0.0.0/0 -m secondary
```

- Das Knotenformat ist:

```
create_node.py -i n -t rtb-private-route-table-id -rg region-id -n eni-CSR-id -r route(x.x.x.x/x) -m
```

Azure-spezifische Konfiguration

- Azure HA-Parameter

The following table specifies the redundancy parameters that are specific to Microsoft Azure:

Parameter Switch	Switch	Description
Node Index	-i	The index that is used to uniquely identify this node. Valid values: 1–255.
Cloud Provider	-p	Specifies the type of Azure cloud: azure, azusgov, or azchina.
Subscription ID	-s	The Azure subscription id.
Resource Group Name	-g	The name of the route table to be updated.
Route Table Name	-t	The name of the route table to be updated.
Route	-r	IP address of the route to be updated in CIDR format. Can be IPv4 or IPv6 address. If a route is unspecified, then the redundancy node is considered to apply to all routes in the routing table of type “virtual appliance”.
Next Hop Address	-n	The IP address of the next hop router. Use the IP address that is assigned to this CSR 1000v on the subnet which utilizes this route table. Can be an IPv4 or IPv6 address.
Mode	-m	Indicates whether this router is the primary or secondary router for servicing this route. Default value is secondary.

Hinweis: Die nach außen gerichtete Schnittstelle muss auf GigabitEthernet1 konfiguriert werden. Diese Schnittstelle wird zum Erreichen der Azure APIs verwendet. HA kann ansonsten nicht ordnungsgemäß funktionieren. Stellen Sie sicher, dass der curl-Befehl Metadaten aus Azure abrufen kann.

```
[guestshell@guestshell ~]$ curl -H "Metadata:true" http://169.254.169.254/metadata/instance?api-version=2020-06-01
```

Schritt 1: Die Authentifizierung für CSR1000v-API-Anrufe muss entweder mit Azure Active Directory (AAD) oder mit Managed Service Identity (MSI) aktiviert werden. Ausführliche Schritte finden Sie unter Konfigurieren der Authentifizierung für CSR1000v-API-Aufrufe. Ohne diesen

Schritt kann der CSR1000v-Router nicht autorisiert werden, die Routing-Tabelle zu aktualisieren.

AD-Parameter

Parameter Name	Switch	Description
Cloud Provider	-p	Specifies which Azure cloud is in use {azure | azusgov | azchina}
Tenant ID	-d	Identifies the AAD instance.
Application ID	-a	Identifies the application in AAD.
Application Key	-k	Access key that is created for the application. Key should be specified in unencoded URL format.

Schritt 2: Installieren Sie das HA python-Paket.

```
[guestshell@guestshell ~]$ pip install csr_azure_ha --user
[guestshell@guestshell ~]$ source ~/.bashrc
```

Schritt 3: Konfigurieren Sie HA-Parameter auf dem primären Router (für diesen Schritt kann MSI oder AAD verwendet werden).

- mit MSI-Authentifizierung.

```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx -g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.1.0.10 -m primary
```

- Mit AD-Authentifizierung (zusätzliche -a, -d, -k Flags erforderlich).

```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx -g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.1.0.10 -m primary -a 1e0f69c3-b6aa-46cf-b5f9-xxxxxxxxx -d ae49849c-2622-4d45-b95e-xxxxxxxxx -k bDEN1k8batJqpeqjAuUvaUCZn5Md6rWEi=
```

Schritt 4: Konfigurieren Sie die HA-Parameter auf dem sekundären Router.

- Mit MSI-Authentifizierung

```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx -g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.1.0.11 -m secondary
```

- Mit AD-Authentifizierung (zusätzliche -a, -d, -k Markierungen erforderlich)

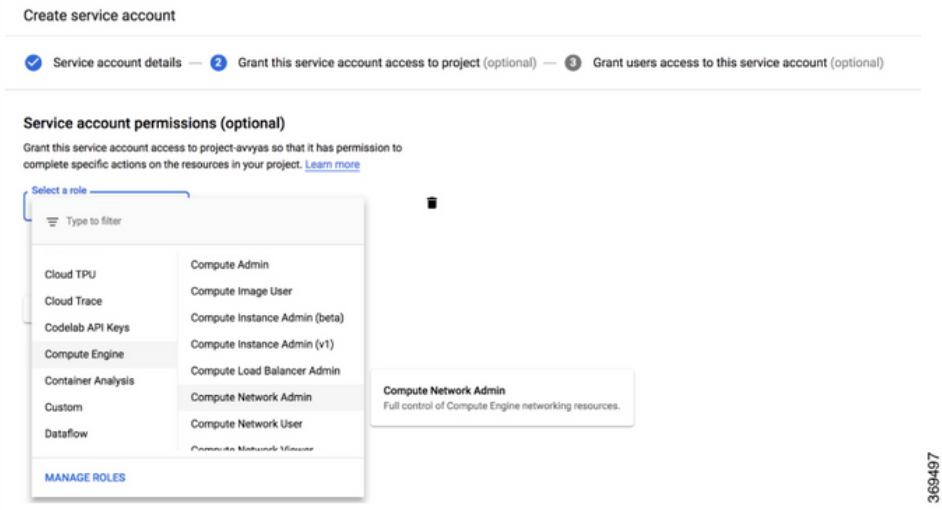
```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx --g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.0.0.11 -m secondary -a 1e0f69c3-b6aa-46cf-b5f9-xxxxxxxxx -d ae49849c-2622-4d45-b95e-xxxxxxxxx -k bDEN1k8batJqpeqjAuUvaUCZn5Md6rWEi=
```

GCP-spezifische Konfiguration

- GCP-HA-Parameter

Parameter	Is this parameter required?	Switch	Description
Node Index	Yes	-i	The index that is used to uniquely identify this node. Valid values: 1-255.
Cloud Provider	Yes	-p	Specify gcp for this parameter.
Project	Yes	-g	Specify the Google Project ID.
routeName	Yes	-a	The route name for which this CSR is next hop. For example from Fig. 2, if we are configuring node on CSR 1, this would be route-vpc2-csr1.
peerRouteName	Yes	-b	The route name for which the BFD peer CSR is next hop. For example from Fig. 2, if we are configuring node on CSR 1, this would be route-vpc2-csr2.
Route	yes	-r	The IP address of the route to be updated in CIDR format. Can be IPv4 or IPv6 address. If a route is unspecified, then the redundancy node is considered to apply to all routes in the routing table of type virtual appliance. Note: Currently Google cloud does not have IPv6 support in VPC.
Next hop address	Yes	-n	The IP address of the next hop router. Use the IP address that is assigned to this CSR 1000v on the subnet which utilizes this route table. The value can be an IPv4 or IPv6 address. Note: Currently Google cloud does not have IPv6 support in VPC.
hopPriority	Yes	-o	The route priority for the route for which the current CSR is the next hop.
VPC	Yes	-v	The VPC network name where the route with the current CSR as the next hop exists.

Hinweis: Stellen Sie sicher, dass das Dienstkonto, das den CSR 1000v-Routern zugeordnet ist, mindestens über eine Administratorberechtigung für das Computernetzwerk verfügt.

Command or Action	Purpose
Ensure that the service account associated with the CSR 1000v routers at least have a Compute Network Admin permission.	 You can also provide the required permissions in a credentials file with name 'credentials.json' and place it under the /home/guestshell directory. The credentials file overrides the permissions supplied through the service account associated with the CSR 1000v instance.

Schritt 1: Installieren Sie das HA python-Paket.

```
[guestshell@guestshell ~]$ pip install csr_gcp_ha --user
[guestshell@guestshell ~]$ source ~/.bashrc
```

Schritt 2: Konfigurieren Sie die HA-Parameter auf dem primären Router.

[guestshell@guestshell ~]$ create_node -i 1 -g -r dest_network -o 200 -n nexthop_ip_addr -a route-vpc2-csr1 -b route-vpc2-csr2 -p gcp -v vpc_name

Schritt 3: Konfigurieren Sie die HA-Parameter auf dem sekundären Router.

[guestshell@guestshell ~]$ create_node -i 1 -g -r dest_network -o 200 -n nexthop_ip_addr -a route-vpc2-csr2 -b route-vpc2-csr1 -p gcp -v vpc_name

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Auslösen eines Failovers mit dem Node_event.py PeerFail-Flag.

[guestshell@guestshell ~]$ node_event.py -i 10 -e peerFail 200: Node_event processed successfully

Schritt 2: Navigieren Sie zur Private Route Table Ihres Cloud-Anbieters, und überprüfen Sie, ob die Route den Next-Hop auf die neue IP-Adresse aktualisiert hat.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Detaillierte HAv3-Konfigurationsschritte finden Sie im Cisco CSR 1000v- und Cisco ISRv-Software-Konfigurationsleitfaden.
- Die Azure HAv2-Konfiguration ähnelt weitgehend der HAv3-Konfiguration, wobei geringfügige Unterschiede bei den Pip-Installationspaketen und der IOS-Redundanzkonfiguration bestehen. Die Dokumentation finden Sie im CSR1000v HA Version 2 Konfigurationshandbuch auf Microsoft Azure.
- Azure HAv1-Konfiguration mit CLI finden Sie im CSR1000v HA Redundancy Deployment Guide auf Microsoft Azure mit AzureCLI 2.0.
- Die AWS HAv1-Konfiguration finden Sie im CSR1000v HA Redundancy Deployment Guide on Amazon AWS.
- Technischer Support und Dokumentation für Cisco Systeme