Configuration de CSR1000v HA version 3 sur AWS, Azure et GCP

Contenu

Introduction

Ce document décrit les étapes à suivre pour configurer les routeurs CSR1000v pour la haute disponibilité version 3 (HAv3) sur Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Nuages AWS, Azure ou GCP.
- Routeurs CSR1000v.
- Cisco IOS®-XE.

Cet article suppose que la configuration réseau sous-jacente a déjà été effectuée et se concentre sur la configuration HAv3.

Vous trouverez des détails complets sur la configuration dans le Guide de configuration du logiciel Cisco CSR 1000v et Cisco ISRv.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Un compte AWS, Azure ou GCP.
- 2 routeurs CSR1000v.
- Un minimum de Cisco IOS®-XE Polaris 16.11.1s

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande.

Informations générales

Cisco vous recommande de connaître les différentes versions HA disponibles :

- HAv1 : La configuration HA est effectuée sous forme de commandes IOS et s'appuie sur BFD comme mécanisme de détection des défaillances.
- HAv2/HAv3 : L'implémentation a été déplacée dans le conteneur de shell invité en tant que scripts python. BFD est facultatif et des scripts personnalisés peuvent être écrits pour détecter les pannes et déclencher le basculement. La configuration d'Azure HAv2 est largement similaire à celle de HAv3 avec des différences mineures dans les packages d'installation pip et la configuration de redondance IOS.
- HAv3 : La mise en oeuvre de la haute disponibilité a été largement supprimée du code Cisco IOS®-XE et s'exécute dans le conteneur de shell invité.

HAv3 est disponible auprès de Cisco IOS®-XE Polaris 16.11.1s et ajoute plusieurs nouvelles fonctionnalités :

- **Agnostique du cloud :** Cette version de haute disponibilité fonctionne sur les routeurs CSR 1000v de n'importe quel fournisseur de services cloud. Bien qu'il existe certaines différences dans la terminologie et les paramètres du cloud, l'ensemble de fonctions et de scripts utilisés pour configurer, contrôler et afficher les fonctionnalités de haute disponibilité est commun aux différents fournisseurs de services cloud. La version 3 de haute disponibilité (HAv3) est prise en charge dans les routeurs CSR 1000v sur AWS, Azure et GCP. La prise en charge du fournisseur GCP a été ajoutée dans 16.11.1. Vérifiez auprès de Cisco si la haute disponibilité est actuellement prise en charge dans les clouds de chaque fournisseur.
- **Opération active/active :** Vous pouvez configurer les deux routeurs Cisco CSR 1000v pour qu'ils soient actifs simultanément, ce qui permet le partage de charge. Dans ce mode de fonctionnement, chaque route d'une table de routage comporte l'un des deux routeurs servant de routeur principal et l'autre de routeur secondaire. Pour activer le partage de charge, prenez toutes les routes et séparez-les entre les deux routeurs Cisco CSR 1000v. Notez que cette fonctionnalité est nouvelle pour les clouds AWS.
- **Revenir au CSR principal après récupération des pannes :** Vous pouvez désigner un routeur Cisco CSR 1000v comme routeur principal pour une route donnée. Alors que ce Cisco CSR 1000v est opérationnel. il s'agit du tronçon suivant de la route. Si ce routeur Cisco CSR 1000v échoue, l'homologue Cisco CSR 1000v prend le relais en tant que tronçon suivant de la route, assurant ainsi la connectivité réseau. Lorsque le routeur d'origine récupère de la panne, il revendique la propriété de la route et est le routeur du tronçon suivant. Cette fonctionnalité est également nouvelle pour les clouds AWS.
- **Scripts fournis par l'utilisateur :** Le shell invité est un conteneur dans lequel vous pouvez

déployer vos propres scripts. HAv3 expose une interface de programmation aux scripts fournis par l'utilisateur. Cela signifie que vous pouvez maintenant écrire des scripts qui peuvent déclencher des événements de basculement et de réversion. Vous pouvez également développer vos propres algorithmes et déclencheurs pour contrôler quels Cisco CSR 1000v fournit les services de transfert pour une route donnée. Cette fonctionnalité est nouvelle pour les clouds AWS.

- **Nouveau mécanisme de configuration et de déploiement :** La mise en oeuvre de la haute disponibilité a été supprimée du code Cisco IOS®-XE. Le code de haute disponibilité s'exécute maintenant dans le conteneur du shell invité. Pour plus d'informations sur le shell invité, reportez-vous à la section Guest Shell du Guide de configuration de la programmabilité. Dans HAv3, la configuration des noeuds de redondance est exécutée dans le shell invité qui utilise un ensemble de scripts Python. Cette fonctionnalité a été introduite pour les clouds AWS.

Note: Les ressources déployées dans AWS, Azure ou GCP à partir des étapes de ce document peuvent entraîner un coût.

Topologie

Avant de commencer la configuration, il est important de bien comprendre la topologie et la conception. Cela permet de résoudre les problèmes potentiels ultérieurement.

Bien que le schéma de topologie du réseau soit basé sur AWS, le déploiement sous-jacent du réseau entre les clouds est relativement similaire. La topologie du réseau est également indépendante de la version HA utilisée, qu'il s'agisse de HAv1, HAv2 ou HAv3.

Pour cet exemple de topologie, la redondance HA est configurée avec les paramètres suivants dans AWS :

- 1x - Région
- 1 x - VPC
- 3x - Zones de disponibilité
- 4x - Interfaces réseau/sous-réseaux (2x Public Facing/2x Private Facing)
- 2x - Tables de routage (publiques et privées)
- 2x - Routeurs CSR1000v (Cisco IOS®-XE 17.01.01)

Il existe deux routeurs CSR1000v dans une paire HA, dans deux zones de disponibilité différentes. La troisième zone est une instance privée, qui simule un périphérique dans un data center privé. En règle générale, tout le trafic normal doit passer par la table de routage privée (ou interne).

Diagramme du réseau

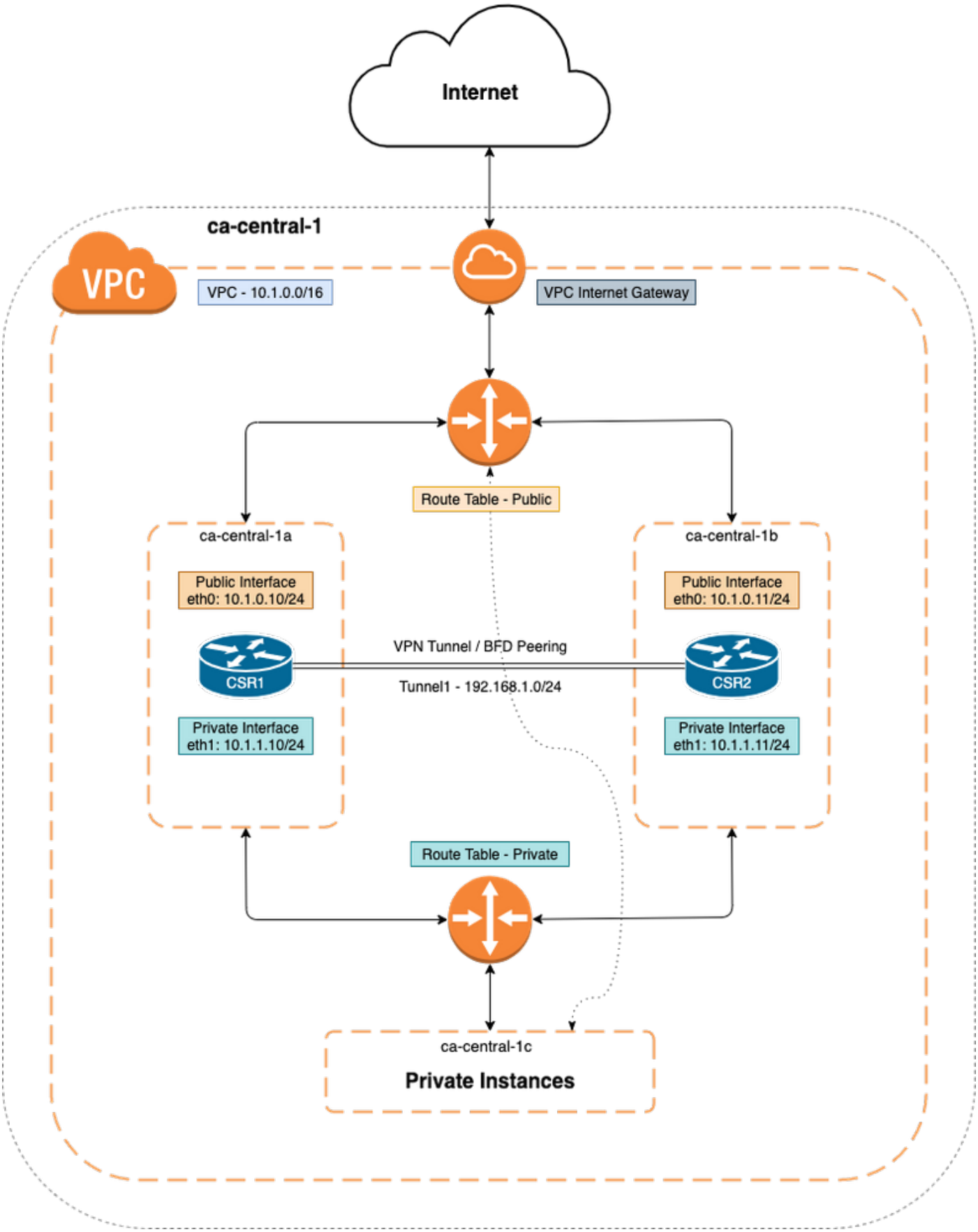


Diagramme du réseau

Configuration des routeurs CSR1000v

Configuration indépendante du cloud

Étape 1. Configurez l'hébergement d'applications IOX et l'interpréteur de commandes, ce qui fournit l'accessibilité ip dans l'interpréteur de commandes. Cette étape peut être configurée automatiquement par défaut lors du déploiement de CSR1000v.

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

Étape 2. Activez et connectez-vous à l'interpréteur de commandes.

```
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 ~]$
```

> **Note**: Pour plus d'informations sur Guestshell, reportez-vous à la section - Programmability Configuration Guide

Étape 3. Confirmer que le shell invité peut communiquer avec Internet.

```
[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
```

Étape 4. (Facultatif) Activez la détection de transfert bidirectionnel (BFD) et un protocole de routage en tant que protocole EIGRP (Enhanced Interior Gateway Routing Protocol) ou BGP (Border Gateway Protocol) dans le tunnel pour la détection des pannes homologues. Configurez un tunnel VxLAN ou IPsec entre les routeurs Cisco CSR 1000v.

- Tunnel IPsec entre les routeurs Cisco CSR 1000v.

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

- Tunnel VxLAN entre les routeurs Cisco CSR 1000v.

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

Étape 4.1. (Facultatif) Configurez le protocole EIGRP sur les interfaces de tunnel.

router eigrp 1 bfd interface Tunnel1 network 192.168.1.0 0.0.0.255

- Des scripts personnalisés peuvent être utilisés pour déclencher le basculement, par exemple :

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

Configuration spécifique à AWS

- Paramètres AWS HA

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.

Étape 1. Configurez l'authentification avec IAM.

Pour que le routeur CSR1000v puisse mettre à jour une table de routage dans le réseau AWS, le routeur doit être authentifié. Dans AWS, vous devez créer une stratégie permettant au routeur CSR 1000v d'accéder à la table de routage. Un rôle IAM est alors créé qui utilise cette stratégie et s'applique à la ressource EC2.

Une fois les instances CSR 1000v EC2 créées, le rôle IAM créé doit être attaché à chaque routeur.

La stratégie utilisée dans le nouveau rôle IAM est la suivante :

{ "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": "*" }] }

Note: Référez-vous à Rôle IAM avec une stratégie et associez-le au VPC pour des étapes détaillées.

Étape 2. Installez le paquet python HA.

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

Étape 3. Configurez les paramètres HA sur le routeur principal.

```
[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
```

Étape 4. Configurez les paramètres HA sur le routeur secondaire.

```
[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
```

- Le format de noeud est le suivant :

```
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
```

Configuration spécifique d'Azure

- Paramètres Azure HA

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.

Note: L'interface externe orientée doit être configurée sur GigabitEthernet1. Il s'agit de l'interface utilisée pour atteindre les API Azure. La HA ne peut pas fonctionner correctement autrement. Dans le shell invité, assurez-vous que la commande curl peut récupérer des métadonnées à partir d'Azure.

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

Étape 1. L'authentification pour les appels API CSR1000v doit être activée avec Azure Active Directory (AAD) ou MSI (Managed Service Identity). Référez-vous à Configurer l'authentification pour les appels de l'API CSR1000v pour des étapes détaillées. Sans cette étape, le routeur

CSR1000v ne peut pas être autorisé à mettre à jour la table de routage.

Paramètres AAD

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.

Étape 2. Installez le paquet python HA.

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

Étape 3. Configurez les paramètres HA sur le routeur principal (vous pouvez utiliser MSI ou AAD pour cette étape).

- Avec authentification MSI.

```
[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
```

- Avec l'authentification AAD (indicateurs supplémentaires -a, -d, -k requis).

```
[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=
```

Étape 4. Configurez les paramètres HA sur le routeur secondaire.

- Avec authentification MSI

```
[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
```

- Avec l'authentification AAD (indicateurs supplémentaires -a, -d, -k requis)

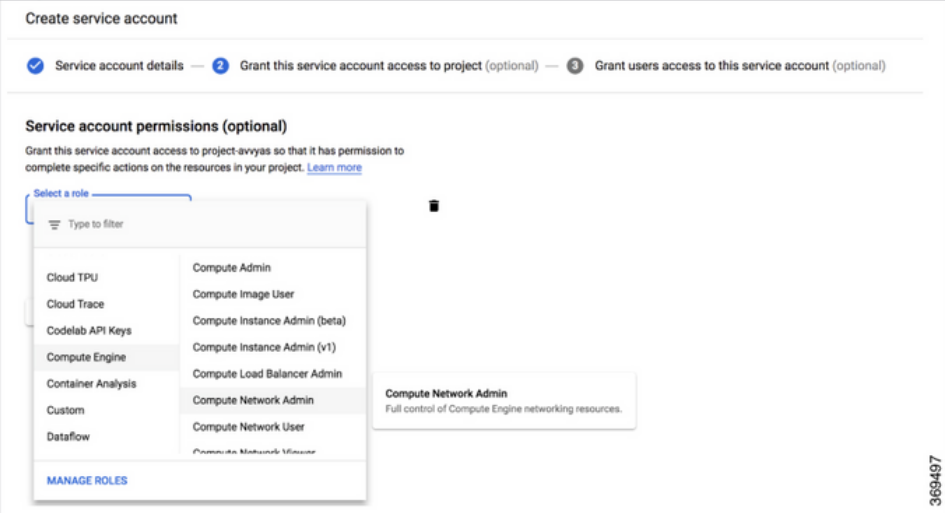
```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx --g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.0.0.11 -m secondary -a 1e0f69c3-b6aa-46cf-b5f9-xxxxxxxxx -d ae49849c-2622-4d45-b95e-xxxxxxxxx -k bDEN1k8batJqpeqjAuUvaUCZn5Md6rWEi=
```

Configuration spécifique du protocole GCP

- Paramètres GCP HA

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.

Note: Assurez-vous que le compte de service associé aux routeurs CSR 1000v dispose au moins d'une autorisation d'administrateur réseau de calcul.

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.

Étape 1. Installez le paquet python HA.

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

Étape 2. Configurez les paramètres HA sur le routeur principal.

[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

Étape 3. Configurez les paramètres HA sur le routeur secondaire.

[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

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Étape 1. Déclenchez un basculement avec l'indicateur node_event.py peerFail.

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

Étape 2. Accédez à la table de routage privé de votre fournisseur de cloud, vérifiez que la route a mis à jour le saut suivant vers la nouvelle adresse IP.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Des étapes détaillées de configuration HAv3 sont disponibles dans le Guide de configuration du logiciel Cisco CSR 1000v et Cisco ISRv
- La configuration d'Azure HAv2 est largement similaire à celle de HAv3 avec des différences mineures dans les packages d'installation pip et la configuration de redondance IOS. La documentation se trouve dans le Guide de configuration de la version 2 de la HA CSR1000v sur Microsoft Azure
- La configuration d'Azure HAv1 avec CLI se trouve dans le Guide de déploiement de la redondance HA CSR1000v sur Microsoft Azure avec AzureCLI 2.0
- La configuration AWS HAv1 se trouve dans le Guide de déploiement de la redondance HA CSR1000v sur Amazon AWS
- Support et documentation techniques - Cisco Systems