تكوين CSR1000V HA الإصدار 3 على AWS و Azure و GCP

المحتويات

المقدمة

يصف هذا المستند خطوات تكوين موجهات CSR1000V للإصدار 3 (HAv3) عالي التوافر على Amazon Web Services (AWS) و Microsoft Azure و Google Cloud Platform (GCP).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- سحب AWS أو Azure أو GCP.
- الموجهات CSR1000v.
- برنامج Cisco IOS®-XE.

يفترض هذا المقال أنه قد تم بالفعل إكمال تكوين الشبكة الأساسية ويركز على تكوين HAv3.

يتم العثور على تفاصيل التكوين الكامل في دليل تكوين البرنامج Cisco CSR 1000v و Cisco ISRv Software.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- حساب AWS أو Azure أو GCP.
- موجهات CSR1000v.
- حد أدنى من Cisco IOS®-XE Polaris 16.11.1s

المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. تم إنشاء جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يوصي cisco أن يتلقى أنت معرفة من مختلف HA صيغة يتوفر:

- HAv1: يتم إجراء تكوين HA وأوامر IOS ويعتمد على BFD آلية الاكتشاف الفشل.
- HAv2/HAv3: تم نقل التنفيذ إلى حاوية Guestshell كنص بيثون. يعد برنامج الاكتشاف مخصصة نصية برامج ثابتة يمكن كما ،اختياري إجراء (BFD) الأداء فائق الإرسال مع HAv3 بكثير حد إلى HAv2 Azure تكوين يشبه. المشغل في الأعطال وتجاوز الأعطال الاختلافات في طفيفة حزم في تثبيت PIP وتكوين تكرار IOS.
- HAv3: تم نقل تنفيذ HA إلى حد كبير من رمز Cisco IOS®-XE ويتم تشغيله في حاوية Guestshell.

يتوفر HAv3 من Cisco IOS®-XE Polaris 16.11.1s ويضيف العديد من الميزات الجديدة:

- **ال** تفاوق **السحابة:** يعمل هذا الإصدار من التوفر العالي على موجهات CSR 1000V على أي خدمة موفر السحابة. يبنما هناك بعض الاختلافات في مصطلحات السحابة والمعلومات، فإن مجموعة الوظائف والبرامج النصية المستخدمة لتكوين ميزات التوفر العالي 3 والتحكم فيها وإظهارها شائعة عبر موفري خدمة السحابة المختلفين. يتم دعم الإصدار من التوفر العالي (HAv3) في موجهات CSR 1000V على AWS و Azure و GCP. تمت إضافة دعم لموفر GCP في 16.11.1. راجع Cisco للحصول على الدعم الحالي للتوفر العالي في بحسب الموفر الفردي.
- **العملية النشطة/النشطة:** يمكنك تكوين كل من موجهات Cisco CSR 1000v لتكون في وضع التشغيل هذا، يحتوي في الحمل. مما يسمح بمشاركة الحمل، وفي نفس الوقت في نطاق كل مسار في جدول مسار على أحد الموجهين الذي يعمل كموجه أساسي والموجه الآخر كموجه ثانوي. للتحكم في مشاركة الحمل، خذ جميع المسارات وقسمها بين الموجهين Cisco CSR 1000V. لاحظ أن هذه الوظيفة جديدة للسحابة المستندة إلى AWS.
- **أطلق إسترداد دعب يساسأ CSR ىلإ خسنلا:** يمكنك تعيين Cisco CSR 1000v موجه أساسي لموجه معين. بينما يكون Cisco CSR 1000v قيد التشغيل. هو الخطوة التالية للمسار. إذا فشل Cisco CSR 1000V هذا، يتولى النظير Cisco CSR 1000V الأمر كالخطوة التالية للمسار، مع الحفاظ على اتصال الشبكة. عند إسترداد الموجه الأصلي من الفشل، فإنه يستعيد ملكية المسار وهو موجه الخطوة التالية. هذه الوظيفة جديدة أيضا للسحابة المستندة إلى AWS.
- **النصوص التفاعلية التي يوفرها المستخدم:** Guestshell عبارة عن حاوية يمكنك من الخلال نشر النصوص التفاعلية الخاصة بك. واجهة برمجة للنصوص HAv3 يعرض. وهذا يعني أنه يمكنك الآن كتابة نصوص تنفيذية النصية التي يوفرها المستخدم. يمكنك أيضا تطوير خوارزميات يمكنها تشغيل كل من أحداث تجاوز الفشل والانسداد. يمكنك التحكم في أي من خدمات إعادة التوجيه من Cisco CSR 1000v والمشغلات الخاصة بك لمسارات معينة. هذه الوظيفة جديدة للسحابة المستندة إلى AWS.
- **آلية تكوين ونشر جديدة:** تم نقل تنفيذ HA من رمز Cisco IOS®-XE. يتم الآن تشغيل التخزين. مزيد من حاوية حاوية حاوية حاوية حاوية حاوية حاوية في العالي التوفر كود المعلومات حول Guestshell، راجع قسم "Guest Shell" في دليل تكوين قابلية البرمجة.

في HAv3، يتم إجراء تكوين عقد التكرار في guestshell الذي يستخدم مجموعة من برامج Python النصية. تم تقديم هذه الميزة الآن للسحابة المستندة إلى AWS.

ملاحظة: يمكن أن تتكون الموارد المنشورة في AWS أو Azure أو GCP من الخطوات الواردة في هذا المستند تكلفة.

طوبولوجيا

قبل بدء التكوين، من المهم فهم المخطط والتصميم بشكل كامل. يساعد ذلك على استكشاف أخطاء أية مشكلات محتملة وإصلاحها فيما بعد.

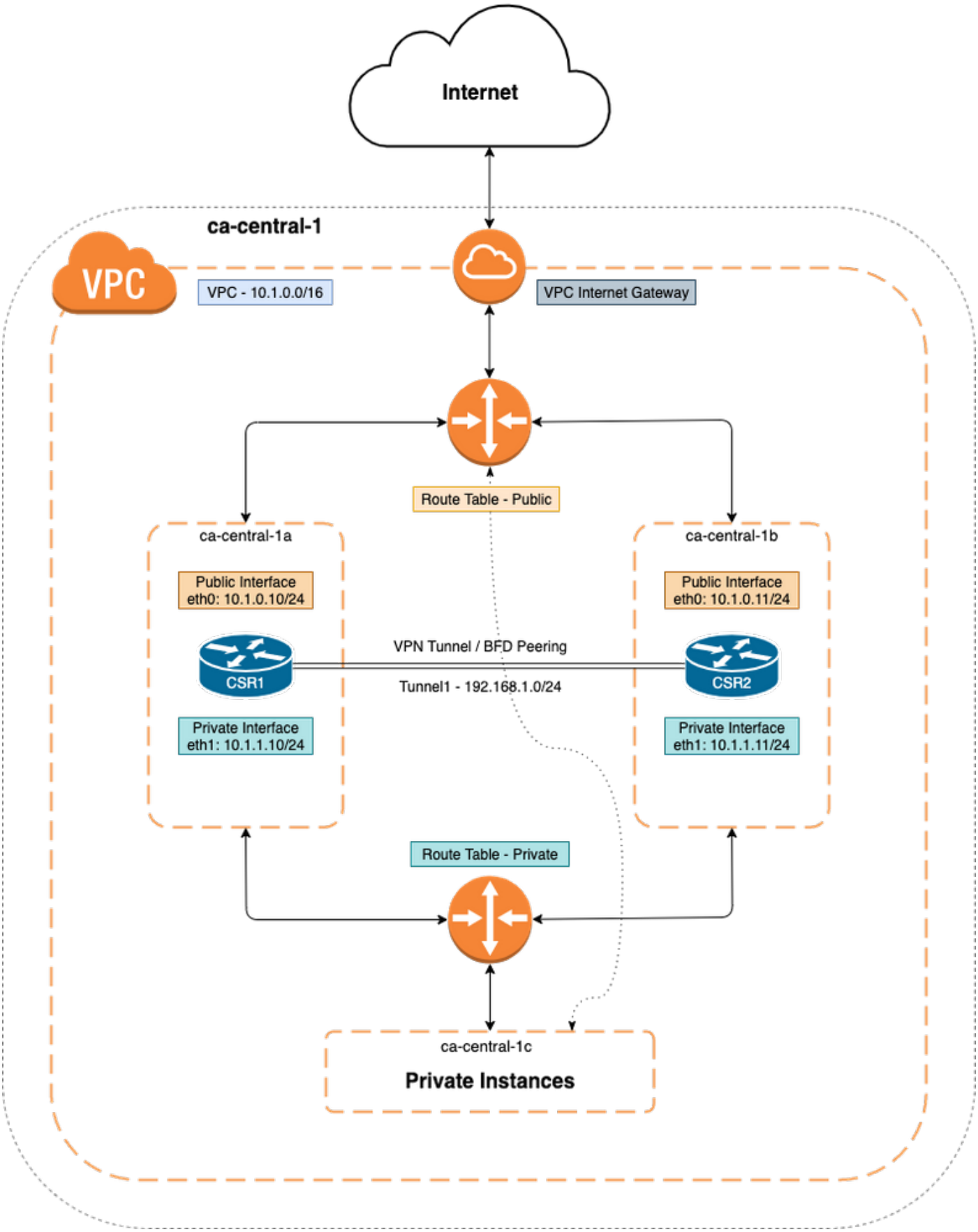
على الرغم من أن مخطط مخطط مخطط الشبكة يستند إلى AWS، إلا أن نشر الشبكة الأساسية بين السحب متماثل نسبيا. كما أن مخطط الشبكة مستقل عن إصدار HA المستخدم، سواء كان HAv1 أو HAv2 أو HAv3.

ل هذا طوبولوجيا مثال، HA شكلت تكرار مع هذا عملية إعداد في AWS:

- 1x - المنطقة
- 1x - VPC
- 3x - مناطق التوفر
- 4X - واجهات الشبكة/الشبكات الفرعية (2X Public Face/2x Private Face)
- 2X - جداول المسارات (العامة والخاصة)
- موجهات 2x - CSR1000v (Cisco IOS®-XE 17.01.01)

هناك موجهات CSR1000v في زوج HA، في منطقتين مختلفتين للتوفر. المنطقة الثالثة هي مثيل خاص، يحاكي جهاز في مركز بيانات خاص. بشكل عام، يجب أن تتدفق جميع حركة المرور العادية عبر جدول المسار الخاص (أو الداخلي).

الرسم التخطيطي للشبكة



الرسم التخطيطي للشبكة

تكوين موجهات CSR1000v

التكوين المستقل للسحابة

الخطوة 1. تكوين إستضافة تطبيقات IOx و Guestshell، يوفر ذلك إمكانية الوصول إلى IP في طبقة الأمان. يمكن تكوين هذه الخطوة تلقائيا بشكل افتراضي عند تطبيق 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

الخطوة 2. تمكين الدخول إلى 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 ~]$
```

> **ملاحظة**: للحصول على مزيد من المعلومات حول Guestshell راجع - [دليل تكوين قابلية البرمجة](#)

الخطوة 3. تأكيد قدرة Guestshell على الاتصال بالإنترنت.

```
[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
```

الخطوة 4. (إختياري) قم بتمكين اكتشاف إعادة التوجيه ثنائي الإتجاه (BFD) لبروتوكول توجيه البوابة الداخلية المحسنة (EIGRP) أو بروتوكول العبارة الحدودية (BGP) إلى النفق لاكتشاف فشل النظير. قم بتكوين نفق VxLAN أو IPsec بين موجهات Cisco CSR 1000V.

- نفق IPsec بين الموجهات 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

- نفق VxLAN بين الموجهات 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

الخطوة 4.1. (إختياري) قم بتكوين EIGRP عبر واجهات النفق.

router eigrp 1 bfd interface Tunnel1 network 192.168.1.0 0.0.0.255

- يمكن إستخدام البرامج النصية المخصصة لتشغيل تجاوز الفشل، على سبيل المثال:

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

التكوين الخاص ب AWS

- معلمات 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.

الخطوة 1. تكوين المصادقة باستخدام IAM.

من أجل أن يقوم الموجه CSR1000V بتحديث جدول توجيه في شبكة AWS، يلزم مصادقة الموجه. في AWS، يجب عليك إنشاء سياسة تسمح للموجه CSR 1000V بالوصول إلى جدول المسار. ثم يتم إنشاء دور IAM يستخدم هذا النهج ويطبق على مورد EC2.

بعد إنشاء مثيلات CSR 1000V EC2، يلزم إرفاق دور IAM الذي تم إنشاؤه بكل موجه

السياسة المستخدمة في دور IAM الجديد هي:

{ "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": "*" }] }

ملاحظة: ارجع إلى للحصول على معرف فئة المورد (VPC) مع سياسة وإقرانه بـ دور IAM

خطوات تفصيلية.

الخطوة 2. ركب HA باي ثون حزمة.

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

الخطوة 3. قم بتكوين معلمات HA على الموجه الأساسي.

```
[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
```

الخطوة 4. قم بتكوين معلمات HA على الموجه الثانوي.

```
[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
```

- تنسيق العقدة هو:

```
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
```

تكوين Azure المحدد

- معلمات 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.

ملاحظة: يجب تكوين الواجهة الأمامية الخارجية على GigabitEthernet1. هذه هي الواجهة التي يمكن أن تعمل HA بشكل صحيح خلاف ذلك. ضمن Guestshell، تأكد من أن الأمر curl يمكن أن يجلب بيانات تطبيقات Azure. المستخدمة للوصول إلى واجهات برمجة التعريف من Azure.

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

الخطوة 1. يجب تمكين مصادقة إستدعاءات CSR1000V API باستخدام Azure Active Directory (AAD) أو معرف الخدمة المدار (MSI). ارجع إلى [تكوين المصادقة لاستدعاءات CSR1000V API](#) للحصول على خطوات تفصيلية. بدون هذه الخطوة، لا يمكن توفيض الموجه CSR1000V لتحديث جدول المسار.

محددات 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.

الخطوة 2. ركب HA بايثون حزمة.

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

الخطوة 3. قم بتكوين معلمات HA على الموجه الأساسي (يمكن إستخدام MSI أو AAD لهذه الخطوة).

- مع مصادقة 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
```

- باستخدام مصادقة AAD (عالمات إضافية -a و -d و -k مطلوبة).

```
[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=
```

الخطوة 4. قم بتكوين معلمات HA على الموجه الثانوي.

- باستخدام مصادقة 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
```

- باستخدام مصادقة AAD (عالمات إضافية -a و -d و -k)

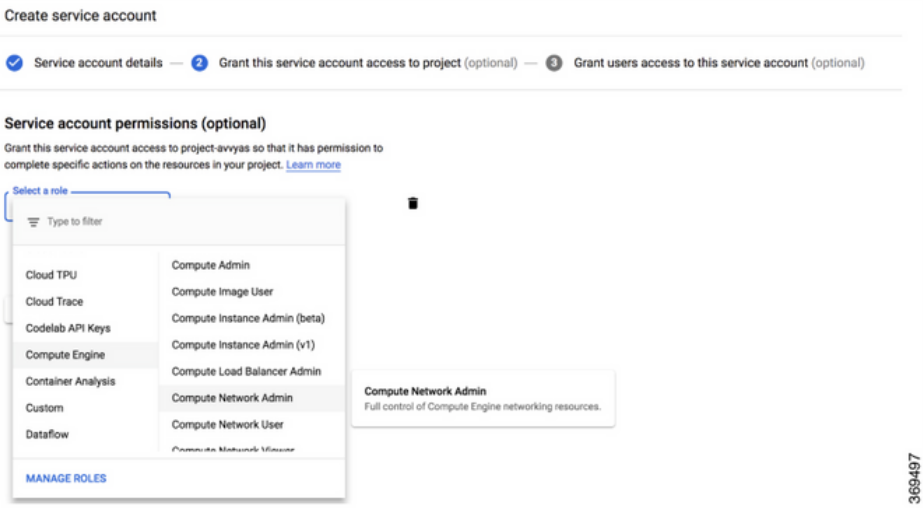
```
[guestshell@guestshell ~]$ create_node -i 10 -p azure -s xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxx --g ResourceGroup -t Private-RouteTable -r 0.0.0.0/0 -n 10.0.0.11 -m secondary -a 1e0f69c3-b6aa-46cf-b5f9-xxxxxxxxx -d ae49849c-2622-4d45-b95e-xxxxxxxxx -k bDEN1k8batJqpeqjAuUvaUCZn5Md6rWEi=
```

تكوين GCP المحدد

- معلمات 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.

ملاحظة: تأكد من أن حساب الخدمة المرتبط بموجهات CSR 1000v لديه على الأقل إذن مسؤول شبكة الكمبيوتر.

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.

الخطوة 1. ركب HA بايثون حزمة.

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

الخطوة 2. قم بتكوين معلمات HA على الموجه الأساسي.

[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

الخطوة 3. قم بتكوين معلمات HA على الموجه الثاني.

[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

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

الخطوة 1. قم بتشغيل تجاوز الفشل باستخدام عالمة node_event.py peerFail.

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

الخطوة 2. انتقل إلى جدول المسار الخاص لمورد السحابة، تحقق من أن المسار قد قام بتحديث الخطوة التالية إلى عنوان IP الجديد.

استكشاف الأخطاء وإصلاحها

ال تتوفر حالياً معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- تم العثور على خطوات تكوين HAv3 التفصيلية في دليل تكوين البرنامج Cisco CSR 1000v و Cisco ISRv Software
- يشبه تكوين Azure HAv2 إلى حد كبير HAv3 مع إختلافات طفيفة في حزم تثبيت PIP وتكوين تكرار IOS. تتوفر الوثائق في دليل تكوين CSR1000V HA الإصدار 2 على Microsoft Azure
- يوجد تكوين Azure HAv1 مع CLI في دليل نشر التكرار CSR1000v HA على Microsoft Azure مع AzureCLI 2.0
- يوجد تكوين AWS HAv1 في دليل نشر التكرار CSR1000v HA على Amazon AWS
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).