Googleクラウドプラットフォームへの CSR1000v/C8000vの導入

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 <u>プロジェクトの設定</u> ステップ1:アカウントの有効で有効なプロジェクトを確認します。 ステップ2:新しいVPCとサブネットを作成します。 ステップ3:仮想インスタンスの導入。 導入の確認 新しいインスタンスへのリモート接続 Bashターミナルを使用してCSR1000v/C8000vにログインします。 PuTTYを使用してCSR1000v/C8000vにログインします。 SecureCRTを使用してCSR1000v/C8000Vにログインします。 追加のVMログイン方法 GCPでのCSR1000v/C8000vへのログインの追加ユーザの許可 新しいユーザ名/パスワードの設定 SSHキーを使用した新しいユーザの設定 CSR1000v/C8000vへのログイン時の設定済みユーザの確認 トラブルシュート 「Operation timed out」エラーメッセージが表示される場合 パスワードが必要な場合 関連情報

概要

このドキュメントでは、Cisco Cloud Services Router(CSR)1000v(CSR1000v)およびCatalyst 8000v(C800v)エッジルータをGoogle Cloud Platform(GCP)に導入して設定する手順について説明 します。

著者: Cisco TACエンジニア、Eric Garcia、Ricardo Neri

前提条件

要件

次の項目に関する知識があることが推奨されます。

•仮想化テクノロジー/仮想マシン(VM)

• クラウドプラットフォーム

使用するコンポーネント

• プロジェクトが作成されたGoogle Cloud Platformのアクティブなサブスクリプション

- ・GCPコンソール
- GCPマーケットプレイス
- Bash端末、Putty、またはSecureCRT
- パブリックおよびプライベートセキュアシェル(SSH)キー

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

17.4.1以降、CSR1000vは同じ機能を備えたC8000vになりますが、SDWANやDNAライセンスなどの新機能が追加されました。 詳細については、公式の製品データシートを確認してください。

<u>Cisco Cloud Services Router 1000vデータシート</u>

Cisco Catalyst 8000Vエッジソフトウェアデータシート

したがって、このガイドはCSR1000vとC8000vルータの両方のインストールに適用されます。

プロジェクトの設定

注:このドキュメントの執筆時点で、新しいユーザは300米ドルの無料クレジットを取得し、1年間の無料利用枠としてGCPを完全に調査できます。これはGoogleによって定義されており、シスコの管理下にありません。

注:このドキュメントでは、パブリックおよびプライベートSSHキーを作成する必要があり ます。詳細については、「<u>GoogleクラウドプラットフォームにCSR1000vを導入するための</u> <u>インスタンスSSHキーの生成」を参照してください</u>

ステップ1:アカウントの有効で有効なプロジェクトを確認します。

アカウントに有効でアクティブなプロジェクトがあることを確認します。これらのプロジェクト は、コンピューティングエンジンの権限を持つグループに関連付ける必要があります。

この導入例では、GCPで作成されたプロジェクトが使用されます。

注:新しいプロジェクトを作成するには、「プロジェクトの作成と管<u>理」を参照してくださ</u> <u>い</u>。

ステップ2:新しいVPCとサブネットを作成します。

新しい仮想プライベートクラウド(VPC)と、CSR1000vインスタンスに関連付ける必要があるサブ ネットを作成します。

デフォルトのVPCまたは以前に作成したVPCとサブネットを使用できます。

コンソールダッシュボードで、図に示すように**[VPCネットワーク] > [VPCネ**ットワーク]を選択し ます。



図に示すように、[Create VPC Network]を選択します。

н	VPC network	VPC networks	VPC NETWORK C REFRESH				
	UD0 activistic						
200	VPC networks	Name Region	Subnets MTU 🕢	Mode	IP address ranges	Gateways	Firewall Rules
C ²	External IP addresses		24 1460	Auto 👻			22
RR	Firewall	us-central1	default		10.128.0.0/20	10.128.0.1	
2.2		europe-west1	default		10.132.0.0/20	10.132.0.1	
>\$	Routes	us-west1	default		10.138.0.0/20	10.138.0.1	
\diamond	VPC network peering	asia-east1	default		10.140.0.0/20	10.140.0.1	
ы	Shared VPC	us-east1	default		10.142.0.0/20	10.142.0.1	
		asia-northeast1	default		10.146.0.0/20	10.146.0.1	
\odot	Serverless VPC access	asia-southeast1	default		10.148.0.0/20	10.148.0.1	
101	Packet mirroring	us-east4	default		10.150.0.0/20	10.150.0.1	
		australia-southeast1	default		10.152.0.0/20	10.152.0.1	

注:現在、CSR1000vはGCPの米国中央地域にのみ導入されています。

図に示すように、VPC名を設定します。

Create a VPC network



Lowercase letters, numbers, hyphens allowed

Description

VPCに関連付けられているサブネット名を設定し、region us-central1を選択します。

図に示すように、us-central1 CIDRの10.128.0.0/20内で有効なIPアドレス範囲を割り当てます。

その他の設定はデフォルトのままにして、[create]ボタンを選択します。

Subnets

 \leftarrow

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. Learn more

Subnet creation mode

- O Custom
- Automatic

New subnet	i ^
Name *	2
Lowercase letters, numbers, hyphens allowed	•
dd a description	
dd a description Region *	
dd a description Region * us-central1	- 0
dd a description Region * us-central1 IP address range *	- 0

注: [automatic]が選択されている場合、GCPはCIDR領域内の自動有効範囲を割り当てます。

作成プロセスが終了すると、図に示すように、新しいVPCが**VPCネットワ**ークセクションに表示

されます。

VPC networks		CREATE VPC NETWORK	C REFRESH			
Name 🛧	Region	Subnets	мти 😧	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

ステップ3:仮想インスタンスの導入。

図に示すように、[コンピュート・エンジン]セクションで、[コンピュート・エンジン] > [VMイン スタンス]を選択します。

A	Home	>	OMMENDATIONS
COMP	PUTE		
۰Ô۰	App Engine	>	VIRTUAL MACHINES
			VM instances
۲	Compute Engine	# >	Instance templates
\$	Kubernetes Engine	>	Sole-tenant nodes
()	Cloud Functions		Machine images
			TPUs
)>	Cloud Run		Migrate for Compute Engine
ş	VMware Engine		Committed use discounts

VMダッシュボードで、図に示すように[インスタンスの作成]タブを選択します。

۲	Compute Engine	VM instances	CREATE INSTANCE 🗄 IMPORT VM	7 REFRESH
Virtual	machines ^	INSTANCES	INSTANCE SCHEDULE	
	VM instances	VM instances are hig	nly configurable virtual machines for running workloads on G	oogle
	Instance templates	infrastructure. <u>Learn r</u>	nore	

シスコ製品を表示するには、図に示すようにGCPマーケットプレイスを使用します。



検索バーに「Cisco CSR」または「Catalyst C8000v」と入力して、要件に適合するモデルとバー ジョンを選択し、[Launch]を選択します。

この導入例では、図に示すように、最初のオプションが選択されています。

🖄 Marketplace

Q csr 1000v

Marketplace > "csr 1000v" > Virtual machines

= Filter Type to filter		Virtual mad	chines
Category	^	7 results	
Compute	(4)	7100010	
Networking	(7)	alialia	Cisco Cloud Services Router 1000V (CSR 1000V) Cisco Systems
Туре			The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The spables enterprise IT to deploy the same enterprise class patworking equipacity in the cloud the
Virtual machines	0		enables enterprise in to deploy the same enterprise-class networking services in the cloud th

cisco

Cisco Cloud Services Router 1000V - 16.12 - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. Th enables enterprise IT to deploy the same enterprise-class networking services in the cloud th



Cisco Cloud Services Router 1000V - 17.2.1r - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The enables enterprise IT to deploy the same enterprise-class networking services in the cloud the

uluiu cisco

Cisco Cloud Services Router 1000V - 17.3 - BYOL

Cisco Systems

The Bring Your Own License (BYOL) of Cisco Cloud Services Router (CSR1000V) delivers ent Google Compute Platform. This software supports all the four CSR Technology packages. The enables enterprise IT to deploy the same enterprise-class networking services in the cloud the

×

🖄 Marketplace	Q cata	alyst 8000v	×
Marketplace > "catalyst 80)00v edge sof	tware - byol" 🗲 Virtua	machines
= Filter Type to filter		Virtual mad	chines
Category	^	1 result	
Compute	(1)	ahaha	Catalyst 8000V Edge Software - BYOL Cisco Systems
Туре		cisco	As part of Cisco's Cloud connect portfolio, the Bring Your Own License (BYOL) version of C 8000V) delivers the maximum performance for virtual enterprise-class networking service
Virtual machines	0		the catalyst oboov (Coboov) biox packages and supports the high-performance versions

注:BYOLは「Bring Your Own License」を意味します。

注:現在、GCPではPay As You Go(PAYG)モデルはサポートされていません。

GCPでは、図に示すように、VMに関連付ける必要がある設定値を入力する必要があります。

図に示すように、GCPにCSR1000v/C8000vを導入するには、ユーザ名とSSH公開キーが必要で す。SSHキーが作成されてい<u>ない場合は、「Google CloudプラットフォームにCSR1000vを導入</u> <u>するためのインスタンスSSHキーの生成」を参照</u>してください。

New Cisco Cloud Services Router 1000V (CSR 1000V)

Deployment name

cisco-csr-1000v-23

Instance name

csr-cisco

Username

cisco

Instance SSH Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC901XkfpuBgq5QR69RsG1Qn

Zone 🕜			
us-central1-f			-
Machine type 📀			
4 vCPUs	¥	15 GB memory	Customize

Boot Disk	
Boot disk type 🕜	
Standard Persistent Disk	•
Boot disk size in GB 🛞	
10	

図に示すように、インスタンスにパブリックIPを関連付けるには、前に作成したVPCとサブネットを選択し、[Ephemeral in external IP]を選択します。

設定後。起動ボタンを選択します。

Networking

Network 🕜

csr-vpc

Subnetwork 🕐

csr-subnet (10.10.1.0/24)

External IP 🕐

Ephemeral

Firewall 🕜

Add tags and firewall rules to allow specific network traffic from the Internet

- Allow TCP port 22 traffic
- Allow HTTP traffic
- Allow TCP port 21 traffic

注:SSHを介してCSRインスタンスに接続するには、ポート22が必要です。HTTPポートは オプションです。

導入が完了したら、[**Compute Engine] > [VM instances]を選択**し、図に示すように新しい CSR1000vが正常に導入されたことを確認します。

VM instances	CREATE INSTANCE	🗄 IMPORT VM	C REFRESH	▶ START / RESUME	STOP
= Filter VM instance:	s				Columns •
Name A Zo	ne Recommendation	In use by Intern	al IP	External IP	Connect
🗌 🤡 csr-cisco us	-central1-f	10.10	.1.2 (nic0)		SSH 🛛 🗧

導入の確認

新しいインスタンスへのリモート接続

GCPでCSR1000v/C8000Vにログインする最も一般的な方法は、Bash端末、Putty、および SecureCRTのコマンドラインです。このセクションでは、前の方法で接続するために必要な設定 を示します。

Bashターミナルを使用してCSR1000v/C8000vにログインします。

新しいCSRにリモート接続するために必要な構文は次のとおりです。

ssh -i private-key-path username@publicIPaddress
例:

\$ ssh -i CSR-sshkey <snip>@X.X.X.X The authenticity of host 'X.X.X.X (X.X.X.X)' can't be established. RSA key fingerprint is SHA256:c3JsVDEt68CeUFGhp9lrYz7tU07htbsPhAwanh3feC4. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added 'X.X.X.X' (RSA) to the list of known hosts. 接続に成功すると、CSR1000vプロンプトが表示されます

\$ ssh -i CSR-sshkey <snip>@X.X.X.X

csr-cisco# show version Cisco IOS XE Software, Version 16.09.01 Cisco IOS Software [Fuji], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.9.1, RELEASE SOFTWARE (fc2) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2018 by Cisco Systems, Inc. Compiled Tue 17-Jul-18 16:57 by mcpre

PuTTYを使用してCSR1000v/C8000vにログインします。

Puttyに接続するには、PuTTYgenアプリケーションを使用して、秘密キーをPEM形式からPPK形式に変換します。

詳細については、「<u>PuTTYgenを使用したPemからPpkファイルへの変換</u>」を参照してください。

秘密キーが適切な形式で生成されたら、Puttyでパスを指定する必要があります。

SSH接続メニューのauthオプションでPrivate key file for authenticationセクションを選択します。

キーが保存されているフォルダを参照し、作成したキーを選択します。次の例では、Puttyメニュ ーのグラフィカルビューと目的の状態を示します。



🕵 PuTTY Configurati	on	?	×
Category:			
- Session	^	Options controlling SSH authentication	
- Terminal - Keyboard		Display pre-authentication banner (SSH-2 only) Bypass authentication entirely (SSH-2 only)	
Bell		Authentication methods	
- Window		Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1)	
Behaviour		Attempt "keyboard-interactive" auth (SSH-2)	
B - Selection		Authentication parameters	
E-Connection		Allow attempted changes of usemame in SSH-2	
Proxy		C:\Users\\ssh\key2_ppk.ppk Browse	
Telnet Rlogin			
SSH Kex			
Host keys			
	¥		
About	Help	Open Cancel	

適切なキーを選択したら、メインメニューに戻り、CSR1000vインスタンスの外部IPアドレスを 使用して、図に示すようにSSH経由で接続します。

🕵 PuTTY Configuratio	n		?	×
Category:				
E Session Logging	^	Basic options for your PuTTY see Specify the destination you want to connec	ssion ct to	
···· Keyboard ···· Bell		Host Name (or IP address)	Port 22	
····· Features ⊡·· Window		Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH	⊖ Ser	ial
Behaviour Translation		Load, save or delete a stored session Saved Sessions		
Golours Connection		Default Settings	Load	
···· Data ···· Proxy			Save	
Telnet Rlogin			Delete	•
Kex Host keys Cipher ⊕Auth	•	Close window on exit: Always Never Only on closed	ean exit	
About H	lelp	Open	Cance	4

注:生成されたSSHキーで定義されたユーザ名/パスワードは、ログインを要求されます。

log in as: cisco
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":

csr-cisco#

SecureCRTを使用してCSR1000v/C8000Vにログインします。

SecureCRTでは、秘密キーのデフォルト形式であるPEM形式の秘密キーが必要です。

SecureCRTでは、メニューで秘密キーへのパスを指定します。

[File] > [Quick Connect] >	[Authentication] > [[Uncheck Password] >	· [PublicKey] >	[Properties]を選
択します。				

次の図は、予想されるウィンドウを示しています。

Quick Connect	×
Protocol: SSH2 ~ Hostname: Port: 22 Firewall:	None ~
Username: Authentication Password PublicKey Keyboard Interactive GSSAPI	Properties
Show quick connect on startup	 Save session ✓ Open in a tab Connect Cancel

[Use session public key string] > [Use identity or certificate file]を選択> [Select ...]ボタン>ディレク トリに移動し、目的のキーを選択> [Select **OK]を選択します(図を参照)。**

Jse global public key setting		Use ses	sion public key se	tting	OK
ession settings				1	Cancel
C:\Users\\.ssh\key2					
Use a certificate from your personal	CAPI store or	a PKCS #11p	rovider DLL		
CAPI V DLL:					
Certificate to use: <pre> </pre>	cates>				
Get username from certificate:	Common Nam	ie V			
Use certificate as raw SSH2 key (ser	rver does not s	support X. 509)		
ingerprint:					
HA-2: e0:82:1d:a8:67:45:eb:96:31:: HA-1: 79:04:f3:8a:0f:99:57:ee:d0:6 4D5: da:82:5e:30:f8:22:ec:a0:04:18:	12:74:28:ac:1/ b:4f:84:bb:93 :71:7e:fe:de:4	a:4b:fa:b6:6e :d3:d1:99:63: 0:63	:67:e9:85:c9:06: 70:a3	0d:3	
<				>	

最後に、図に示すように、SSH経由でインスタンスの外部IPアドレスに接続します。

Quick Connect		×
Protocol: Hostname: Port:	SSH2 V 22 Firewall:	None
Username: Authentication PublicKey Keyboard GSSAPI Password	Interactive	Properties
Show quick co	onnect on startup	 Save session ✓ Open in a tab Connect Cancel

注:生成されたSSHキーで定義されたユーザ名/パスワードは、ログインを要求されます。

csr-cisco# show logging Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator. <snip> *Jan 7 23:16:13.315: %SEC_log in-5-log in_SUCCESS: log in Success [user: cisco] [Source: X.X.X.X] [localport: 22] at 23:16:13 UTC Thu Jan 7 2021 csr-cisco#

追加のVMログイン方法

注:詳細な方法を使用してLinux VMに接続するドキュメントを参照してください。

GCPでのCSR1000v/C8000vへのログインの追加ユーザの許可

CSR1000vインスタンスにログインすると、次の方法で追加ユーザを設定できます。

新しいユーザ名/パスワードの設定

新しいユーザとパスワードを設定するには、次のコマンドを使用します。

enable configure terminal username <username> privilege <privilege level> secret <password> end 例: csr-cisco# configure terminal Enter configuration commands, one per line. End with CNTL/Z.

csr-cisco(config)# username cisco privilege 15 secret cisco csr-cisco(config)# end csr-cisco# 新しいユーザがCSR1000v/C8000vインスタンスにログインできるようになりました。

SSHキーを使用した新しいユーザの設定

CSR1000vインスタンスにアクセスするには、公開キーを設定します。インスタンスメタデータのSSHキーは、CSR1000vへのアクセスを提供しません。

SSHキーを使用して新しいユーザを設定するには、次のコマンドを使用します。

configure terminal
ip ssh pubkey-chain
username <username>
key-string
<public ssh key>
exit
end

csr-cisco(config)#

注: Cisco CLIの最大行数は254文字であるため、キー文字列はこの制限に適合しない可能性 があるため、キー文字列を端末回線に合わせて折り返すと便利です。この制限を克服する方 法の詳細については、「<u>GoogleクラウドプラットフォームにCSR1000vを導入するためのイ</u> ンスタンスSSHキーを生成する」を参照してください

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2me0+TRsSLiwHigv281yw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPq34DNfcFhqlja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlks3PCVGOtW1HxxTU4
FCkmEAg4NEgMVLSm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKIoGB9gx/+DlRvurVXfCdg
3Cmxm2swHmb6MlrEtqIv cisco
Ś
csr-cisco# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
csr-cisco(config)#
csr-cisco(config)# ip ssh pubkey-chain
csr-cisco(conf-ssh-pubkey)# username cisco
csr-cisco(conf-ssh-pubkey-user) # key-string
csr-cisco(conf-ssh-pubkey-data)#ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
csr-cisco(conf-ssh-pubkey-
```

data)#6vkCn29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281

csr-cisco(conf-ssh-pubkeydata)#yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s csr-cisco(conf-ssh-pubkeydata)#ADnODPO+OfTK/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk csr-cisco(conf-ssh-pubkeydata)#s3PCVGOtW1HxxTU4FCkmEAg4NEqMVLSm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKI csr-cisco(conf-ssh-pubkey-data)#oGB9qx/+DlRvurVXfCdq3Cmxm2swHmb6MlrEtqIv cisco csr-cisco(conf-ssh-pubkey-data)# exit csr-cisco(conf-ssh-pubkey-user)# end csr-cisco#

CSR1000v/C8000vへのログイン時の設定済みユーザの確認

設定が正しく設定されていることを確認するには、作成したクレデンシャルを使用してログイン するか、追加のクレデンシャルを使用して公開キーの秘密キーペアを使用してログインします。

ルータ側から、ターミナルIPアドレスを使用した成功ログを確認します。

csr-cisco# show clock
*00:21:56.975 UTC Fri Jan 8 2021
csr-cisco#

csr-cisco# show logging
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml
disabled, filtering disabled)

<snip>

*Jan 8 00:22:24.907: %SEC_log in-5-log in_SUCCESS: log in Success [user: <snip>] [Source: <snip>] [localport: 22] at 00:22:24 UTC Fri Jan 8 2021 csr-cisco#

トラブルシュート

「Operation timed out」エラーメッセージが表示される場合

\$ ssh -i CSR-sshkey <snip>@X.X.X.X
ssh: connect to host <snip> port 22: Operation timed out
考えられる原因:

•インスタンスの展開が完了していません。

パブリックアドレスは、VMのnic0に割り当てられたものではありません。
 ソリューション:

VMの導入が完了するまで待ちます。通常、CSR1000vの導入は完了までに最大5分かかります。

パスワードが必要な場合

パスワードが必要な場合:

• ユーザ名または秘密キーが正しくありません。 ソリューション:

ユーザ名が、CSR1000v/C8000v導入時に指定したものと同じであることを確認します。
 秘密キーが展開時に含まれていたものと同じであることを確認します。

関連情報

- <u>Cisco Cloud Services Router 1000vデータシート</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>