

Google Cloud PlatformでのCSR1000v/C8000vの導入

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[プロジェクト設定](#)

[ステップ 1: アカウントの有効でアクティブ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。](#)

[導入の検証](#)

[新しいインスタンスへのリモート接続](#)

[BashターミナルでCSR1000v/C8000vにログインします。](#)

[CSR1000v/C8000vにPuTTYでログインします。](#)

[CSR1000v/C8000vにSecureCRTでログインします。](#)

[その他のVMログイン方法](#)

[追加ユーザがGCPでCSR1000v/C8000vにログインすることを許可](#)

[新しいユーザ名/パスワードの設定](#)

[SSHキーを使用した新規ユーザの設定](#)

[CSR1000v/C8000vへのログイン時の設定ユーザの確認](#)

[トラブルシューティング](#)

[「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](#)

はじめに

このドキュメントでは、Google Cloud Platform(GCP)でCisco CSR1000v(C1000v)とCatalyst 8000v(C800v)を導入して設定する手順について説明します。

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

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 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市場
- 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、クリアな(デフォルト)設定で作業を開始しています。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以降では、CSR1000vは同じ機能を持つC8000vになりますが、SD-WANやCisco DNAライセンスなどの新機能が追加されています。詳細については、公式製品データシートを確認してください。


[Cisco Cloud Services Router 1000vデータシート](#)

[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ルータとC8000vルータの両方のインストールに適用されません。

プロジェクト設定

 注：このドキュメントが作成された時点で、新規ユーザはGCPを1年間の無料利用枠として完全に検討するための300米ドルの無料クレジットを取得できます。これはGoogleによって定義され、シスコの管理下にありません。


 注：このドキュメントでは、公開SSHキーと秘密SSHキーの作成が必要です。詳細については、「[Google Cloud PlatformでCSR1000vを導入するためのインスタンスSSHキーの生成](#)」を参照してください。

ステップ 1：アカウントの有効でアクティブ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てください。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られている必要があります。

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。

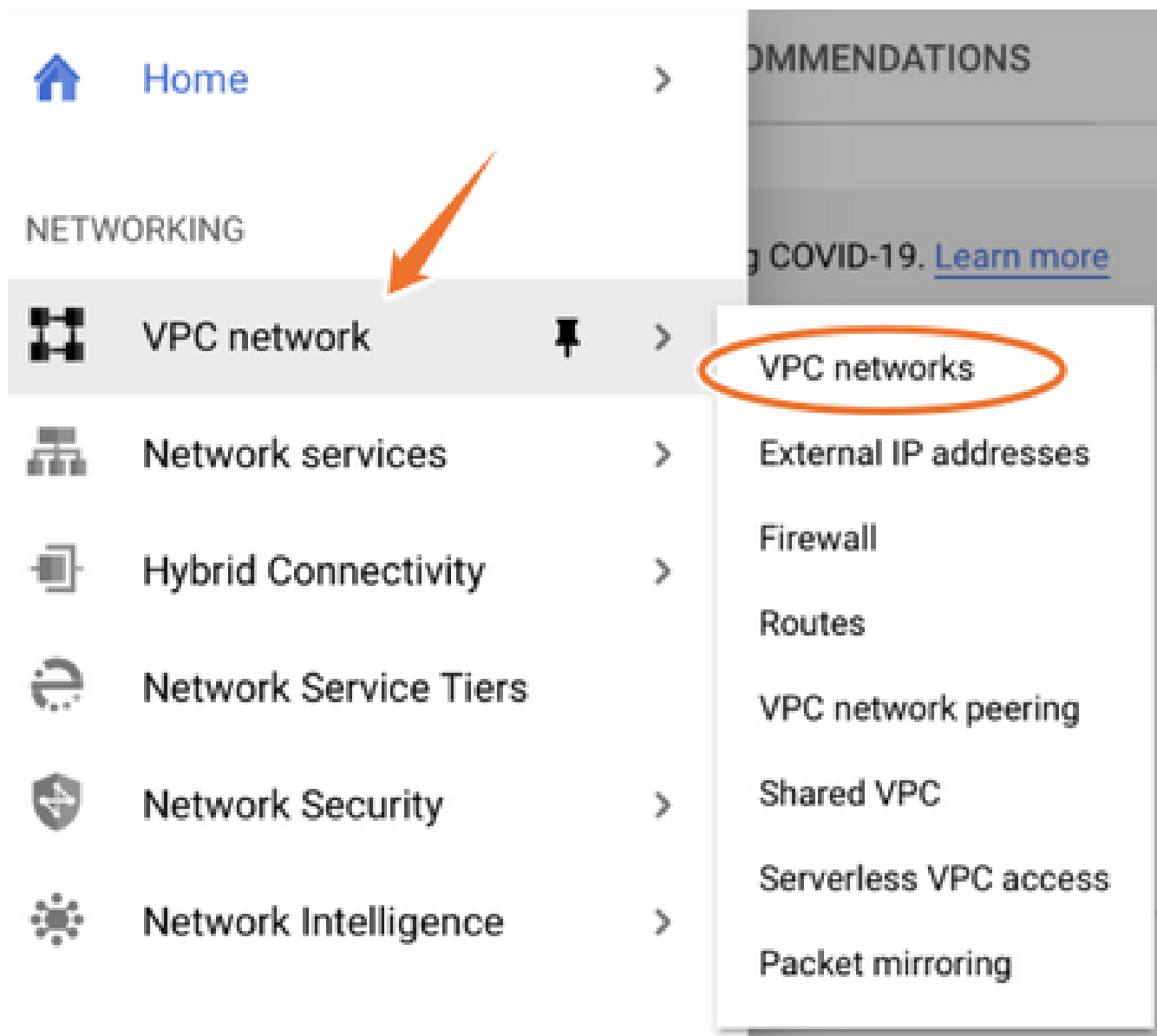
 注：新しいプロジェクトを作成するには、「[プロジェクトの作成と管理](#)」を参照してください。

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、図のように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。

Name ↑	Region	Subnets	MTU ⓘ	Mode	IP address ranges	Gateways	Firewall Rules
▼ default		24	1460	Auto ▼			22
	us-central1	default			10.128.0.0/20	10.128.0.1	
	europa-west1	default			10.132.0.0/20	10.132.0.1	
	us-west1	default			10.138.0.0/20	10.138.0.1	
	asia-east1	default			10.140.0.0/20	10.140.0.1	
	us-east1	default			10.142.0.0/20	10.142.0.1	
	asia-northeast1	default			10.146.0.0/20	10.146.0.1	
	asia-southeast1	default			10.148.0.0/20	10.148.0.1	
	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

Name *

csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

VPCに関連付けられたサブネット名を設定し、リージョンus-central1を選択します。

図に示すように、us-central1 CIDR内の有効なIPアドレス範囲10.128.0.0/20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

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

- Custom
 Automatic

New subnet


Name *
csr-subnet

Lowercase letters, numbers, hyphens allowed

[Add a description](#)

Region *
us-central1

IP address range *
10.10.1.0/24

 注: 「automatic」が選択されている場合、GCPはリージョンCIDR内の有効な自動範囲を割り当てます。

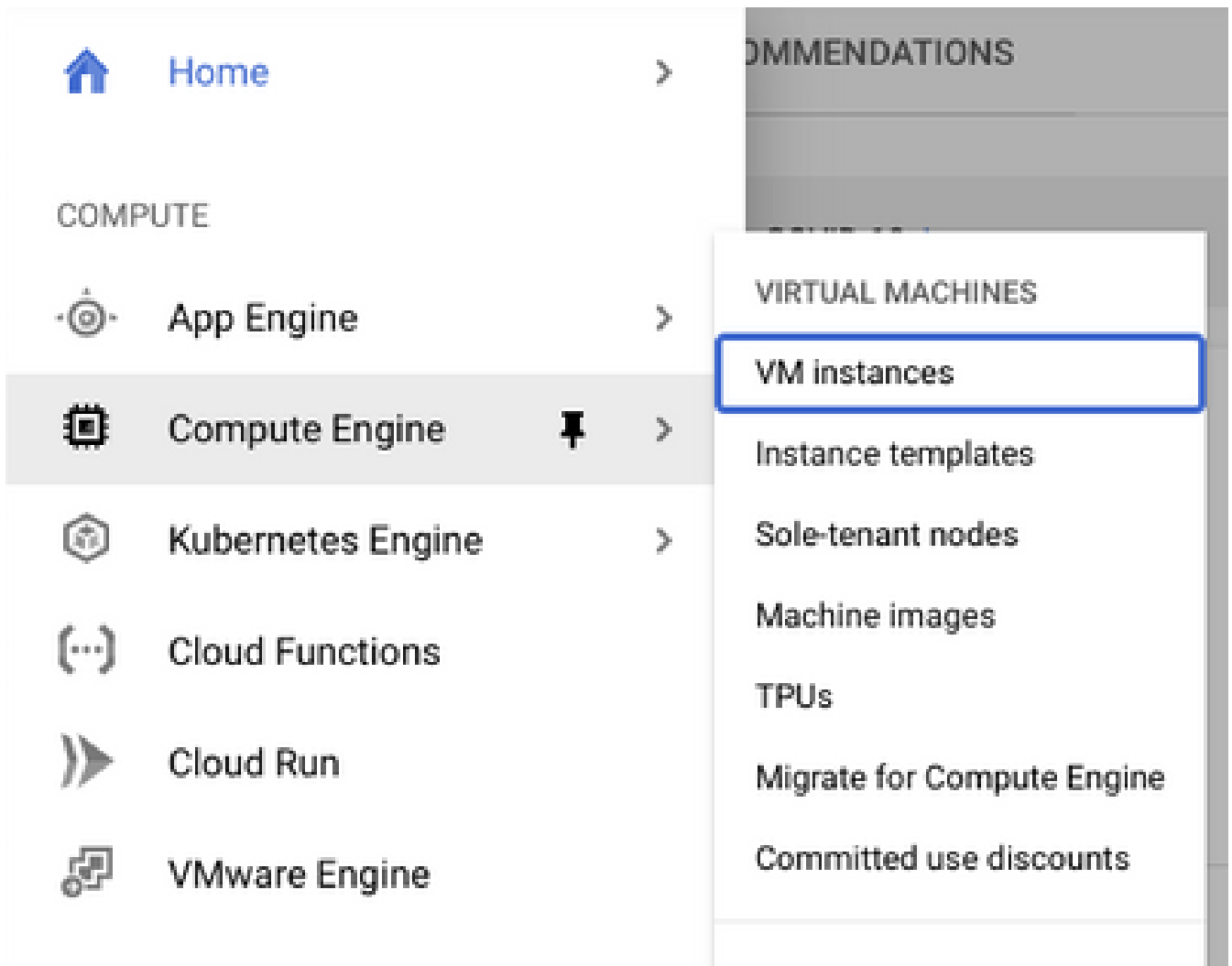
作成プロセスが完了すると、図のように、新しいVPCがVPCネットワークセクションに表示されます。

VPC networks [+ CREATE VPC NETWORK](#) [REFRESH](#)

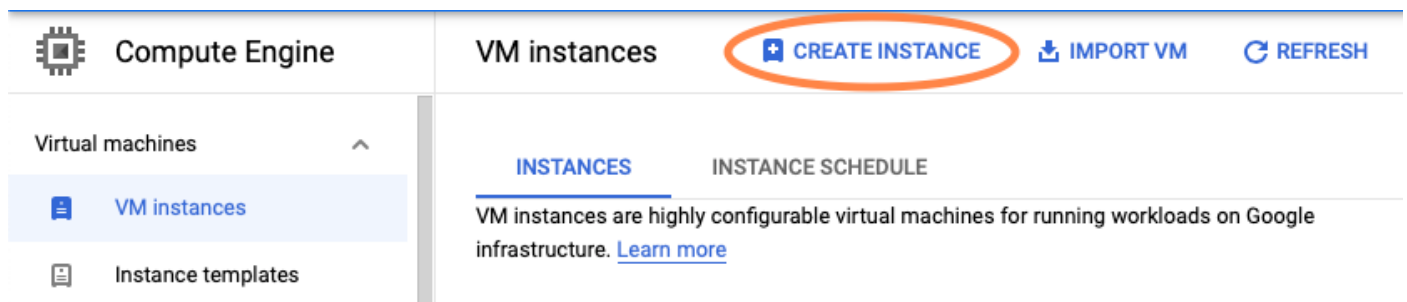
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

ステップ 3 : 仮想インスタンスの導入。

Compute Engineセクションで、図のようにCompute Engine > VMインスタンスを選択します。



VMダッシュボードが表示されたら、図のようにCreate Instanceタブを選択します。



シスコ製品を表示するには、図に示すようにGCP Marketplaceを使用します。



Create an instance

To create a VM instance, select one of the options:



New VM instance

Create a single VM instance from scratch



New VM instance from template

Create a single VM instance from an existing template



New VM instance from machine image

Create a single VM instance from an existing machine image



Marketplace

Deploy a ready-to-go solution onto a VM instance

検索バーでCisco CSR またはCatalyst C8000vと入力し、要件に適合するモデルとバージョンを選択して、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。

Filter Type to filter

Category

Compute

(4)

Networking

(7)

Type

Virtual machines

3

Virtual machines

7 results

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

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 16.12 - BYOL**

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 17.2.1r - BYOL**

Cisco Systems

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

**Cisco Cloud Services Router 1000V - 17.3 - BYOL**

Cisco Systems

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

Marketplace > "catalyst 8000v edge software - byol" > Virtual machines

Filter Type to filter

Virtual machines

Category



Compute

(1)

Networking

(1)

Type

Virtual machines




1 result




Catalyst 8000V Edge Software - BYOL

Cisco Systems

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 the Catalyst 8000V (C8000V) DNA packages and supports the high-performance versions

 注:BYOLは「Bring Your Own License (個人所有ライセンスの持ち込み)」の略です。

 注：現在、GCPはPay As You Go(PAYG)モデルをサポートしていません。

図に示すように、GCPでは、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で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キーを作成していない場合は、『[Google Cloud PlatformでCSR1000vを導入するためのインスタンスSSHキーの生成](#)』を参照してください。

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

Deployment name

Instance name

Username

Instance SSH Key

Zone ?

Machine type ?

15 GB memory

[Customize](#)

Boot Disk

Boot disk type ?

Boot disk size in GB ?

前に作成したVPCとサブネットを選択し、図のようにインスタンスにパブリックIPが関連付けられるように、外部IPでEphemeralを選択します。

設定が完了したら、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経由で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、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するために、Compute Engine > VM instancesの順に選択します。

VM instances							
CREATE INSTANCE							
IMPORT VM							
REFRESH							
START / RESUME							
STOP							
Filter VM instances							
Columns							
Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect	
<input type="checkbox"/> <input checked="" type="checkbox"/>	csr-cisco	us-central1-f		10.10.1.2 (nic0)		SSH	

導入の検証

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、以前の方法で接続するために必要な設定について説明します。

BashターミナルでCSR1000v/C8000vにログインします。

新しいCSRにリモートで接続するために必要な構文は次のとおりです。

```
<#root>
```

```
ssh -i private-key-path username@publicIPAddress
```

以下に例を挙げます。

```
<#root>
```

```
$  
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:c3JsVDEt68CeUFGhp91rYz7tU07htbsPhAwanh3feC4.  
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.
```

接続が成功すると、CSR1000vプロンプトが表示されます

```
<#root>
```

```
$  
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, RELEASED FOR FIELD  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2018 by Cisco Systems, Inc.  
Compiled Tue 17-Jul-18 16:57 by mcpre
```

CSR1000v/C8000vにPuTTYでログインします。

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

詳細については、『[PuTTYgenを使用したPemからPpkファイルへの変換](#)』を参照してください。

秘密鍵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 connection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ック表示と目的の状態を示す画像を示します。



Category:

- ... Keyboard
- ... Bell
- ... Features
- [-] Window
 - ... Appearance
 - ... Behaviour
 - ... Translation
 - [+] Selection
 - ... Colours
- [-] **Connection**
 - ... Data
 - ... Proxy
 - ... Telnet
 - ... Rlogin
 - [-] **SSH**
 - ... Kex
 - ... Host keys
 - ... Cipher
 - [+] **Auth**
 - ... TTY
 - ... X11
 - ... Tunnels

Options controlling SSH authentication

- Display pre-authentication banner (SSH-2 only)
- Bypass authentication entirely (SSH-2 only)

Authentication methods

- Attempt authentication using Pageant
- Attempt TIS or CryptoCard auth (SSH-1)
- Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

- Allow agent forwarding
- Allow attempted changes of username in SSH-2

Private key file for authentication:

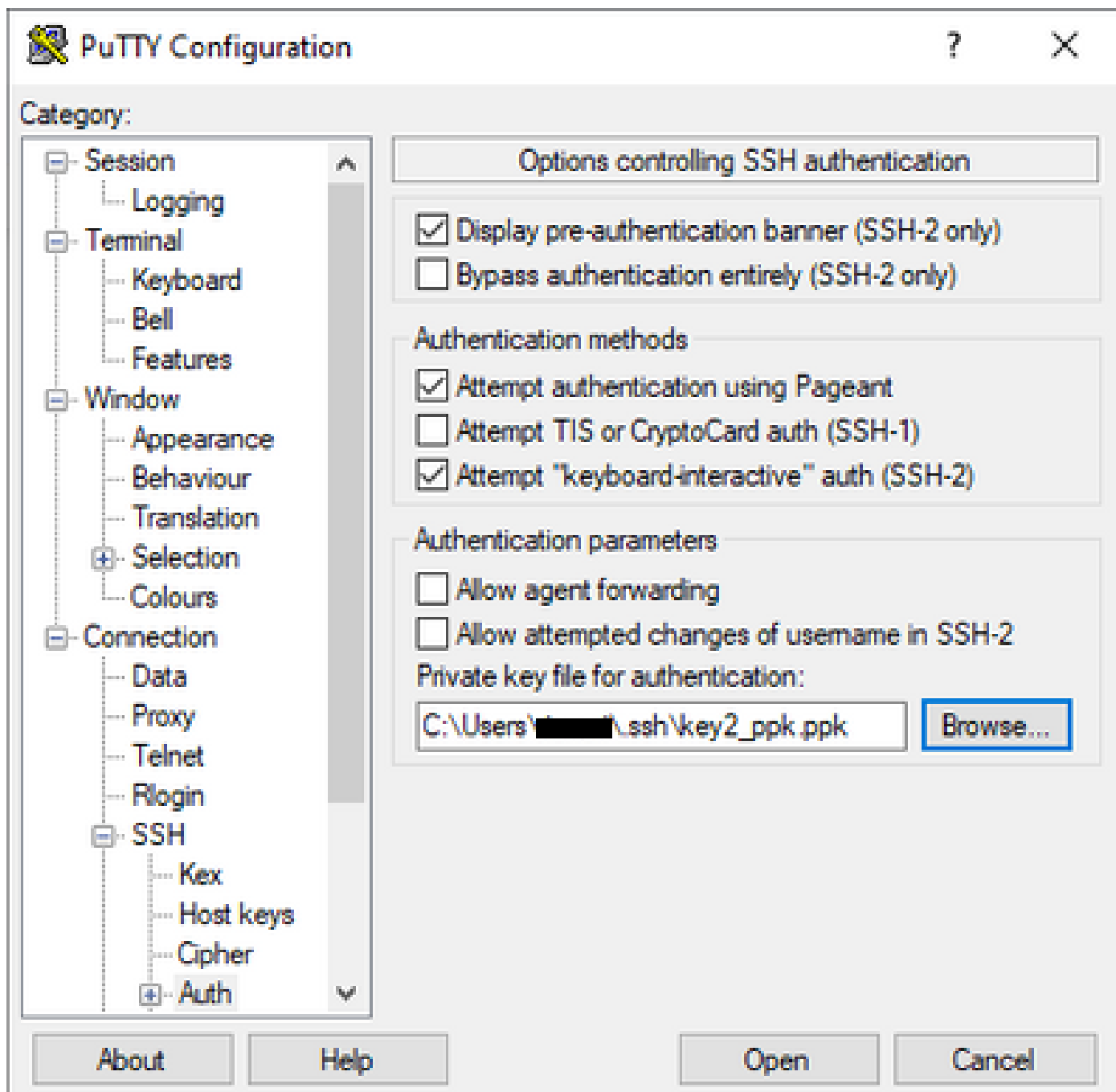
Browse...

About

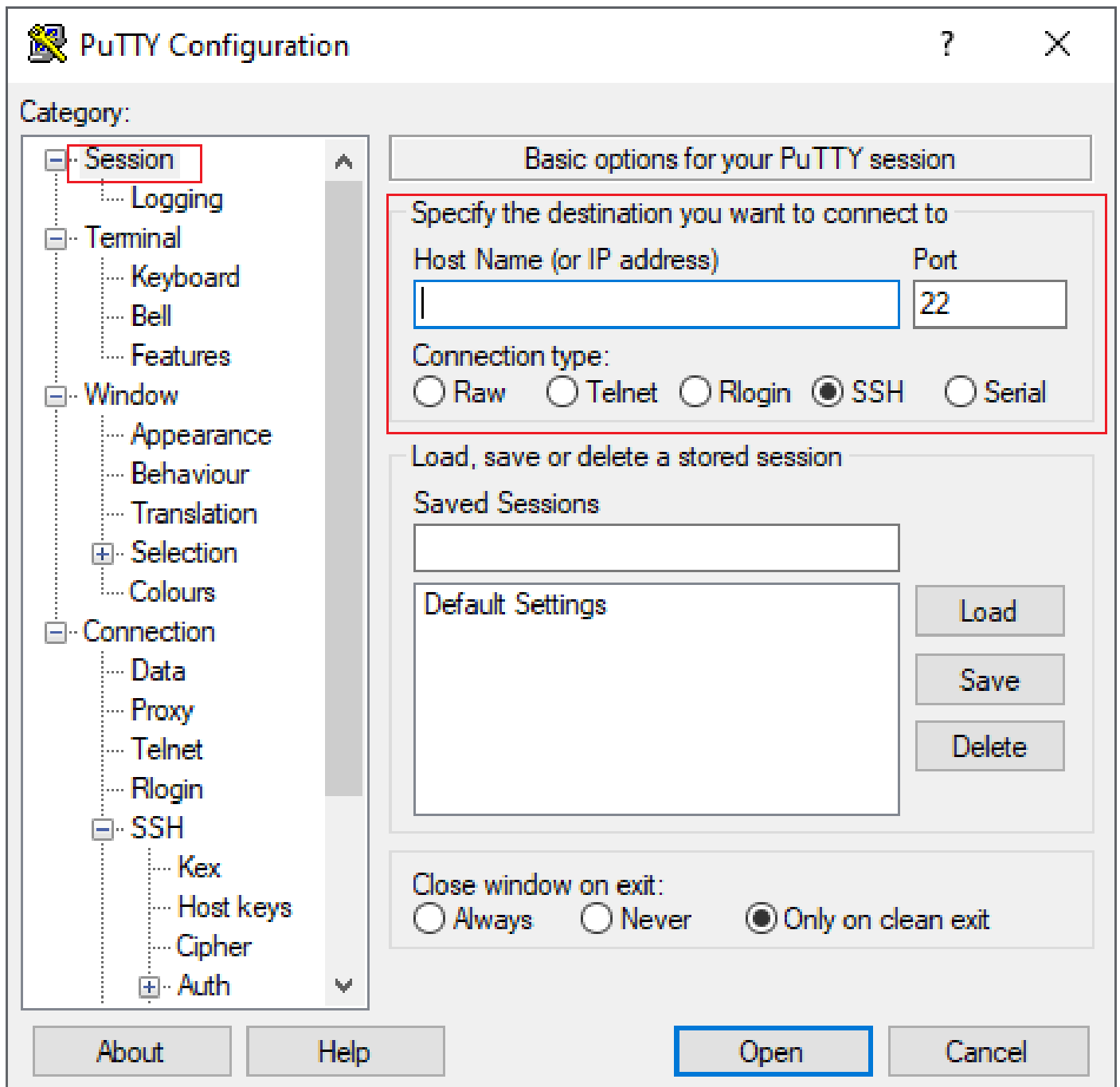
Help


Open

Cancel



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



 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、ログインするよう要求されます。

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

```
csr-cisco#
```

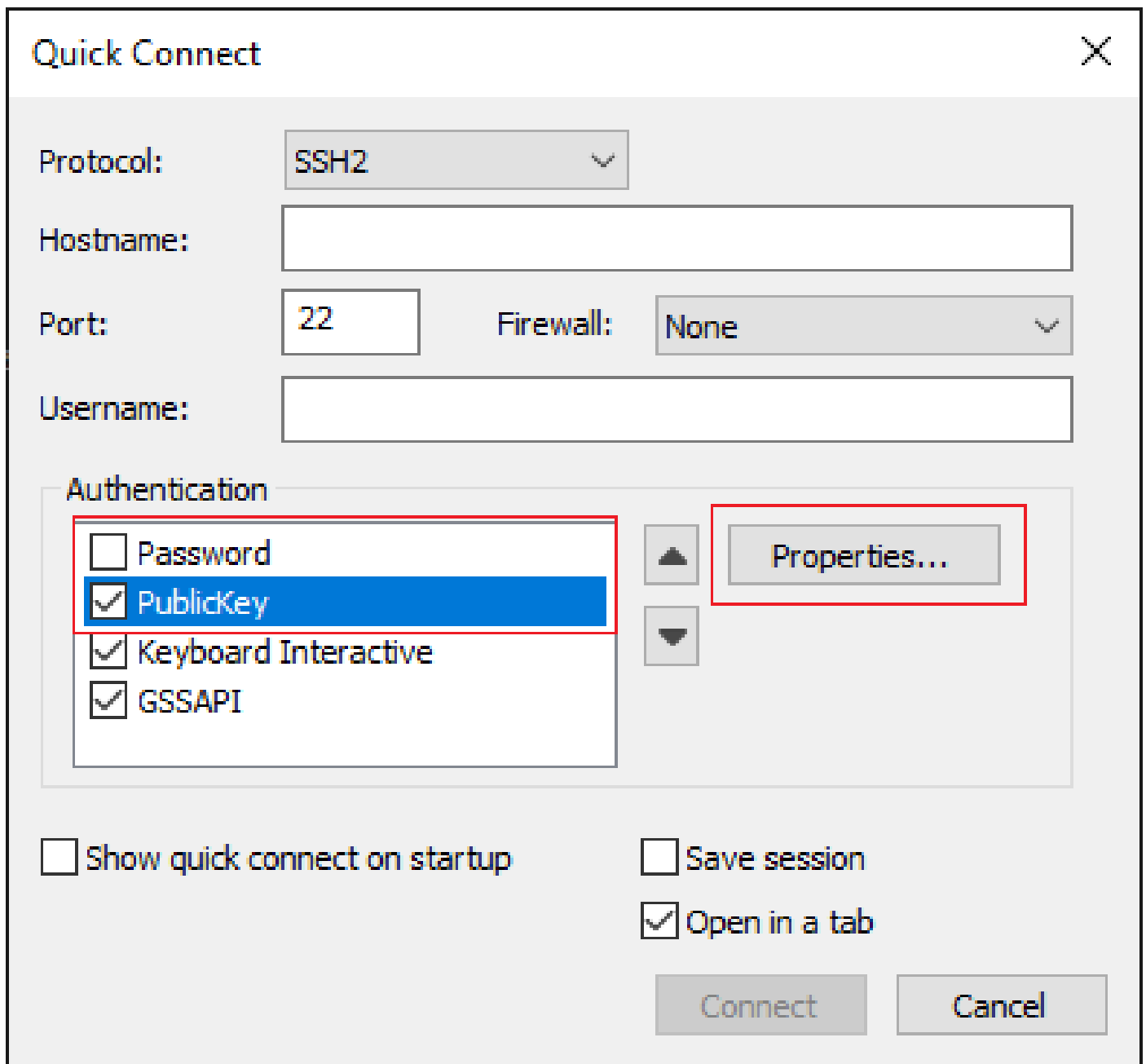
CSR1000v/C8000VにSecureCRTでログインします。

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

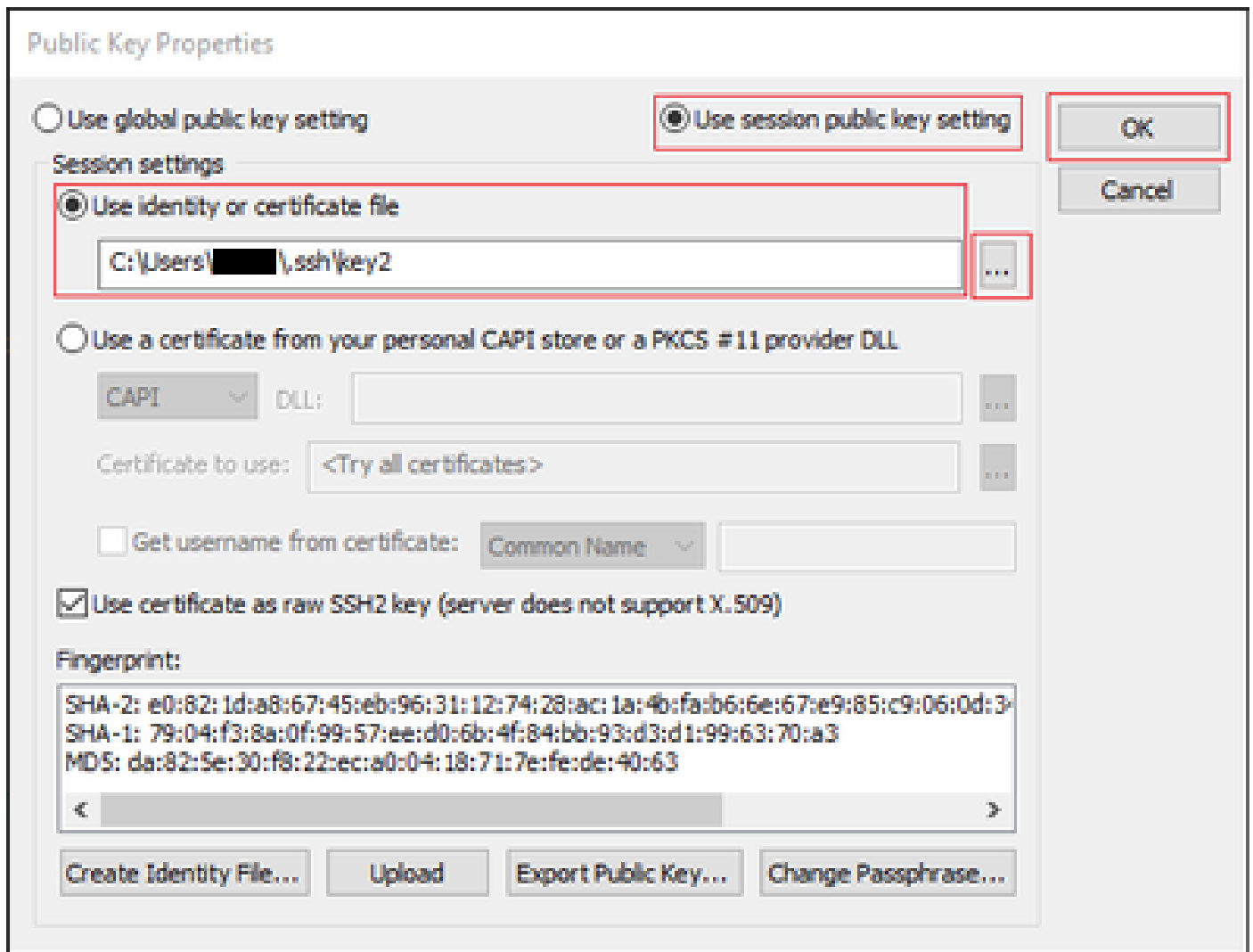
SecureCRTでは、メニューで秘密キーへのパスを指定します。

File > Quick Connect > Authentication > Uncheck Password > PublicKey > Propertiesの順に選択します。

次の図は、想定されるウィンドウを示しています。



図に示すように、Use session public key string > Select Use identity or certificate file > Select ... buttonの順に選択し、ディレクトリに移動して目的のキーを選択し、OKを選択します。



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

Quick Connect ✕

Protocol: SSH2

Hostname: |

Port: 22 Firewall: None

Username:

Authentication


- PublicKey
- Keyboard Interactive
- GSSAPI
- Password

Properties...

Show quick connect 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、ログインするよう要求されます。

```
<#root>
```

```
csr-cisco#
```

```
show logging
```

```
Syslog logging: enabled (0 messages dropped, 3 messages rate-limited, 0 flushes, 0 overruns, xml 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] [local]
```

csr-cisco#

その他のVMログイン方法

 注：ドキュメント『[高度な方法を使用したLinux VMへの接続](#)』を参照してください。

追加ユーザがGCPでCSR1000v/C8000vにログインすることを許可

CSR1000vインスタンスへのログインが成功すると、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。

```
<#root>
```

```
enable
```

```
configure terminal
```

```
username <username> privilege <privilege level> secret <password>
```

```
end
```

以下に例を挙げます。

```
<#root>
```

```
csr-cisco#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
csr-cisco(config)#
```

```
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キーを使用した新規ユーザの設定

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。

新しいユーザにSSHキーを設定するには、次のコマンドを使用します。

```
<#root>
configure terminal

ip ssh pubkey-chain


username <username>

key-string

<public ssh key>

exit

end
```

 注: Cisco CLIの行の最大長は254文字であるため、キー文字列はこの制限に適合しません。キー文字列は端末行に適合するように囲んでおくと便利です。この制限を克服する方法の詳細については、「[Google Cloud PlatformでCSR1000vを導入するためのインスタンスSSHキーの生成](#)」を参照してください。 _

```
<#root>
$
fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2me0+TRsSLiwhigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
```

```
/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1ks3PCVG0tW1HxxTU4
FCkmEAg4NEqMVLsm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKIoGB9qx/+D1RvurVXfCdq
3Cmxm2swHmb6MlrEtqIv cisco
$
```

```
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 AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
6vkCn29bwsQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
ADnODPO+OfTK/OZPg34DNfcFhg1ja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
s3PCVG0tW1HxxTU4FCkmEAg4NEqMVLsm26nLvrNK6z71RMcIKZZcST+SL61Qv33gkUKI
```

```
csr-cisco(conf-ssh-pubkey-data)#
```

```
oGB9qx/+D1RvurVXfCdq3Cmxm2swHmb6MlrEtqIv 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ユーザの確認

設定が正しく行われたことを確認するには、作成したクレデンシャルを使用するか、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でログインします。

ルータ側から、端末のIPアドレスを使用してログイン成功ログを確認します。

```
<#root>
```

```
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)
```

```
<snip>
```

```
*Jan 8 00:22:24.907: %SEC_log in-5-log in_SUCCESS: log in Success [user: <snip>] [Source: <snip>] [local]
csr-cisco#
```

トラブルシューティング

「Operation Timed Out」 エラーメッセージが表示される場合

```
<#root>
```

```
$
```

```
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に割り当てられているものではありません。

ソリューション：

VMの導入が完了するのを待ちます。通常、CSR1000vの導入が完了するまでに最大5分かかりません。

パスワードが必要な場合

パスワードが必要な場合：

```
<#root>
```

```
$
```

```
ssh -i CSR-sshkey <snip>@X.X.X.X
```

```
Password:
```

```
Password:
```

考えられる原因：

- ユーザー名または秘密キーが正しくありません。
- MacOSやLinuxなどの新しいバージョンのOperative Systemでは、OpenSSHユーティリティのデフォルトでRSAは有効になっていません。

ソリューション：

- ユーザ名が、CSR1000v/C8000vの導入時に指定したユーザ名と同じであることを確認します。
- 秘密キーが導入時に指定したものと同じであることを確認します。
- sshコマンドで受け付けるキーのタイプを指定します。

```
<#root>
```

```
ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i <private_key> <user>@<host_ip>
```

関連情報

- [Cisco Cloud Services Router 1000vデータシート](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。