

Déployer un CSR1000v/C8000v sur la plateforme cloud de Google

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration du projet](#)

[Étape 1. Assurez-vous qu'un projet valide et actif pour le compte.](#)

[Étape 2. Créez un VPC et un sous-réseau.](#)

[Étape 3. Déploiement d'instance virtuelle.](#)

[Vérifier le déploiement](#)

[Se connecter à distance à la nouvelle instance](#)

[Connectez-vous à CSR1000v/C8000v avec Bash Terminal](#)

[Connectez-vous à CSR1000v/C8000v avec PuTTY](#)

[Connectez-vous à CSR1000v/C8000V avec SecureCRT](#)

[Méthodes de connexion de VM supplémentaires](#)

[Autoriser les utilisateurs supplémentaires à se connecter à CSR1000v/C8000v dans GCP](#)

[Configurer un nouveau nom d'utilisateur/mot de passe](#)

[Configurer un nouvel utilisateur avec une clé SSH](#)

[Vérification des utilisateurs configurés lors de la connexion à CSR1000v/C8000v](#)

[Dépannage](#)

[Si le message d'erreur « Opération expirée » s'affiche.](#)

[Si un mot de passe est requis](#)

[Informations connexes](#)

Introduction

Ce document décrit la procédure de déploiement et de configuration d'un routeur de services cloud Cisco 1000v (CSR1000v) et d'un routeur de périphérie Catalyst 8000v (C800v) sur la plateforme cloud Google (GCP).

Contribué par Eric Garcia, Ricardo Neri, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologies de virtualisation / machines virtuelles (VM)

- Plates-formes cloud

Components Used

- Abonnement actif à Google Cloud Platform avec un projet créé
- console GCP
- Marché GCP
- Terminal Bash, Putty ou SecureCRT
- Clés SSH (Secure Shell) publiques et privées

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 en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

À partir de la version 17.4.1, le CSR1000v devient le C8000v avec les mêmes fonctionnalités, mais de nouvelles fonctionnalités sont ajoutées, telles que SDWAN et les licences DNA. Pour de plus amples informations, veuillez vérifier la fiche technique officielle des produits :

[Fiche technique du routeur de services cloud Cisco 1000v](#)

[Fiche technique du logiciel de périphérie Cisco Catalyst 8000V](#)

Par conséquent, ce guide s'applique à l'installation des routeurs CSR1000v et C8000v.

Configuration du projet

Note: Au moment de l'écriture de ce document, les nouveaux utilisateurs ont 300 USD de crédits gratuits pour explorer pleinement GCP en tant que Free Tier pendant un an. Cela est défini par Google et n'est pas sous le contrôle de Cisco.

Remarque : Ce document nécessite la création de clés SSH publiques et privées. Pour plus d'informations, consultez [Générer une clé SSH d'instance pour déployer un CSR1000v dans la plate-forme cloud Google](#)

Étape 1. Assurez-vous qu'un projet valide et actif pour le compte.

Assurez-vous que votre compte a un projet valide et actif, qu'il doit être associé à un groupe avec des autorisations pour Compute Engine.

Pour cet exemple de déploiement, un projet créé dans le GCP est utilisé.

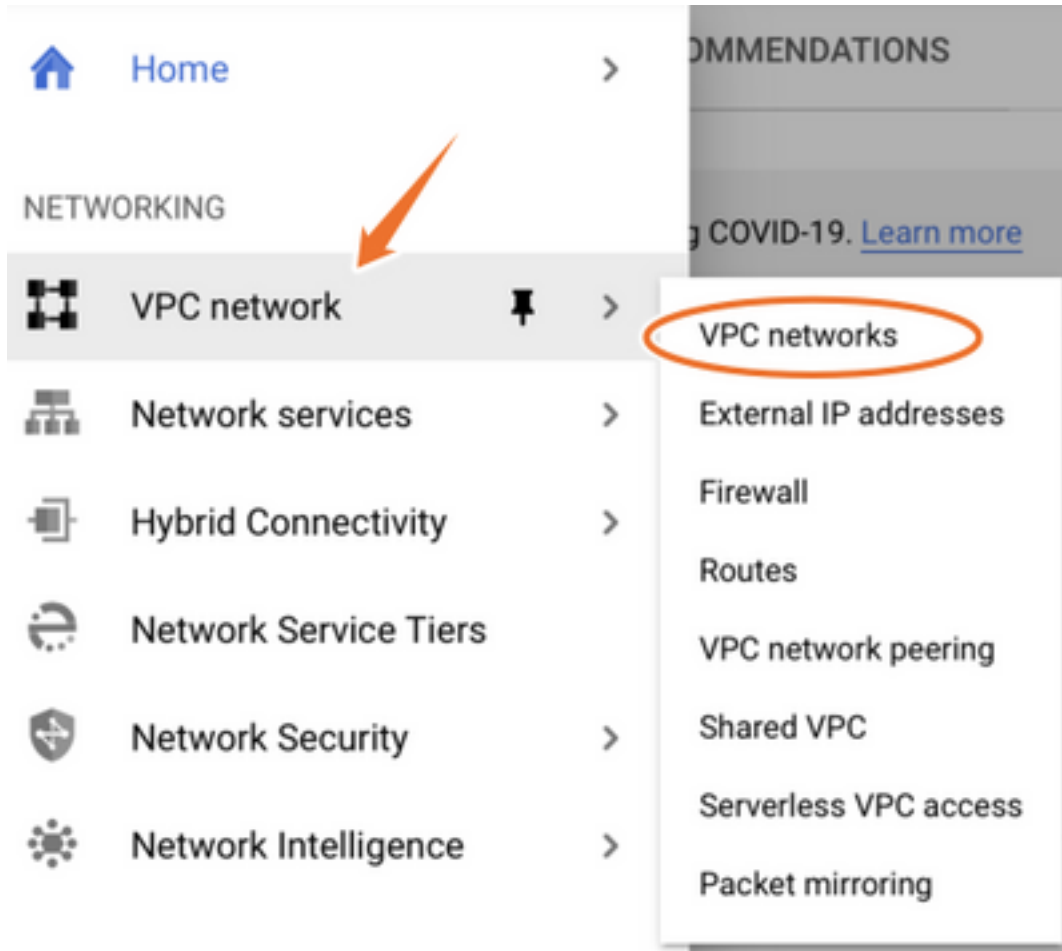
Note: Pour créer un nouveau projet, reportez-vous à [Créer et gérer des projets](#).

Étape 2. Créez un VPC et un sous-réseau.

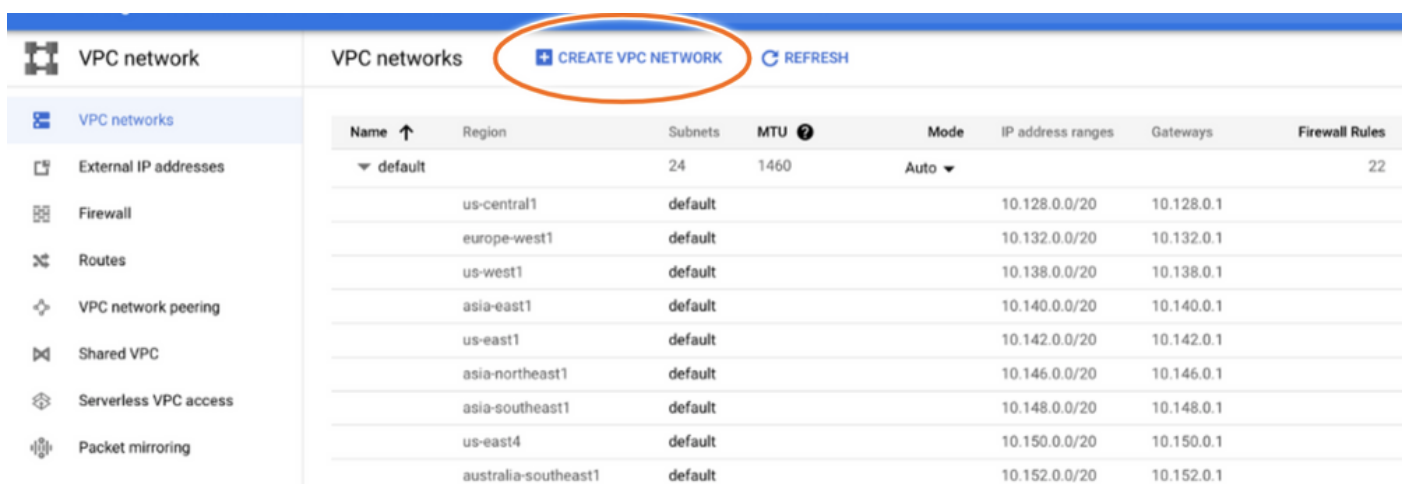
Créez un nouveau cloud privé virtuel (VPC) et un sous-réseau qui doit être associé à l'instance CSR1000v.

Il est possible d'utiliser le VPC par défaut ou un VPC et un sous-réseau précédemment créés.

Dans le tableau de bord de la console, sélectionnez **Réseau VPC > Réseaux VPC** comme indiqué dans l'image.



Sélectionnez **Créer un réseau VPC** comme indiqué dans l'image.



Note: Actuellement, CSR1000v est uniquement déployé dans la région centré-us sur GCP.

Configurez le nom du VPC comme indiqué dans l'image.

← Create a VPC network

Name *

csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Configure the name of the subnet associated with the VPC and select the region **us-central1**.

Assign a valid IP address range in the us-central1 CIDR of 10.128.0.0/20. as the image shows.

Leave the other parameters by default and select **Créer** button :

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

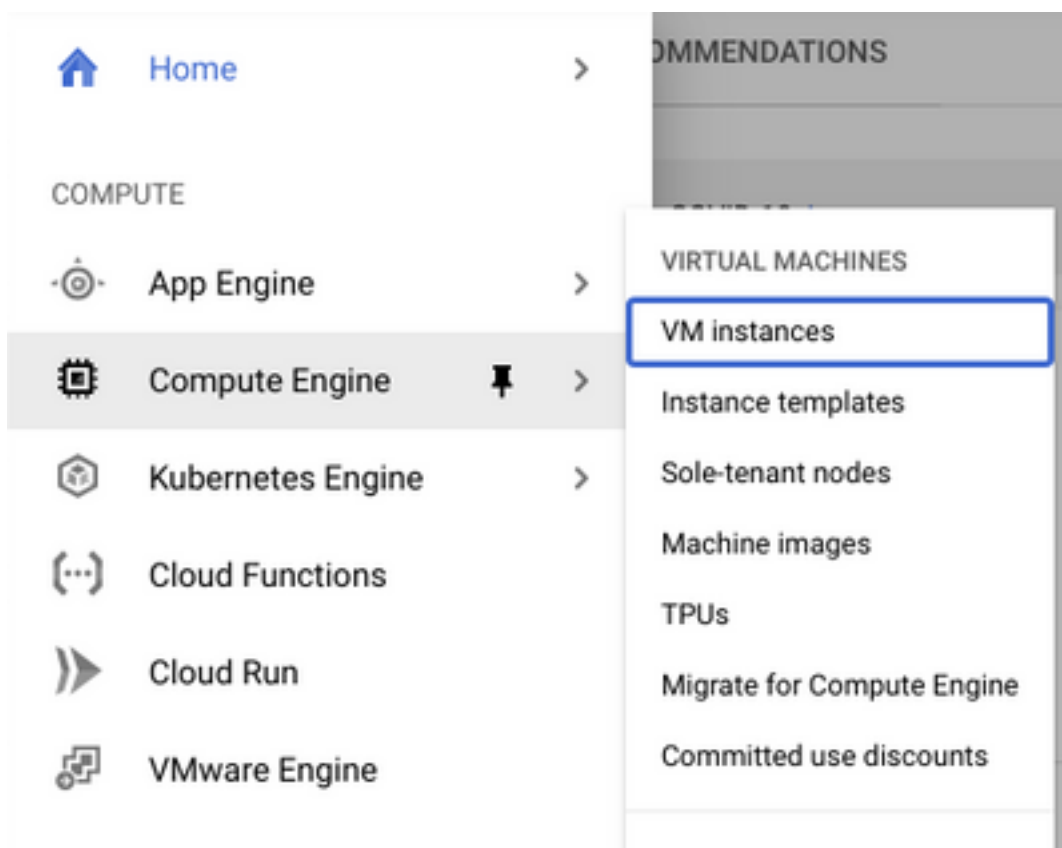
Note: Si l'option « automatique » est sélectionnée, le protocole GCP attribue une plage valide automatique dans le CIDR de la région.

Une fois le processus de création terminé, le nouveau VPC apparaît dans la section **Réseaux VPC** comme illustré dans l'image.

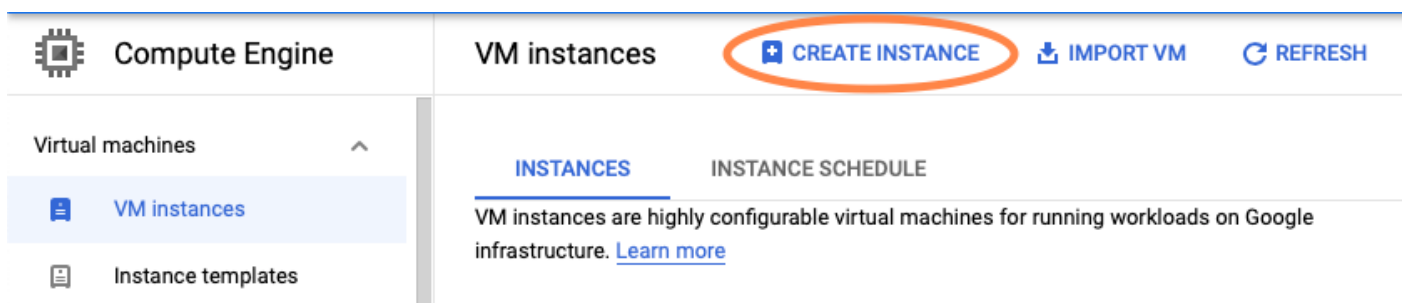
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc	us-central1	1	1460	Custom	10.10.1.0/24	10.10.1.1
		csr-subnet				

Étape 3. Déploiement d'instance virtuelle.

Dans la section **Moteur de calcul**, sélectionnez **Moteur de calcul > Instances de VM** comme indiqué dans l'image.



Une fois dans le **tableau de bord de la VM**, sélectionnez l'onglet **Créer une instance** comme indiqué dans l'image.



Utilisez le marché GCP comme indiqué sur l'image, afin d'afficher les produits Cisco.

← 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

Dans la barre de recherche, tapez **Cisco CSR** ou **Catalyst C8000v**, choisissez le modèle et la version correspondant à vos besoins et sélectionnez **Lancer**.

Pour cet exemple de déploiement, la première option a été sélectionnée, comme l'illustre l'image.

Filter Type to filter

Category



Compute

(4)

Networking

(7)

Type

Virtual machines



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

Filter Type to filter

Category ^

Compute (1)


Networking (1)

Type

Virtual machines

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

Note : BYOL signifie “ Bring Your Own License ”.

Remarque : actuellement, GCP ne prend pas en charge le modèle de paiement au fur et à mesure (PAYG).

Le protocole GCP doit entrer les valeurs de configuration qui doivent être associées à la machine virtuelle, comme le montre l'image :

Un nom d'utilisateur et une clé publique SSH sont nécessaires pour déployer un CSR1000v/C8000v dans GCP, comme l'illustre l'image. Reportez-vous à [Générer une clé SSH d'instance pour déployer un CSR1000v dans la plate-forme cloud Google](#) si les clés SSH n'ont pas été créées.



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 ?

Sélectionnez le VPC et le sous-réseau créés précédemment et choisissez Ephéméral dans l'adresse IP externe, afin qu'une adresse IP publique soit associée à l'instance comme illustré dans l'image.

Une fois configuré. Sélectionnez le bouton **de lancement**.

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

Note: Le port 22 est nécessaire pour se connecter à l'instance CSR via SSH. Le port HTTP est facultatif.

Une fois le déploiement terminé, sélectionnez **Moteur de calcul > Instances de VM** afin de vérifier que le nouveau CSR1000v a été correctement déployé comme indiqué dans l'image.

VM instances [+ CREATE INSTANCE](#) [↓ IMPORT VM](#) [↻ REFRESH](#) ▶ START / RESUME ■ STOP ||

Filter VM instances Columns

<input type="checkbox"/> Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/> csr-cisco	us-central1-f			10.10.1.2 (nic0)	[REDACTED]	SSH ▾ ⋮

Vérifier le déploiement

Se connecter à distance à la nouvelle instance

Les méthodes les plus courantes pour se connecter à un CSR1000v/C8000V dans GCP sont la ligne de commande dans un terminal Bash, Putty et SecureCRT. Dans cette section, la configuration requise pour se connecter aux méthodes précédentes.

Connectez-vous à CSR1000v/C8000v avec Bash Terminal

La syntaxe requise pour se connecter à distance au nouveau CSR est la suivante :

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

Exemple :

```
$ 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.
```

Si la connexion réussit, l'invite CSR1000v s'affiche.

```
$ 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
```

Connectez-vous à CSR1000v/C8000v avec PuTTY

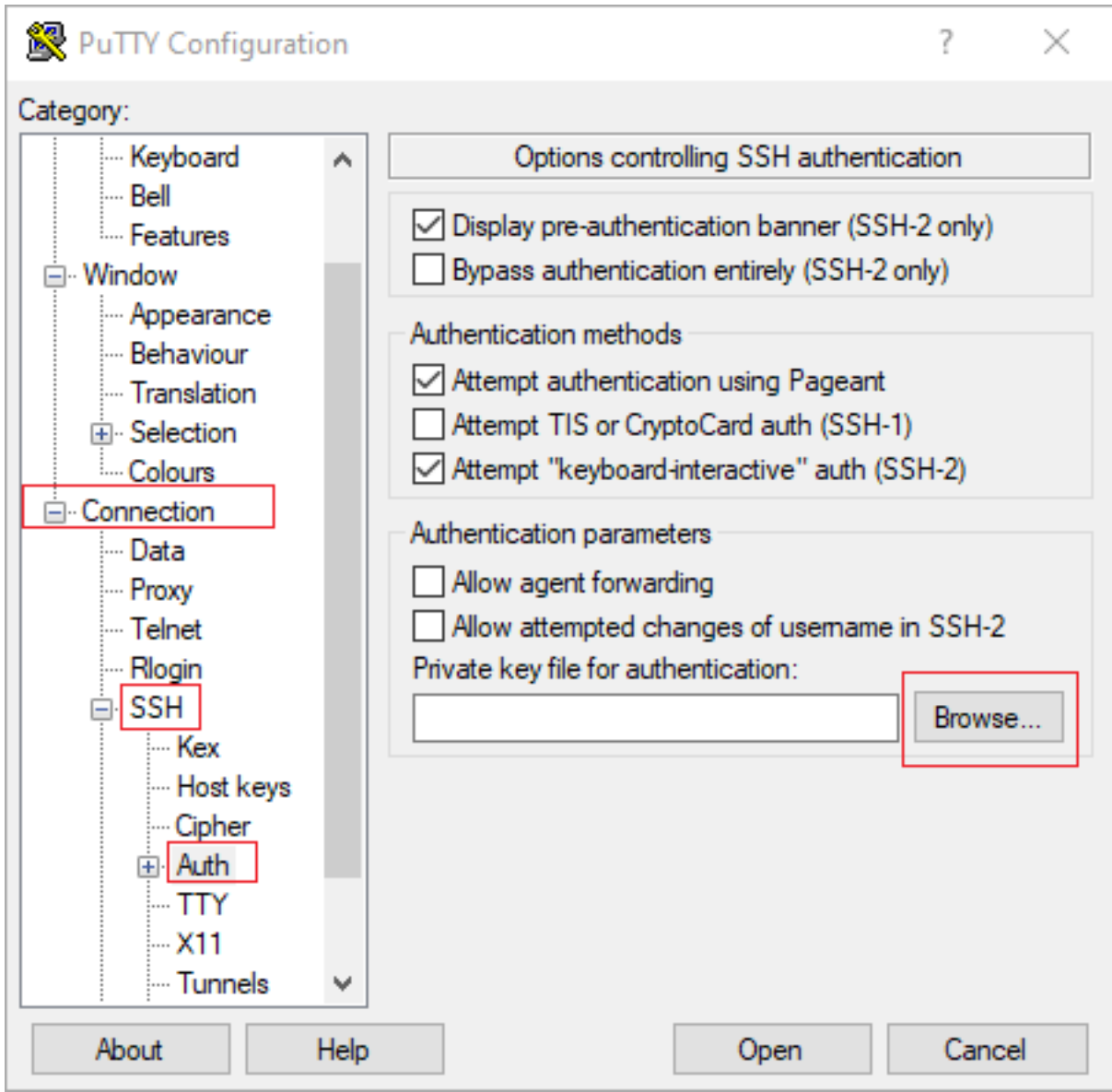
Pour vous connecter à Putty, utilisez l'application PuTTYgen afin de convertir la clé privée du format PEM au format PPK.

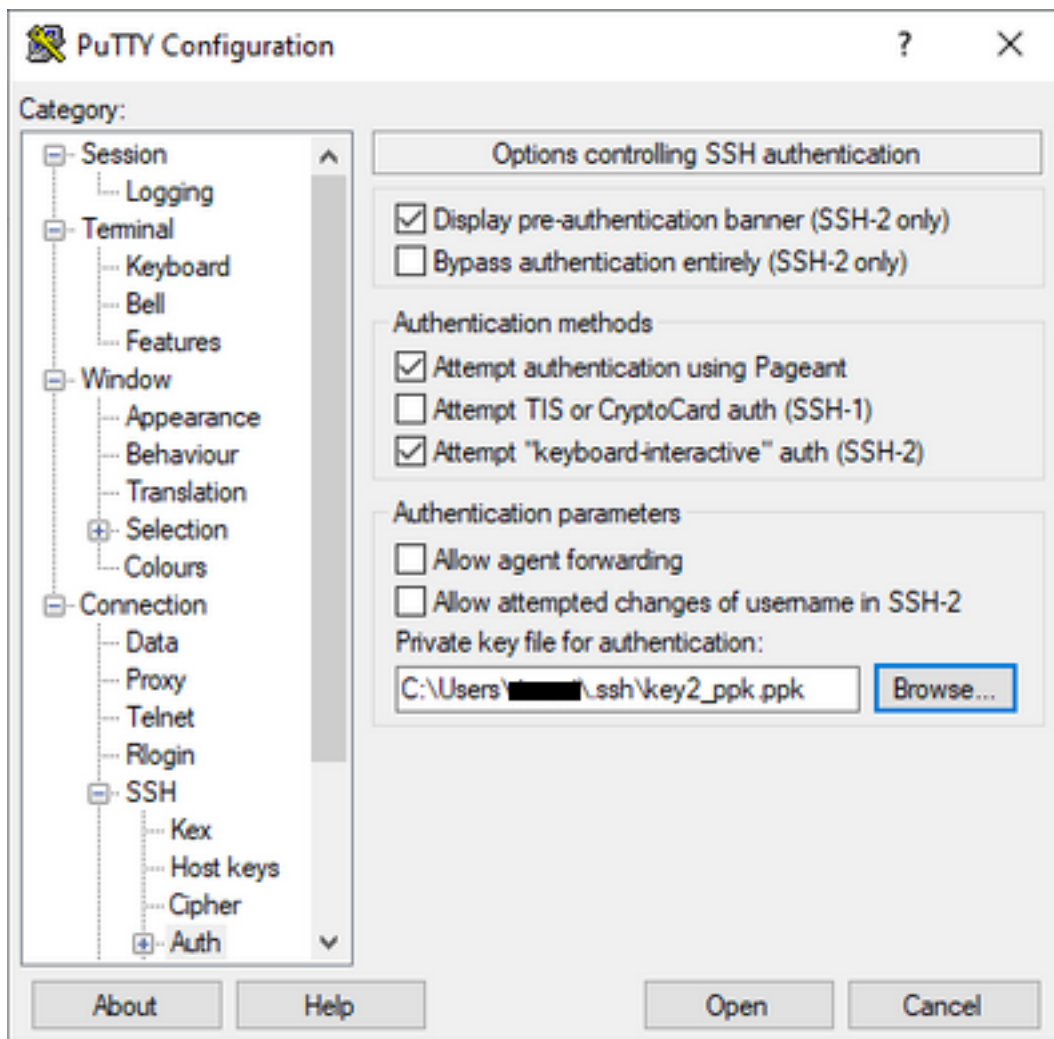
Pour plus d'informations, reportez-vous à [Convertir le fichier Pem en fichier Ppk à l'aide de PuTTYgen](#).

Une fois la clé privée générée au format approprié, vous devez spécifier le chemin dans Putty.

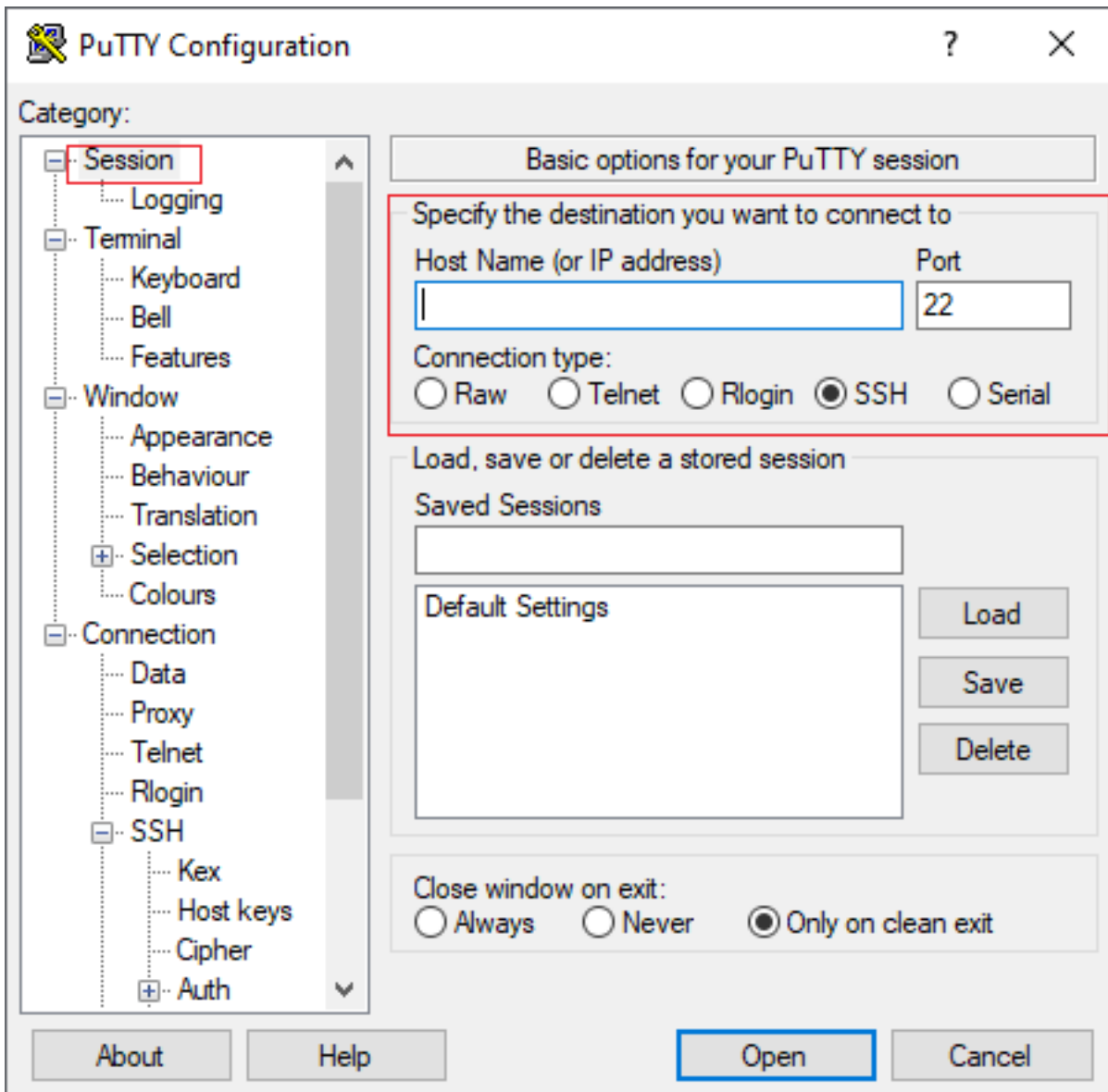
Sélectionnez le **fichier de clé privée pour l'authentification** dans l'option auth du menu **connexion** SSH.

Accédez au dossier dans lequel la clé est stockée et sélectionnez la clé créée. Dans cet exemple, les images montrent la vue graphique du menu Putty et l'état souhaité :





Une fois la clé appropriée sélectionnée, revenez au menu principal et utilisez l'adresse IP externe de l'instance CSR1000v pour vous connecter via SSH, comme illustré dans l'image.



Note: Le nom d'utilisateur/mot de passe défini dans les clés SSH générées sont requis pour se connecter.

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

```
csr-cisco#
```

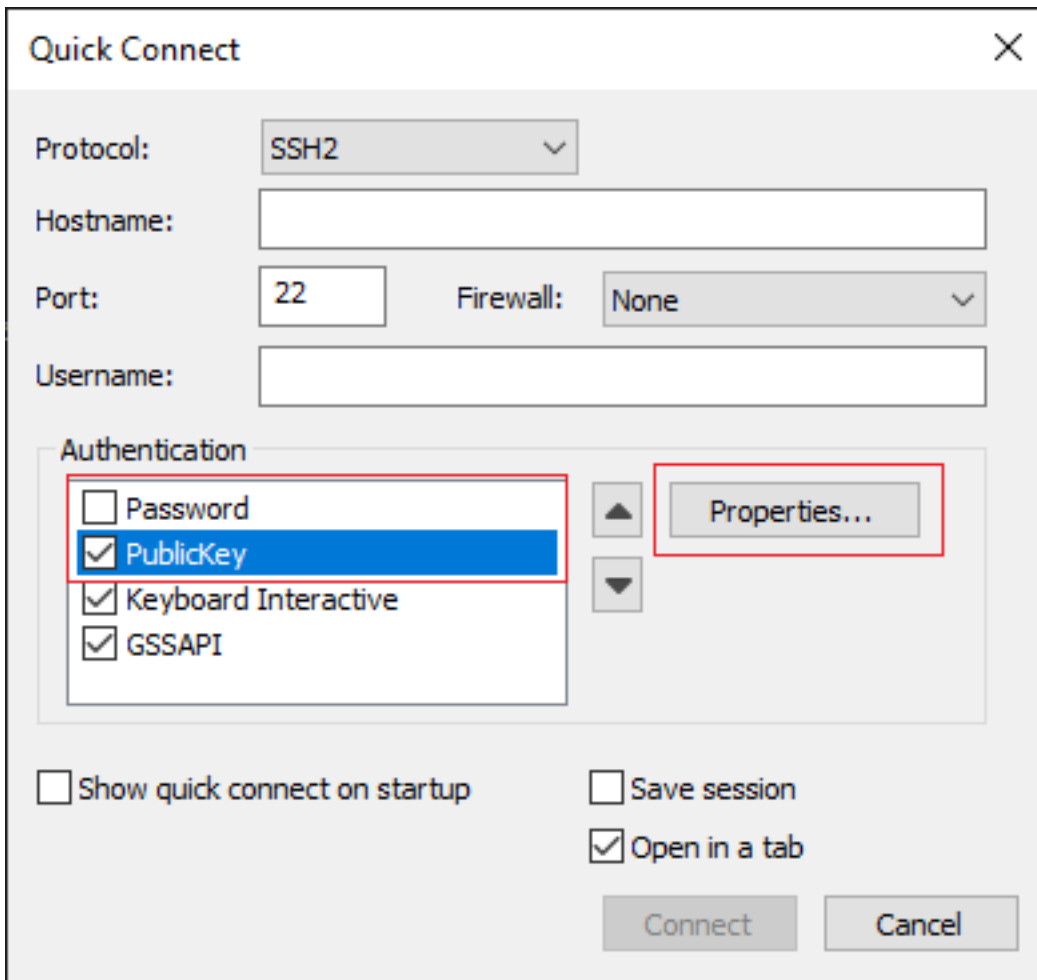
Connectez-vous à CSR1000v/C8000V avec SecureCRT

SecureCRT nécessite la clé privée au format PEM, qui est le format par défaut des clés privées.

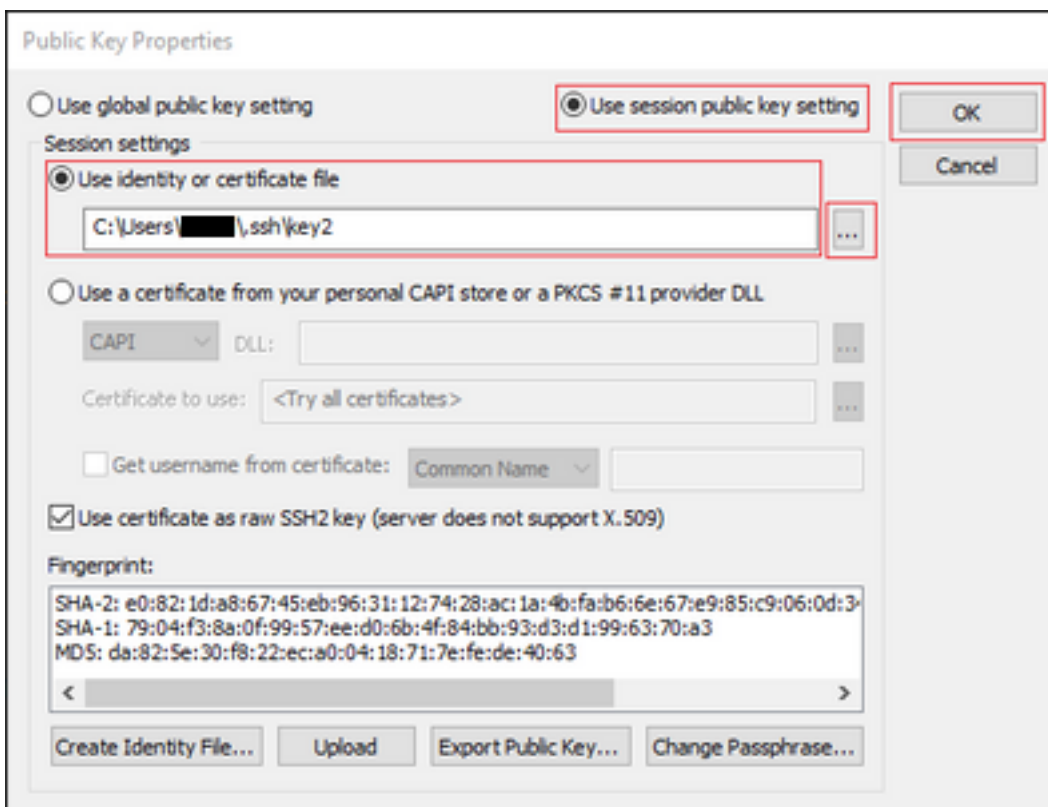
Dans SecureCRT, spécifiez le chemin d'accès à la clé privée dans le menu :

Fichier > Connexion rapide > Authentification > Décochez Mot de passe > Clé publique > Propriétés.

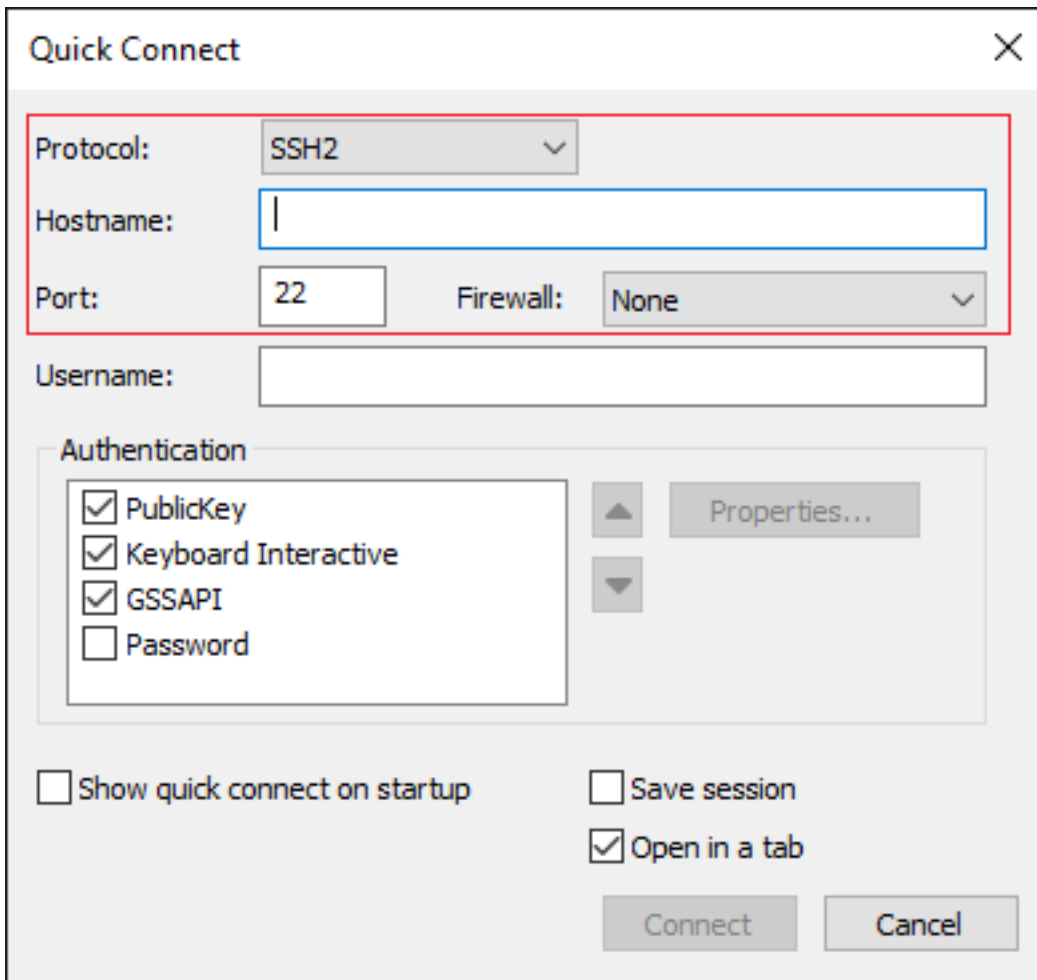
L'image montre la fenêtre attendue :



Sélectionnez **Utiliser la chaîne de clé publique de session** > Sélectionner **Utiliser le fichier d'identité ou de certificat** > Sélectionner ... bouton > Naviguez jusqu'au répertoire et sélectionnez la touche souhaitée > Sélectionnez **OK** comme indiqué dans l'image.



Enfin, connectez-vous à l'adresse IP externe de l'instance via SSH, comme illustré dans l'image.



Note: Le nom d'utilisateur/mot de passe défini dans les clés SSH générées sont requis pour se connecter.

```
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#
```

Méthodes de connexion de VM supplémentaires

Note: Reportez-vous à la section [Connexion aux machines virtuelles Linux à l'aide de la documentation des méthodes avancées](#).

Autoriser les utilisateurs supplémentaires à se connecter à CSR1000v/C8000v dans GCP

Une fois la connexion à l'instance CSR1000v réussie, il est possible de configurer d'autres utilisateurs avec les méthodes suivantes :

Configurer un nouveau nom d'utilisateur/mot de passe

Utilisez ces commandes pour configurer un nouvel utilisateur et un nouveau mot de passe :

```
enable
configure terminal
username <username> privilege <privilege level> secret <password>
end
```

Exemple :

```
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#
```

Un nouvel utilisateur peut désormais se connecter à l'instance CSR1000v/C8000v.

Configurer un nouvel utilisateur avec une clé SSH

Pour accéder à l'instance CSR1000v, configurez la clé publique. Les clés SSH des métadonnées d'instance ne fournissent pas d'accès à CSR1000v.

Utilisez ces commandes pour configurer un nouvel utilisateur avec une clé SSH :

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

Note: La longueur de ligne maximale au niveau de l'interface de ligne de commande Cisco est de 254 caractères. Par conséquent, la chaîne de clé peut ne pas correspondre à cette limite. Il est pratique d'envelopper la chaîne de clé pour qu'elle s'adapte à une ligne de terminal. Les détails sur la façon de surmonter cette limitation sont expliqués dans [Générer une clé SSH d'instance pour déployer un CSR1000v dans la plate-forme cloud de Google](#)

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRlcvSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlks3PCVGotW1HxxTU4
FCkmeAg4NEqMVLsm26nLvrNK6z7lRmcIKZZcST+SL6lQv33gkUKIoGB9qx/+DlRvurVXfCdq
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/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlk
csr-cisco(conf-ssh-pubkey-
data)#s3PCVGOTw1HxxTU4FCkmEAg4NEqMVLsm26nLvrNK6z71RmcIKZZcST+SL6lQv33gkUKI
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#

```

Vérification des utilisateurs configurés lors de la connexion à CSR1000v/C8000v

Afin de confirmer que la configuration a été correctement définie, connectez-vous avec les informations d'identification créées ou avec la paire de clés privées pour la clé publique avec les informations d'identification supplémentaires.

Du côté du routeur, consultez le journal de connexion réussi avec l'adresse IP du terminal.

```

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#

```

Dépannage

Si le message d'erreur « Opération expirée » s'affiche.

```

$ ssh -i CSR-sshkey <snip>@X.X.X.X
ssh: connect to host <snip> port 22: Operation timed out

```

Causes possibles:

- L'instance n'a pas terminé son déploiement.
- L'adresse publique n'est pas celle affectée à nic0 dans la machine virtuelle.

Solution :

Attendez la fin du déploiement de la machine virtuelle. En règle générale, un déploiement CSR1000v prend jusqu'à 5 minutes.

Si un mot de passe est requis

Si un mot de passe est requis :

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

```
Password:
```

```
Password:
```

Cause possible:

- Le nom d'utilisateur ou la clé privée est incorrect.

Solution :

- Assurez-vous que le nom d'utilisateur est identique à celui spécifié lors du déploiement de CSR1000v/C8000v.
- Assurez-vous que la clé privée est la même que celle que vous avez incluse au moment du déploiement.

Informations connexes

- [Fiche technique du routeur de services cloud Cisco 1000v](#)
- [Support et documentation techniques - Cisco Systems](#)