Déployer un CSR1000v/C8000v sur la plate-forme cloud Google

Table des matières

Introduction

Ce document décrit la procédure pour déployer et configurer un Cisco CSR1000v et un Catalyst 8000v (C800v) sur Google Cloud Platform (GCP).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Technologies de virtualisation / Machines virtuelles (VM)

- Plates-formes cloud

Composants utilisés

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

- Un abonnement actif à Google Cloud Platform avec un projet créé
- console GCP
- marché des BPC
- 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 routeur CSR1000v devient C8000v avec les mêmes fonctionnalités, mais de nouvelles fonctionnalités ont été ajoutées, telles que SD-WAN et la licence Cisco DNA. Pour plus d'informations, veuillez consulter 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

Remarque : au moment de la rédaction de ce document, les nouveaux utilisateurs disposent de 300 USD de crédits gratuits pour explorer pleinement GCP en tant que niveau gratuit pendant un an. Ceci est défini par Google et ne relève pas du 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 Google Cloud Platform

Étape 1. Assurez-vous qu'un projet valide et actif est associé au compte.

Assurez-vous que votre compte dispose d'un projet valide et actif, ceux-ci doivent être associés à

un groupe avec des autorisations pour le moteur de calcul.

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

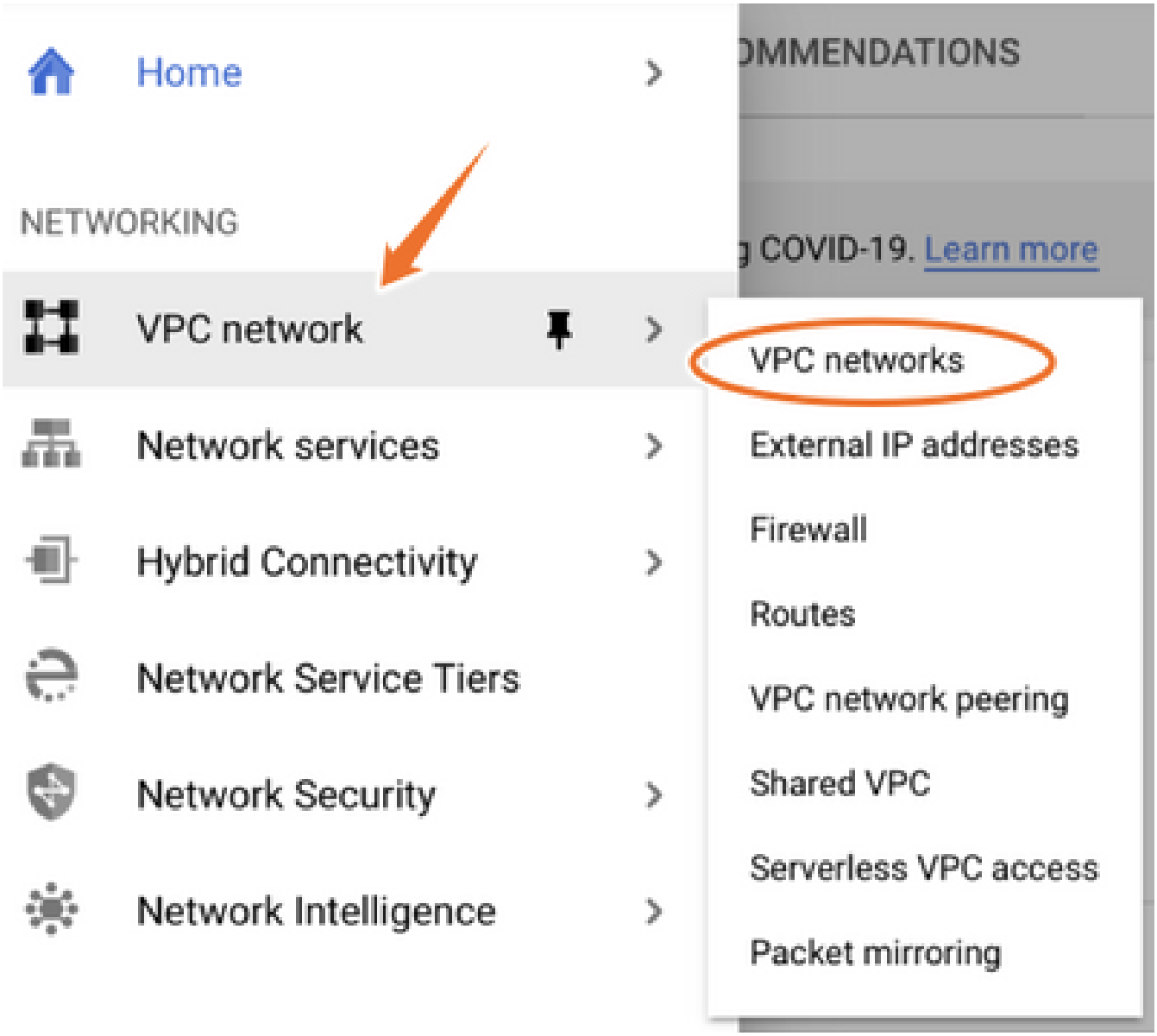
Remarque : pour créer un nouveau projet, reportez-vous à la section Créer et gérer des projets.

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

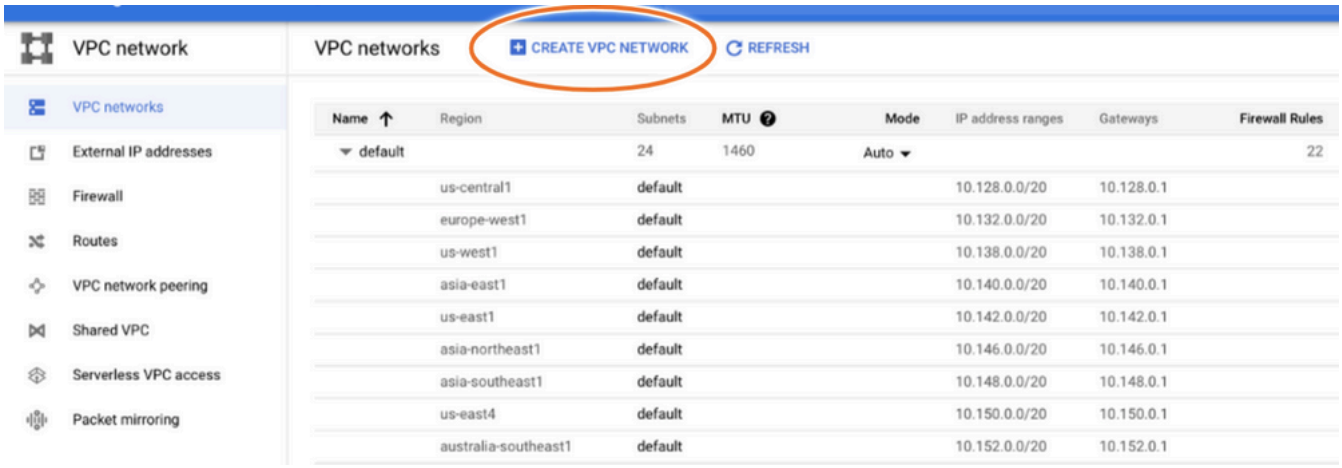
Créez un nouveau cloud privé virtuel (VPC) et un sous-réseau qui doivent être associés à l'instance CSR1000v.

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 VPC network > VPC networks comme illustré dans l'image.

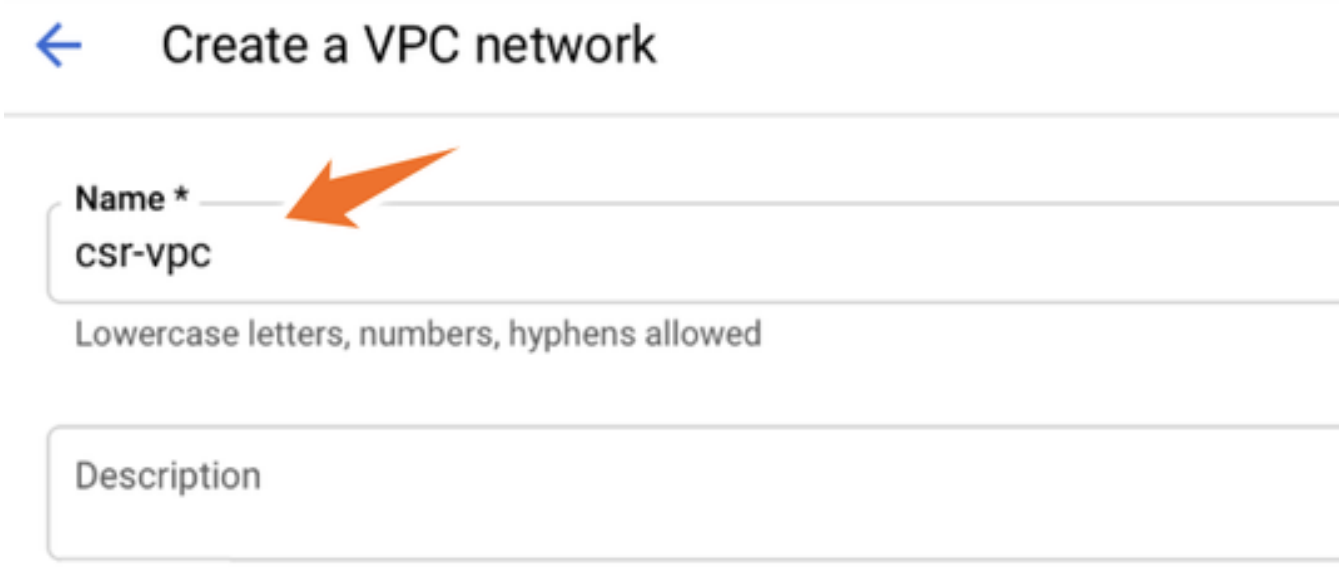


Sélectionnez Create VPC Network comme indiqué dans l'image.



Remarque : actuellement, CSR1000v est uniquement déployé dans la région centrale des États-Unis sur GCP.

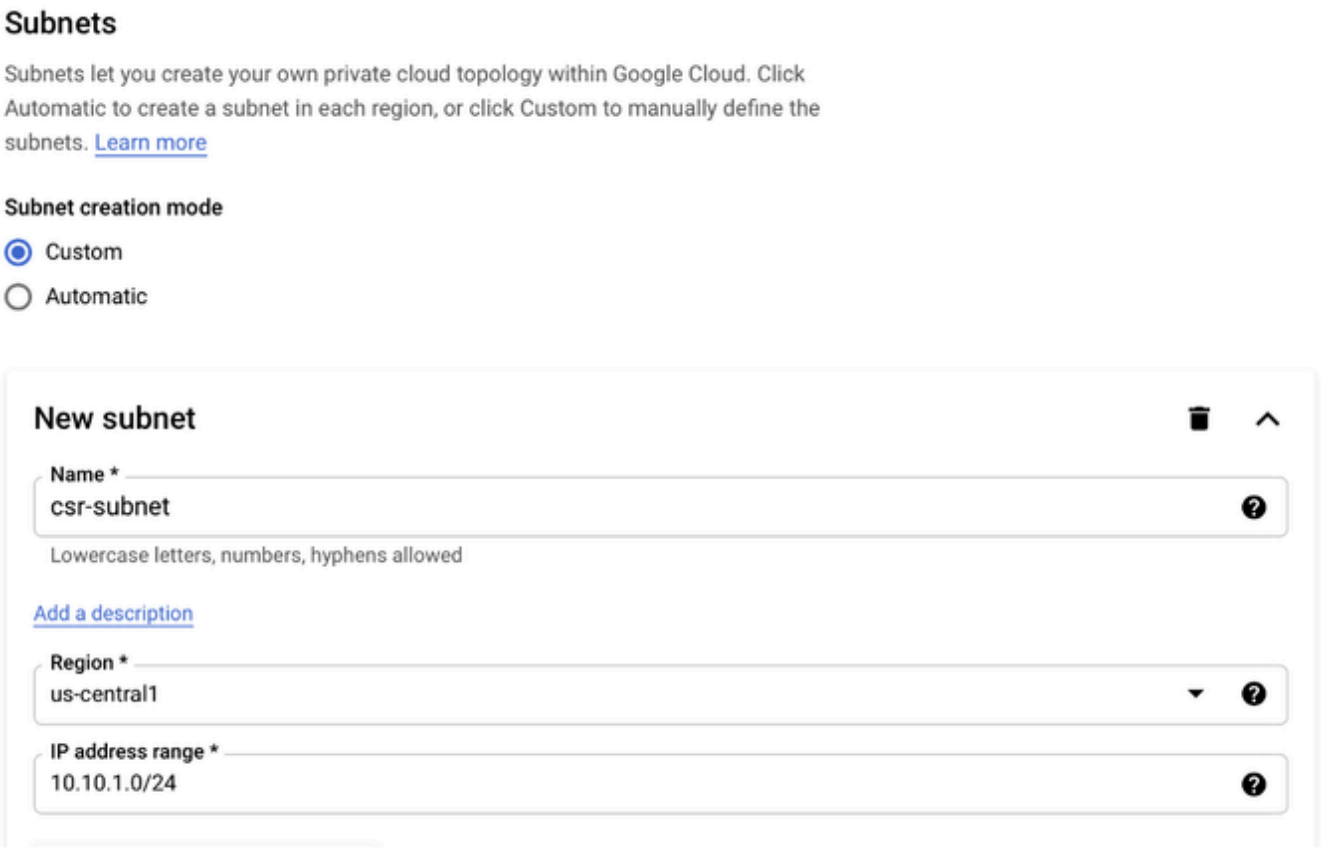
Configurez le nom du VPC comme indiqué dans l'image.



Configurez le nom de sous-réseau associé au VPC et sélectionnez region us-central1.

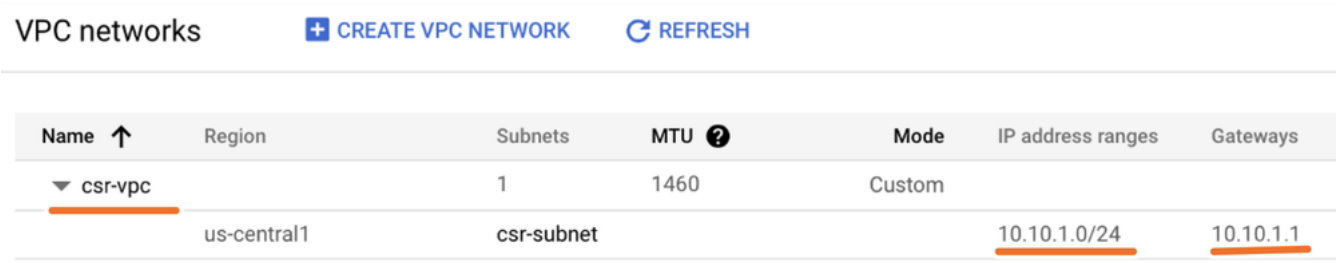
Attribuez une plage d’adresses IP valide dans le CIDR us-central1 de 10.128.0.0/20. comme illustré dans l’image.

Conservez les autres paramètres par défaut et sélectionnez le bouton Créer :



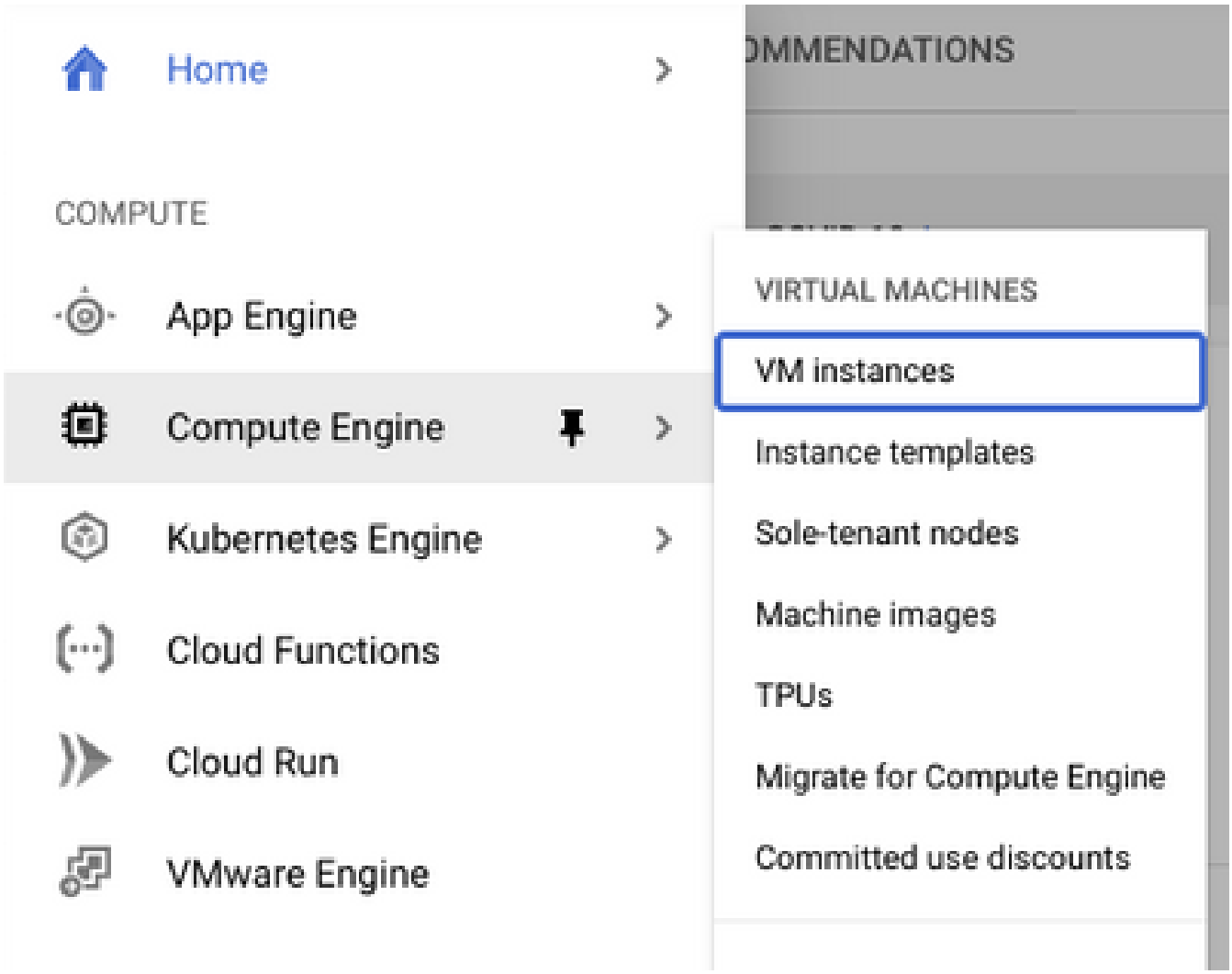
Remarque : si l'option Automatique est sélectionnée, GCP attribue automatiquement une plage valide dans la région CIDR.

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

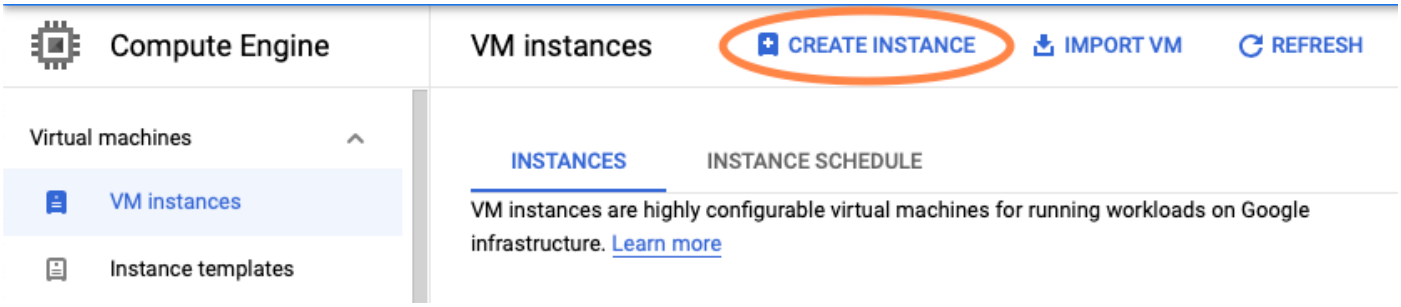


Étape 3. Déploiement d'instance virtuelle.

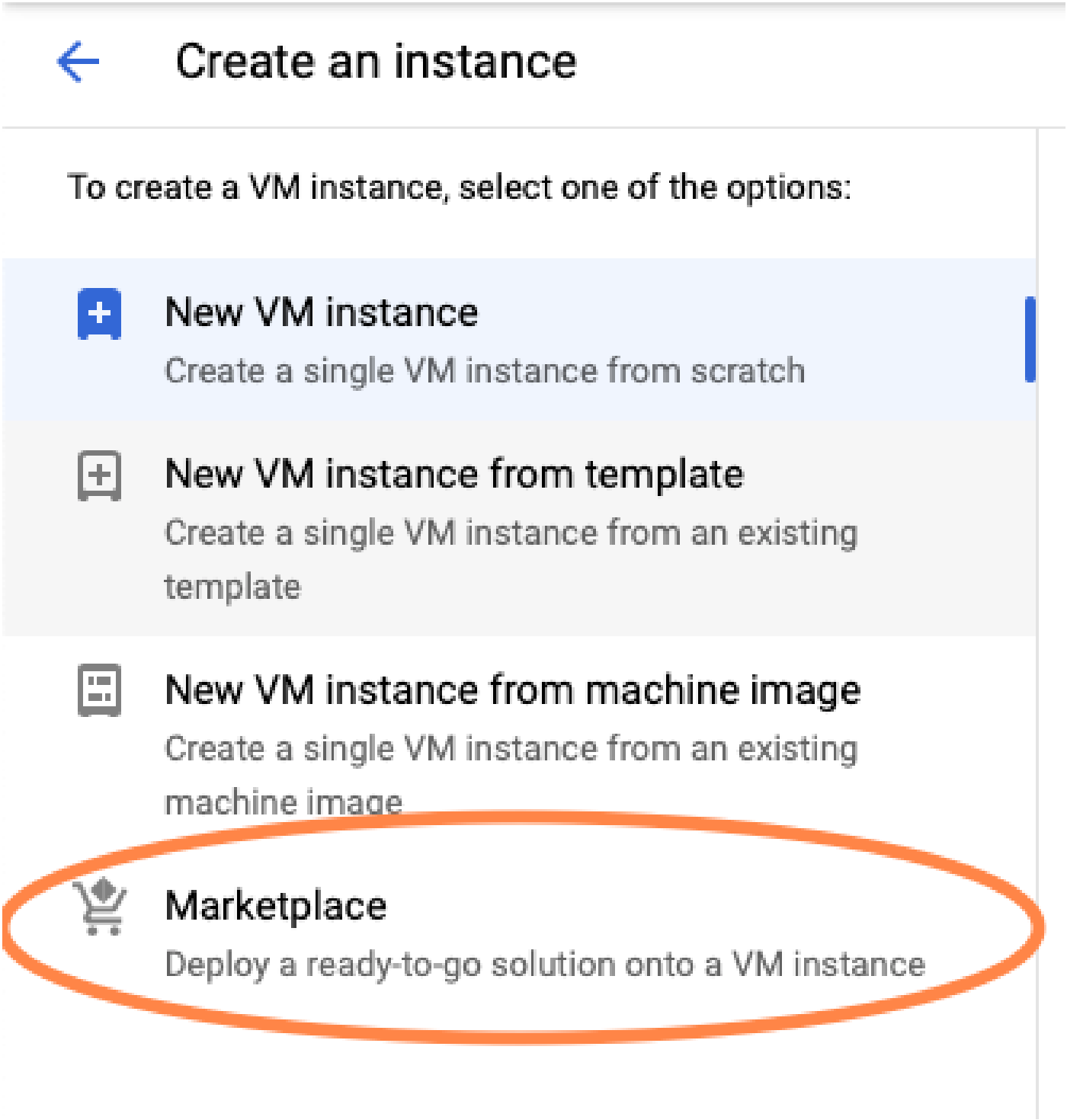
Dans la section Moteur de calcul, sélectionnez Moteur de calcul > Instances de VM comme indiqué dans l'image.



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



Utilisez la place de marché GCP comme illustré dans l'image, afin d'afficher les produits Cisco.



Dans la barre de recherche, tapez Cisco CSR ou Catalyst C8000v, choisissez le modèle et la version qui correspondent à vos besoins et sélectionnez Launch.

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

Marketplace

csr 1000v

Marketplace > "csr 1000v" > Virtual machines

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 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 - 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

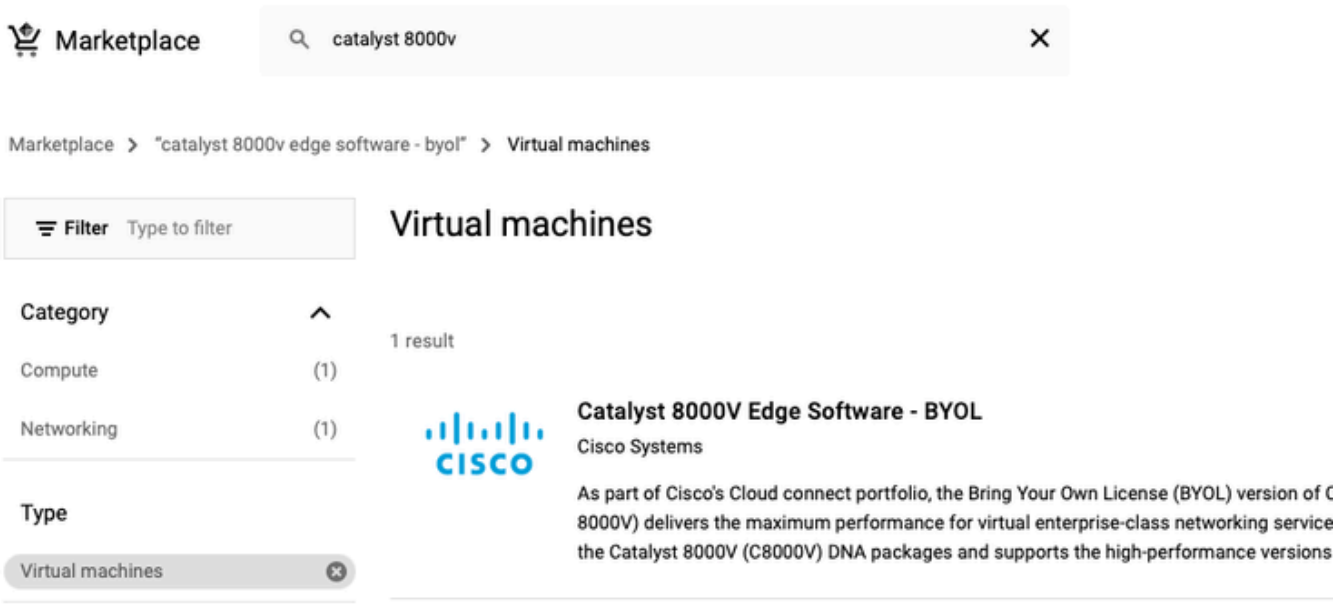
Cisco Systems

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. Th
enables enterprise IT to deploy the same enterprise-class networking services in the cloud th

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. Th
enables enterprise IT to deploy the same enterprise-class networking services in the cloud th

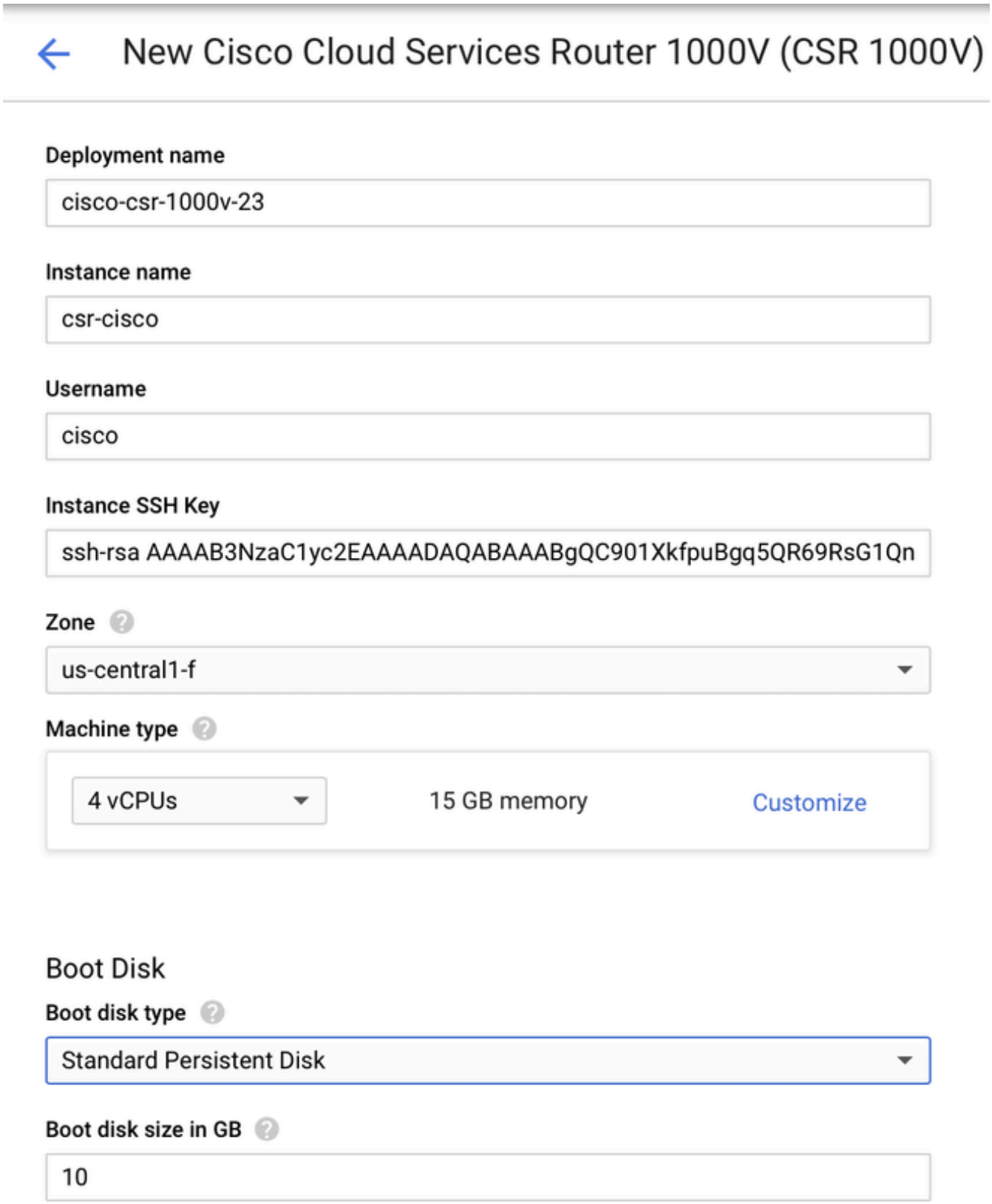


Remarque : BYOL signifie « Bring Your Own License » (Apportez votre propre licence).

Remarque : Actuellement, GCP ne prend pas en charge le modèle de paiement à l'utilisation (PAYG).

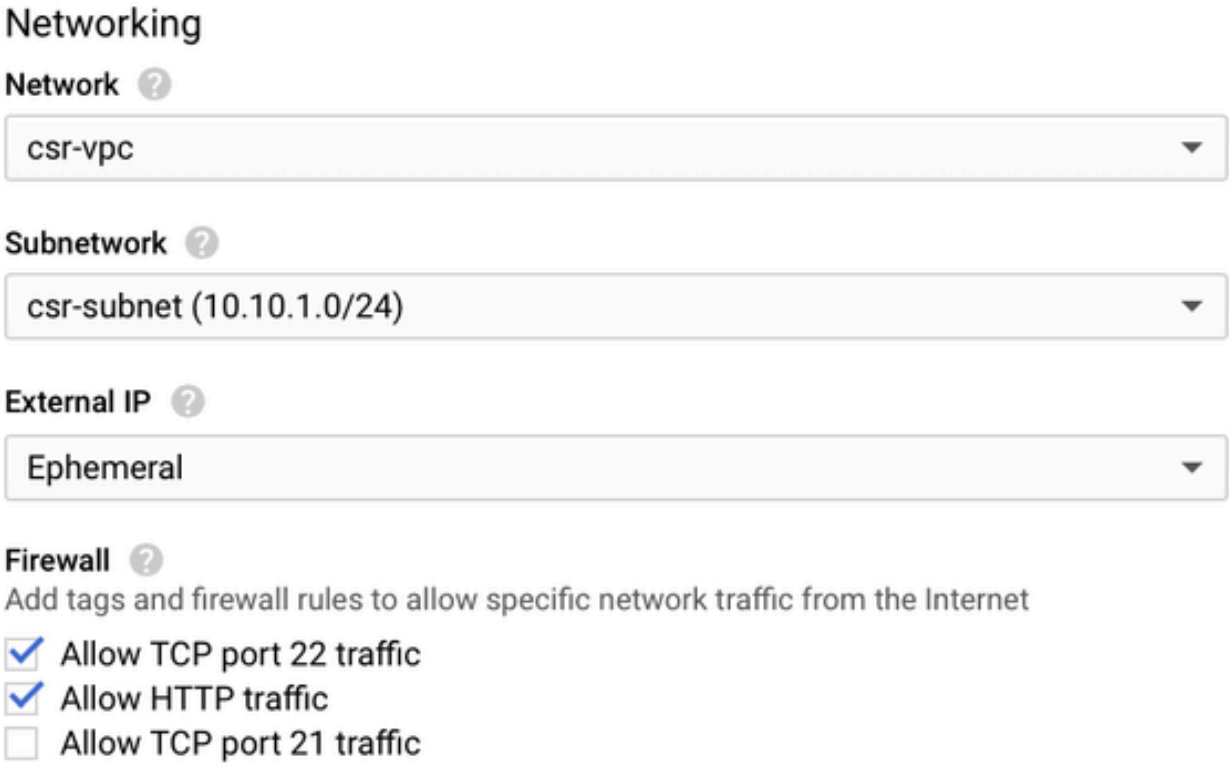
Le protocole GCP nécessite d'entrer les valeurs de configuration qui doivent être associées à la machine virtuelle, comme indiqué dans l'image :

Un nom d'utilisateur et une clé publique SSH sont requis pour déployer un CSR1000v/C8000v dans GCP, comme illustré dans l'image. Veuillez vous reporter à Générer une clé SSH d'instance pour déployer un CSR1000v dans Google Cloud Platform si les clés SSH n'ont pas été créées.



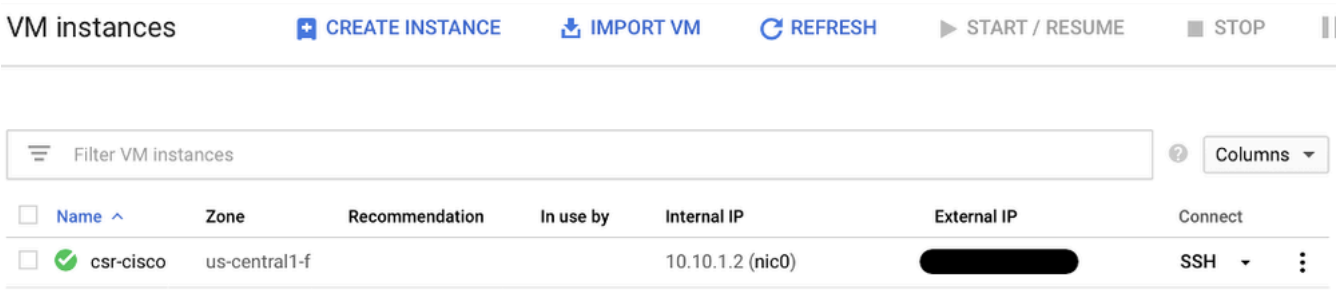
Sélectionnez le VPC et le sous-réseau créés avant et choisissez Ephémère dans l'IP externe, afin d'avoir une IP publique associée à l'instance comme indiqué dans l'image.

Une fois cette configuration terminée. Sélectionnez le bouton de lancement.



Remarque : 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 Compute Engine > VM instances afin de vérifier que le nouveau CSR1000v a été déployé avec succès comme indiqué dans l'image.



Vérifier le déploiement

Connexion 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 nécessaire 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 :

<#root>

ssh -i private-key-path username@publicIPaddress

Exemple :

<#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:c3JsVDEt68CeUFGhp9lrYz7tUO7htbsPhAwanh3feC4.
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

<#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, RELEA
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.

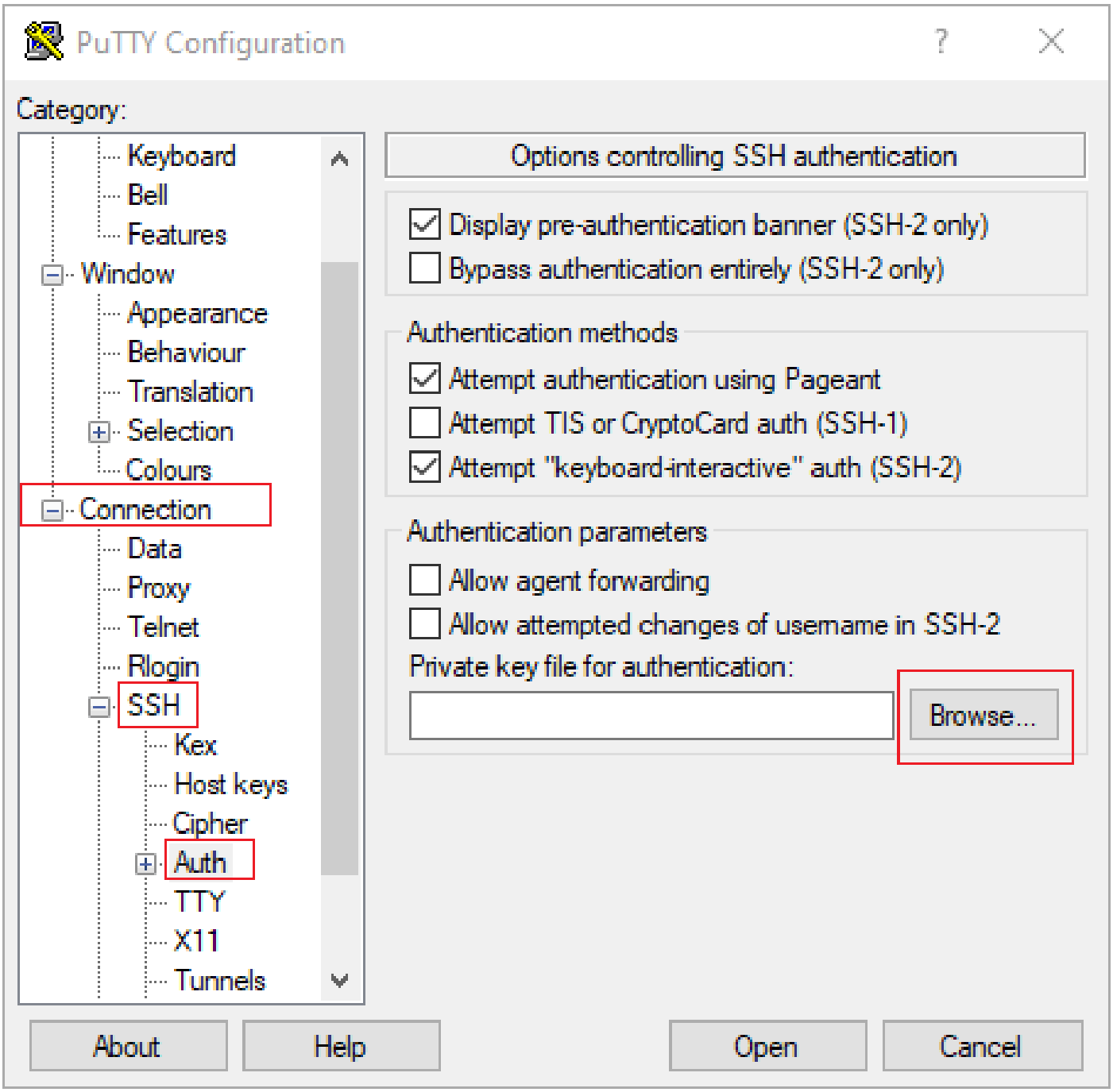
Pour plus d'informations, reportez-vous à Convert Pem to Ppk File Using PuTTYgen.

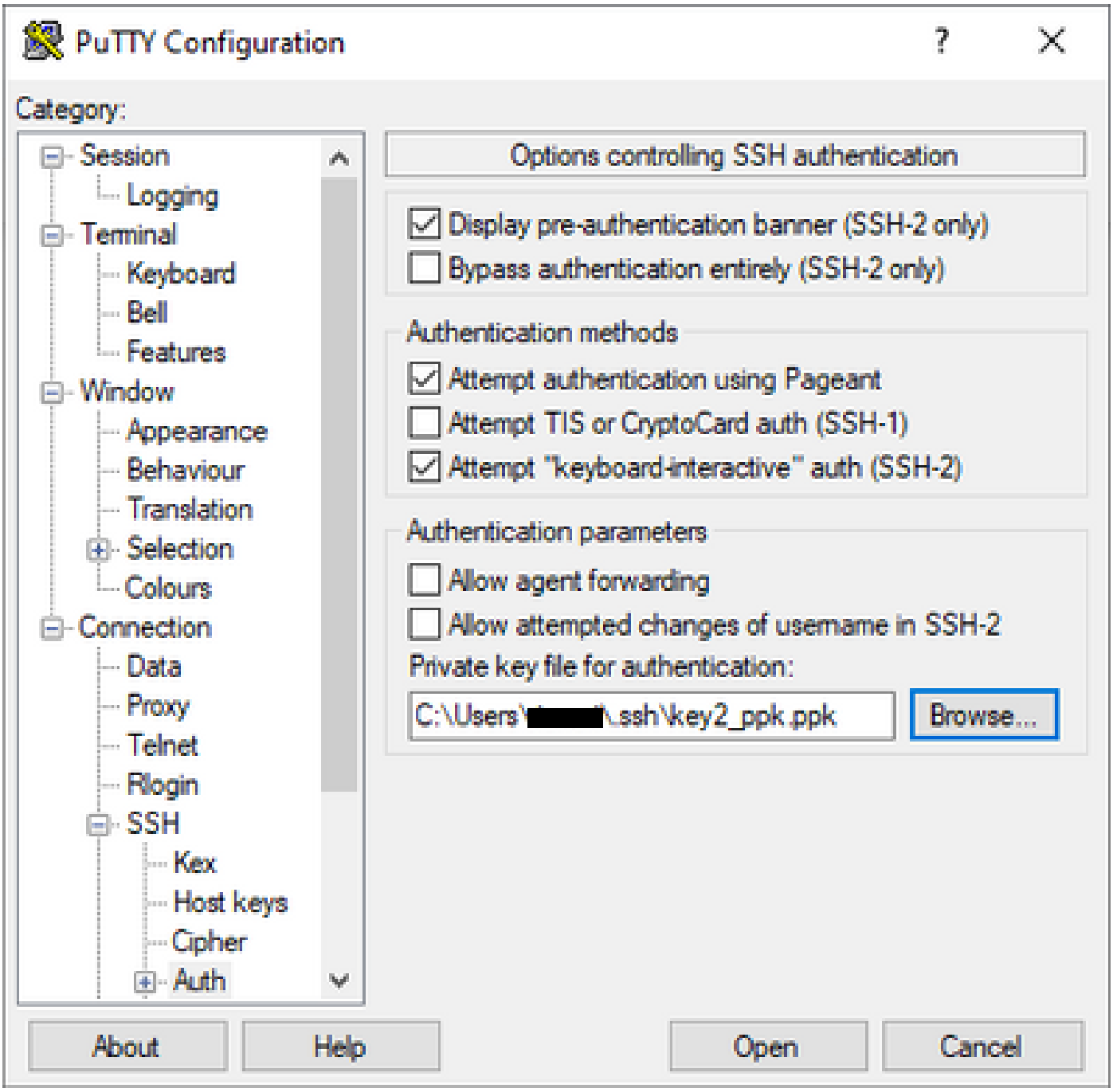
Une fois que la clé privée est générée dans le format approprié, vous devez spécifier le chemin dans Putty.

Sélectionnez la section Fichier de clé privée pour l'authentification dans l'option auth du menu de connexion SSH.

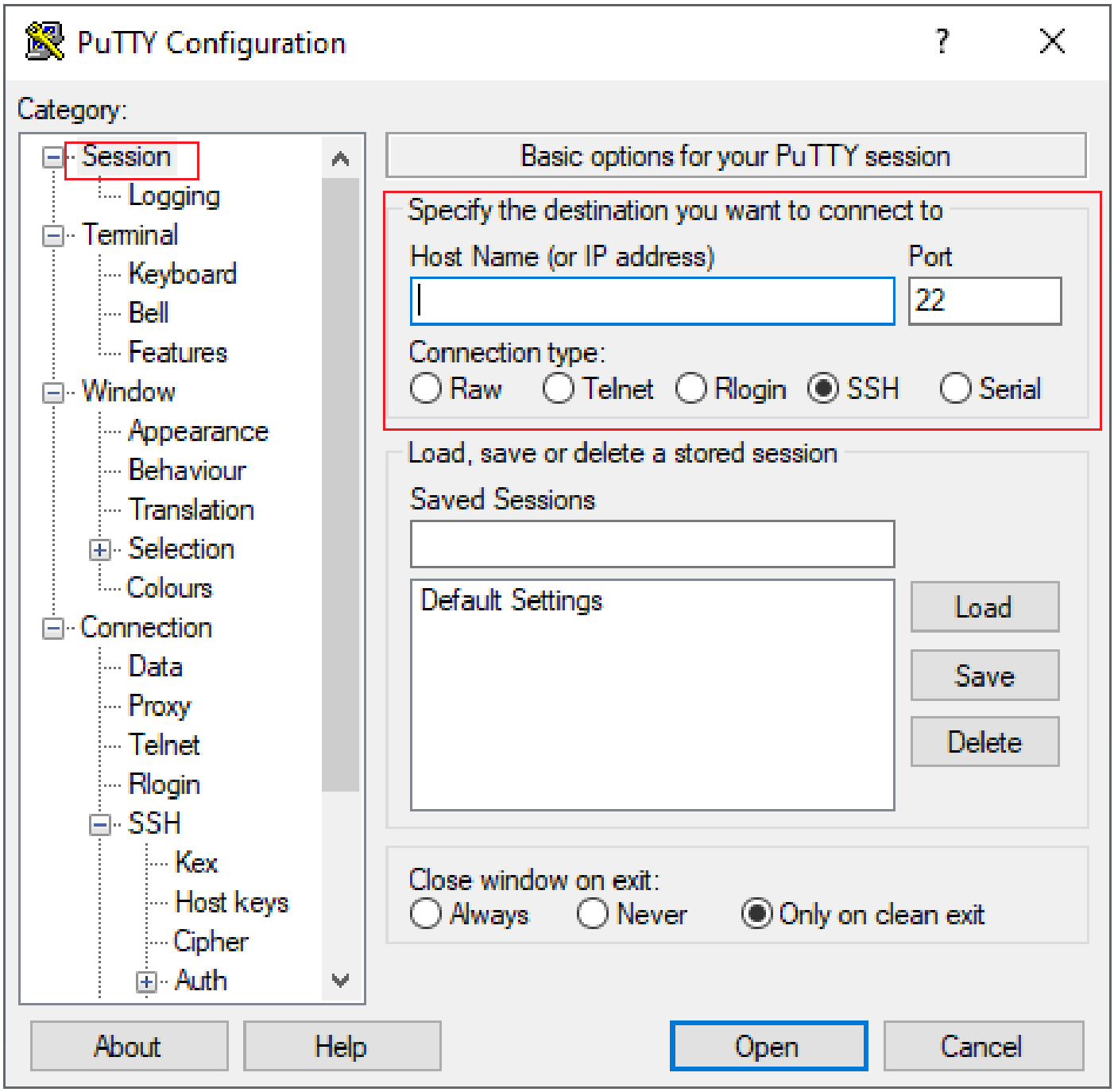
Accédez au dossier dans lequel la clé est stockée et sélectionnez la clé créée. Dans cet exemple,

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.



Remarque : le nom d'utilisateur/mot de passe défini dans les clés SSH générées est demandé pour se connecter.

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

csr-cisco#
```

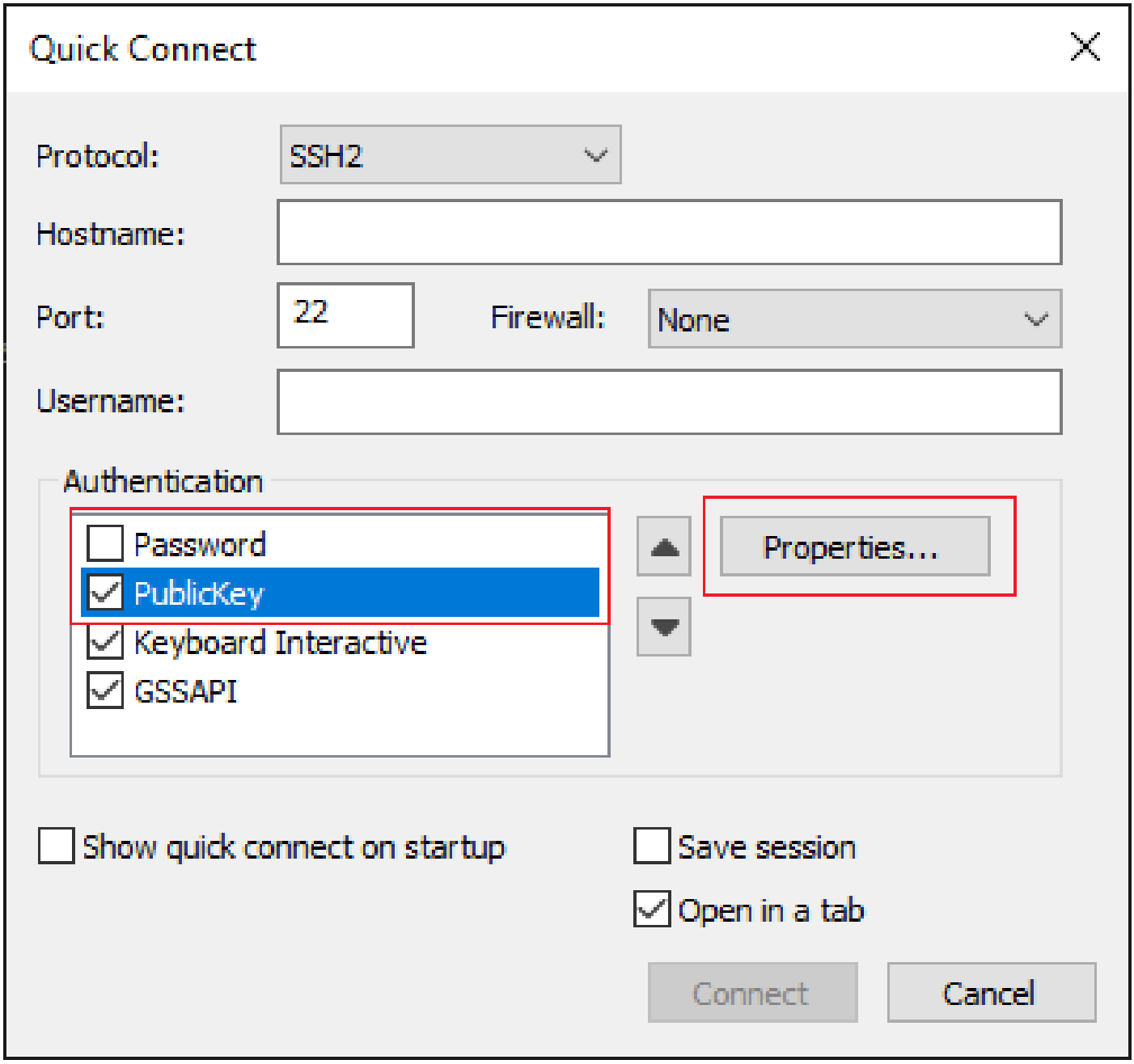
Connectez-vous à CSR1000v/C8000V avec SecureCRT

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

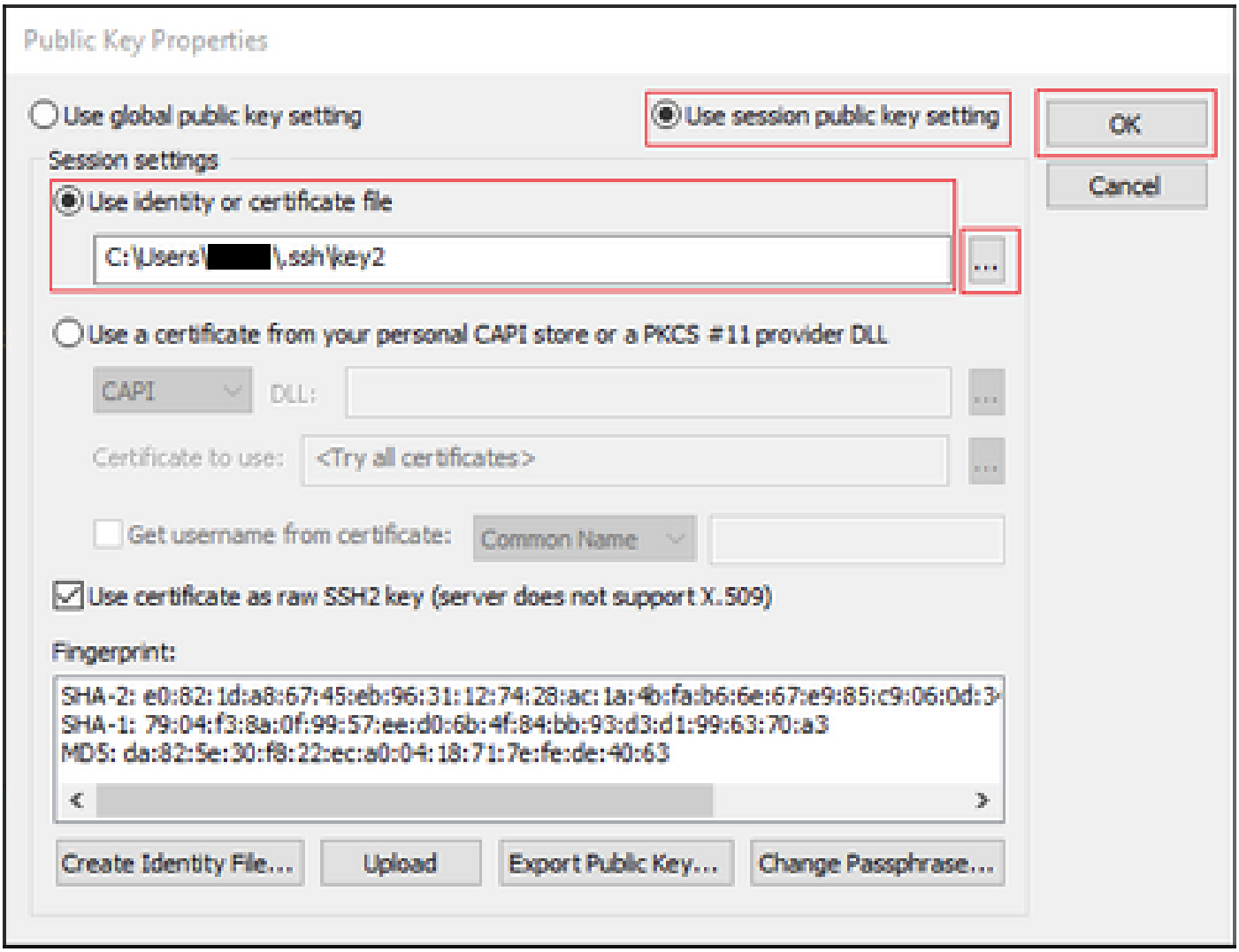
Dans SecureCRT, spécifiez le chemin d'accès à la clé privée dans le menu :

Fichier > Connexion rapide > Authentification > Désactiver le mot de passe > Clé publique > Propriétés.

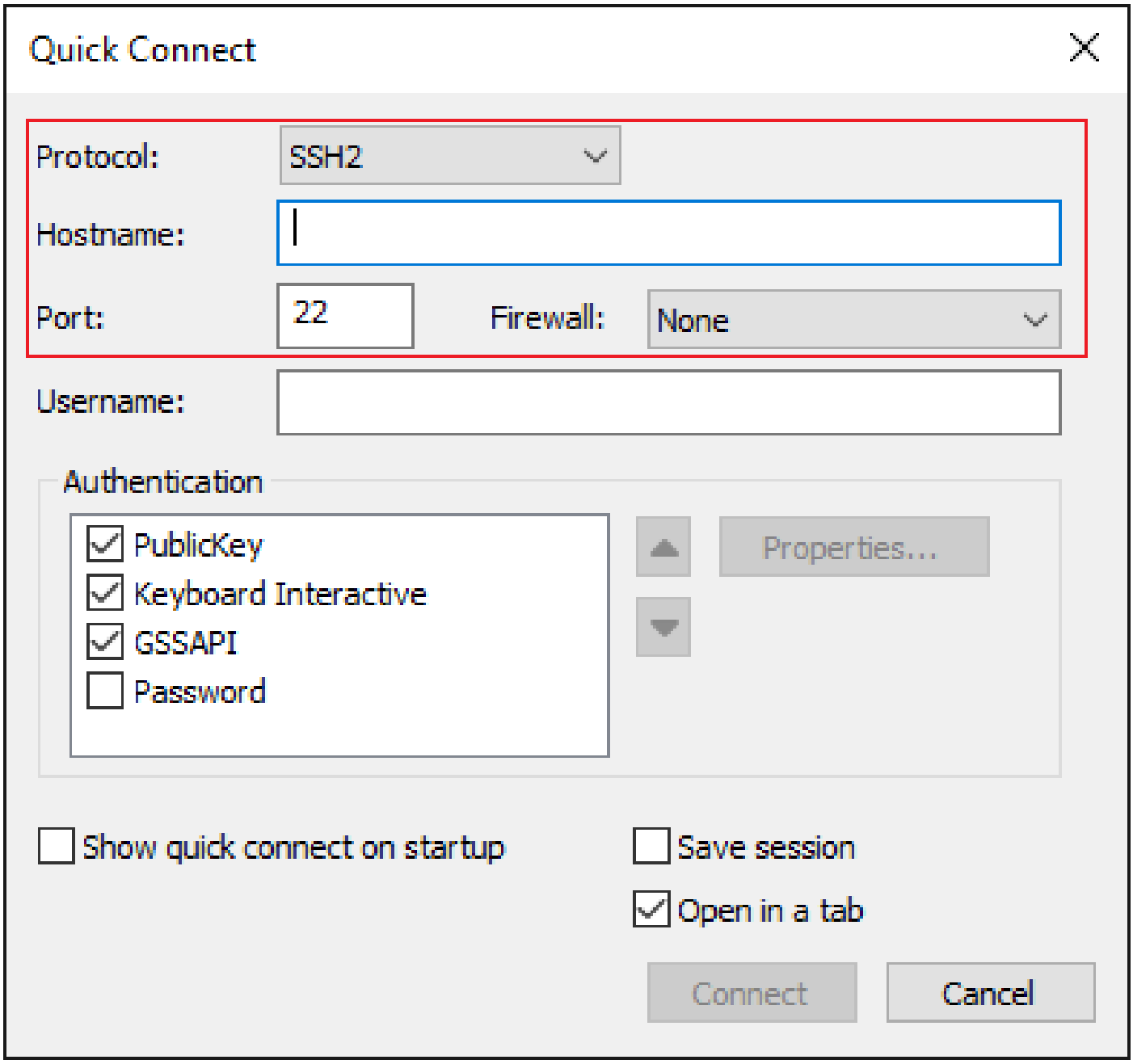
L'image présente la fenêtre attendue :



Sélectionnez Use session public key string > Select Use identity or certificate file > Select ... button > Naviguez jusqu'au répertoire et sélectionnez la clé souhaitée > Select OK comme indiqué dans l'image.



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



Remarque : le nom d'utilisateur/mot de passe défini dans les clés SSH générées est demandé pour se connecter.

<#root>

```
csr-cisco#
```

```
show logging
```

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

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] [loca
```

```
csr-cisco#
```

Méthodes de connexion VM supplémentaires

Remarque : reportez-vous à la documentation Connect to Linux VMs using advanced methods.

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

Une fois connecté à l'instance CSR1000v, il est possible de configurer des utilisateurs supplémentaires 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 :

<#root>

```
enable
```

```
configure terminal
```

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

```
end
```

Exemple :

<#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#
```

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

Configurer un nouvel utilisateur avec une clé SSH

Afin d'obtenir l'accès à l'instance de CSR1000v, configurez la clé publique. Les clés SSH dans les métadonnées d'instance ne fournissent pas d'accès à CSR1000v.

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

<#root>

```
configure terminal

ip ssh pubkey-chain

username <username>

key-string

<public ssh key>

exit

end
```

Remarque : la longueur de ligne maximale de l'interface de ligne de commande Cisco est de 254 caractères. Par conséquent, la chaîne de clé ne peut pas être adaptée à cette limite. Il est donc pratique d'envelopper la chaîne de clé pour qu'elle corresponde 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 Google Cloud Platform

---

<#root>

```
$

fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDldzZ/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 AAAAB3NzaC1yc2EAAAADAQABAAABAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC

csr-cisco(conf-ssh-pubkey-data)#
6vkCn29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv28l

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)#
s3PCVGOtW1HxxTU4FCkmEAg4NEqMVLSm26nLvrNK6z7lRMcIKZZcST+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, veuillez vous connecter 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 avec succès avec l'adresse IP du terminal.

```
<#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 disabl

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

Dépannage

Si le message d'erreur « Operation Timed Out » s'affiche.

```
<#root>

$

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 attribuée à nic0 dans la machine virtuelle.

Solution :

Attendez la fin du déploiement de la VM. Généralement, un déploiement CSR1000v prend jusqu'à 5 minutes.

Si un mot de passe est requis

Si un mot de passe est requis :

```
<#root>

$

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


Password:
Password:
```

Cause possible:

- Le nom d'utilisateur ou la clé privée est incorrect.
- Sur les versions plus récentes des systèmes d'exploitation comme MacOS ou Linux, l'utilitaire OpenSSH n'a pas activé RSA par défaut.

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 identique à celle que vous avez incluse au moment du déploiement.
- Spécifiez le type de clé acceptée dans la commande ssh :

```
<#root>

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

Informations connexes

- Fiche technique du routeur de services cloud Cisco 1000v
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.