

# Bereitstellung eines CSR1000v/C8000v auf der Google Cloud-Plattform

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Projekteinrichtung](#)

[Schritt 1: Stellen Sie ein gültiges und aktives Projekt für das Konto sicher.](#)

[Schritt 2: Erstellen Sie einen neuen VPC und ein neues Subnetz.](#)

[Schritt 3: Bereitstellung virtueller Instanzen.](#)

[Bereitstellung überprüfen](#)

[Remote-Verbindung zur neuen Instanz](#)

[Anmeldung bei CSR1000v/C8000v mit Bash Terminal](#)

[Anmeldung bei CSR1000v/C8000v mit PuTTY](#)

[Anmeldung bei CSR1000v/C8000V mit SecureCRT](#)

[Zusätzliche VM-Anmeldungsmethoden](#)

[Autorisieren zusätzlicher Benutzer für die Anmeldung bei CSR1000v/C8000v in GCP](#)

[Neuen Benutzernamen/Kennwort konfigurieren](#)

[Konfigurieren eines neuen Benutzers mit SSH-Schlüssel](#)

[Überprüfung der konfigurierten Benutzer bei der Anmeldung bei CSR1000v/C8000v](#)

[Fehlerbehebung](#)

[Wenn die Fehlermeldung "Operation timed out" \(Vorgang ist abgelaufen\) angezeigt wird.](#)

[Wenn ein Kennwort erforderlich ist](#)

[Zugehörige Informationen](#)

## Einleitung

Dieses Dokument beschreibt das Verfahren zur Bereitstellung und Konfiguration eines Cisco Cloud Services Router 1000v (CSR1000v) und Catalyst 8000v (C800v) Edge Router auf der Google Cloud-Plattform (GCP).

Unterstützt von Eric Garcia, Ricardo Neri, Cisco TAC Engineers.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Virtualisierungstechnologien/virtuelle Systeme (VMs)

- Cloud-Plattformen

## Verwendete Komponenten

- Ein aktives Abonnement für Google Cloud Platform mit einem erstellten Projekt
- GCP-Konsole
- GCP-Marktplatz
- Bash Terminal, Putty oder SecureCRT
- Public und Private Secure Shell (SSH)-Schlüssel

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Ab dem 17.4.1 wird der CSR1000v zum C8000v mit derselben Funktionalität, aber neuen Funktionen wie SDWAN und DNA-Lizenzierung hinzugefügt. Weitere Informationen finden Sie im offiziellen Produktdatenblatt:

[Cisco Cloud Services Router 1000v - Datenblatt](#)

[Datenblatt zur Cisco Catalyst 8000V Edge-Software](#)

Daher ist dieses Handbuch für die Installation von CSR1000v- und C8000v-Routern geeignet.

## Projekteinrichtung

**Anmerkung:** Derzeit ist dieses Dokument geschrieben, neue Benutzer haben 300 USD an kostenlosen Credits, um GCP als Freier Tier für ein Jahr vollständig zu erkunden. Dies wird von Google definiert und unterliegt nicht der Kontrolle von Cisco.

**Hinweis:** In diesem Dokument müssen öffentliche und private SSH-Schlüssel erstellt werden. Weitere Informationen finden Sie unter [Generate an Instance SSH Key to Deploy a CSR1000v in Google Cloud Platform](#)

### Schritt 1: Stellen Sie ein gültiges und aktives Projekt für das Konto sicher.

Stellen Sie sicher, dass Ihr Konto über ein gültiges und aktives Projekt verfügt. Diese müssen einer Gruppe mit Berechtigungen für Compute Engine zugeordnet sein.

Für diese Beispielbereitstellung wird ein im GCP erstelltes Projekt verwendet.

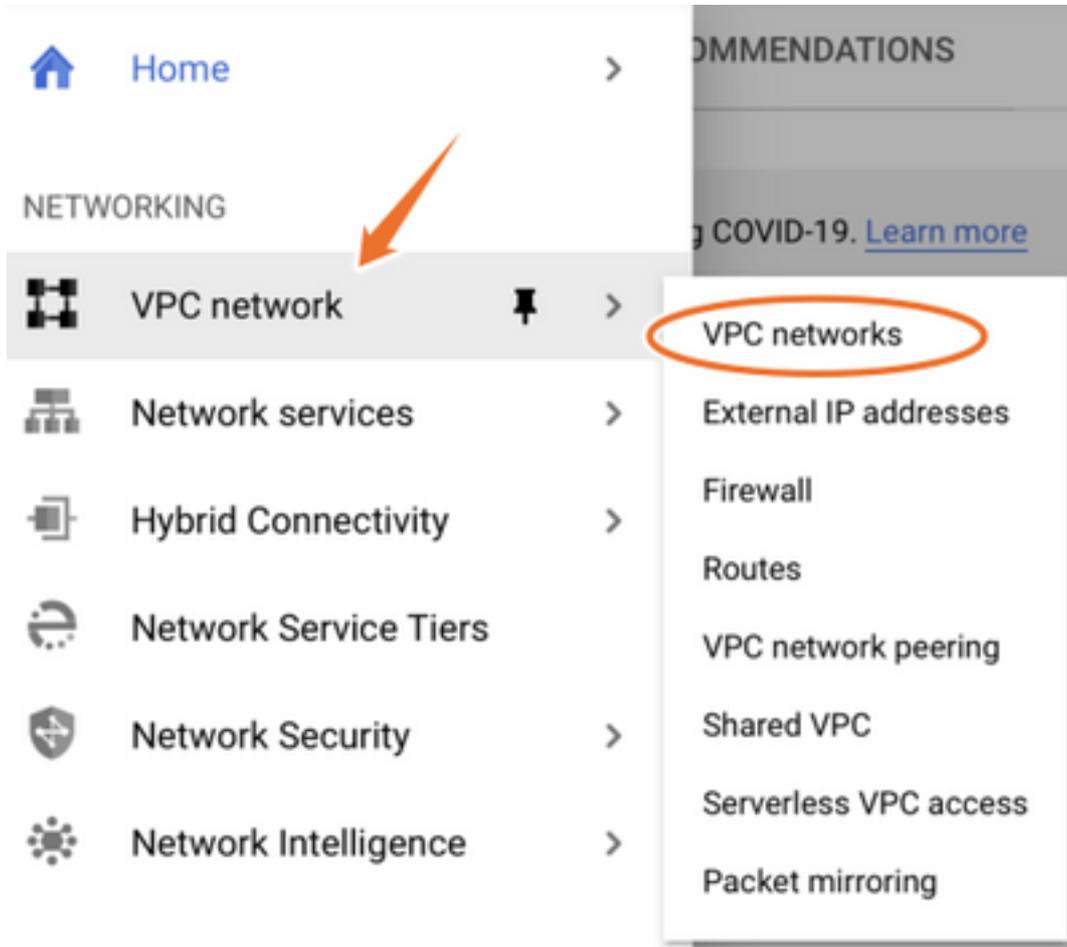
**Anmerkung:** Informationen zum Erstellen eines neuen Projekts finden Sie unter [Erstellen und Verwalten von Projekten](#).

## Schritt 2: Erstellen Sie einen neuen VPC und ein neues Subnetz.

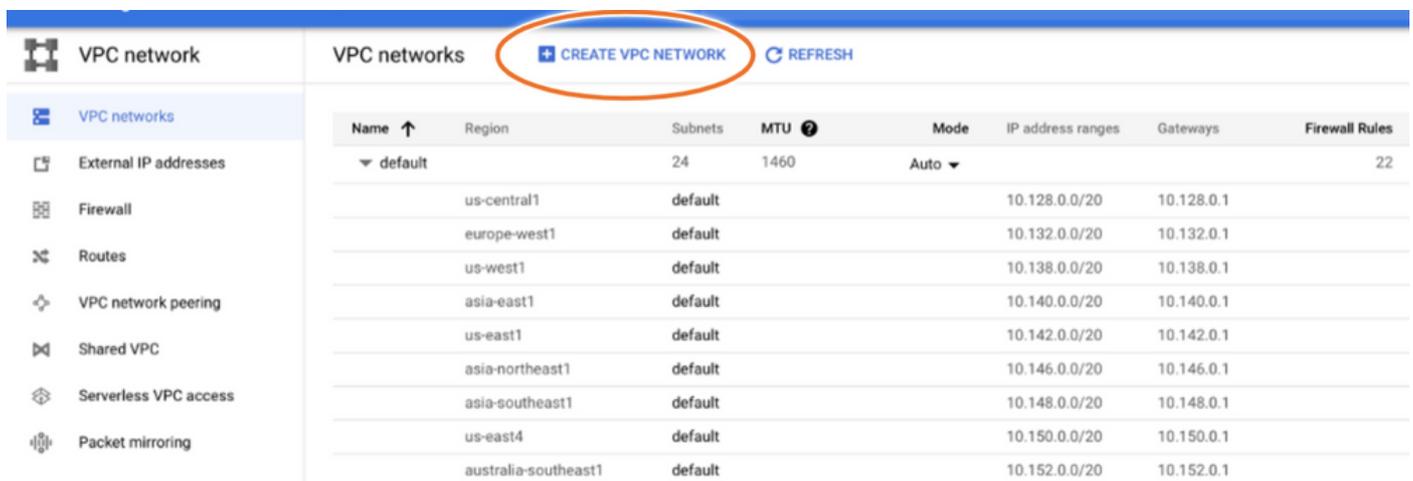
Erstellen Sie eine neue Virtual Private Cloud (VPC) und ein Subnetz, das der CSR1000v-Instanz zugeordnet werden muss.

Es ist möglich, den Standard-VPC oder ein zuvor erstelltes VPC und Subnetz zu verwenden.

Wählen Sie im Konsolen-Dashboard **VPC-Netzwerk > VPC-Netzwerke** aus, wie im Bild gezeigt.



Wählen Sie **VPC-Netzwerk erstellen**, wie im Bild gezeigt.



**Anmerkung:** Derzeit wird CSR1000v nur in der us-zentralen Region auf GCP bereitgestellt.

Konfigurieren Sie den VPC-Namen wie im Bild gezeigt.

## ← Create a VPC network

Name \*

csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Konfigurieren Sie den dem VPC zugeordneten Subnetznamen, und wählen Sie Region **us-central1** aus.

Weisen Sie innerhalb des us-central1 CIDR von 10.128.0.0/20 einen gültigen IP-Adressbereich zu. wie im Bild gezeigt.

Lassen Sie andere Standardeinstellungen unverändert, und wählen Sie **die** Schaltfläche **Erstellen** aus:

### 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 \*

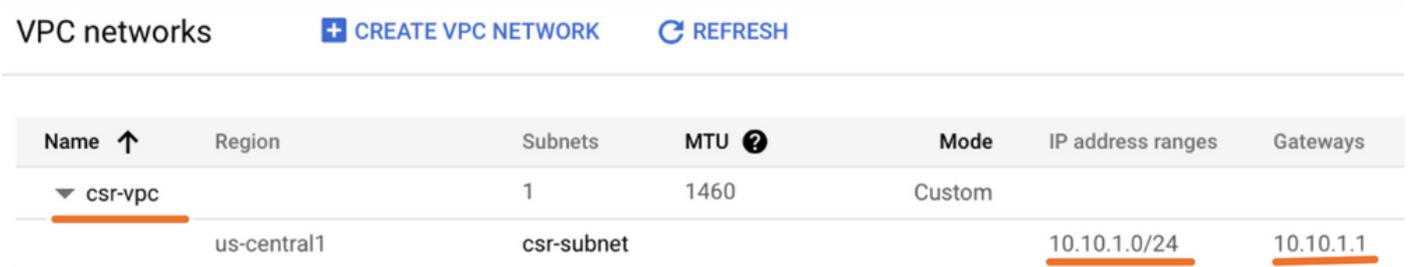
us-central1

IP address range \*

10.10.1.0/24

**Anmerkung:** Wenn "Automatic" (Automatisch) ausgewählt ist, weist GCP einen automatisch gültigen Bereich innerhalb des CIDR der Region zu.

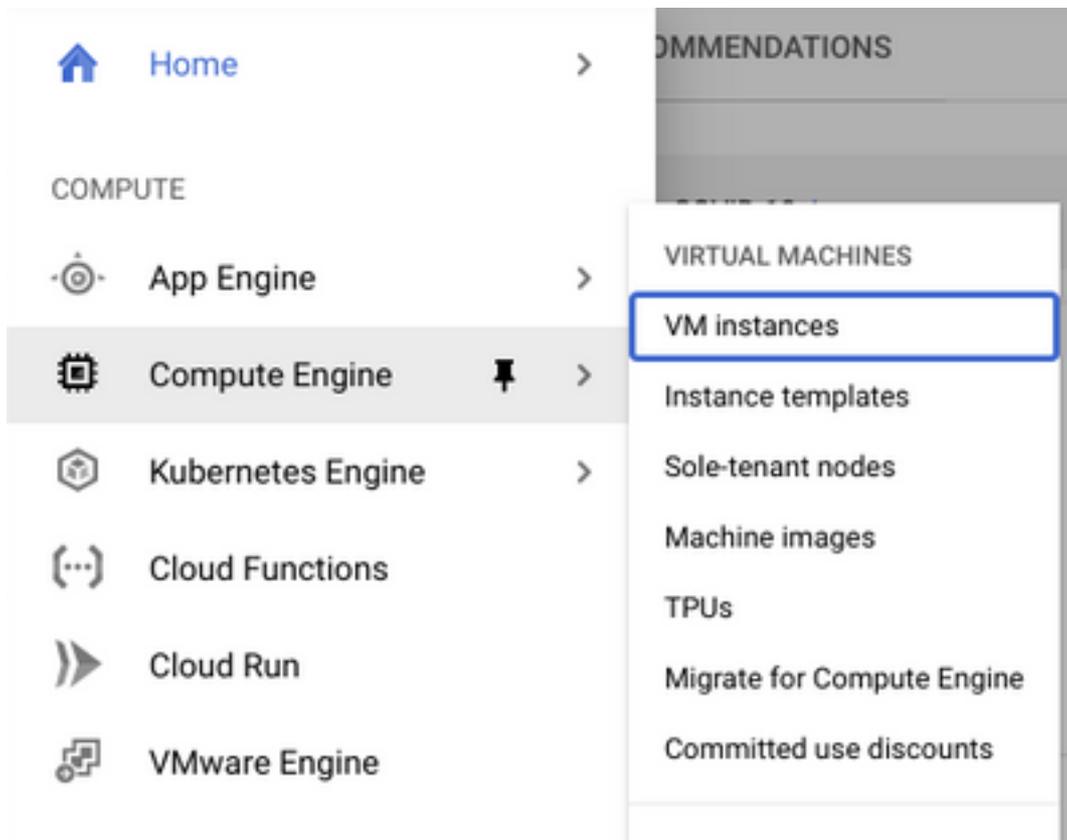
Nach Abschluss des Erstellungsprozesses wird das neue VPC im Abschnitt **VPC-Netzwerke** angezeigt, wie im Bild gezeigt.



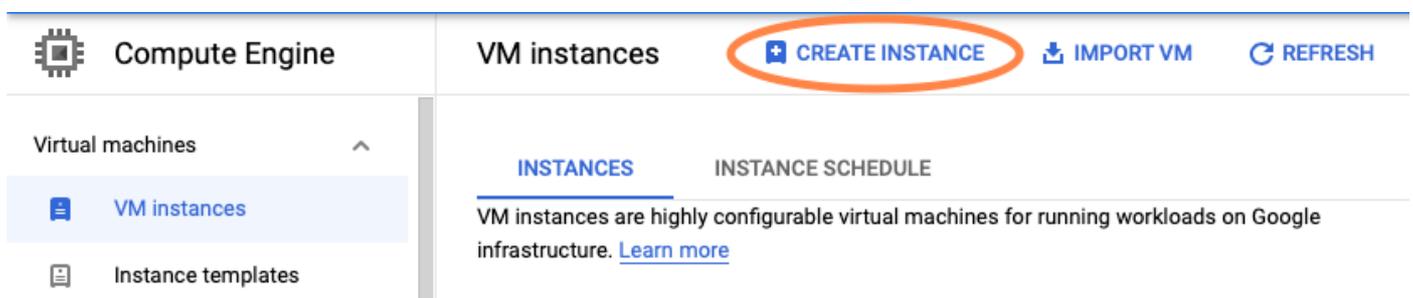
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			<u>10.10.1.0/24</u>	<u>10.10.1.1</u>

### Schritt 3: Bereitstellung virtueller Instanzen.

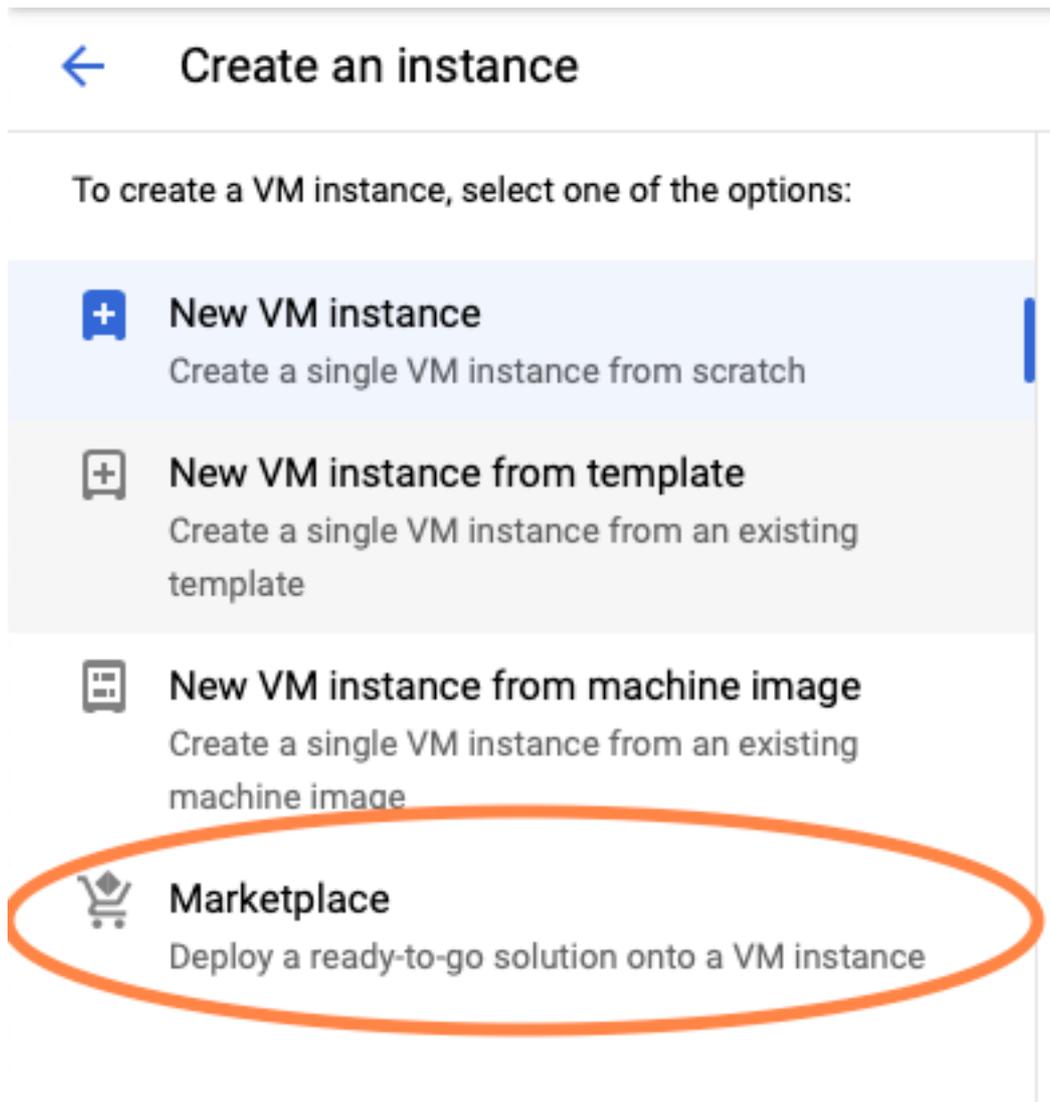
Wählen Sie im Abschnitt **Compute Engine** die Option **Compute Engine > VM-Instanzen** aus, wie im Image gezeigt.



Wählen Sie im **VM-Dashboard** die Registerkarte **Create Instance (Instanz erstellen)** aus, wie im Bild gezeigt.



Verwenden Sie GCP Marketplace wie im Bild gezeigt, um Cisco Produkte anzuzeigen.



Geben Sie in der Suchleiste **Cisco CSR** oder **Catalyst C8000v** ein, wählen Sie das Modell und die Version aus, die Ihre Anforderungen erfüllt, und wählen Sie **Starten aus**.

Für diese Beispielbereitstellung wurde die erste Option wie im Bild gezeigt ausgewählt.

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 Google Compute Platform.

**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 Google Compute Platform.

**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 Google Compute Platform.

**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 Google Compute Platform.

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

**Hinweis:** BYOL steht für "Bring Your Own License".

**Hinweis:** Derzeit unterstützt GCP kein Pay As You Go (PAYG)-Modell.

GCP muss die Konfigurationswerte eingeben, die dem virtuellen System zugeordnet werden müssen, wie im Bild gezeigt:

Ein Benutzername und ein öffentlicher SSH-Schlüssel sind erforderlich, um ein CSR1000v/C8000v in GCP bereitzustellen, wie im Bild gezeigt. Weitere Informationen finden Sie unter [Generate a Instance SSH Key to Deploy a CSR1000v in Google Cloud Platform](#), wenn die SSH-Schlüssel nicht erstellt wurden.



## 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 ?

Wählen Sie VPC und Subnetz aus, die vor dem Angriff erstellt wurden, und wählen Sie Ephemeral in externer IP aus, um eine öffentliche IP, wie im Bild gezeigt, mit der Instanz zu verknüpfen.

Nach der Konfiguration Wählen Sie die Schaltfläche **Starten** aus.

## 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

**Anmerkung:** Port 22 ist erforderlich, um über SSH eine Verbindung zur CSR-Instanz herzustellen. Der HTTP-Port ist optional.

Wählen Sie nach Abschluss der Bereitstellung **Compute Engine > VM-Instanzen aus**, um zu überprüfen, ob der neue CSR1000v erfolgreich bereitgestellt wurde, wie im Image gezeigt.

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)	<span style="background-color: black; color: black;">[REDACTED]</span>	SSH ▼ ⋮

## Bereitstellung überprüfen

### Remote-Verbindung zur neuen Instanz

Die gebräuchlichsten Methoden zur Anmeldung bei einem CSR1000v/C8000V in GCP sind die Befehlszeile in einem Bash-Terminal, Putty und SecureCRT. In diesem Abschnitt wird die Konfiguration beschrieben, die für die Verbindung mit den vorherigen Methoden erforderlich ist.

### Anmeldung bei CSR1000v/C8000v mit Bash Terminal

Die Syntax für die Remote-Verbindung mit dem neuen CSR lautet wie folgt:

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

## Beispiel:

```
$ 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.
```

Wenn die Verbindung erfolgreich hergestellt wurde, wird die Eingabeaufforderung CSR1000v angezeigt

```
$ 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
```

## Anmeldung bei CSR1000v/C8000v mit PuTTY

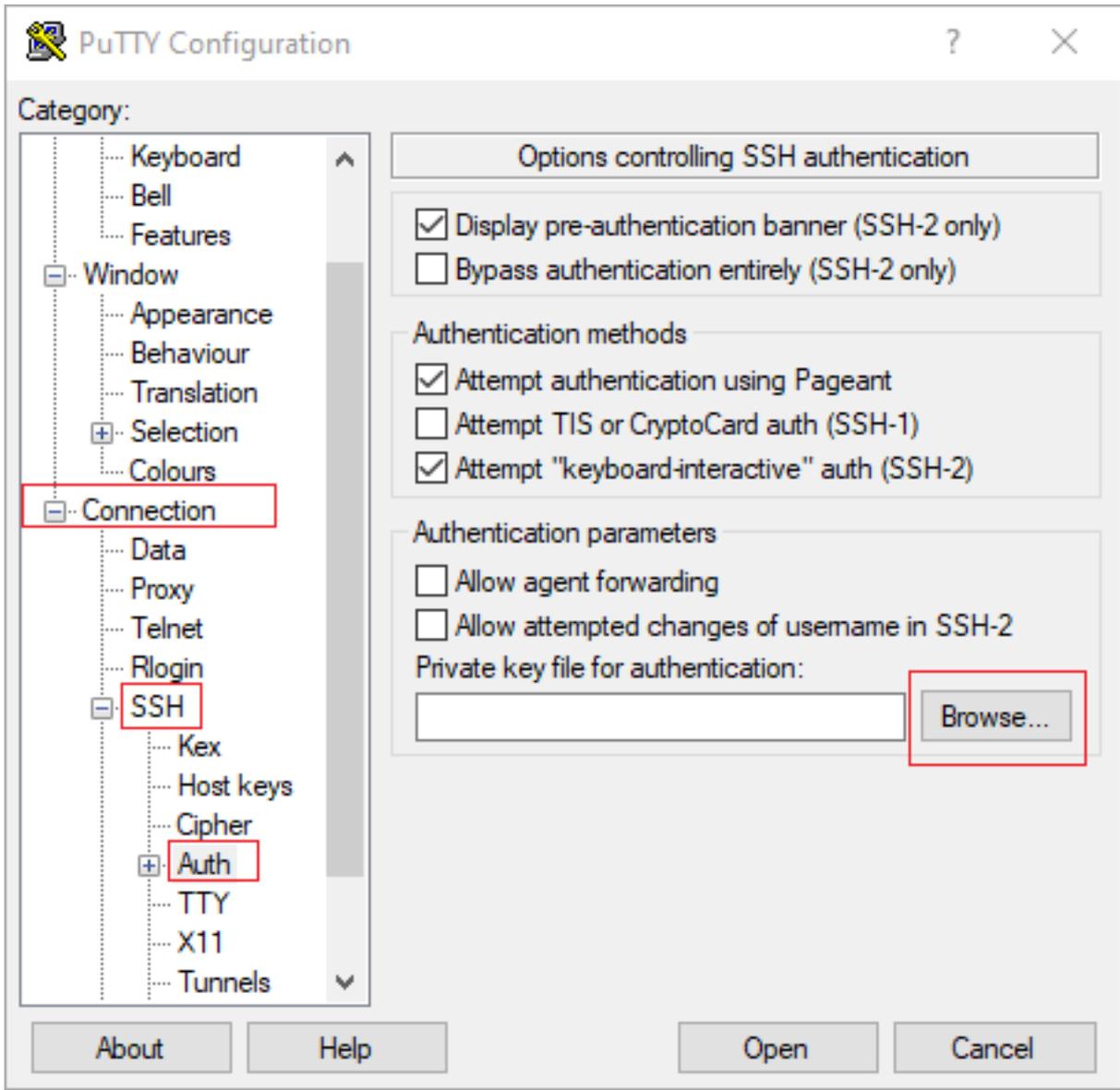
Um eine Verbindung mit Putty herzustellen, verwenden Sie die Anwendung PuTTYgen, um den privaten Schlüssel vom PEM in das PPK-Format zu konvertieren.

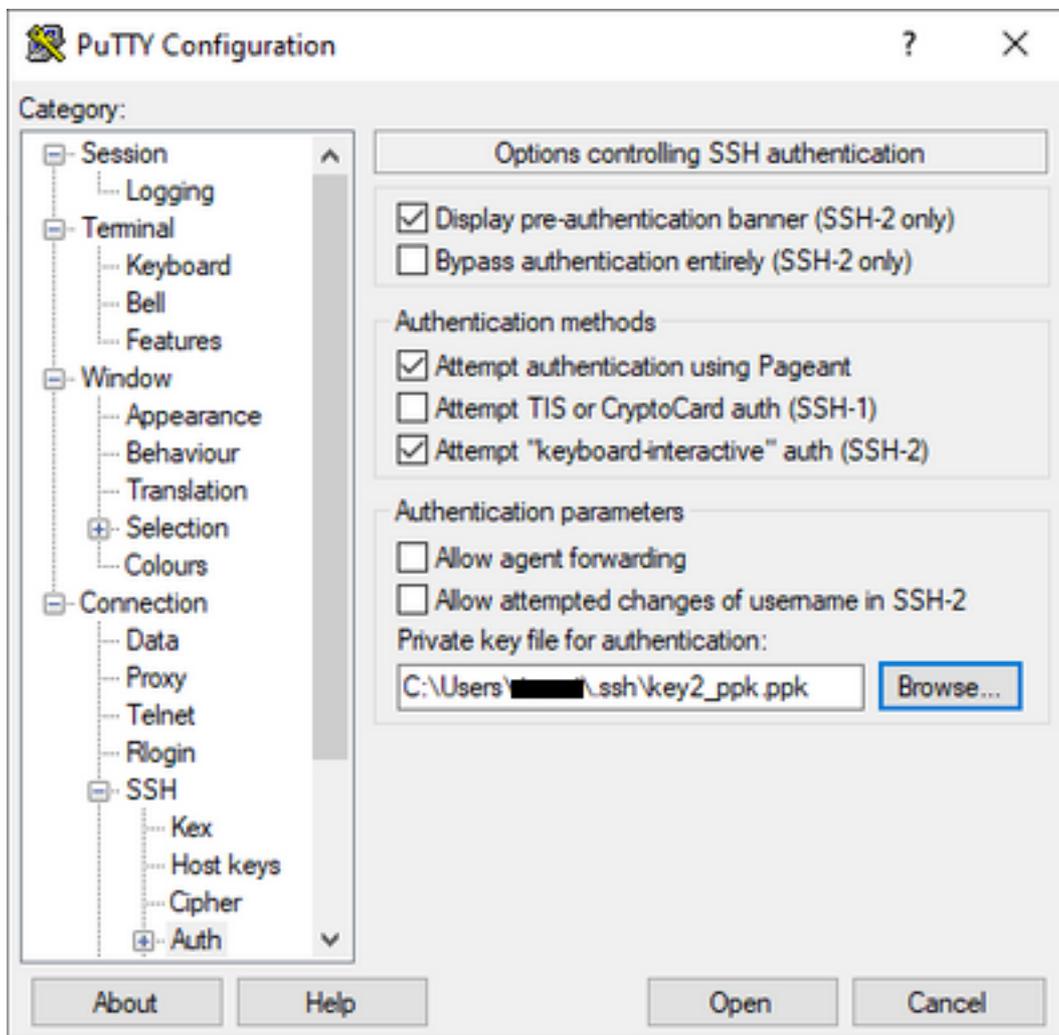
Weitere Informationen finden Sie unter [Pem in Ppk-Datei mithilfe von PuTTYgen umwandeln](#).

Nachdem der private Schlüssel im richtigen Format generiert wurde, müssen Sie den Pfad in Putty angeben.

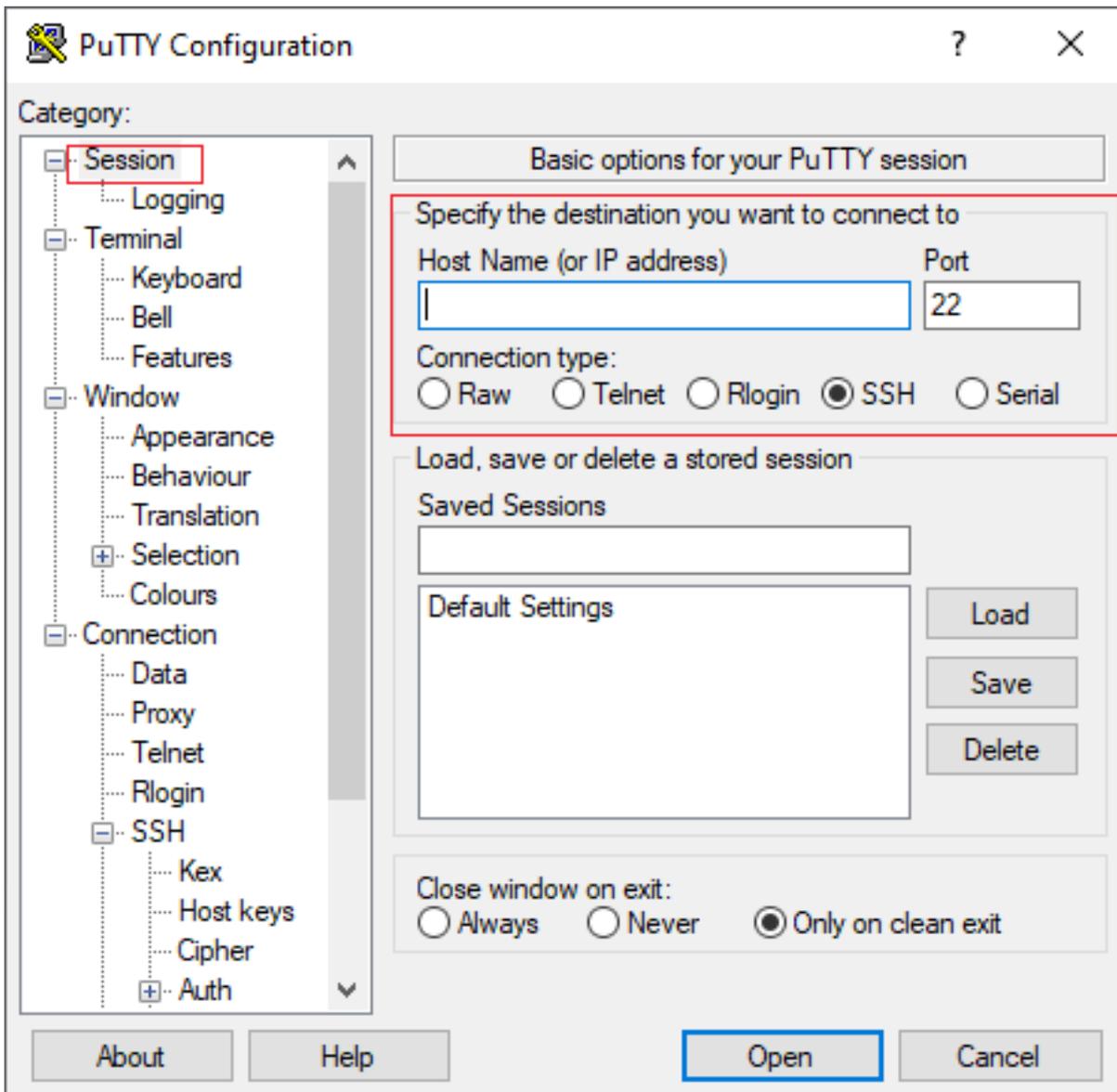
Wählen Sie im **Menü SSH-Verbindung** die **private Schlüsseldatei** für die **Authentifizierung** aus.

Navigieren Sie zu dem Ordner, in dem der Schlüssel gespeichert ist, und wählen Sie den erstellten Schlüssel aus. In diesem Beispiel zeigen die Bilder die grafische Ansicht des Putty-Menüs und den gewünschten Zustand:





Wenn Sie den richtigen Schlüssel ausgewählt haben, kehren Sie zum Hauptmenü zurück, und verwenden Sie die externe IP-Adresse der CSR1000v-Instanz, um eine Verbindung über SSH herzustellen, wie im Bild gezeigt.



**Anmerkung:** Der in den generierten SSH-Schlüsseln definierte Benutzername/Kennwort wird zur Anmeldung angefordert.

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

```
csr-cisco#
```

## Anmeldung bei CSR1000v/C8000V mit SecureCRT

SecureCRT benötigt den privaten Schlüssel im PEM-Format, das das Standardformat für die privaten Schlüssel ist.

Geben Sie in SecureCRT den Pfad zum privaten Schlüssel im Menü an:

**Datei > Schnellverbindung > Authentifizierung > Kennwort deaktivieren > Öffentlicher Schlüssel > Eigenschaften.**

Das Bild zeigt das erwartete Fenster:

Quick Connect

Protocol: SSH2

Hostname:

Port: 22 Firewall: None

Username:

Authentication

Password

**PublicKey**

Keyboard Interactive

GSSAPI

Show quick connect on startup  Save session

Open in a tab

Wählen Sie **Session Public Key String** > Wählen Sie **Identitäts- oder Zertifikatsdatei verwenden** > Wählen Sie ... > Navigieren Sie zum Verzeichnis, und wählen Sie die gewünschte Taste > OK wählen, wie im Bild gezeigt.

Public Key Properties

Use global public key setting  **Use session public key setting**

Session settings

**Use identity or certificate file**

Use a certificate from your personal CAPI store or a PKCS #11 provider DLL

CAPI:  DLL:

Certificate to use:

Get username from certificate:

Use certificate as raw SSH2 key (server does not support X.509)

Fingerprint:

SHA-2: e0:82:1d:a8:67:45:eb:96:31:12:74:28:ac:1a:4b:fa:b6:6e:67:e9:85:c9:06:0d:3

SHA-1: 79:04:f3:8a:0f:99:57:ee:d0:6b:4f:84:bb:93:d3:d1:99:63:70:a3

MDS: da:82:5e:30:f8:22:ec:a0:04:18:71:7e:fe:de:40:63

Stellen Sie schließlich die Verbindung mit der externen IP-Adresse der Instanz über SSH her, wie

im Bild gezeigt.

The image shows a 'Quick Connect' dialog box with the following fields and options:

- Protocol: SSH2 (dropdown)
- Hostname: (empty text box)
- Port: 22 (text box)
- Firewall: None (dropdown)
- Username: (empty text box)
- Authentication section:
  - PublicKey
  - Keyboard Interactive
  - GSSAPI
  - Password
- Properties... button
- Checkboxes:  Show quick connect on startup,  Save session,  Open in a tab
- Buttons: Connect, Cancel

**Anmerkung:** Der in den generierten SSH-Schlüsseln definierte Benutzername/Kennwort wird zur Anmeldung angefordert.

```
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#
```

## Zusätzliche VM-Anmeldungsmethoden

**Anmerkung:** Weitere Informationen finden Sie [in der](#) Dokumentation zu ["Connect to Linux VMs using Advanced Method"](#).

## Autorisieren zusätzlicher Benutzer für die Anmeldung bei CSR1000v/C8000v in GCP

Nach erfolgreicher Anmeldung bei der CSR1000v-Instanz können weitere Benutzer mit den

folgenden Methoden konfiguriert werden:

## Neuen Benutzernamen/Kennwort konfigurieren

Verwenden Sie die folgenden Befehle, um einen neuen Benutzer und ein neues Kennwort zu konfigurieren:

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

### Beispiel:

```
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#
```

Ein neuer Benutzer kann sich jetzt bei der CSR1000v/C8000v-Instanz anmelden.

## Konfigurieren eines neuen Benutzers mit SSH-Schlüssel

Um Zugriff auf die CSR1000v-Instanz zu erhalten, konfigurieren Sie den öffentlichen Schlüssel. SSH-Schlüssel in den Instanzmetadaten bieten keinen Zugriff auf CSR1000v.

Verwenden Sie die folgenden Befehle, um einen neuen Benutzer mit einem SSH-Schlüssel zu konfigurieren:

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

**Anmerkung:** Die maximale Leitungslänge in der Cisco CLI beträgt 254 Zeichen. Die Schlüsselzeichenfolge passt also möglicherweise nicht zu dieser Einschränkung. Es empfiehlt sich, die Schlüsselzeichenfolge in eine Terminalleitung einzubinden. Details zum Überwinden dieser Einschränkung finden Sie unter [Generate an Instance SSH Key to Deploy a CSR1000v in Google Cloud Platform](#)

```
$ fold -b -w 72 /mnt/c/Users/ricneri/.ssh/key2.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDldzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bWSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiWHigv28lyw5xhn1U
ck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/sADnODPO+OfTK
/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfqlks3PCVG0tW1HxxTU4
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+TRsSLiwHigv28l
csr-cisco(conf-ssh-pubkey-
data)#yw5xhn1Uck/AYpy9E6TyEEu9w6Fz0xTG2Qhe1n9b5Les6K9PFP/mR6WUMbfmaFredV/s
csr-cisco(conf-ssh-pubkey-
data)#ADnODPO+OfTK/OZPg34DNfcFhglja5GzudRb3S4nBBhDzuVrVC9RbA4PHVMXrLbIfq1k
csr-cisco(conf-ssh-pubkey-
data)#s3PCVG0tW1HxxTU4FCkMEAg4NEqMVLsm26nLvrNK6z71RmcIKZzcST+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#

```

## Überprüfung der konfigurierten Benutzer bei der Anmeldung bei CSR1000v/C8000v

Um zu bestätigen, dass die Konfiguration korrekt konfiguriert wurde, melden Sie sich mit den erstellten Anmeldeinformationen oder mit dem privaten Schlüsselpaar für den öffentlichen Schlüssel mit den zusätzlichen Anmeldeinformationen an.

Von der Routerseite aus sehen Sie das Erfolgsprotokoll mit der Terminal-IP-Adresse.

```

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#

```

## Fehlerbehebung

**Wenn die Fehlermeldung "Operation timed out" (Vorgang ist abgelaufen) angezeigt wird.**

```

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

```

Mögliche Ursachen:

- Die Instanz hat ihre Bereitstellung noch nicht abgeschlossen.
- Die Public-Adresse ist nicht die, die nic0 im VM zugewiesen ist.

Lösung:

Warten Sie, bis die VM-Bereitstellung abgeschlossen ist. In der Regel dauert die CSR1000v-Bereitstellung bis zu 5 Minuten.

## Wenn ein Kennwort erforderlich ist

Falls ein Kennwort erforderlich ist:

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

Password:

Password:

Mögliche Ursache:

- Der Benutzername oder der private Schlüssel ist falsch.

Lösung:

- Stellen Sie sicher, dass der Benutzername derselbe ist, der bei der Bereitstellung von CSR1000v/C8000v angegeben wurde.
- Stellen Sie sicher, dass der private Schlüssel derselbe ist, den Sie zur Bereitstellungszeit angegeben haben.

## Zugehörige Informationen

- [Cisco Cloud Services Router 1000v - Datenblatt](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)