

Implementazione di un CSR1000v/C8000v sulla piattaforma Google Cloud

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Impostazione progetto](#)

[Passaggio 1. Assicura un progetto valido e attivo per l'account.](#)

[Passaggio 2. Creare un nuovo VPC e una nuova subnet.](#)

[Passaggio 3. Distribuzione istanza virtuale.](#)

[Verifica distribuzione](#)

[Connessione remota alla nuova istanza](#)

[Accedere a CSR1000v/C800v con Bash Terminal](#)

[Accedere a CSR1000v/C800v con PuTTY](#)

[Accedere a CSR1000v/C800V con SecureCRT](#)

[Metodi aggiuntivi di accesso VM](#)

[Autorizzazione di altri utenti ad accedere a CSR1000v/C800v in GCP](#)

[Configura nuovo nome utente/password](#)

[Configurazione di un nuovo utente con la chiave SSH](#)

[Verifica degli utenti configurati al momento dell'accesso a CSR1000v/C800v](#)

[Risoluzione dei problemi](#)

[Se viene visualizzato il messaggio di errore "Operation Timed Out" \(Timeout operazione\).](#)

[Se è richiesta una password](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la procedura per distribuire e configurare un Cisco CSR1000v e Catalyst 8000v (C800v) sulla piattaforma Google Cloud (GCP).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Tecnologie di virtualizzazione/macchine virtuali (VM)

- Piattaforme cloud

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Una sottoscrizione attiva alla piattaforma Google Cloud con un progetto creato
- Console GCP
- GCP marketplace
- Bash terminal, Putty o SecureCRT
- Chiavi SSH (Secure Shell) pubbliche e private

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

A partire dalla versione 17.4.1, CSR1000v diventa il modello C8000v con le stesse funzionalità ma con l'aggiunta di nuove funzionalità come la licenza SD-WAN e Cisco DNA. Per ulteriori riferimenti, si prega di verificare la scheda tecnica ufficiale dei prodotti:

[Scheda tecnica di Cisco Cloud Services Router 1000v](#)

[Scheda tecnica del software Cisco Catalyst 8000V Edge](#)

Pertanto, questa guida è applicabile sia all'installazione dei router CSR1000v che C8000v.

Impostazione progetto

 Nota: al momento della stesura di questo documento, i nuovi utenti hanno 300USD di crediti gratuiti per esplorare GCP come Free Tier per un anno. Questo è definito da Google e non è sotto il controllo di Cisco.

 Nota: questo documento richiede la creazione di chiavi SSH pubbliche e private. Per ulteriori informazioni, consultare il documento sulla [generazione di una chiave SSH di istanza per distribuire un CSR1000v nella piattaforma Google Cloud](#)

Passaggio 1. Assicura un progetto valido e attivo per l'account.

Verificare che l'account disponga di un progetto valido e attivo, che deve essere associato a un

gruppo con autorizzazioni per il motore di calcolo.

Per questo esempio di distribuzione, viene utilizzato un progetto creato nel GCP.

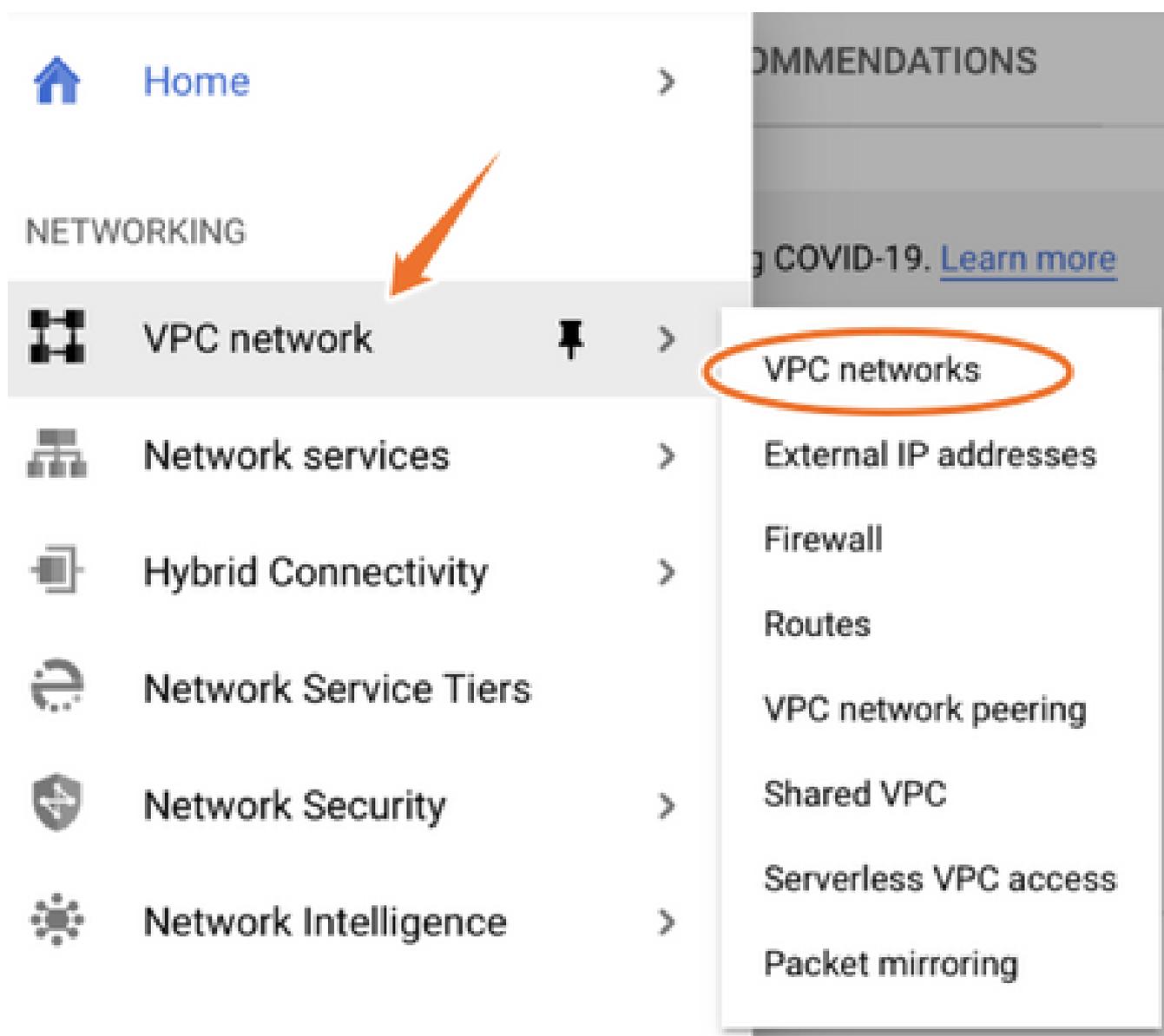
 Nota: per creare un nuovo progetto, vedere [Creazione e gestione di progetti](#).

Passaggio 2. Creare un nuovo VPC e una nuova subnet.

Creare un nuovo Virtual Private Cloud (VPC) e una subnet da associare all'istanza di CSR1000v.

È possibile utilizzare il VPC predefinito o un VPC e una subnet creati in precedenza.

Nel dashboard della console, selezionare Rete VPC > Reti VPC come mostrato nell'immagine.



Selezionare Create VPC Network (Crea rete VPC) come mostrato nell'immagine.

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	

 Nota: attualmente, CSR1000v è implementato solo nell'area centrale degli Stati Uniti su GCP.

Configurare il nome VPC come mostrato nell'immagine.

← Create a VPC network

Name * 
csr-vpc

Lowercase letters, numbers, hyphens allowed

Description

Configurare il nome della subnet associato al VPC e selezionare la regione us-central1.

Assegnare un intervallo di indirizzi IP valido nella CIDR us-central1 pari a 10.128.0.0/20. come mostrato nell'immagine.

Accettare le altre impostazioni come predefinite e selezionare il pulsante Crea:

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

 Nota: se si seleziona "automatico", GCP assegna un intervallo valido automatico all'interno del CIDR dell'area.

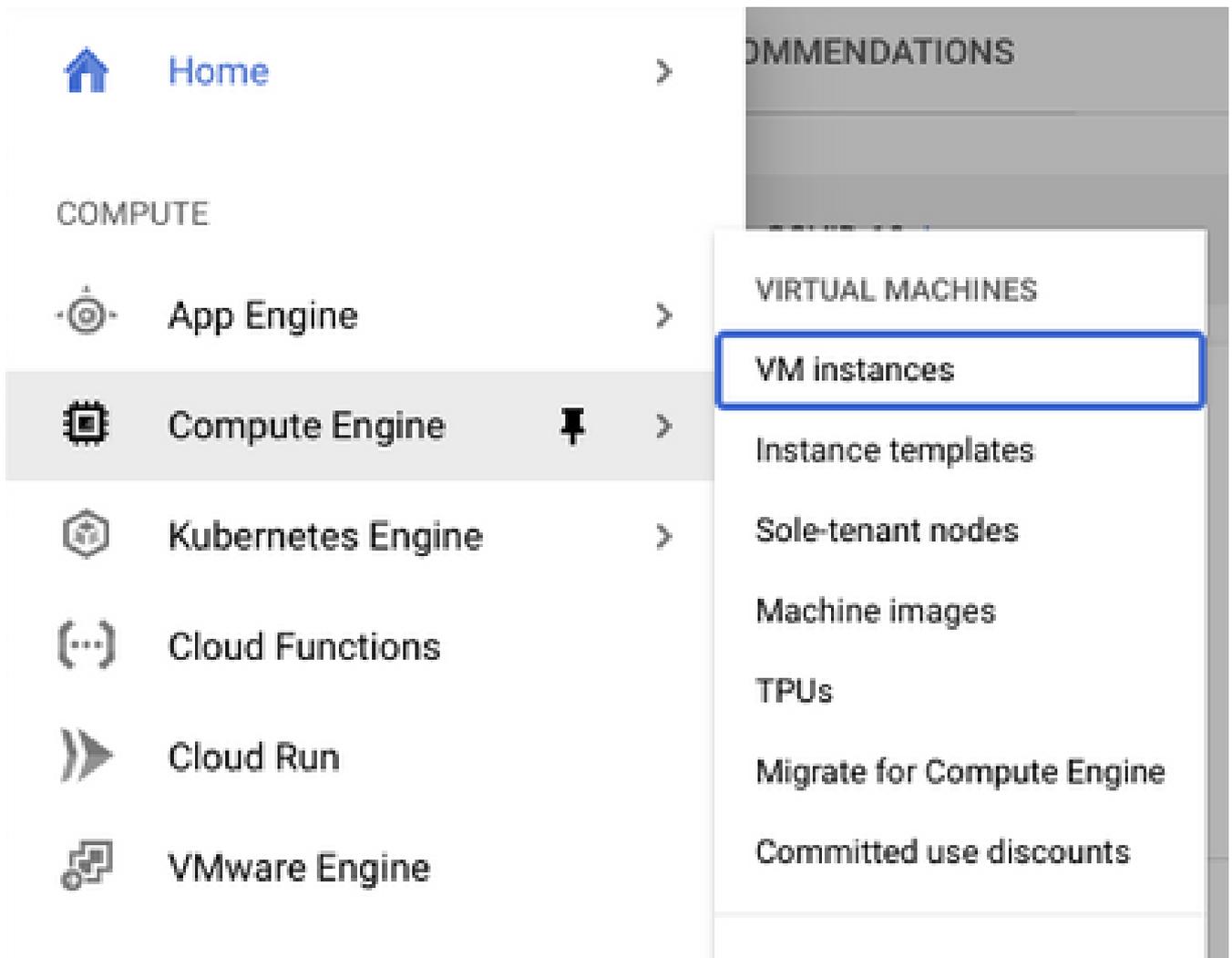
Al termine del processo di creazione, il nuovo VPC viene visualizzato nella sezione Reti VPC come mostrato nell'immagine.

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

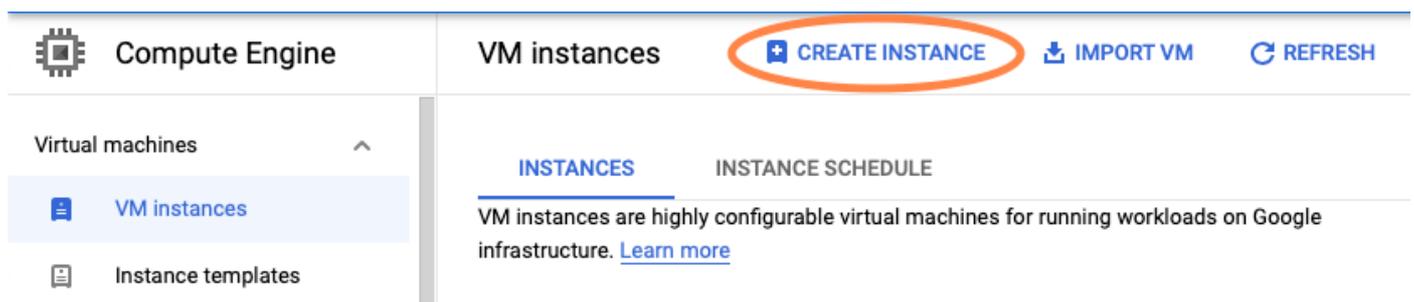
Name ↑	Region	Subnets	MTU ?	Mode	IP address ranges	Gateways
▼ csr-vpc		1	1460	Custom		
	us-central1	csr-subnet			10.10.1.0/24	10.10.1.1

Passaggio 3. Distribuzione istanza virtuale.

Nella sezione Motore di calcolo, selezionate Motore di calcolo > Istanze VM come mostrato nell'immagine.



Una volta nel dashboard VM, selezionare la scheda Crea istanza come mostrato nell'immagine.



Per visualizzare i prodotti Cisco, usare GCP marketplace come mostrato nell'immagine.



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

Nella barra di ricerca, digitare Cisco CSR o Catalyst C800v, scegliere il modello e la versione che soddisfano le proprie esigenze e selezionare Launch (Avvia).

Per questa distribuzione di esempio, è stata selezionata la prima opzione come mostrato nell'immagine.

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 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.

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

Filter Type to filter

Virtual machines

Category



1 result

Compute

(1)

Networking

(1)

Type

Virtual machines



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

Nota: BYOL sta per "Bring Your Own License".

Nota: al momento, GCP non supporta il modello PAYG (Pay As You Go).

GCP richiede di immettere i valori di configurazione da associare alla VM, come mostrato nell'immagine:

Per installare un CSR100v/C800v in GCP, è necessario specificare un nome utente e una chiave pubblica SSH, come mostrato nell'immagine. Se le chiavi SSH non sono state create, consultare il documento sulla [generazione di una chiave SSH di istanza per distribuire un CSR1000v nella piattaforma Google Cloud](#).

← 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 ?

Selezionare il VPC e la subnet creati in precedenza, quindi scegliere Temporale nell'IP esterno per associare un IP pubblico all'istanza, come mostrato nell'immagine.

Dopo la configurazione. Selezionare il pulsante di avvio.

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

 Nota: la porta 22 è necessaria per il collegamento all'istanza CSR tramite SSH. La porta HTTP è facoltativa.

Una volta completata la distribuzione, selezionare Compute Engine > VM instance (Motore di calcolo > Istanze VM) per verificare che il nuovo CSR1000v sia stato distribuito correttamente, come mostrato nell'immagine.

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 type="checkbox"/>  csr-cisco	us-central1-f			10.10.1.2 (nic0)		SSH ▾ ⋮

Verifica distribuzione

Connessione remota alla nuova istanza

I metodi più comuni per accedere a un CSR1000v/C800V in GCP sono la riga di comando in un terminale Bash, Putty e SecureCRT. In questa sezione, la configurazione necessaria per connettersi ai metodi precedenti.

Accedere a CSR1000v/C800v con Bash Terminal

La sintassi necessaria per la connessione remota al nuovo CSR è la seguente:

```
<#root>
```

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

Esempio:

```
<#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.
```

Se la connessione ha esito positivo, viene visualizzato il prompt di CSR1000v

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

Accedere a CSR1000v/C800v con PuTTY

Per connettersi a Putty, utilizzare l'applicazione PuTTYgen per convertire la chiave privata dal formato PEM al formato PPK.

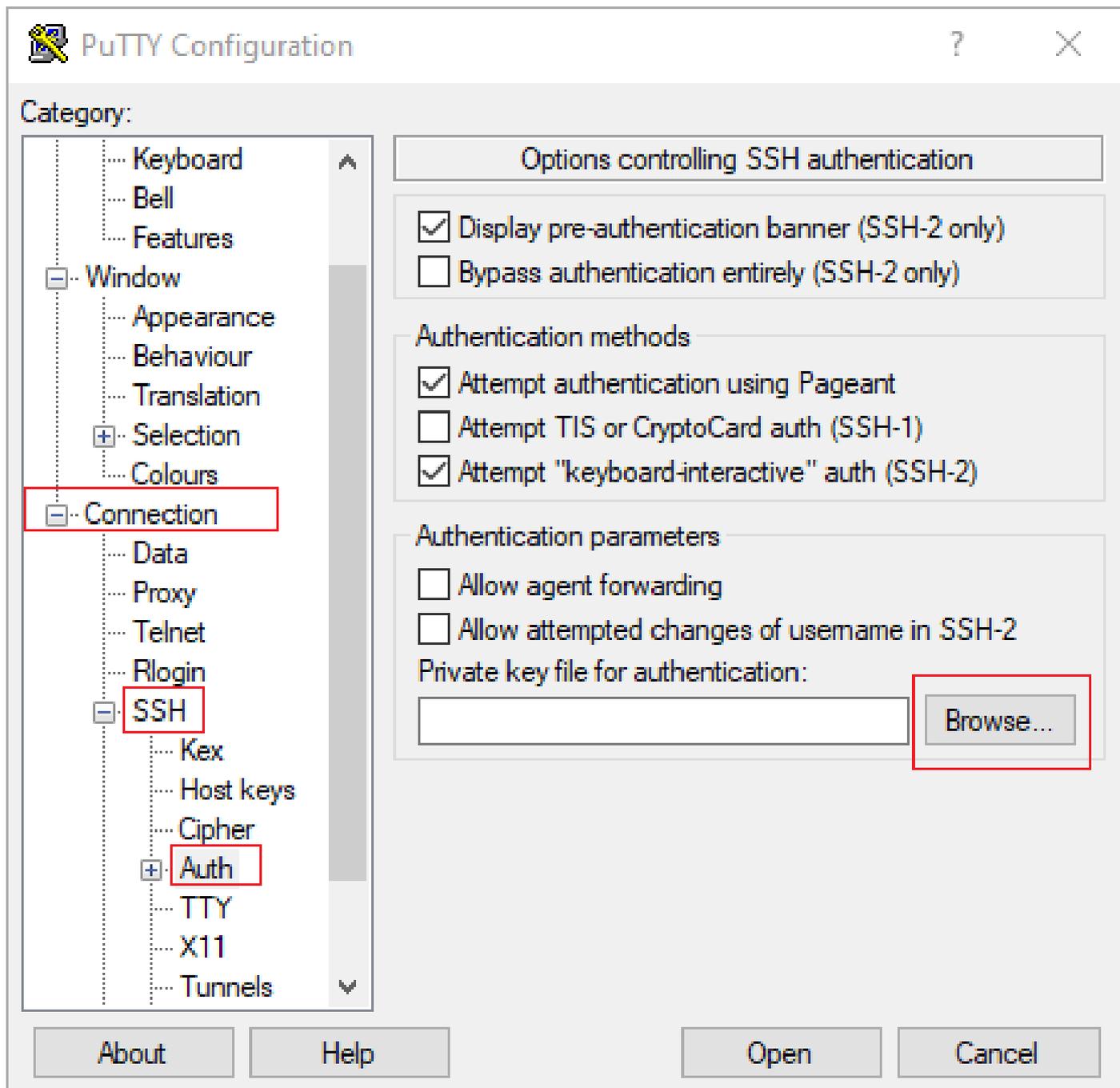
Per ulteriori informazioni, fare riferimento a [Converti file Pem in Ppk utilizzando PuTTYgen](#).

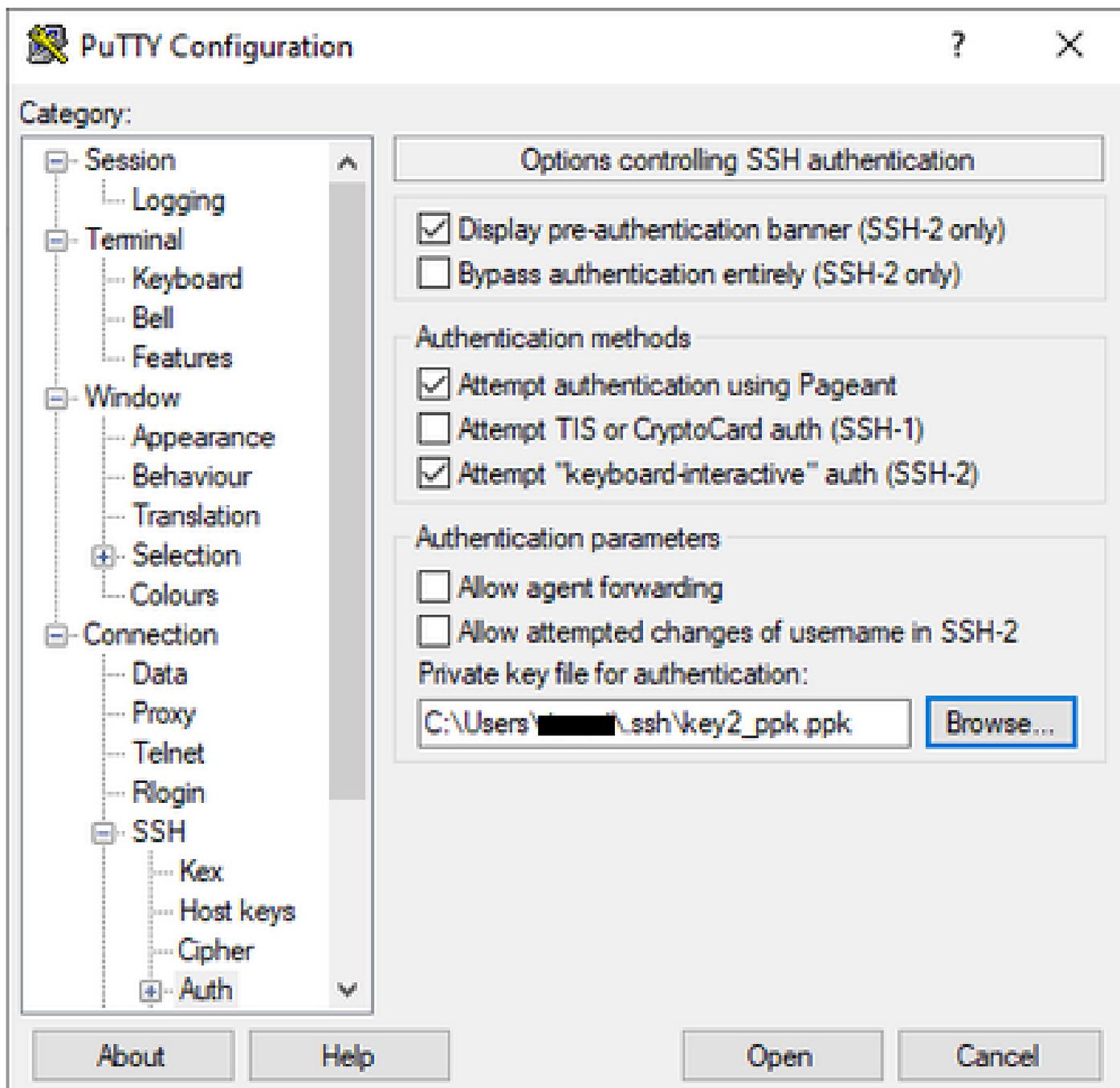
Dopo aver generato la chiave privata nel formato corretto, è necessario specificare il percorso in Putty.

Selezionare la sezione Private Key file for authentication nel menu auth option of the SSH

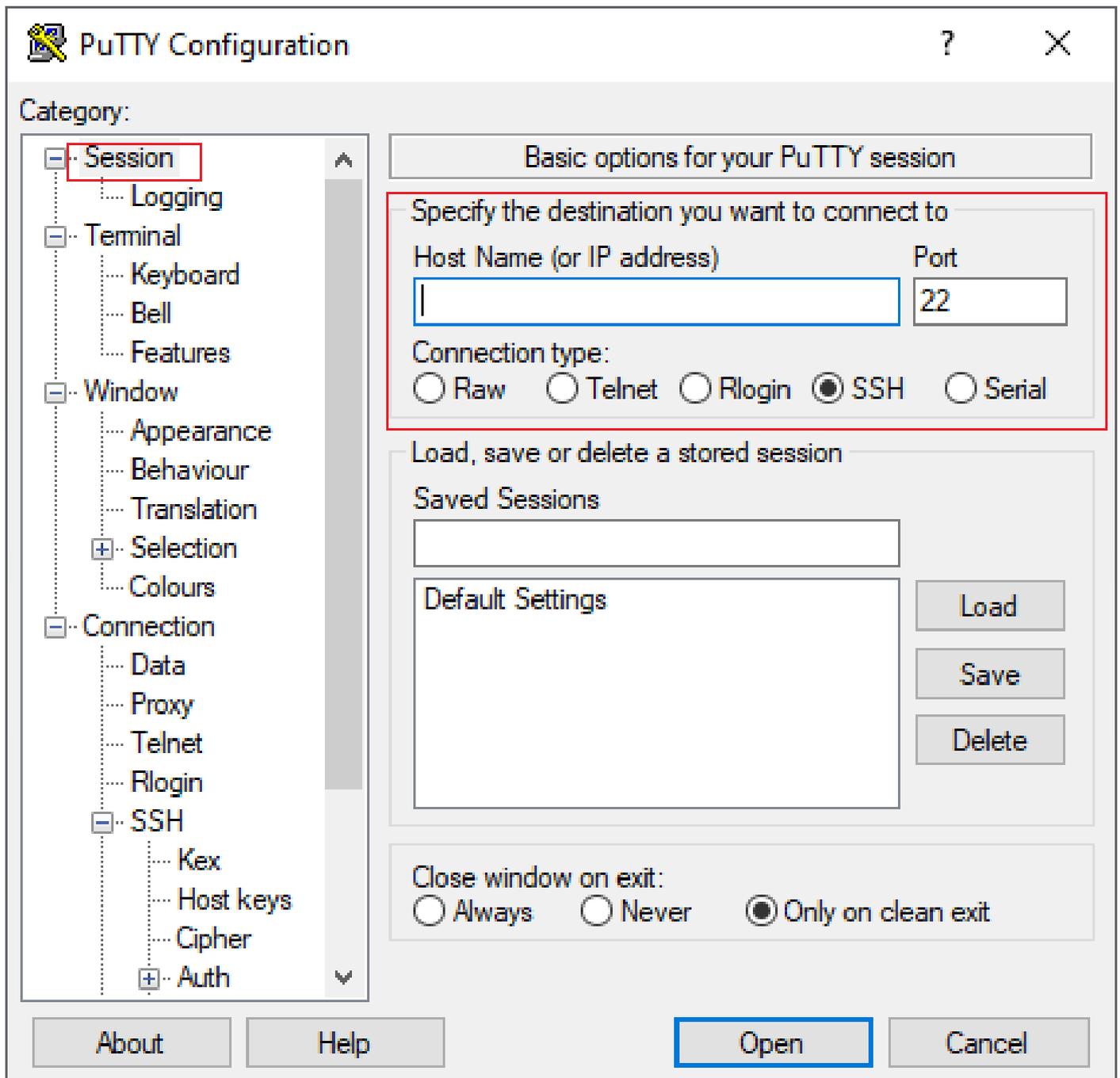
connection.

Individuare la cartella in cui è memorizzata la chiave e selezionare la chiave creata. In questo esempio, le immagini mostrano la visualizzazione grafica del menu PuTTY e lo stato desiderato:





Dopo aver selezionato la chiave corretta, tornare al menu principale e utilizzare l'indirizzo IP esterno dell'istanza di CSR1000v per connettersi tramite SSH, come mostrato nell'immagine.



 Nota: per accedere, è necessario specificare il nome utente e la password definiti nelle chiavi SSH generate.

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

```
csr-cisco#
```

Accedere a CSR1000v/C800V con SecureCRT

SecureCRT richiede la chiave privata in formato PEM, che è il formato predefinito per le chiavi private.

In SecureCRT specificare il percorso della chiave privata nel menu:

File > Connessione rapida > Autenticazione > Deseleziona password > Chiave pubblica > Proprietà.

Nell'immagine è illustrata la finestra prevista:

Quick Connect

Protocol: SSH2

Hostname:

Port: 22 Firewall: None

Username:

Authentication

- Password
- PublicKey
- Keyboard Interactive
- GSSAPI

Properties...

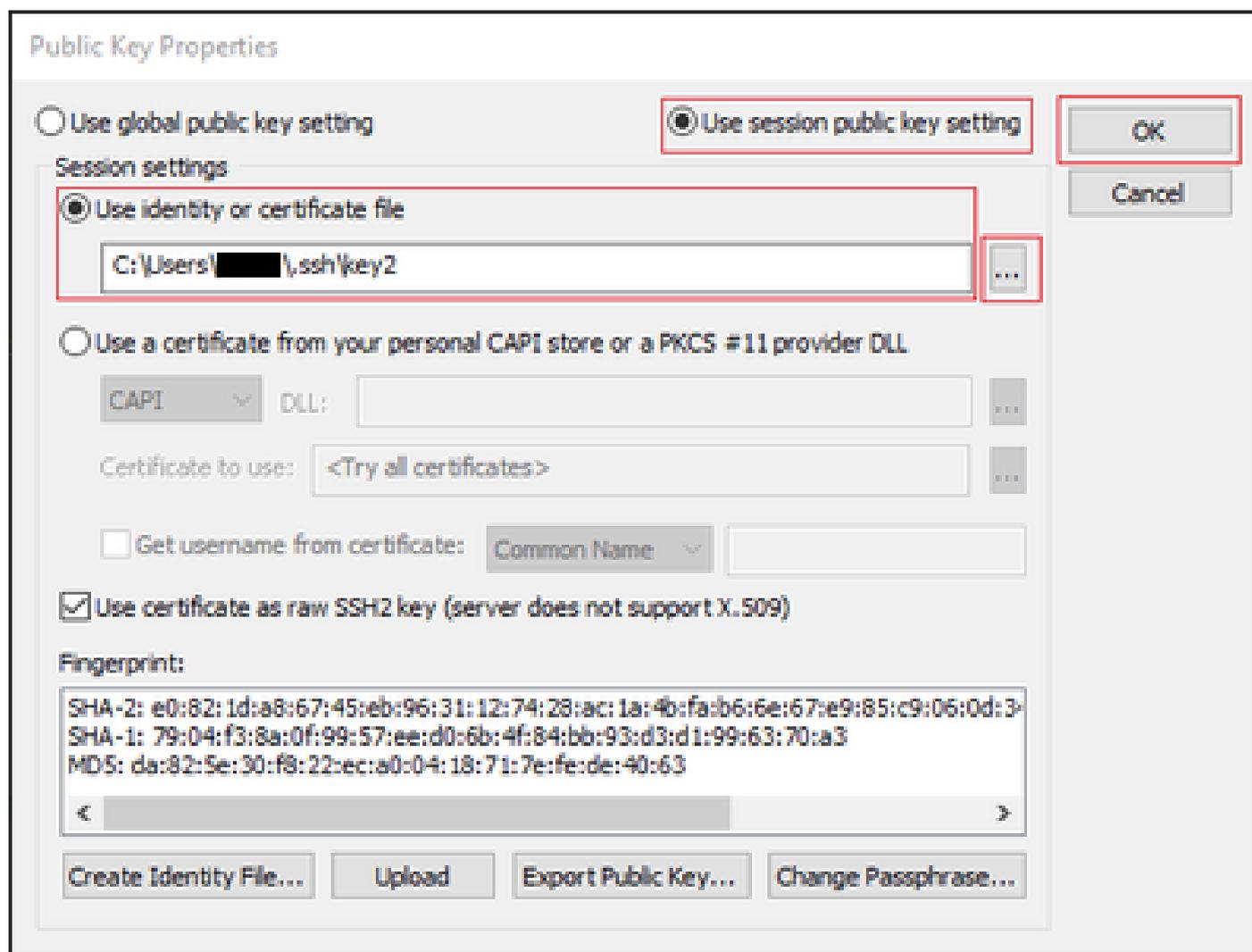
Show quick connect on startup Save session

Open in a tab

Connect Cancel

Selezionare Usa stringa chiave pubblica sessione > Seleziona Usa identità o file di certificato > Seleziona ... pulsante > Passare alla directory e selezionare la chiave desiderata > Seleziona OK

come mostrato nell'immagine.



Infine, collegarsi all'IP esterno dell'indirizzo dell'istanza tramite SSH, come mostrato nell'immagine.

Quick Connect

Protocol: SSH2

Hostname: |

Port: 22 Firewall: None

Username:

Authentication

- PublicKey
- Keyboard Interactive
- GSSAPI
- Password

Show quick connect on startup

Save session

Open in a tab

Connect Cancel

 Nota: per accedere, è necessario specificare il nome utente e la password definiti nelle chiavi SSH generate.

```
<#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#

Metodi aggiuntivi di accesso VM

 Nota: fare riferimento alla sezione [Connessione a VM Linux utilizzando la documentazione sui metodi avanzati](#).

Autorizzazione di altri utenti ad accedere a CSR1000v/C800v in GCP

Una volta eseguito il login all'istanza di CSR1000v, è possibile configurare altri utenti con questi metodi:

Configura nuovo nome utente/password

Utilizzare i seguenti comandi per configurare un nuovo utente e una nuova password:

```
<#root>
```

```
enable
```

```
configure terminal
```

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

```
end
```

Esempio:

```
<#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 nuovo utente può ora accedere all'istanza di CSR1000v/C8000v.

Configurazione di un nuovo utente con la chiave SSH

Per accedere all'istanza di CSR1000v, configurare la chiave pubblica. Le chiavi SSH nei metadati dell'istanza non consentono di accedere a CSR1000v.

Utilizzare questi comandi per configurare un nuovo utente con una chiave SSH:

```
<#root>
```

```
configure terminal
```

```
ip ssh pubkey-chain
```

```
username <username>
```

```
key-string
```

```
<public ssh key>
```

```
exit
```

```
end
```

 Nota: la lunghezza massima della linea nella CLI di Cisco è 254 caratteri, quindi la stringa della chiave non può superare questa limitazione. È consigliabile avvolgere la stringa della chiave per adattarla a una linea terminale. Per informazioni dettagliate su come superare questo limite, vedere [Generate an Instance SSH Key to Deploy a CSR1000v in Google Cloud Platform.](#)

```
<#root>
```

```
$
```

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

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQD1dzZ/iJi3VeHs4qDoxOP67jebaGwC6vkC
n29bwSQ4CPJGVRLcVSNPcPPqVydiXVEOG8e9gFszkpk6c2meO+TRsSLiwHigv281yw5xhn1U
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 AAAAB3NzaC1yc2EAAAADAQABAAQD1dzZ/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#
```

Verifica degli utenti configurati al momento dell'accesso a CSR1000v/C800v

Per verificare che la configurazione sia stata impostata correttamente, eseguire l'accesso con le credenziali create o con la coppia di chiavi private per la chiave pubblica con le credenziali aggiuntive.

Dal lato router, vedere il log di accesso riuscito con l'indirizzo IP del terminale.

```
<#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#
```

Risoluzione dei problemi

Se viene visualizzato il messaggio di errore "Operation Timed Out" (Timeout operazione).

```
<#root>
```

```
$
```

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

```
ssh: connect to host <snip> port 22: Operation timed out
```

Possibili cause:

- Distribuzione dell'istanza non completata.
- L'indirizzo pubblico non è quello assegnato a nic0 nella macchina virtuale.

Soluzione:

Attendere il completamento dell'installazione della macchina virtuale. In genere, un'installazione di CSR1000v richiede fino a 5 minuti.

Se è richiesta una password

Se è richiesta una password:

```
<#root>
```

```
$
```

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

```
Password:
```

```
Password:
```

Possibile causa:

- Il nome utente o la chiave privata non è corretta.
- Nelle versioni più recenti di sistemi operativi come MacOS o Linux, l'utility OpenSSH non ha RSA abilitato per impostazione predefinita.

Soluzione:

- Verificare che il nome utente sia lo stesso specificato durante l'implementazione di CSR1000v/C8000v.
- Verificare che la chiave privata sia la stessa inclusa al momento della distribuzione.
- Specificare il tipo di chiave accettata nel comando ssh:

```
<#root>
```

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

Informazioni correlate

- [Scheda tecnica di Cisco Cloud Services Router 1000v](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).