Distribuisci il connettore di risorse di accesso sicuro in Azure

Sommario

Introduzione

In questo documento viene descritto come distribuire un connettore di risorse passo per passo in Azure.

Prerequisiti

Raccogliere le informazioni necessarie e comprendere

- Ottenere l'immagine del connettore.
    - È possibile scaricare l'immagine una sola volta e utilizzarla per un numero qualsiasi di connettori in qualsiasi gruppo di connettori.
    - Se si utilizza un'immagine scaricata in precedenza, verificare che la versione dell'immagine sia la più recente.
    - Per ulteriori informazioni, vedere [Ottenere l'immagine del connettore](#).
- Copiare la chiave di provisioning per il gruppo di connettori specifico per cui si distribuiscono i connettori.
  Fare riferimento alla sezione [Provisioning delle chiavi per i connettori di risorsa](#).

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso amministratore dashboard Cisco Secure Access
- Accesso al portale di Azure

- Cisco Secure Client
- Computer Windows con ZTA registrato

Componenti usati

Le informazioni di questo documento si basano sul test eseguito in un ambiente lab utilizzando i componenti successivi:

- Client ZTNA
- Accesso sicuro
- Azzurro
- Risorsa privata

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.

Configurazione

Configurazioni in Accesso sicuro

Accedere al [Dashboard di accesso protetto](#) e passare a **Connect** > **Network Connections** > **Connector Groups**
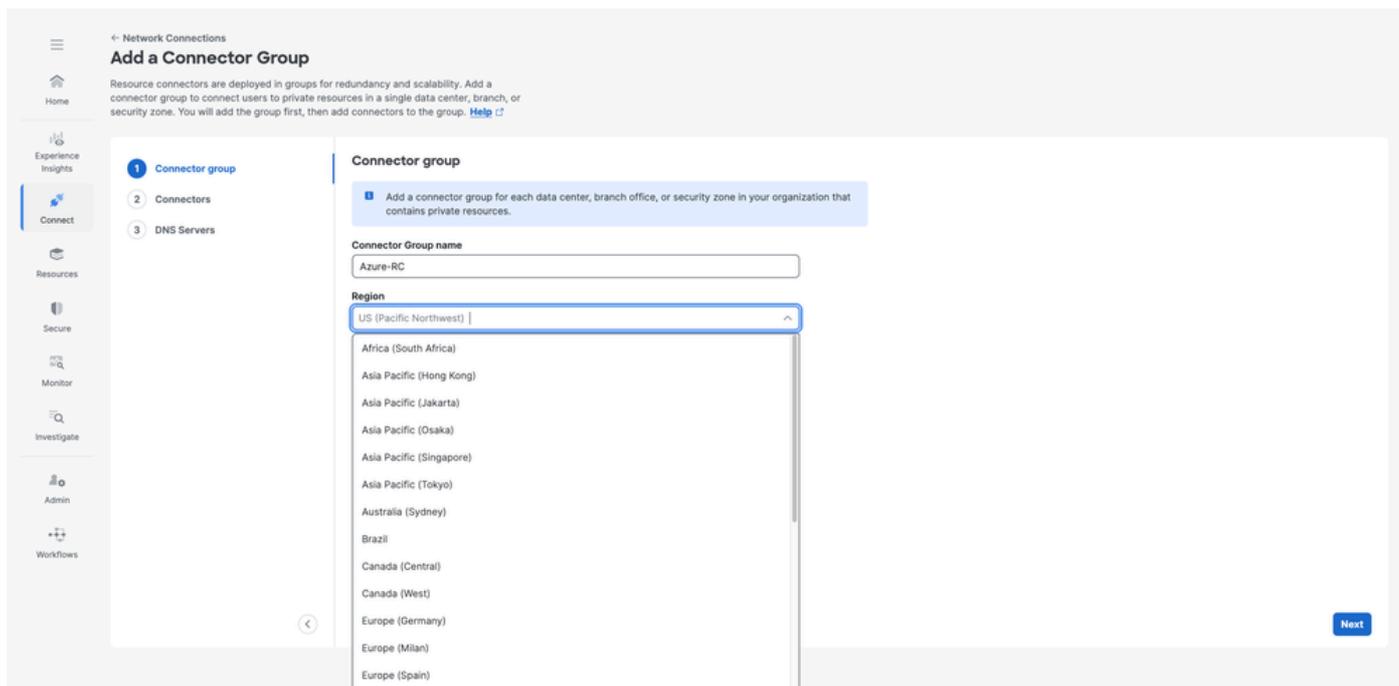
- Fare clic su add

Accesso sicuro - Gruppi di connettori
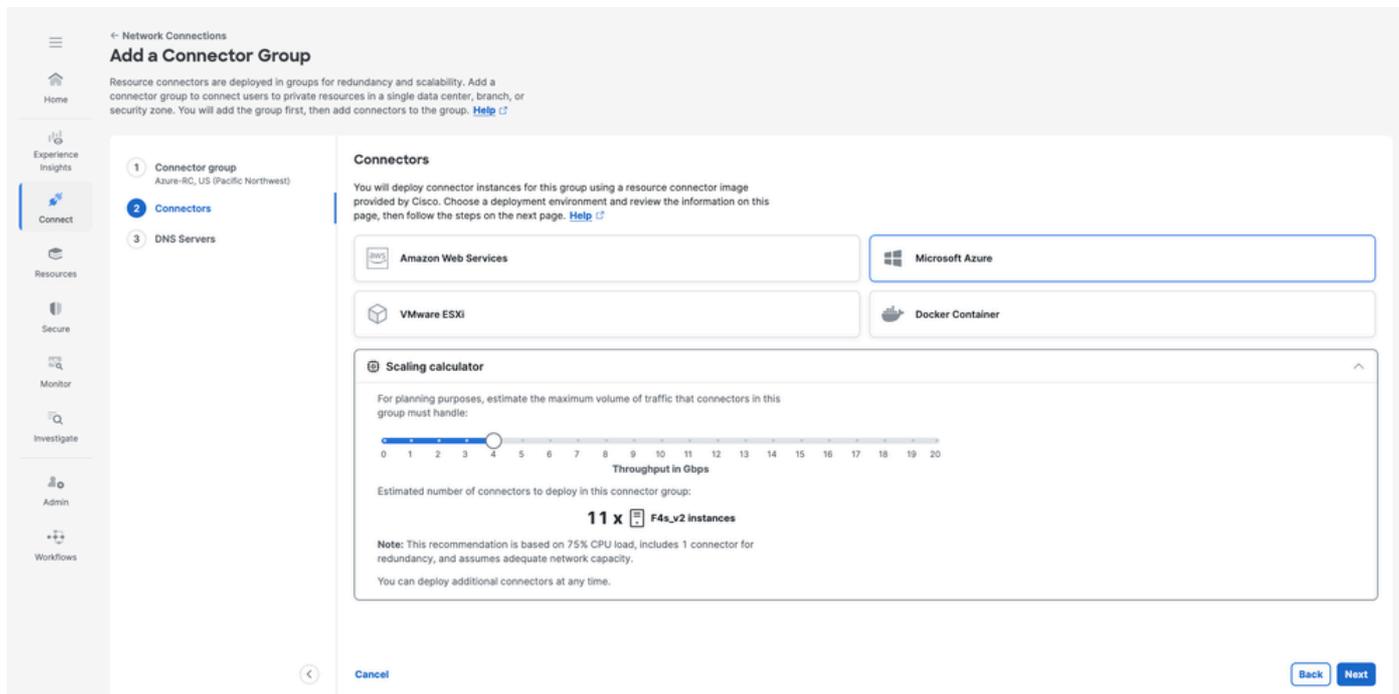
- Specificare la Connector Group Name e la Region

- Fare clic su Next

Accesso sicuro - Configurazione gruppi di connettori

- Scegliere Microsoft Azure e utilizzare per Scaling Calculator determinare le risorse necessarie


Accesso sicuro - Revisione della configurazione del connettore di risorse

- Sfruttare l'opzione per DNS Servers risolvere domini specifici tramite server DNS dedicati. Questa è una procedura ottimale per le organizzazioni con più domini interni.
- Fare clic su Save
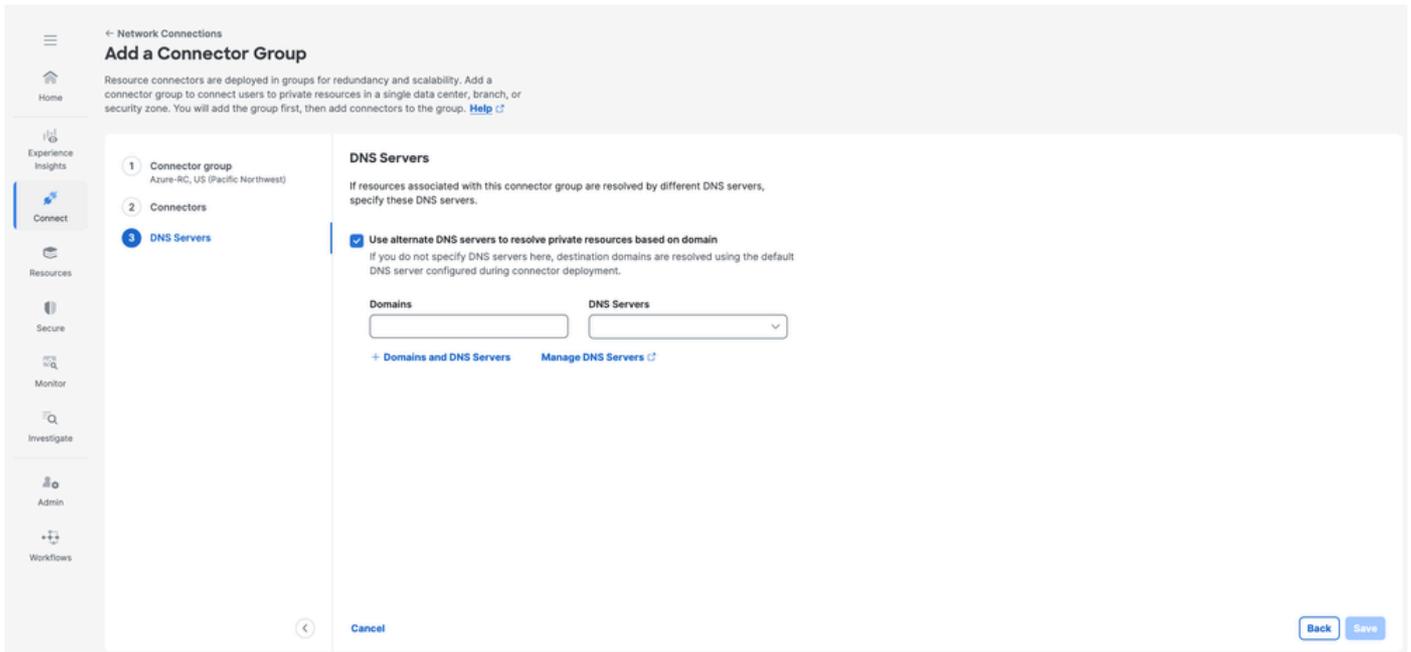
Accesso sicuro - Configurazione connettore risorse

- A questo punto, assicurarsi di copiare il Provisioning Key. Sarà necessario in seguito in Azure durante la distribuzione di Connettore risorse per abilitare la registrazione con il tenant di accesso sicuro.
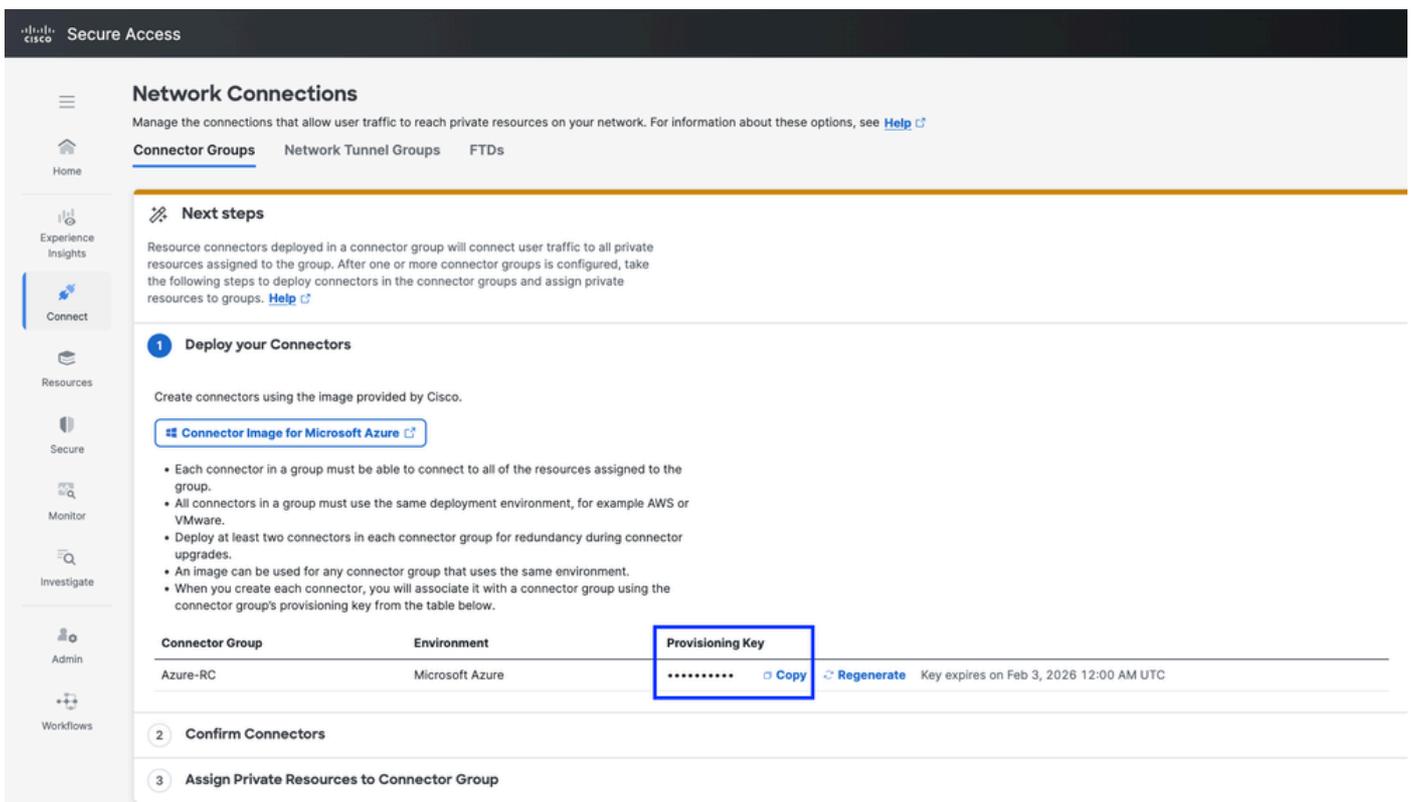
Accesso sicuro - Configurazione connettore risorse

Configurazioni in Azure

Passare al [portale di Azure](#), quindi passare a Microsoft Azure Marketplace e cercare l'immagine

Cisco Secure Access Resource Connector:

Accesso sicuro - Creazione connettore risorse in Azure

- Selezionare la scheda appropriata Subscription e Plan fare clic su Create

- Esaminare la configurazione di Disks, Networking e della chiave pubblica SSH

Home > Cisco Secure Access Resource Connector >

Create a virtual machine

Help me create a low cost VM   Help me create a VM optimized for high availability   Help me choose the right VM size for my workload

Run with Azure Spot discount ⓘ	☐
Size * ⓘ	Standard_F4s_v2 - 4 vcpus, 8 GiB memory ($119.14) ⌄
	See all sizes
Enable Hibernation ⓘ	☐
	ⓘ Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more ↗

Administrator account

Authentication type ⓘ	⦿ SSH public key
	◯ Password
	ⓘ Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.
Username * ⓘ	azureuser ✓
SSH public key source	Generate new key pair ⌄
SSH Key Type	⦿ RSA SSH Format
	◯ Ed25519 SSH Format
	ⓘ Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.
Key pair name *	Azure-RC_key ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ	⦿ None
	◯ Allow selected ports
Select inbound ports	Select one or more ports ⌄
	ⓘ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

< Previous   Next : Disks >   **Review + create**

⚠ Attenzione: Non perdere la chiave SSH privata; in caso contrario, non è possibile accedere alla CLI di RC e deve essere ridistribuita per la risoluzione dei problemi.

Home > Marketplace > Cisco Secure Access Resource Connector >

Create a virtual machine ··· 🤖 [Help me choose the right VM size for my workload] [Help me create a VM optimized for high availability] [Help me create a low cost VM]

Basics   **Disks**   Networking   Management   Monitoring   Advanced   Tags   Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more ⊡

ℹ There is a charge for the underlying storage resources consumed by your virtual machine. Learn more ⊡

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host ⓘ   ☐

> ℹ Encryption at host is not registered for the selected subscription. Learn more ⊡

OS disk

OS disk size ⓘ | Image default (52 GiB)   ⌄ |

OS disk type * ⓘ | Premium SSD (locally-redundant storage)   ⌄ |

Delete with VM ⓘ   ☑

Key management ⓘ | Platform-managed key   ⌄ |

Enable Ultra Disk compatibility ⓘ   ☐

Data disks for Azure-RC

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM ⓘ

Create and attach a new disk   Attach an existing disk

⌄ **Advanced**

Accesso sicuro - Creazione connettore risorse in Azure

- Incolla nel Provisioning Key User data campo il testo copiato da Cisco Secure Access

KEY=XXXXXXXXXXXXXXXXXXXXXX

Create a virtual machine

··· [Help me choose the right VM size for my workload] [Help me create a VM optimized for high availability] [Help me create a low cost VM]

Select a VM application to install

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. Learn more about custom data for VMs ⬚

Custom data

> ℹ️ Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. Learn more about custom data for VMs ⬚

User data

Pass a script, configuration file, or other data that will be accessible to your applications throughout the lifetime of the virtual machine. Don't use user data for storing your secrets or passwords. Learn more about user data for VMs ⬚

Enable user data   ☑

User data *   KEY="xxxxxxxxxxxxxxxxxxxxxxxxx"

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance   ☐
with NVMe ℹ️
                          ℹ️ The selected image and size are not supported for NVMe.
                          See supported VM images and sizes ⬚

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to

[< Previous] [Next : Tags >] [**Review + create**]

Accesso sicuro - Creazione connettore risorse in Azure

- Rivedere e fare clic su Create per procedere con la creazione del Resource Connector

Accesso sicuro - Creazione connettore risorse in Azure

- Dopo aver fatto clic su Create, verrà visualizzata un'opzione per il download della chiave privata. Fare clic su Download private key and create resource

Accesso sicuro - Creazione connettore risorse in Azure

⚠️

Attenzione: Non perdere la chiave SSH privata; in caso contrario, non è possibile accedere alla CLI di RC e deve essere ridistribuita per la risoluzione dei problemi.

- Dopodiché potrai vedere lo stato del tuo Resource Connector

Accesso sicuro - Distribuzione del connettore di risorse in Azure

- Passare quindi a [Dashboard di accesso sicuro](#) per confermare la connessione e la Resource Connector distribuzione completa nel tenant di accesso sicuro
- Fare clic su **Connect** > **Network Connections** > **Connector Groups**
- Sotto l'opzione 2 Conferma connettori fare clic suConfirm Connectorsper terminare la distribuzione

Accesso sicuro - Conferma connettore risorse

Ora è possibile visualizzare il nuovo connettore di risorse distribuito e connesso nel tenant Secure Access:

Accesso sicuro - Connettore risorse

Verifica

Accesso dalla CLI di Inbuild Bastion

In Azure, accedere al connettore delle risorse e fare clic su Bastion:

- Authentication Type: Scegli SSH Private key from Local File
- **Username**: È necessario utilizzare acadmin
- **Local File**: Scegliere il file scaricato private key in precedenza

Accesso sicuro - Accesso alla riga di comando di Connettore risorse

Accesso a RC dal terminale MAC-OS

Aprire il terminale e usare ssh -i <percorso-file-chiave-privata> acadmin@x.x.x.x per collegarsi al connettore delle risorse.

Accesso sicuro - Accesso alla riga di comando di Connettore risorse

Accesso da Windows - Putty

Per utilizzare la chiave privata, è necessario convertire il SSH private key da .pem a .ppk formart utilizzando Puttygen:

- Salva la chiave privata in formato ppk
- Avviare l'applicazione putty e navigare SSH > Auth > Credentials e sfogliare SSH private key in .ppk formato
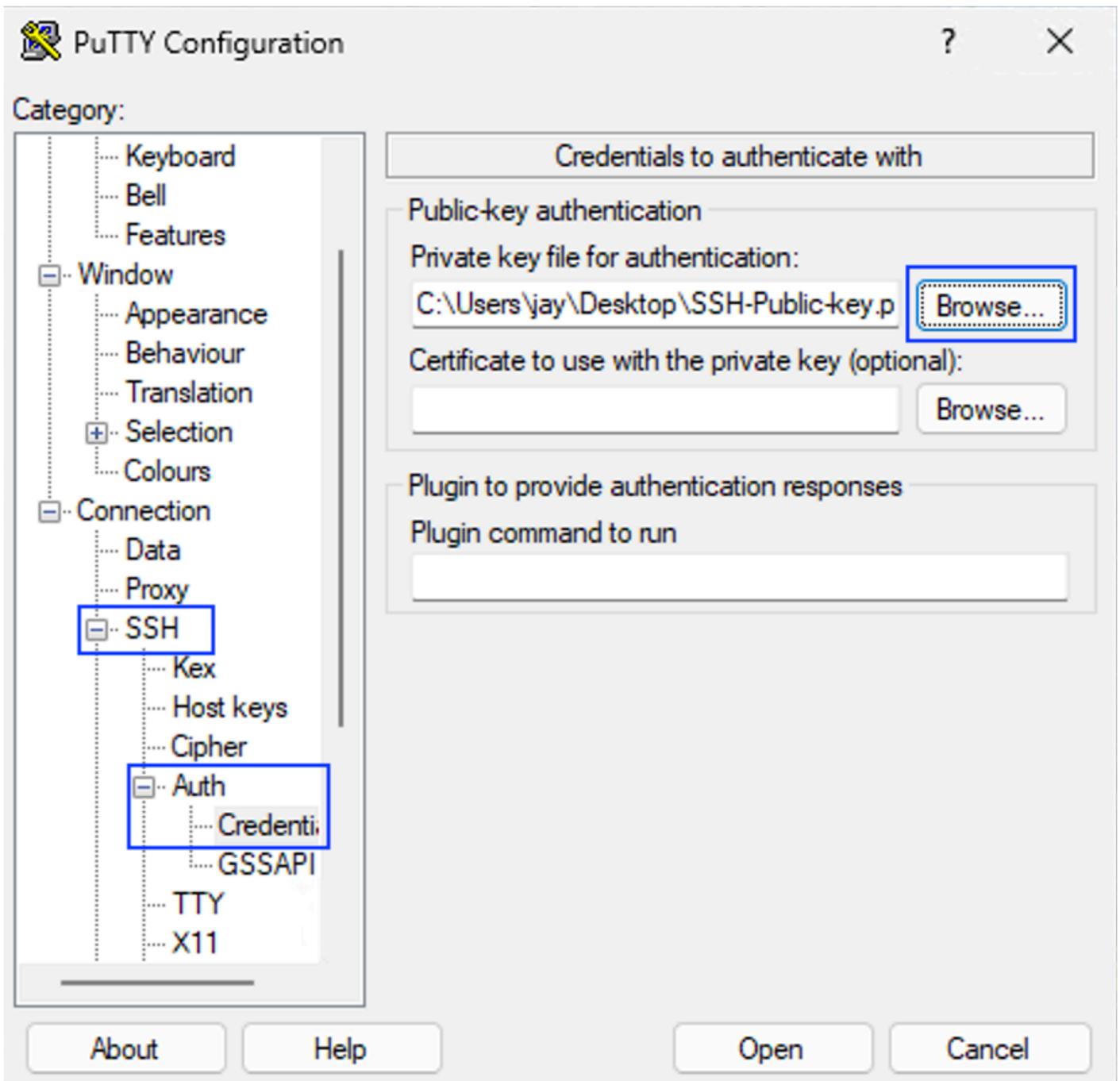
- Individuare Sessione inserire l'indirizzo IP del connettore di risorse e fare clic su Open

Suggerimento: username: passphrase acadmin: passphrase configurata durante la conversione della chiave privata dal formato .pem al formato .ppk

```
routeadd      || Allows (non-persistent) routes to be added with network and gate
way
routedel      || Allows (non-persistent) added routes to be deleted with network
              and gateway. This will not permit deletion of system created rou
tes
routeshow     || Shows all the routes in the system
sshkey        || Manages SSH public keys for acadmin user (add, list, delete, cle
an)
stats         || Displays a series of statistics
tcpdump       || Provides packet capture information on VM interface IP
techsupport   || Provides software version, VPN tunnel state, system monitoring
              metrics, snapshot info and software logs
version       || Shows the software version running in the VM
================================================================================
==
Linux Native
================================================================================
==
Command       || Description

clear         || Clears screen
date          || Provides system time
df            || Provides disk and partition usage
free          || Shows memory that is free and used
history       || Provides the list of commands previously executed
iostat        || Shows cpu and disk utilization
mpstat        || Shows detailed CPU utilization
netstat       || Shows all open network connections
nslookup      || Finds all DNS records for website
ping          || Confirms network connectivity
reboot        || Reboots the VM
tcptraceroute || Traceroutes pathway using TCP
traceroute    || Traceroutes pathway using ICMP packets
uptime        || Shows current time and how long the system has been up and runni
ng
vmstat        || Shows VM memory statistics
```

Risoluzione dei problemi

Per accedere al comando di risoluzione dei problemi, accedere a .

⚠️   Attenzione: Non perdere la chiave SSH privata; in caso contrario, non è possibile accedere alla CLI di RC e deve essere ridistribuita per la risoluzione dei problemi.

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Altri documenti ad accesso sicuro](#)

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).