

Déployer Secure Access Resource Connector dans Azure

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Configurations dans Secure Access](#)

[Configurations dans Azure](#)

[Vérifier](#)

[Accès depuis l'interface de ligne de commande intégrée Bastion](#)

[Accès à RC à partir du terminal MAC-OS](#)

[Accès à partir de Windows - Putty](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment déployer un connecteur de ressources étape par étape dans Azure.

Conditions préalables

Rassembler les informations requises et comprendre les

- Obtenir l'image du connecteur.
 - Vous pouvez télécharger l'image une seule fois et l'utiliser pour un nombre illimité de connecteurs dans un groupe de connecteurs.
 - Si vous utilisez une image précédemment téléchargée, assurez-vous qu'il s'agit de la dernière version.
 - Pour plus d'informations, consultez [Obtenir l'image du connecteur](#).
- Copiez la clé d'approvisionnement pour le groupe de connecteurs spécifique pour lequel vous déployez des connecteurs.
Voir [Clés d'approvisionnement pour les connecteurs de ressources](#).

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès administrateur au tableau de bord Cisco Secure Access

- Accès au portail Azure
- Client sécurisé Cisco
- Ordinateur Windows avec ZTA inscrit

Composants utilisés

Les informations contenues dans ce document sont basées sur le test effectué dans un environnement de travaux pratiques à l'aide des composants suivants :

- Client ZTNA
- Accès sécurisé
- Azure
- Ressource privée

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.

Configurer

Configurations dans Secure Access

Connectez-vous au [tableau de bord Secure Access](#) et accédez à **Connect > Network Connections > Connector Groups**

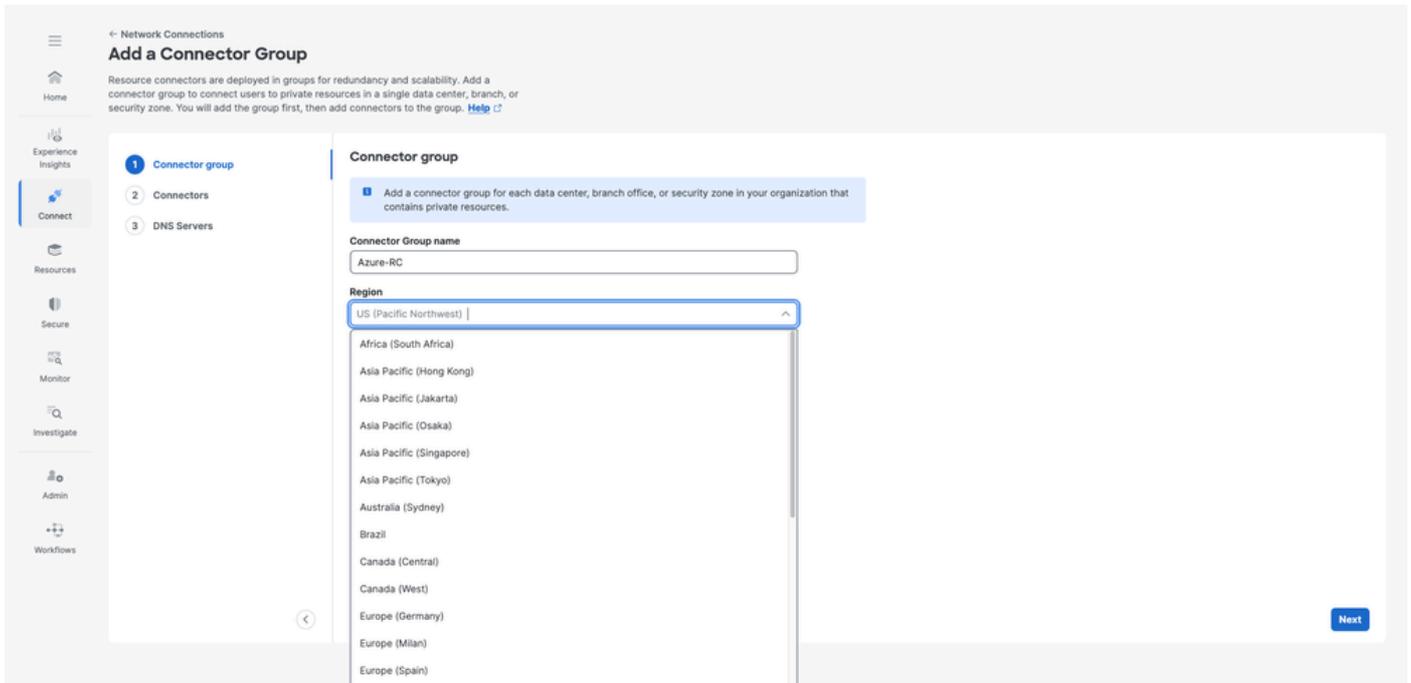
- Cliquez sur add

The screenshot shows the Cisco Secure Access interface for Network Connections. The 'Connector Groups' tab is selected. A 'Next steps' section provides instructions on assigning private resources. Below, a table lists three connector groups: FedRamp-RC, RC-ESXI, and RC-TEST, all with a 'Connected' status. An 'Add' button is highlighted in the top right of the table area.

Connector Group	Secure Access Region	Status	Connectors	Resources	Requests	Average CPU load
FedRamp-RC VMware ESXi	US (Pacific Northwest)	Connected	1	0	0	3%
RC-ESXI VMware ESXi	US (Pacific Northwest)	Connected	1	16	0	5%
RC-TEST VMware ESXi	US (Pacific Northwest)	Connected	1	0	0	5%

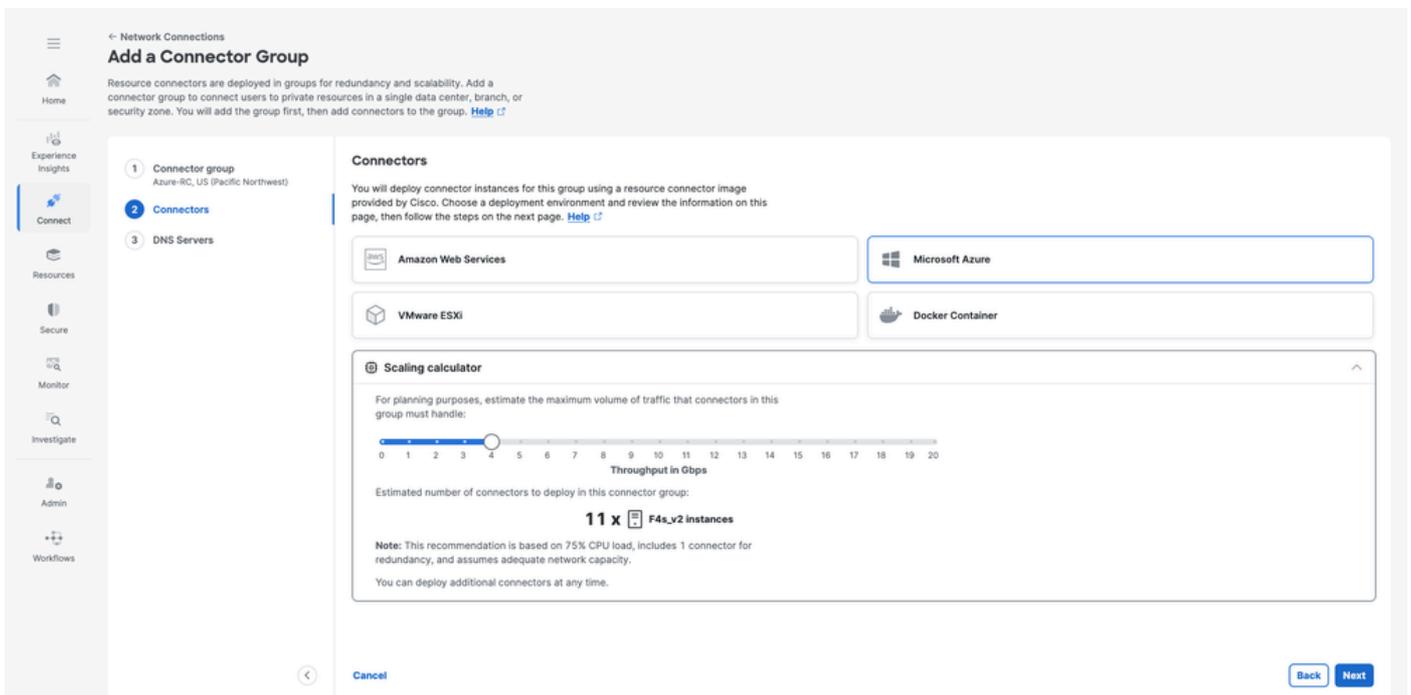
Accès sécurisé - Groupes de connecteurs

- Spécifiez le Connector Group Name et le Region
- Cliquer Next



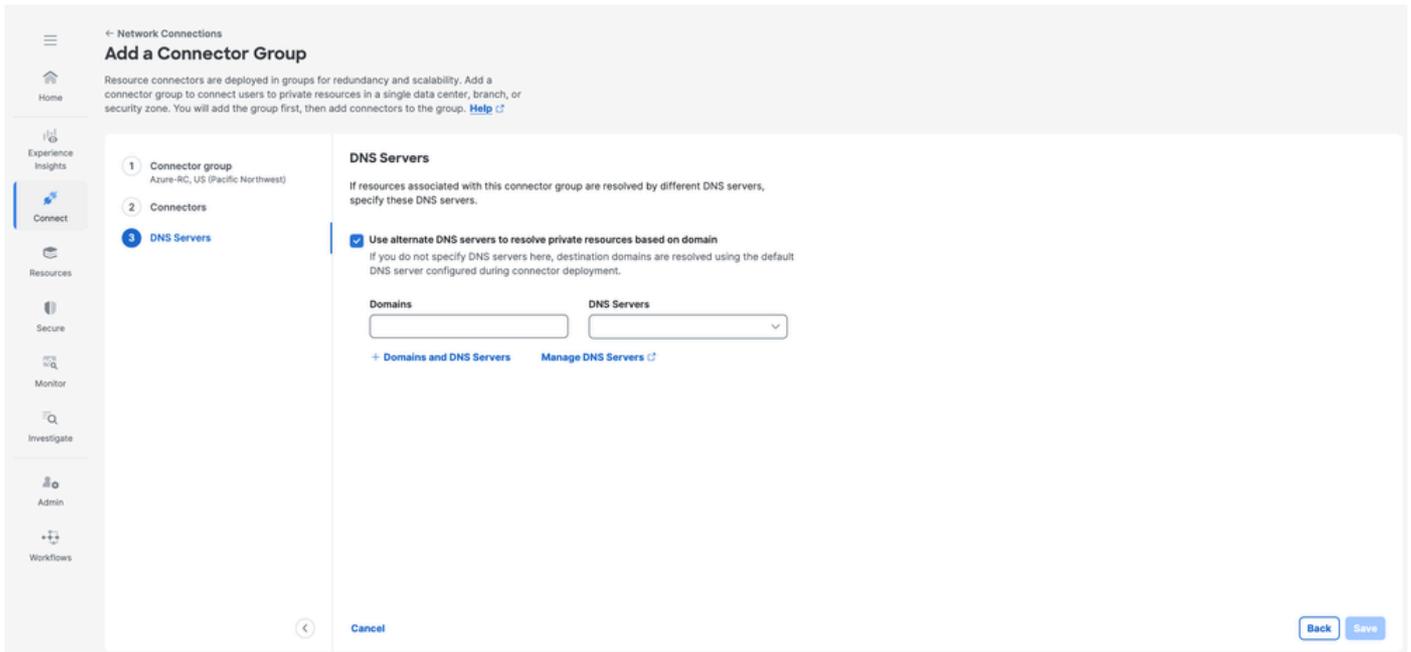
Accès sécurisé - Configuration des groupes de connecteurs

- Choisissez Microsoft Azure et utilisez la Scaling Calculator pour déterminer les ressources nécessaires



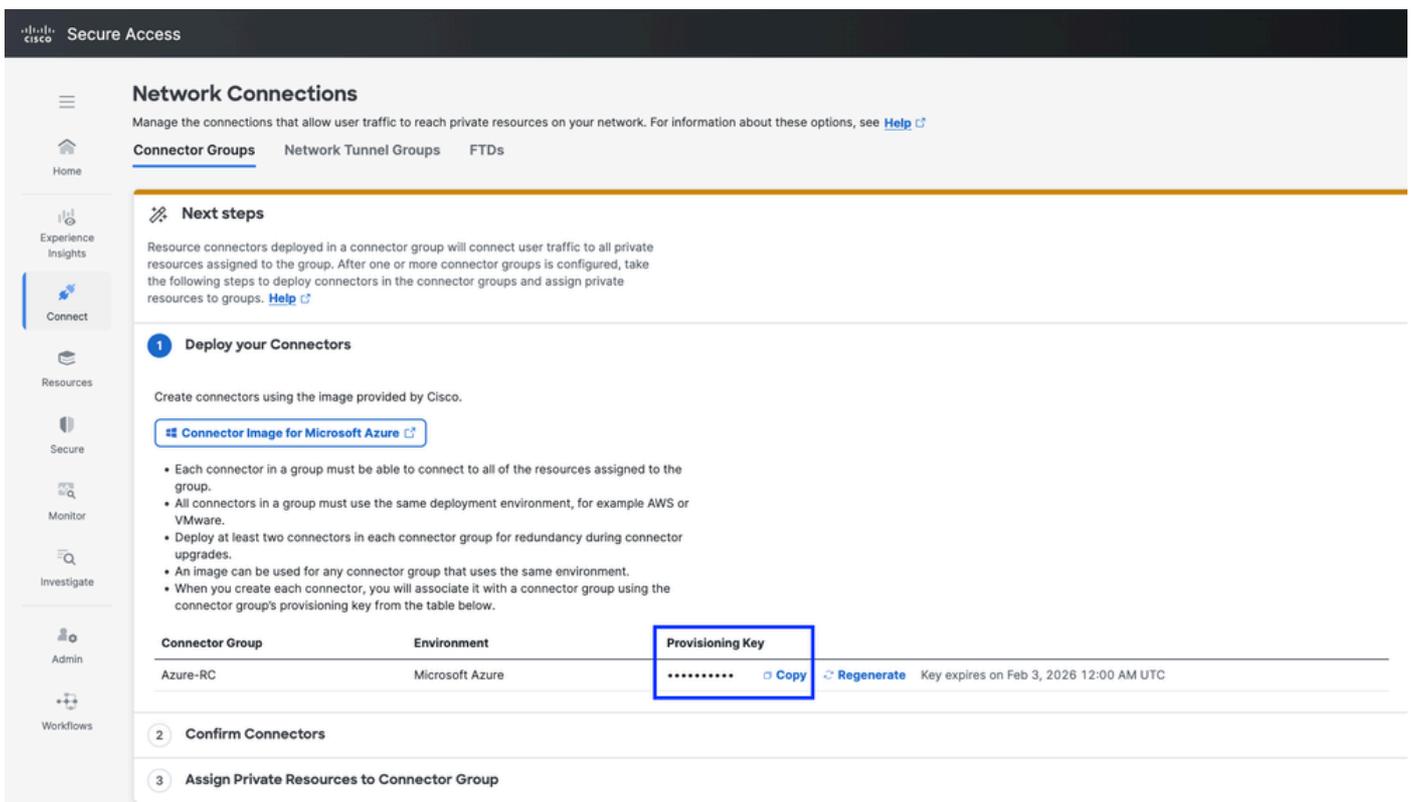
Accès sécurisé - Examen de la configuration du connecteur de ressources

- Utilisez l'option DNS Servers pour résoudre des domaines spécifiques via des serveurs DNS dédiés. Il s'agit d'une pratique recommandée pour les entreprises possédant plusieurs domaines internes.
- Cliquer Save



Accès sécurisé - Configuration du connecteur de ressources

- À ce stade, assurez-vous que vous copiez le Provisioning Key. Vous en aurez besoin ultérieurement dans Azure lors du déploiement de Resource Connector pour activer l'inscription auprès de votre locataire d'accès sécurisé.



Accès sécurisé - Configuration du connecteur de ressources

Configurations dans Azure

Accédez au [portail Azure](#), puis à Microsoft Azure Marketplace et recherchez l'image Cisco Secure

Access Resource Connector :

The screenshot shows the Microsoft Azure Marketplace search interface. The search bar contains 'Cisco Secure Access Resource Connector'. The results show one item: 'Cisco Secure Access Resource Connector' by Cisco Systems, Inc. The card includes the Cisco logo, the product name, the publisher name, and the category 'Virtual Machine'. A description states: 'Cisco Secure Access resource connectors securely forward authorized remote user traffic to resources on your network using Software plan starts at less than \$0.001/3 years'. There is a 'Create' button and a heart icon for favorites. The left sidebar shows navigation options like 'Get Started', 'Management', and 'My Marketplace'. The top navigation bar includes 'Microsoft Azure', a search bar, and 'Copilot'.

Accès sécurisé - Création du connecteur de ressources sur Azure

- Sélectionnez le Subscription approprié, puis Plan cliquez sur Create

The screenshot shows the product page for 'Cisco Secure Access Resource Connector' in the Azure Marketplace. The page header includes the Microsoft Azure logo, a search bar, and 'Copilot'. The breadcrumb trail is 'Home > Marketplace > Cisco Secure Access Resource Connector'. The product name is 'Cisco Secure Access Resource Connector' by Cisco Systems, Inc. The category is 'Virtual Machine'. There is a 'Add to Favorites' button and a badge indicating 'Azure benefit eligible'. Below this, there are dropdown menus for 'Subscription' and 'Plan' (Cisco Secure Access Resource Conne...). A 'Create' button and a 'Start with a pre-set configuration' button are visible. A link 'Want to deploy programmatically? Get started' is also present. The page has tabs for 'Overview', 'Plans + Pricing', 'Usage Information + Support', and 'Ratings + Reviews'. The 'Overview' tab is active, showing a description: 'Cisco Secure Access protects your internal/private resources, user devices, and corporate reputation from malicious and unwelcome activity, safeguarding both inbound and internet-bound traffic using a suite of access and security controls. Zero Trust Network Access to private/internal resources. To protect your private internal resources, Secure Access offers secure, granular Zero Trust Network Access to those resources. Resource Connectors forward traffic securely to private internal resources. Resource connectors are virtual machines deployed in your Azure environment that forward remote user traffic to your applications without requiring open inbound ports in your firewall. Resource connectors simplify setting up Zero Trust Access without any need for complex network configurations. More information. For more information about Cisco Secure Access, see https://www.cisco.com/site/us/en/products/security/secure-access/index.html. For more information about Secure Access options for connecting user traffic to private resources, see https://cisco.com/go/secure-access-network-connection-methods-documentation. To deploy this resource connector image, see https://www.cisco.com/go/secure-access-resource-connectors-azure-documentation. More products from Cisco Systems, Inc. See All

- Vérifiez la configuration de Disks et de la clé publique Networking SSH

Microsoft Azure Search resources, services, and docs (G+) Copilot

Home > Marketplace > Cisco Secure Access Resource Connector >

Create a virtual machine

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

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region * [Deploy to an Azure Extended Zone](#)

Availability options

Security type [Configure security features](#)

Image * [See all images](#) | [Configure VM generation](#)

VM architecture Arm64 x64

i Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * [See all sizes](#)

Enable Hibernation **i** Hibernate does not currently support Trusted launch and Confidential virtual machines for this image. [Learn more](#)

[< Previous](#) [Next : Disks >](#) [Review + create](#)

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 *
[See all sizes](#)

Enable Hibernation
i Hibernation does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#)

Administrator account

Authentication type SSH public key Password
i 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 *

SSH public key source

SSH Key Type RSA SSH Format Ed25519 SSH Format
i 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 *

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
i 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



Mise en garde : Ne perdez pas la clé SSH privée ; sinon, vous ne pouvez pas accéder à l'interface de ligne de commande RC et devez la redéployer pour le dépannage.

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

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

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network [Edit virtual network](#)

Subnet * [Edit subnet](#) 172.28.0.0 - 172.28.0.255 (256 addresses)

Public IP [Create new](#)
i Public IP addresses have a nominal charge. [Estimate price](#)

NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

Select inbound ports
i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Delete public IP and NIC when VM is deleted

Enable accelerated networking The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options None

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

Accès sécurisé - Création du connecteur de ressources sur Azure

- Collez la copie Provisioning Key de Cisco Secure Access dans le User data champ

KEY=XXXXXXXXXXXXXXXXXXXX

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

your VM after creation. Learn more >

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

i 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="xxxxxxxxxxxxxxxxxxxxxxxxxxxx"

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe

i 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

Accès sécurisé - Création du connecteur de ressources sur Azure

- Vérifiez et cliquez sur **Create** afin de poursuivre la création de votre Resource Connector

Create a virtual machine

Help me create a VM optimized for high availability

Help me choose the right VM size for my workload

Help me create a low cost VM

Validation passed

Subscription	cx-iac-sspt-zu-azure (cxssecurity)
Resource group	(new) Jai-Azure-RG
Virtual machine name	Azure-RC
Region	West US
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Cisco Secure Access Resource Connector - Gen2
VM architecture	x64
Size	Standard F4s v2 (4 vcpus, 8 GiB memory)
Enable Hibernation	No
Authentication type	SSH public key
Username	azureuser
SSH Key format	Ed25519
Key pair name	Azure-RC_key
Public inbound ports	None
Azure Spot	No

Disks

OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	vnet-westus
Subnet	snet-westus-1
Public IP	(new) Azure-RC-ip
Accelerated networking	Off

< Previous Next > Create

Accès sécurisé - Création du connecteur de ressources sur Azure

- Une fois que vous avez cliqué sur **Create**, une option de téléchargement de la clé privée apparaît. Cliquez sur **Download private key and create resource**

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Marketplace > Cisco Secure Access Resource Connector >

Create a virtual machine

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

Validation passed

Subscription	cx-tac-sspt-zu-azure (cxsecurity)
Resource group	(new) Jai-Azure-RG
Virtual machine name	Azure-RC
Region	West US
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Cisco Secure Access Resource Connector - Gen2
VM architecture	x64
Size	Standard F4s v2 (4 vcpus, 8 GiB memory)
Enable Hibernation	No
Authentication type	SSH public key
Username	azureuser
SSH Key format	Ed25519
Key pair name	Azure-RC_key
Public inbound ports	None
Azure Spot	No

Generate new key pair

An SSH key pair contains both a public key and a private key. **Azure doesn't store the private key.** After the SSH key resource is created, you won't be able to download the private key again. [Learn more](#)

[Download private key and create resource](#)

[Return to create a virtual machine](#)

Disks	
OS disk size	Image default
OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking	
Virtual network	vnet-westus
Subnet	snet-westus-1
Public IP	(new) Azure-RC-ip

< Previous | Next > | **Create**

Accès sécurisé - Création du connecteur de ressources sur Azure



Mise en garde : Ne perdez pas la clé SSH privée ; sinon, vous ne pouvez pas accéder à l'interface de ligne de commande RC et devez la redéployer pour le dépannage.

- Après cela, vous pouvez voir la progression de votre Resource Connector

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home >

CreateVm-cisco.cisco-resource-connector-cisco-sec-20260119144612 | Overview

Deployment

Search | Delete | Cancel | Redeploy | Download | Refresh

Overview

Inputs

Outputs

Template

Deployment is in progress

Deployment name: CreateVm-cisco.cisco-resource-connector-cisco... Start time: 1/19/2026, 3:08:05 PM
 Subscription: cx-tac-sspt-20-azure (cxsecurity) Correlation ID: d6369344-515a-4f8b-ad8e-6f8dccc87418
 Resource group: Jai-Azure-RG

Resource	Type	Status	Operation details
Azure-RC	Microsoft.Compute/virtualMachines	Created	Operation details
azure-rc708	Microsoft.Network/networkInterfaces	OK	Operation details
network-interface-associated-virtual-network-2026011915	Microsoft.Resources/deployments	OK	Operation details
Azure-RC-ip	Microsoft.Network/publicIPAddresses	OK	Operation details
Azure-RC-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

Accès sécurisé - Déploiement du connecteur de ressources sur Azure

- Accédez ensuite à [Secure Access Dashboard](#) afin de confirmer la connexion et le déploiement réussi Resource Connector dans votre locataire Secure Access
- Cliquez sur **Connect > Network Connections > Connector Groups**
- Sous l'option 2 Confirm Connectors, cliquez sur **Confirm Connectors** pour mettre fin au déploiement

Next steps

Resource connectors deployed in a connector group will connect user traffic to all private resources assigned to the group. After one or more connector groups is configured, take the following steps to deploy connectors in the connector groups and assign private resources to groups. [Help](#)

1 Deploy your Connectors

Create connectors using the image provided by Cisco.

[Connector Image for Microsoft Azure](#)

- Each connector in a group must be able to connect to all of the resources assigned to the group.
- All connectors in a group must use the same deployment environment, for example AWS or VMware.
- Deploy at least two connectors in each connector group for redundancy during connector upgrades.
- An image can be used for any connector group that uses the same environment.
- When you create each connector, you will associate it with a connector group using the connector group's provisioning key from the table below.

Connector Group	Environment	Provisioning Key
Azure-RC	Microsoft Azure	***** Copy Regenerate Key expires on Feb 3, 2026 12:00 AM UTC

2 Confirm Connectors

Deployed connectors will appear in this list when they contact Secure Access. You must confirm that each connector is expected before it can transmit traffic.

Connectors to confirm

#	Connector ID	Connector Group	Secure Access Region	Origin IP Address	Announced time	Enable	Revoke
1	01000000-0000-0000-0000-000000000000	Azure-RC	US (Pacific Northwest)	10.10.10.10	Jan 19, 2026 8:10 PM UTC	<input checked="" type="checkbox"/>	X Revoke

[Confirm connectors](#)

Accès sécurisé - Confirmation du connecteur de ressource

Vous pouvez maintenant voir votre nouveau connecteur de ressources déployé et connecté dans votre locataire d'accès sécurisé :

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#)

Connector Groups Network Tunnel Groups FTDs

Next steps

Resource connectors deployed in a connector group will connect user traffic to all private resources assigned to the group. After one or more connector groups is configured, take the following steps to deploy connectors in the connector groups and assign private resources to groups. [Help](#)

1 Assign Private Resources to Connector Group

Connector Groups Last 24 Hours

Manage all of the connectors (virtual machines) and associated resources that are deployed in your network for this Connector Group. [Help](#)

Search Secure Access Region Status Environment 4 Connector Groups [Add](#)

Connector Group	Secure Access Region	Status	Connectors	Resources	Requests	Average CPU load
Azure-RC Microsoft Azure	US (Pacific Northwest)	Connected	1	0	0	0%
FedRamp-RC VMware ESXI	US (Pacific Northwest)	Connected	1	0	0	3%
RC-ESXI VMware ESXI	US (Pacific Northwest)	Connected	1	16	0	5%
RC-TEST VMware ESXI	US (Pacific Northwest)	Connected	1	0	0	5%

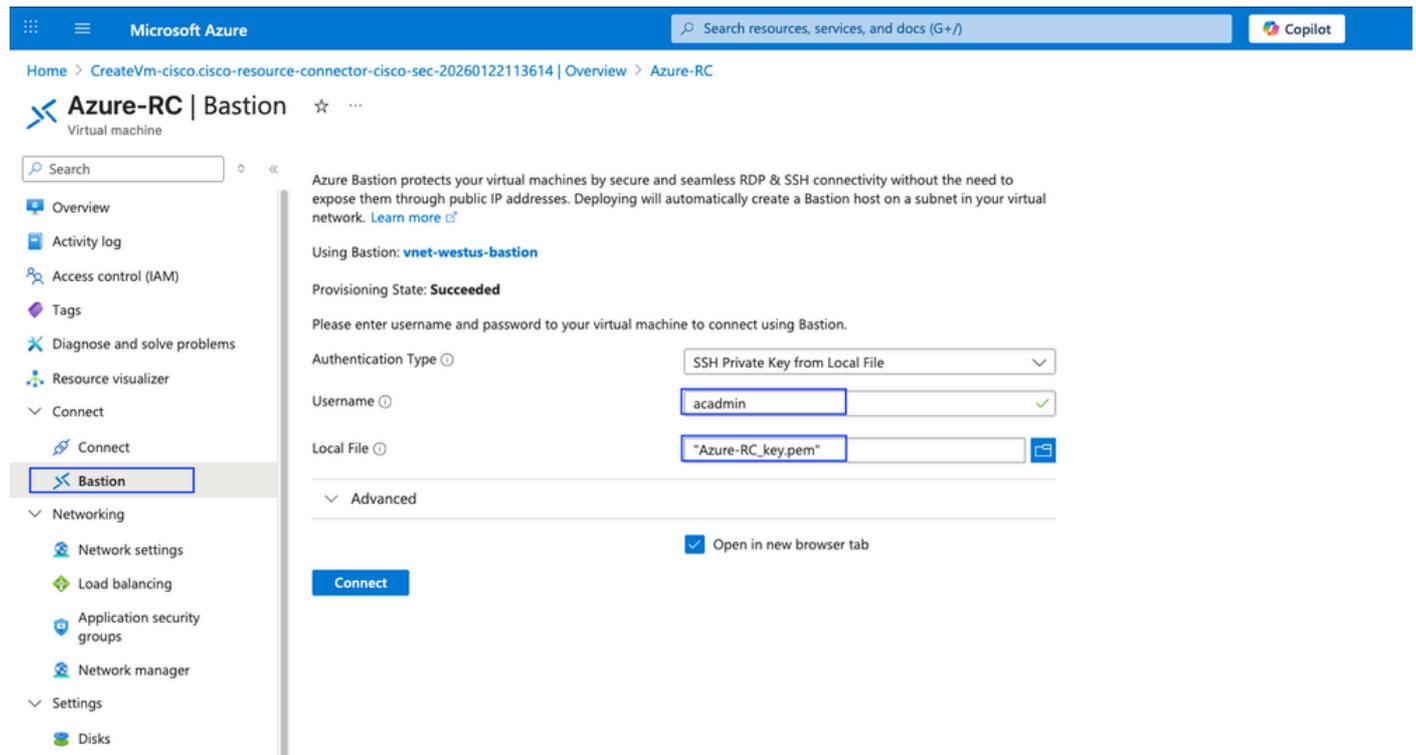
Accès sécurisé - Connecteur de ressources

Vérifier

Accès depuis l'interface de ligne de commande intégrée Bastion

Dans Azure, accédez à votre connecteur de ressources et cliquez sur Bastion:

- Authentication Type: Choisir SSH Private key from Local File
- Username: Vous devez utiliser acadmin
- Local File: Sélectionnez le private key téléchargé précédemment



The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, a search bar, and the Copilot icon. Below the navigation bar, the breadcrumb trail reads: Home > CreateVm-cisco.cisco-resource-connector-cisco-sec-20260122113614 | Overview > Azure-RC. The main content area is titled "Azure-RC | Bastion" and includes a search bar and a left-hand navigation menu. The menu items are: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Bastion (highlighted), Networking (with sub-items: Network settings, Load balancing, Application security groups, Network manager), Settings, and Disks. The main content area displays the Bastion configuration page. It includes a description of Azure Bastion, the name of the Bastion host (vnet-westus-bastion), and the provisioning state (Succeeded). Below this, there is a section for connecting to the virtual machine, which includes fields for Authentication Type (SSH Private Key from Local File), Username (acadmin), and Local File ("Azure-RC_key.pem"). There is also an "Advanced" section with a checkbox for "Open in new browser tab" and a "Connect" button.

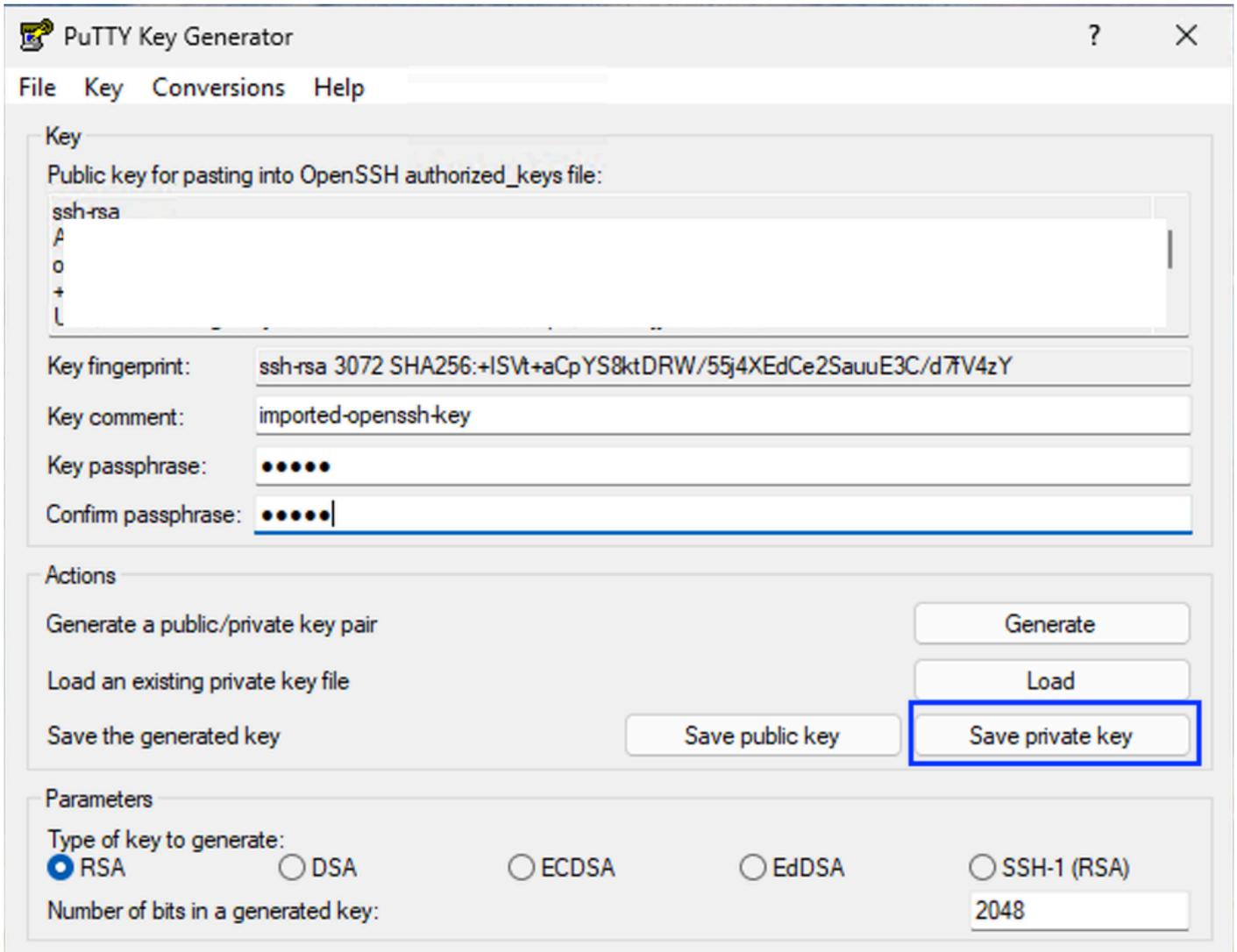

```
Downloads — ssh -i ~/Downloads/Azure-RC_key.pem acadmin@i-... 243x59
You have entered the Console Mode on this Resource Connector.
Type 'help' to get a list of supported commands.

Following is the list of commands available:
=====
Resource Connector Specific
=====
Command      || Description
-----
diagnostic   || Run a series of connectivity tests
help         || Provides the list of commands available
routeadd     || Allows (non-persistent) routes to be added with network and gateway
routedel     || Allows (non-persistent) added routes to be deleted with network
              and gateway. This will not permit deletion of system created routes
routeshow    || Shows all the routes in the system
sshkey       || Manages SSH public keys for acadmin user (add, list, delete, clean)
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
tcptracroute|| Traceroutes pathway using TCP
tracroute    || Traceroutes pathway using ICMP packets
uptime       || Shows current time and how long the system has been up and running
vmstat       || Shows VM memory statistics
$
```

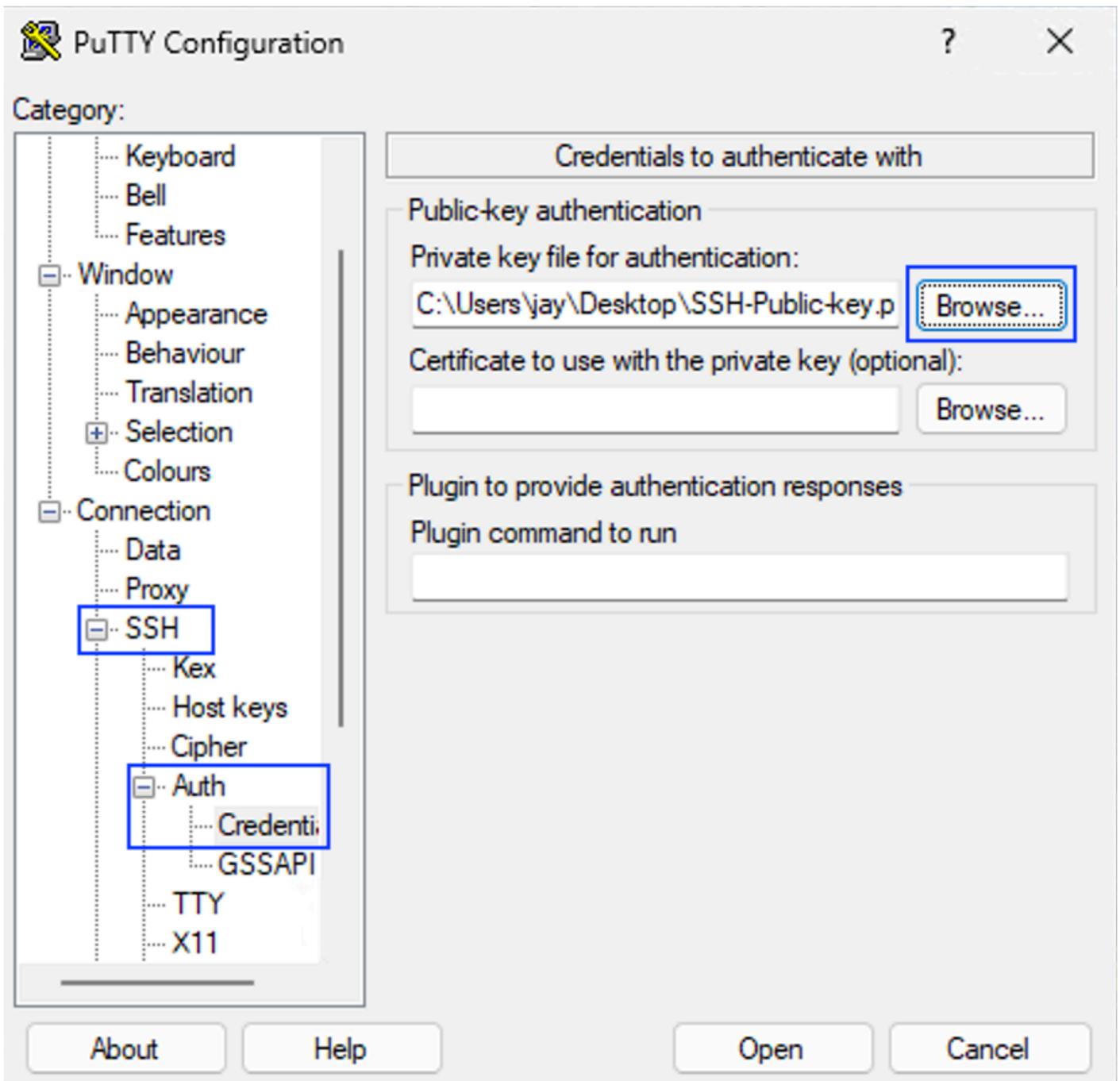
Accès sécurisé : accès à la ligne de commande du connecteur de ressources

Accès à partir de Windows - Putty

Afin d'utiliser la clé privée, vous devez convertir le SSH private key de à formart.pem en .ppk utilisant Puttygen:



- Enregistrez la clé privée au format .ppk
- Lancez l'application putty, accédez à SSH > Auth > Credentials et parcourez votre SSH private key dans .ppk format



- Accédez à Session l'adresse IP du connecteur de ressources et cliquez sur Open



Conseil : username (nom d'utilisateur) : acadmin phrase de passe : la phrase de passe configurée lors de la conversion de la clé privée du format .pem au format .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
tcptracroute|| Traceroutes pathway using TCP
tracroute    || Traceroutes pathway using ICMP packets
uptime       || Shows current time and how long the system has been up and runni
ng
vmstat       || Shows VM memorv statistics

```

Dépannage

Afin d'accéder à la commande de dépannage, accédez à .



Mise en garde : Ne perdez pas la clé SSH privée ; sinon, vous ne pouvez pas accéder à l'interface de ligne de commande RC et devez la redéployer pour le dépannage.

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Autres documents d'accès sécurisé](#)

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.