

# AzureでSecure Accessリソースコネクタを展開する

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [設定](#)

#### [セキュアアクセスの設定](#)

#### [Azureの構成](#)

### [確認](#)

#### [Inbuild Bastion CLIからのアクセス](#)

#### [MAC-OS端末からのRCへのアクセス](#)

#### [Windowsからのアクセス-Putty](#)

### [トラブルシューティング](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Azureでステップバイステップのリソースコネクタをデプロイする方法について説明します。

## 前提条件

必要な情報を収集し、

- コネクタイメージを取得します。
  - イメージは1回ダウンロードするだけで、任意のコネクタグループ内の任意の数のコネクタに使用できます。
  - 以前にダウンロードしたイメージを使用する場合は、イメージが最新バージョンであることを確認します。
  - 詳細については、「[コネクタイメージの取得](#)」を参照してください。
- コネクタを展開する特定のコネクタグループのプロビジョニングキーをコピーします。  
「[リソースコネクタのプロビジョニングキー](#)」を参照してください。

## 要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Accessダッシュボードの管理者アクセス

- Azureポータルアクセス
- Cisco Secure Client
- ZTAが登録されているWindowsマシン

## 使用するコンポーネント

このドキュメントの情報は、次のコンポーネントを使用してラボ環境で実行されたテストに基づいています。

- ZTNAクライアント
- セキュアなアクセス
- Azure
- プライベートリソース

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### セキュアアクセスの設定

[セキュアアクセスダッシュボード](#)にログインし、[接続](#)>[ネットワーク接続](#)>[コネクタグループ](#)に移動します

- addをクリックします。

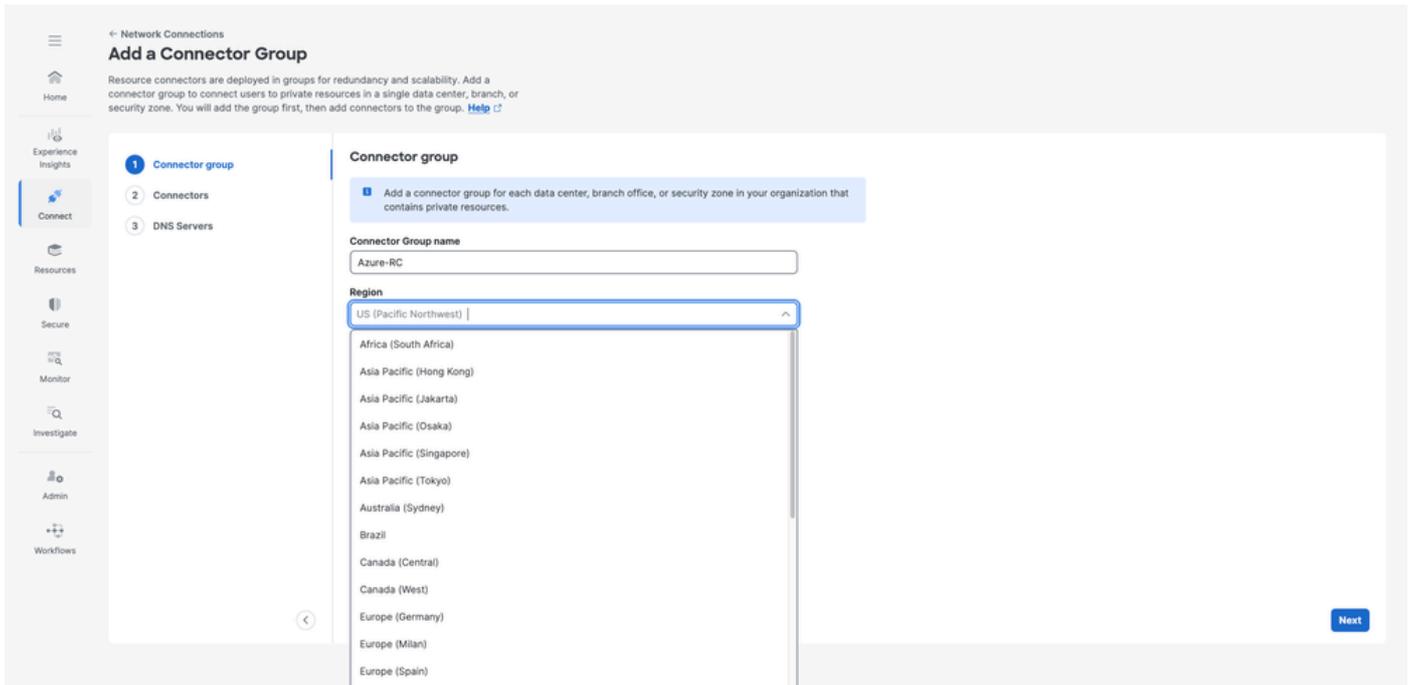
The screenshot shows the Cisco Secure Access Network Connections dashboard. The 'Connector Groups' tab is selected, displaying a table of existing connector groups. The table has columns for Connector Group, Secure Access Region, Status, Connectors, Resources, Requests, and Average CPU load. There are three connector groups listed: FedRamp-RC, RC-ESXI, and RC-TEST. An 'Add' button is visible in the top right corner of the table area.

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

### セキュアアクセス – コネクタグループ

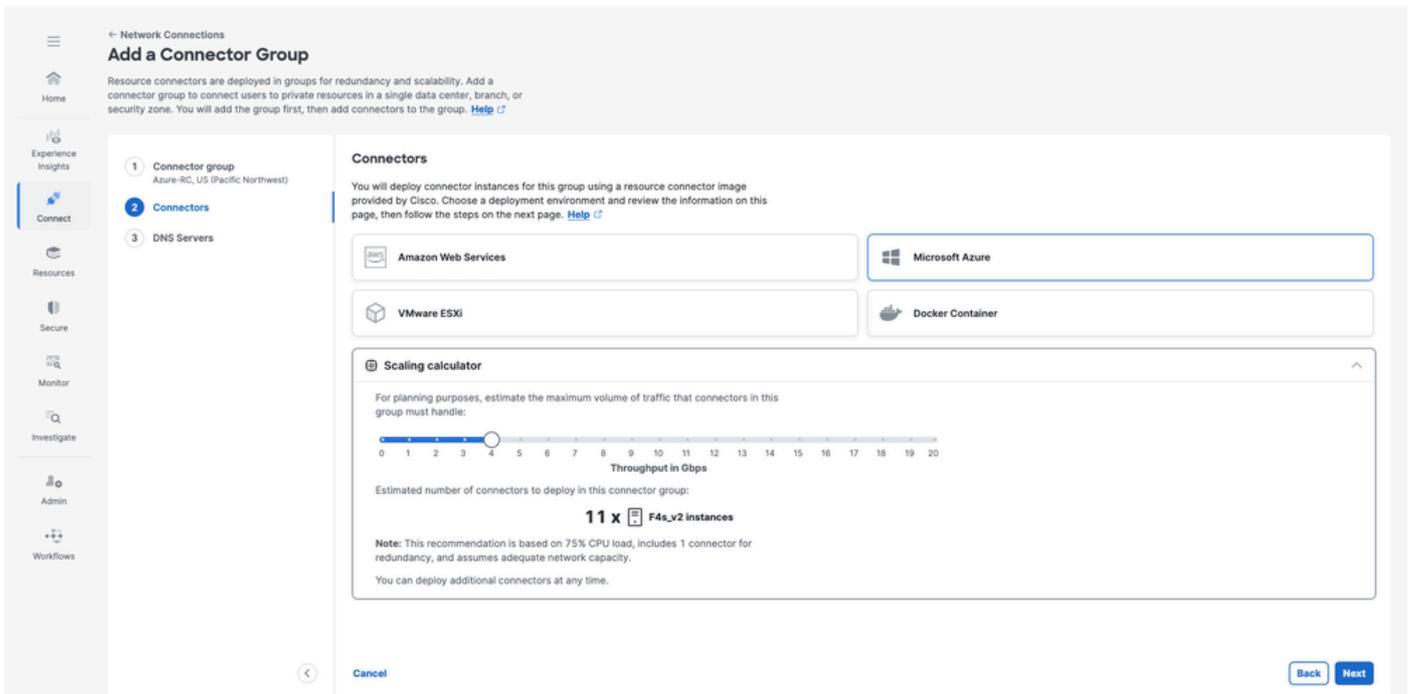
- コネクタグループ名とリージョンを指定します。

- [Next] をクリックします。



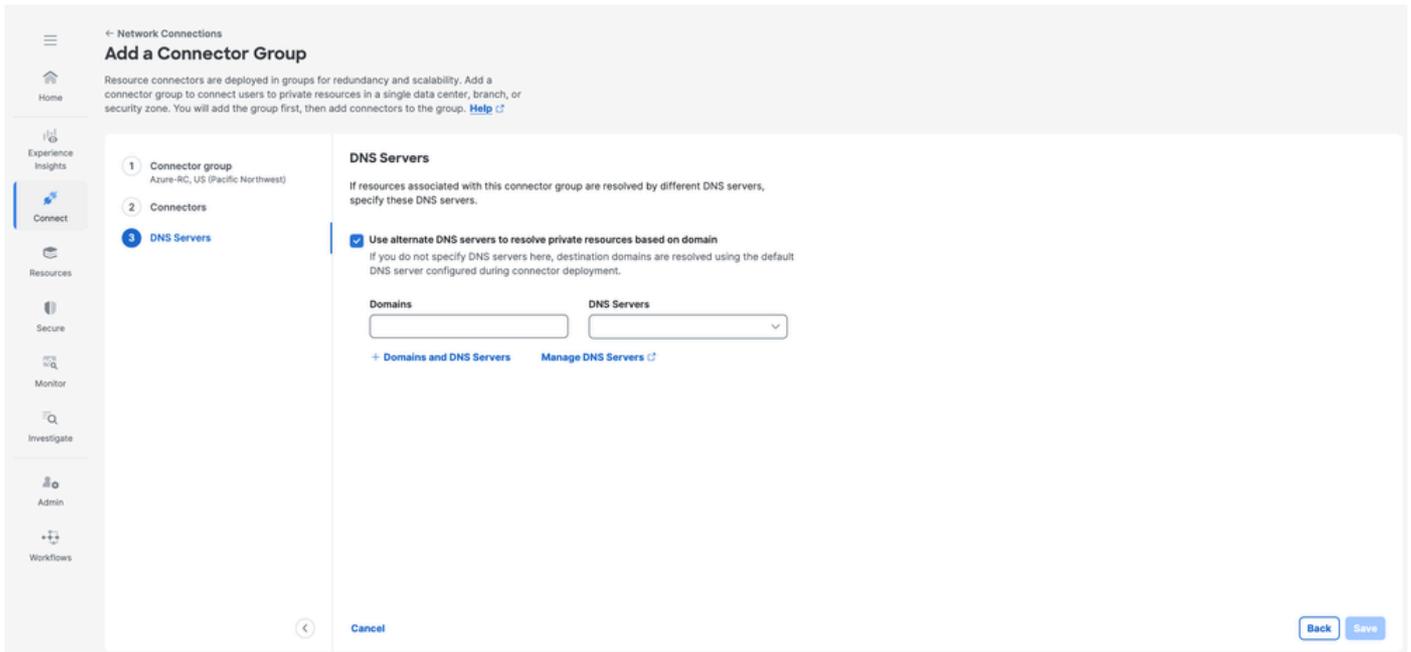
## セキュアアクセス：コネクタグループの設定

- Microsoft Azure を選択し、Scaling Calculator を使用して、必要なリソースを決定します



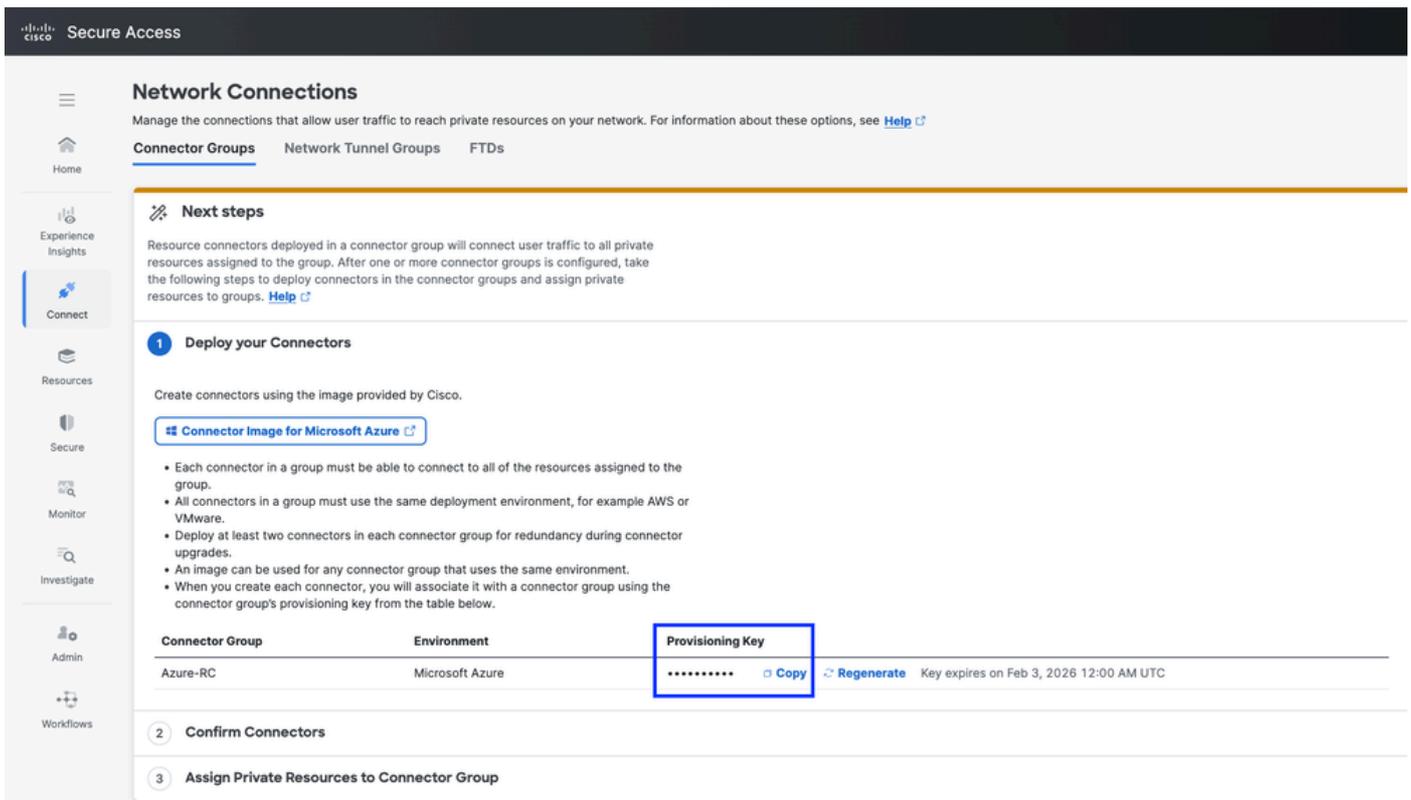
## セキュアアクセス – リソースコネクタ設定のレビュー

- DNS Servers オプションを活用し、専用のDNSサーバを介して特定のドメインを解決します。これは、複数の内部ドメインを持つ組織にとってベストプラクティスであると考えられています。
- [Save] をクリックします。



## セキュアアクセス：リソースコネクタの設定

- この段階で、プロビジョニングキーをコピーします。後でAzureでリソースコネクタのデプロイ中に、セキュアアクセステナントへの登録を有効にする必要があります。



## セキュアアクセス：リソースコネクタの設定

### Azureの構成

[Azure Portal](#)に移動してMicrosoft Azure Marketplaceに移動し、Cisco Secure Access Resource Connectorイメージを検索します。

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

Home > Marketplace

Get Started

Service Providers

Search with AI

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Infrastructure Services (1)

Security (1)

AI Apps and Agents (0)

Analytics (0)

Blockchain (0)

Databases (0)

DevOps (0)

Private Marketplace (0)

Search: Cisco Secure Access Resource Connector

Filters: Publisher name: All, Product Type: All, Publisher Type: All, Operating System: All, Pricing: All

Options:  Azure benefit eligible only,  Azure services only

New! Get AI-generated suggestions for 'cisco secure access resource connector' View suggestions

Showing 1 to 1 of 1 results for 'Cisco Secure Access Resource Connector'. Clear search



Cisco Secure Access Resource Connector  
Cisco Systems, Inc.  
Virtual Machine  
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

Create

Navigation: Previous Page 1 of 1 Next

## セキュアアクセス – Azureでのリソースコネクタの作成

- 適切なSubscriptionとPlanを選択し、Createをクリックします。

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

Home > Marketplace > Cisco Secure Access Resource Connector

Cisco Systems, Inc.



### Cisco Secure Access Resource Connector

Cisco Systems, Inc. | Virtual Machine

Azure benefit eligible

Subscription: [Dropdown] Plan: Cisco Secure Access Resource Conne... Create Start with a pre-set configuration

Want to deploy programmatically? Get started

Overview Plans + Pricing Usage Information + Support Ratings + Reviews

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

## セキュアアクセス – Azureでのリソースコネクタの作成

- ディスク、ネットワーキング、およびSSH公開キーの設定を確認します

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** Hibernation does not currently support Trusted launch and Confidential virtual machines. [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** Hibernate 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



注意：秘密SSHキーを失わないでください。失わないと、RC CLIにアクセスできず、トラブルシューティングのために再展開する必要があります。

# 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**

## セキュアアクセス – Azureでのリソースコネクタの作成

- Cisco Secure Accessからコピーされたプロビジョニングキーをユーザーデータフィールドに貼り付けます

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 will create soon. ...

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="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

### 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

## セキュアアクセス – Azureでのリソースコネクタの作成

- リソースコネクタの作成を続行するには、確認して「作成」をクリックします

## 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-uac-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  |

### 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

## セキュアアクセス – Azureでのリソースコネクタの作成

- Create をクリックすると、秘密キーをダウンロードするオプションが表示されます。Download private key and create resource をクリックします

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-scpt-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

**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**

### 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

## セキュアアクセス – Azureでのリソースコネクタの作成



注意：秘密SSHキーを失わないでください。失わないと、RC CLIにアクセスできず、トラブルシューティングのために再展開する必要があります。

- その後、リソースコネクタの進行状況を確認できます

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-scpt-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 | <a href="#">Operation details</a> |
| azure-rc708   | Microsoft.Network/networkInterfaces     | OK      | <a href="#">Operation details</a> |
| network-interface-associated-virtual-network-2026011915 | Microsoft.Resources/deployments         | OK      | <a href="#">Operation details</a> |
| Azure-RC-ip   | Microsoft.Network/publicIPAddresses     | OK      | <a href="#">Operation details</a> |
| Azure-RC-nsg  | Microsoft.Network/networkSecurityGroups | OK      | <a href="#">Operation details</a> |

## セキュアアクセス – Azureでのリソースコネクタの配置

- 次に、[Secure Access Dashboard](#)に移動し、リソースコネクタの接続を確認して、セキュアアクセステナントに正しく導入します
- Connect > Network Connections > Connector Groupsの順にクリックします。
- オプション2のコネクタの確認で、コネクタの確認をクリックして導入を完了します

**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 | ***** <a href="#">Copy</a> <a href="#">Regenerate</a> 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 | ...          | Azure-RC        | US (Pacific Northwest) | ...               | Jan 19, 2026 8:10 PM UTC | <input checked="" type="checkbox"/> | <a href="#">X Revoke</a> |

[Confirm connectors](#)

## セキュアアクセス – リソースコネクタの確認

これで、セキュアアクセステナントに導入され、接続された新しいリソースコネクタを確認できます。

**Network Connections**

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

**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<br>Microsoft Azure | US (Pacific Northwest) | Connected | 1          | 0         | 0        | 0%               |
| FedRamp-RC<br>VMware ESXI   | US (Pacific Northwest) | Connected | 1          | 0         | 0        | 3%               |
| RC-ESXI<br>VMware ESXI      | US (Pacific Northwest) | Connected | 1          | 16        | 0        | 5%               |
| RC-TEST<br>VMware ESXI      | US (Pacific Northwest) | Connected | 1          | 0         | 0        | 5%               |

## セキュアアクセス – リソースコネクタ

# 確認

## Inbuild Bastion CLIからのアクセス

Azureでリソースコネクタにアクセスし、Bastionをクリックします。

- Authentication Type: Choose SSH Private key from Local File
- ユーザ名: acadmin を使用する必要があります。
- Local File : 前にダウンロードした秘密キーを選択します。

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 path is: 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 (with sub-item: Disks). The main content area displays the Bastion configuration for the virtual machine. It includes a description of Azure Bastion, the provisioning state 'Succeeded', and a 'Connect' button. The configuration fields are: 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 checked option 'Open in new browser tab'.

```
cdn.bastionglobal.azure.com/2020-07-15/index.react.html?datapath=ee6d...
Import bookmarks... Quicker Backlog Training Tech Articles Work Links Personal TC-EE Related LAB Secure-Access CSA-IFT Sec
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
traceroute   || Traceroutes pathway using ICMP packets
uptime       || Shows current time and how long the system has been up and running
vmstat       || Shows VM memory statistics
7:00 PM 10/11/2020 27d 50:00:00 25 ~ $
```

## セキュアアクセス – リソースコネクタのコマンドラインへのアクセス

### MAC-OS端末からのRCへのアクセス

端末を開き、ssh -i <private-key-file-path> [acadmin@x.x.x.x](#)を使用して、リソースコネクタに接続します。

```
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.

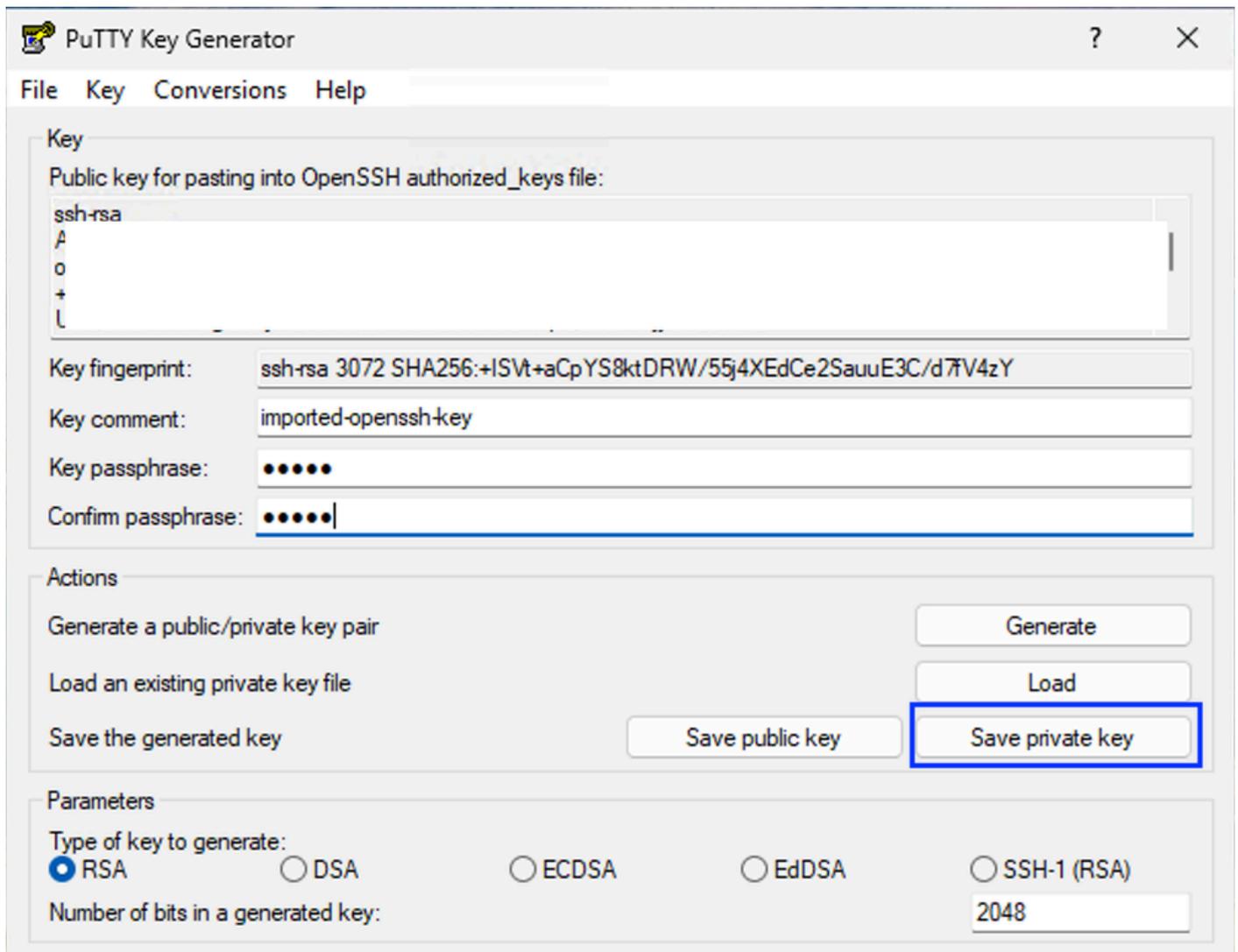
Following is the list of commands available:
=====
Resource Connector Specific
=====
Command      || Description
-----
diagnostic   || Run a series of connectivity tests
help         || Provides the list of commands available
routeadd     || Allows (non-persistent) routes to be added with network and 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
$
```

## セキュアアクセス – リソースコネクタのコマンドラインへのアクセス

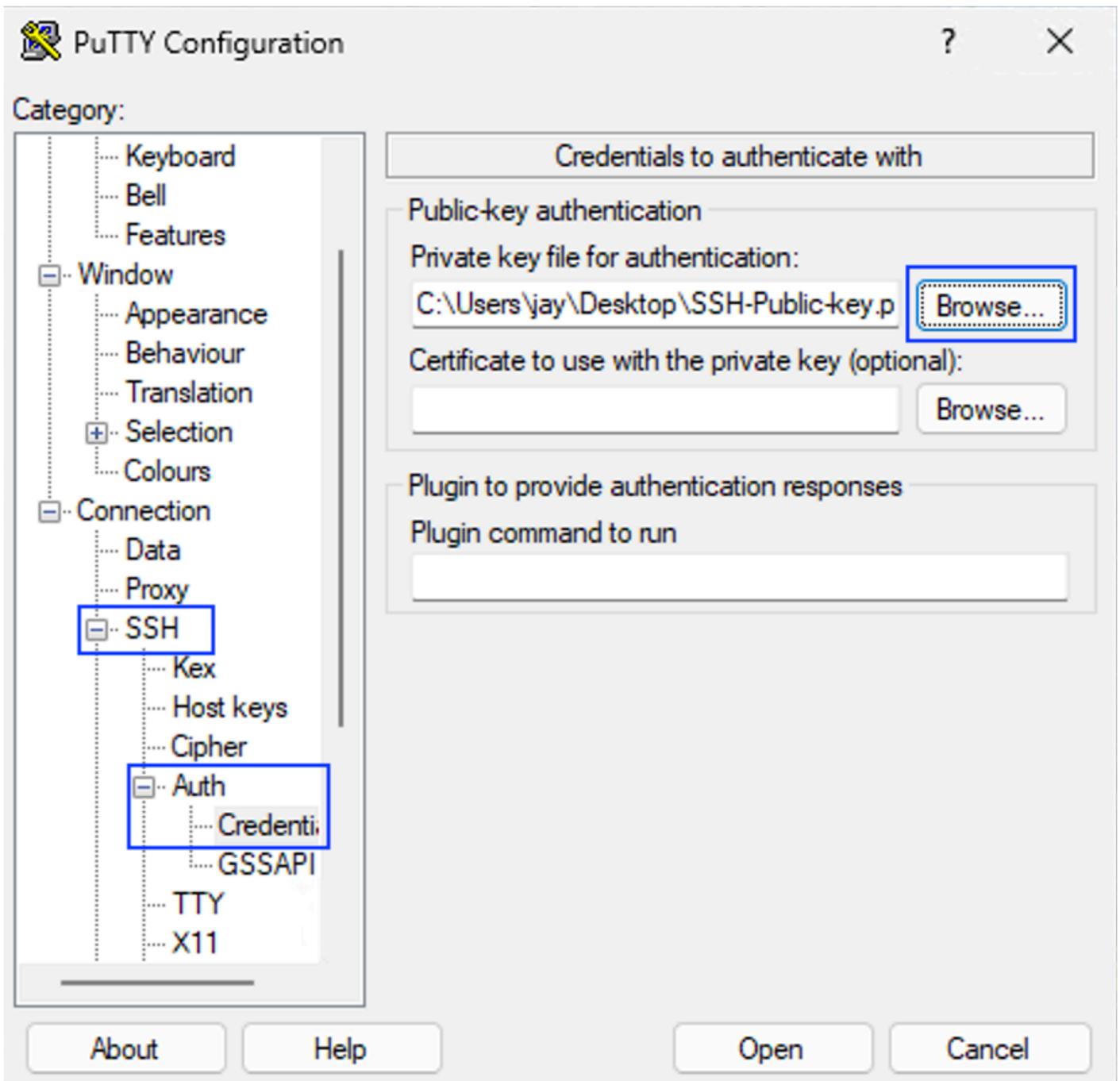
### Windowsからのアクセス – Putty

秘密キーを使用するには、Puttygenを使用して、SSH秘密キーを.pemから.ppkに変換する必要があります

。



- 秘密キーを.ppk形式で保存します
- puttyアプリケーションを起動し、SSH > Auth > Credentialsに移動して、SSH秘密キーを.ppk形式で参照します



- Sessionpageに移動し、リソースコネクタのIPアドレスを入力して、Openをクリックします



ヒント：ユーザ名：acadminパスフレーズ：秘密キーを.pemから.ppk形式に変換するときに設定されるパスフレーズ

```

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
traceroute || 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

```

## トラブルシューティング

トラブルシューティングコマンドにアクセスするには、にアクセスします。



注意：秘密SSHキーを失わないでください。失わないと、RC CLIにアクセスできず、トラブルシューティングのために再展開する必要があります。

## 関連情報

- [シスコのテクニカルサポートとダウンロード](#)
- [その他のセキュアアクセスに関する文書](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。