AzureでSecure Accessリソースコネクタを展開する

内容

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

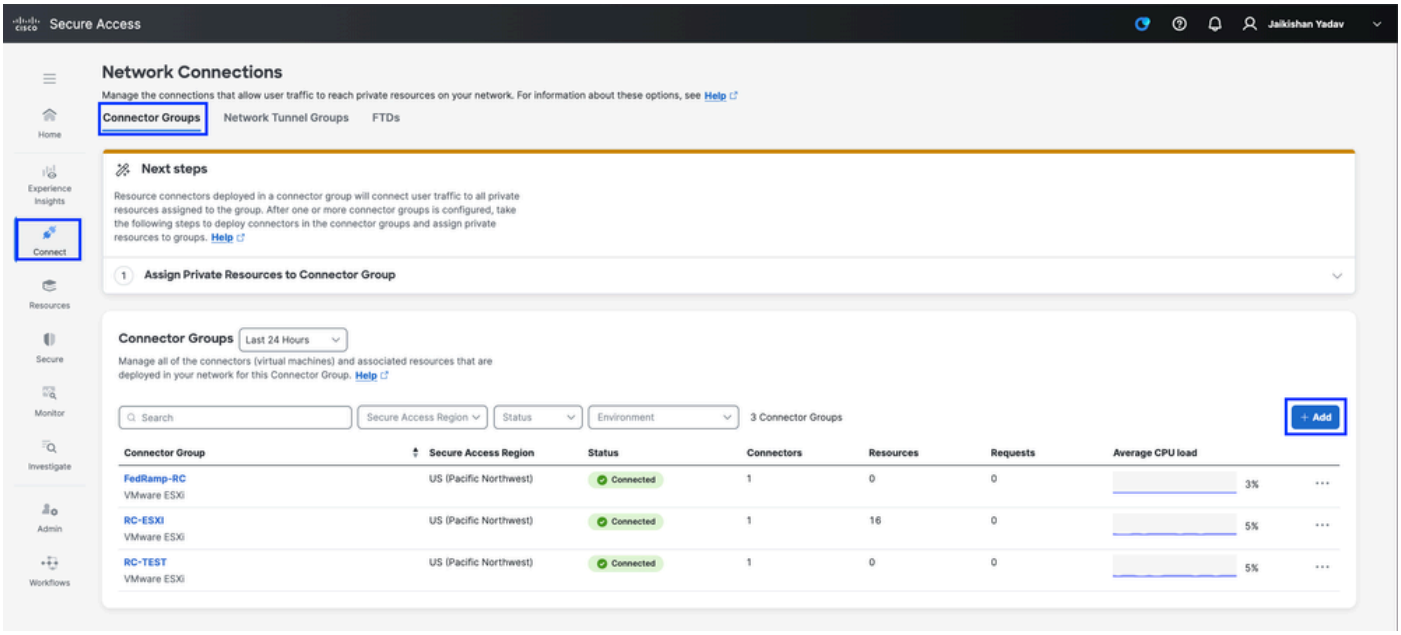
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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

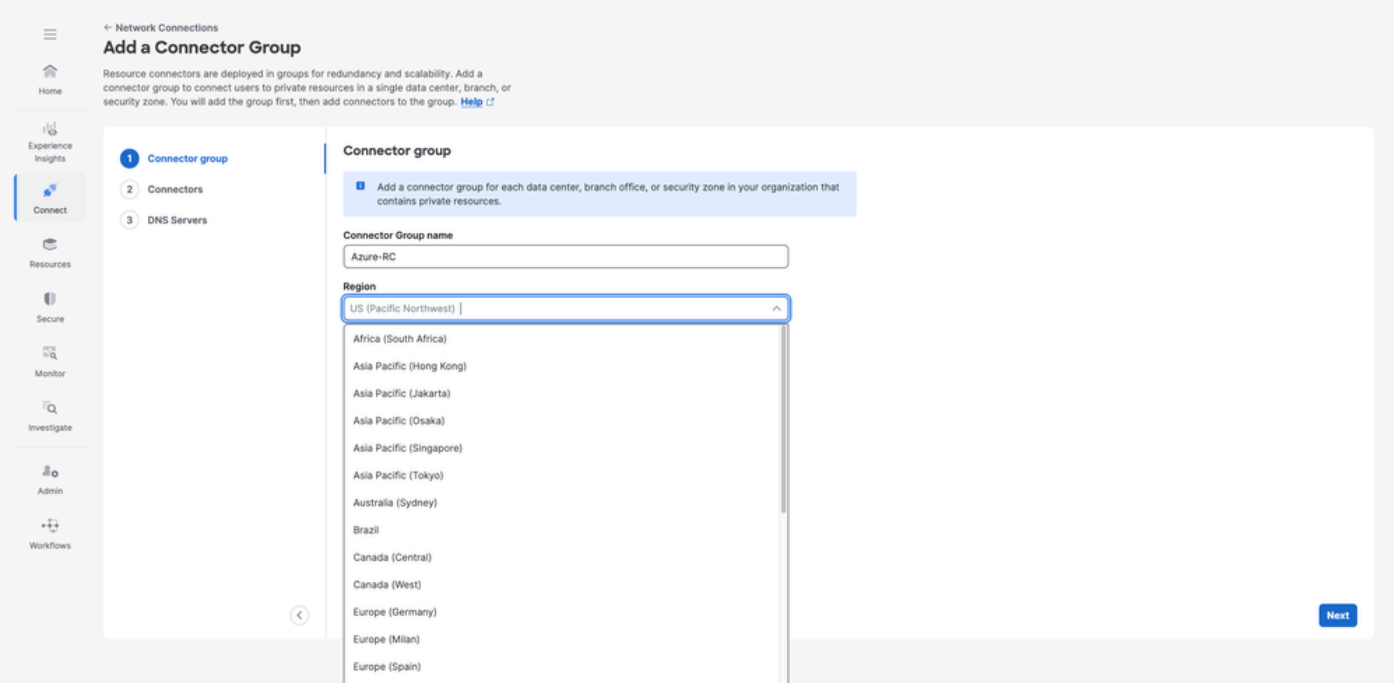
- addをクリックします。



セキュアアクセス – コネクタグループ

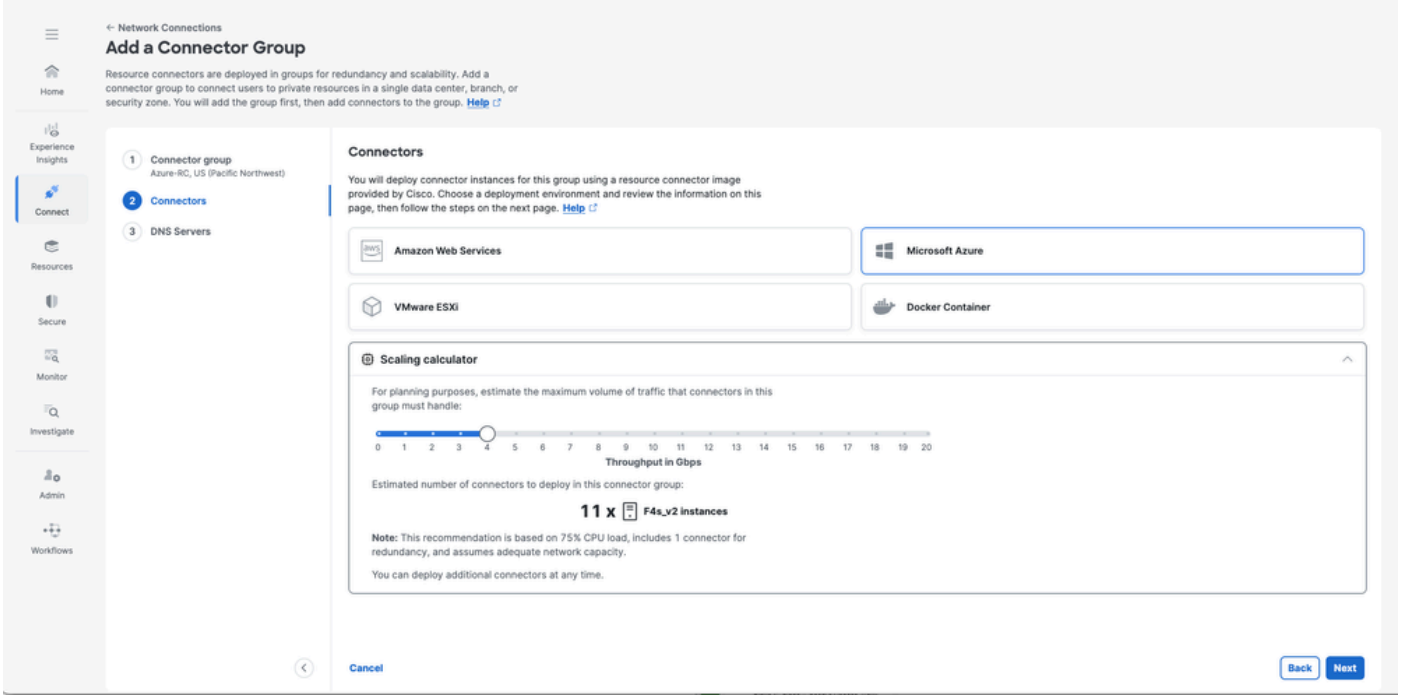
- コネクタグループ名とリージョンを指定します。

- [Next] をクリックします。



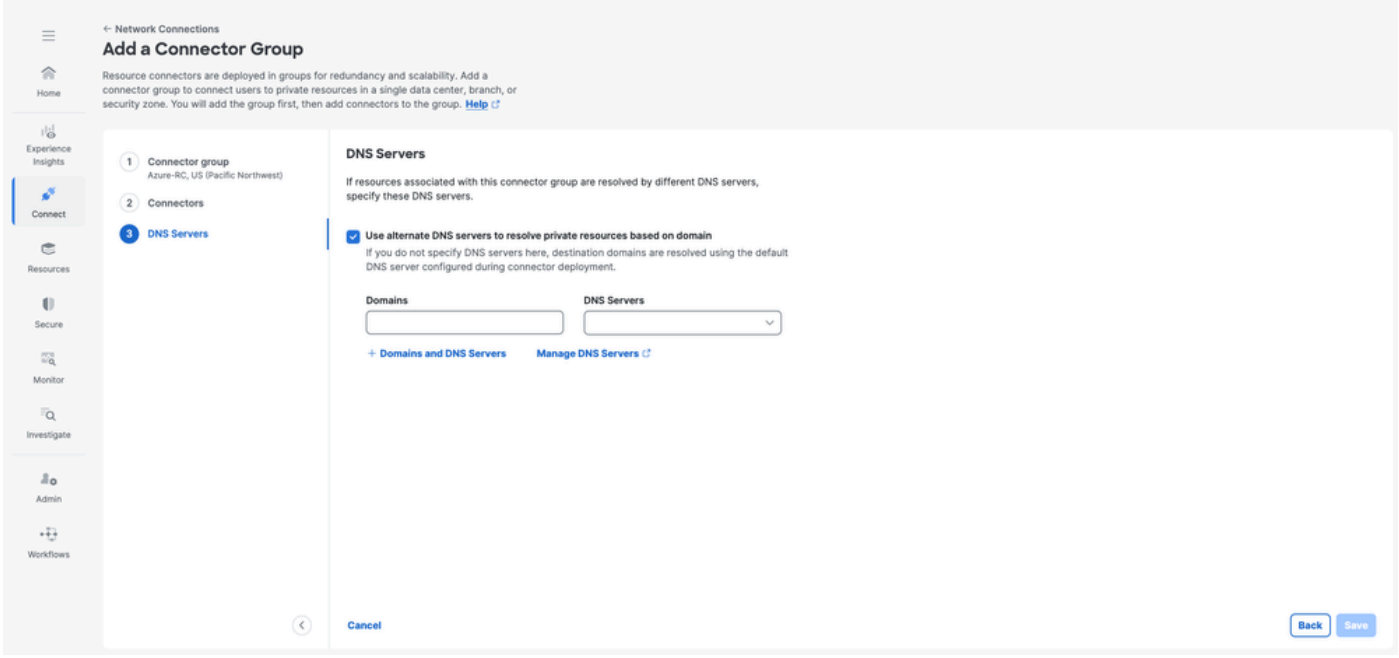
セキュアアクセス：コネクタグループの設定

- 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



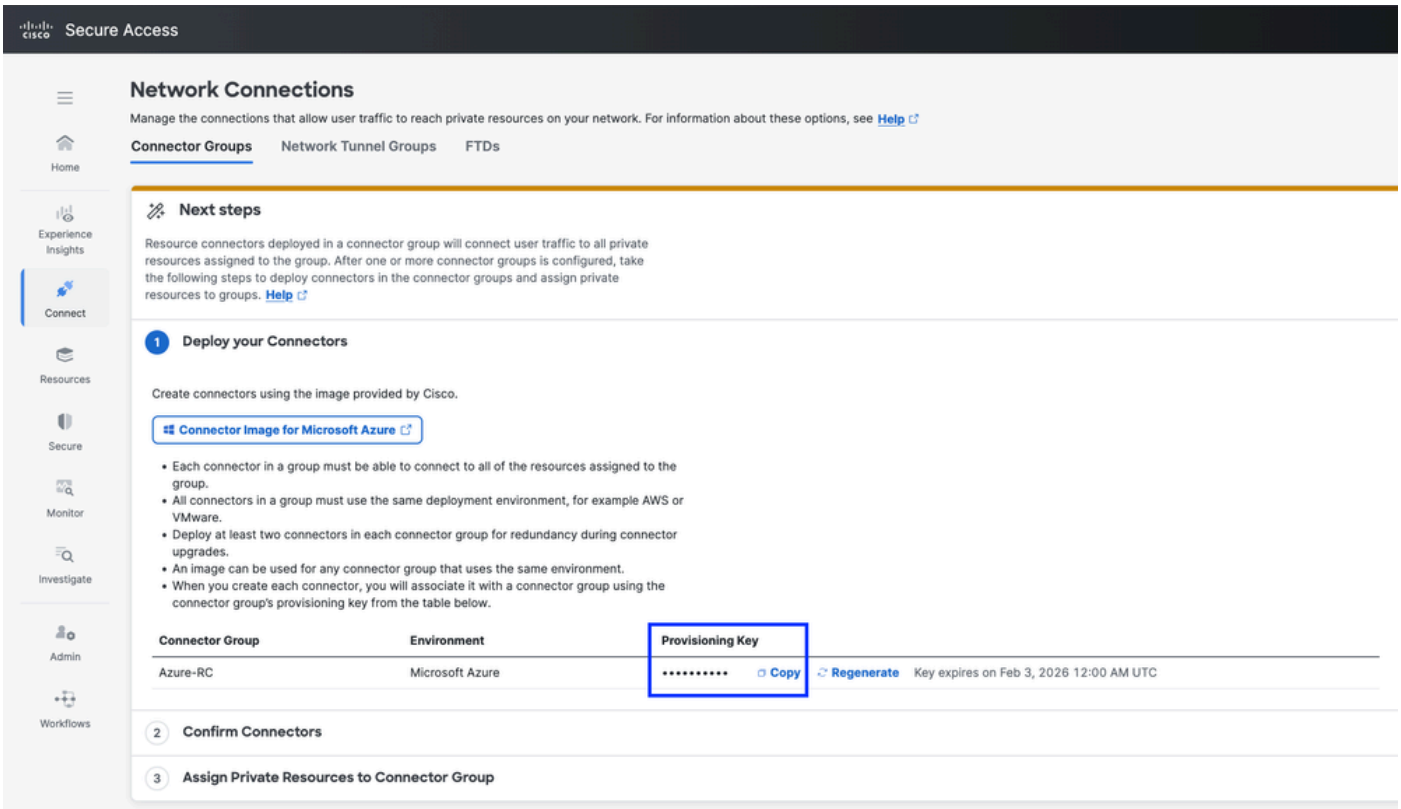
セキュアアクセス – リソースコネクタ設定のレビュー

- 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

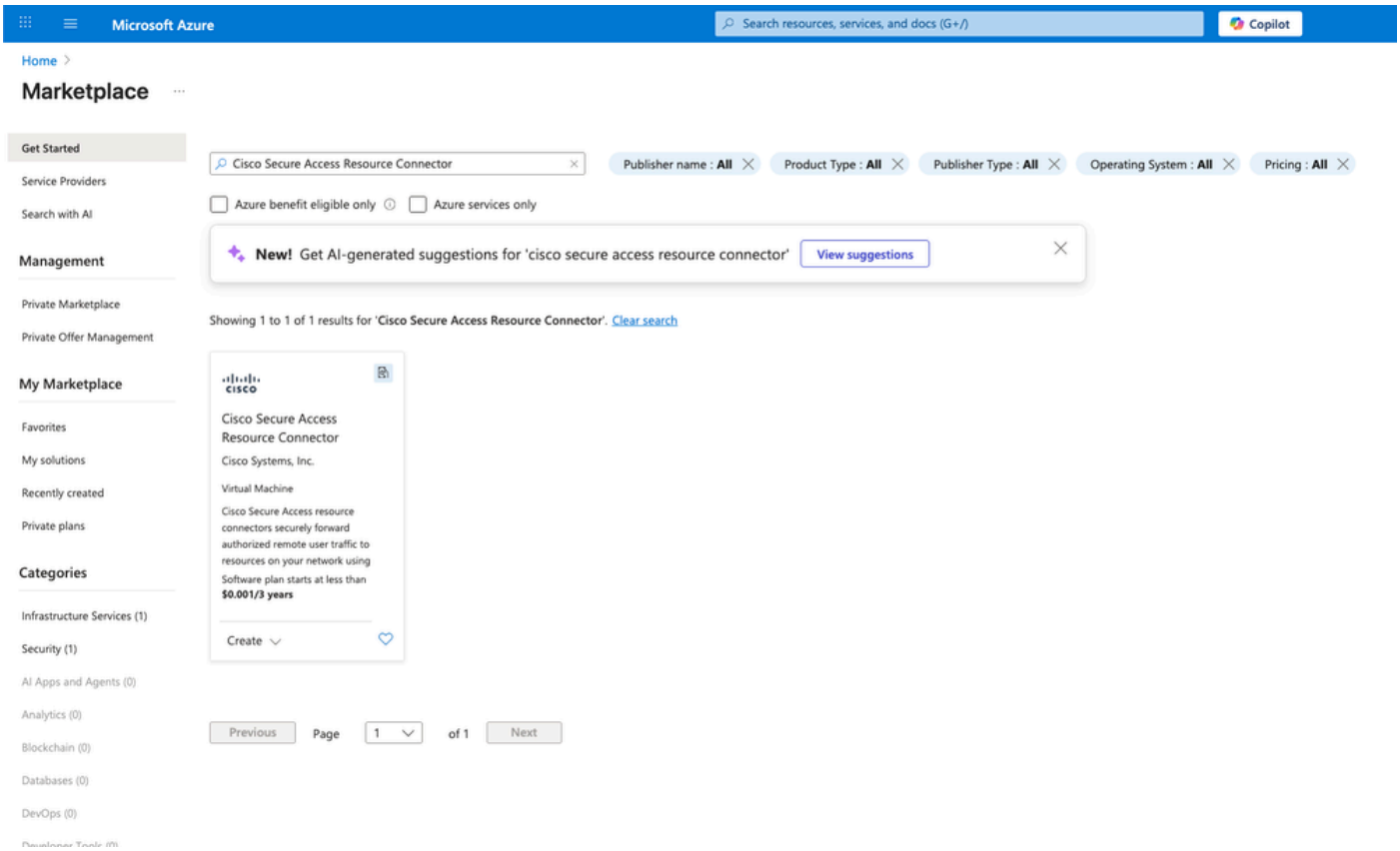
- この段階で、プロビジョニングキーをコピーします。後でAzureでリソースコネクタのデプロイ中に、セキュアアクセステナントへの登録を有効にする必要があります。



セキュアアクセス：リソースコネクタの設定

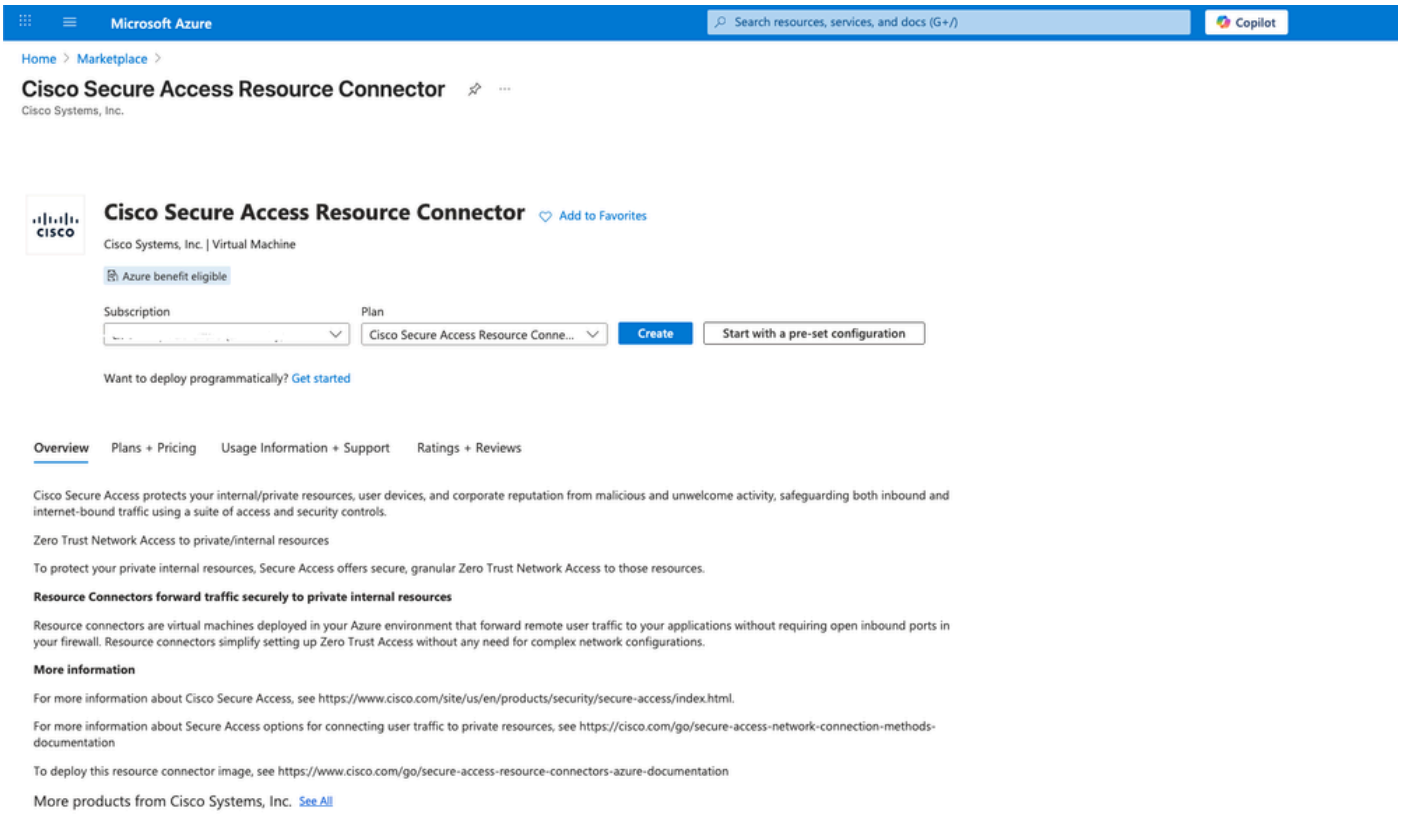
Azureの構成

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。



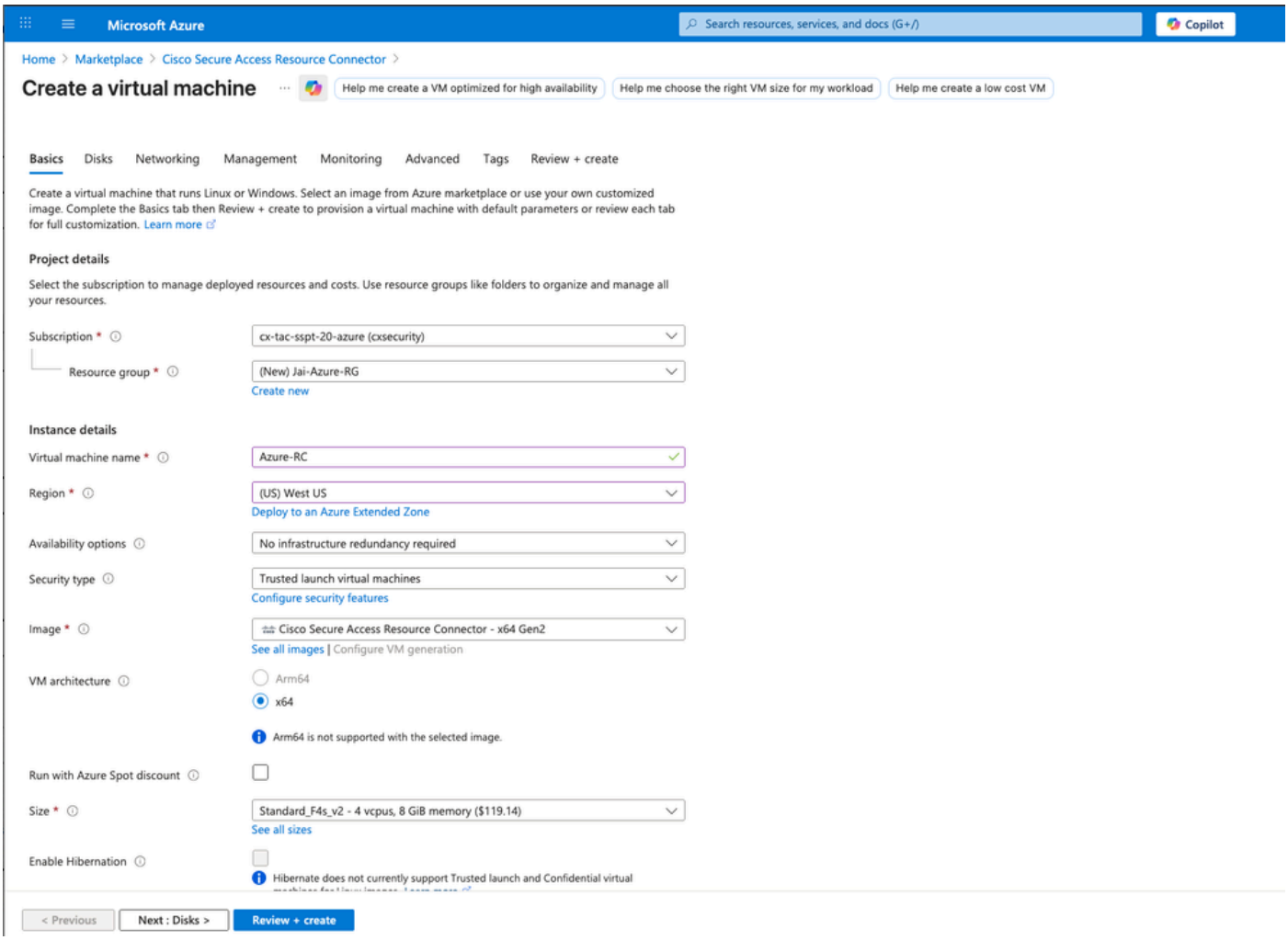
セキュアアクセス – Azureでのリソースコネクタの作成

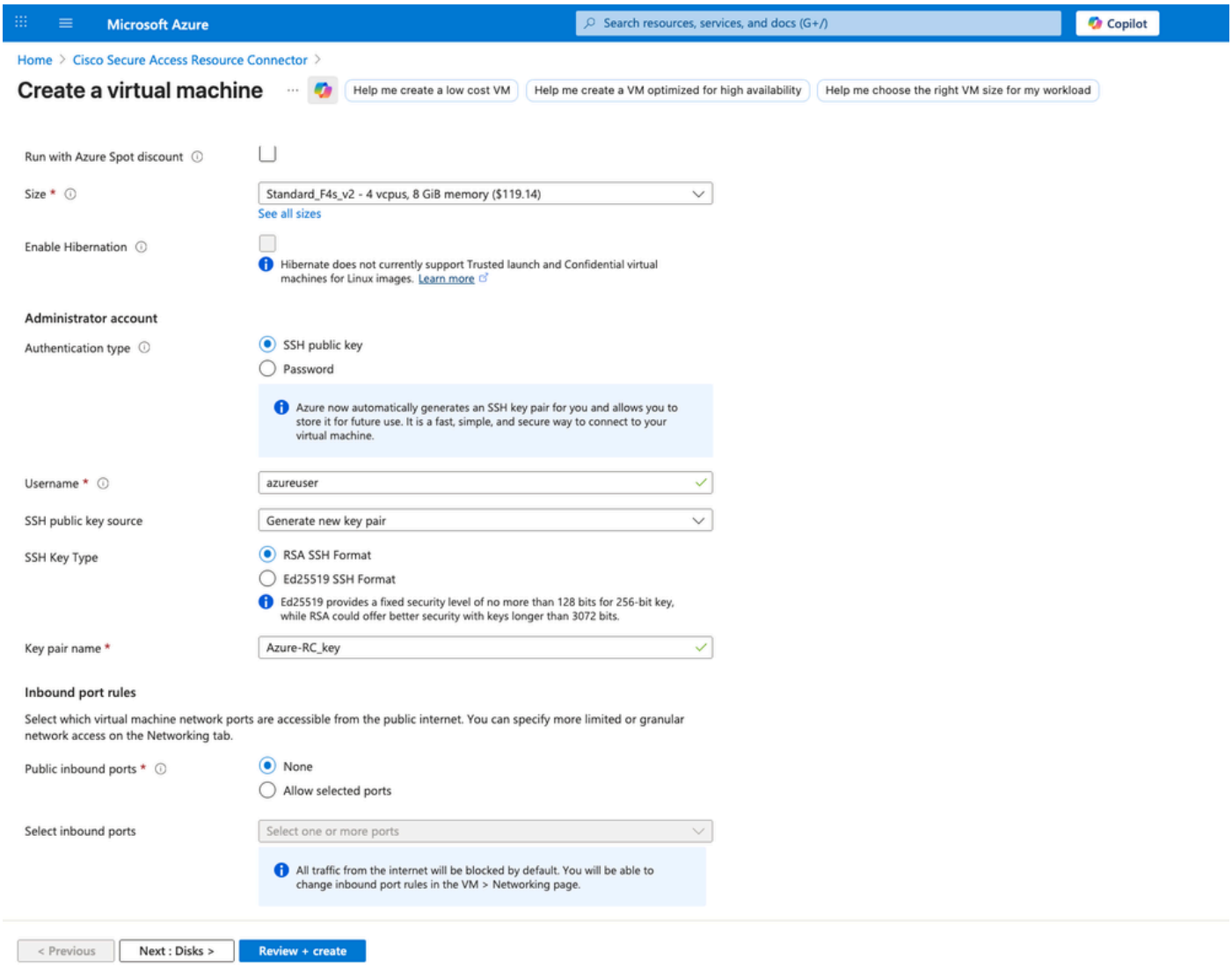
- 適切なSubscriptionとPlanを選択し、Createをクリックします。



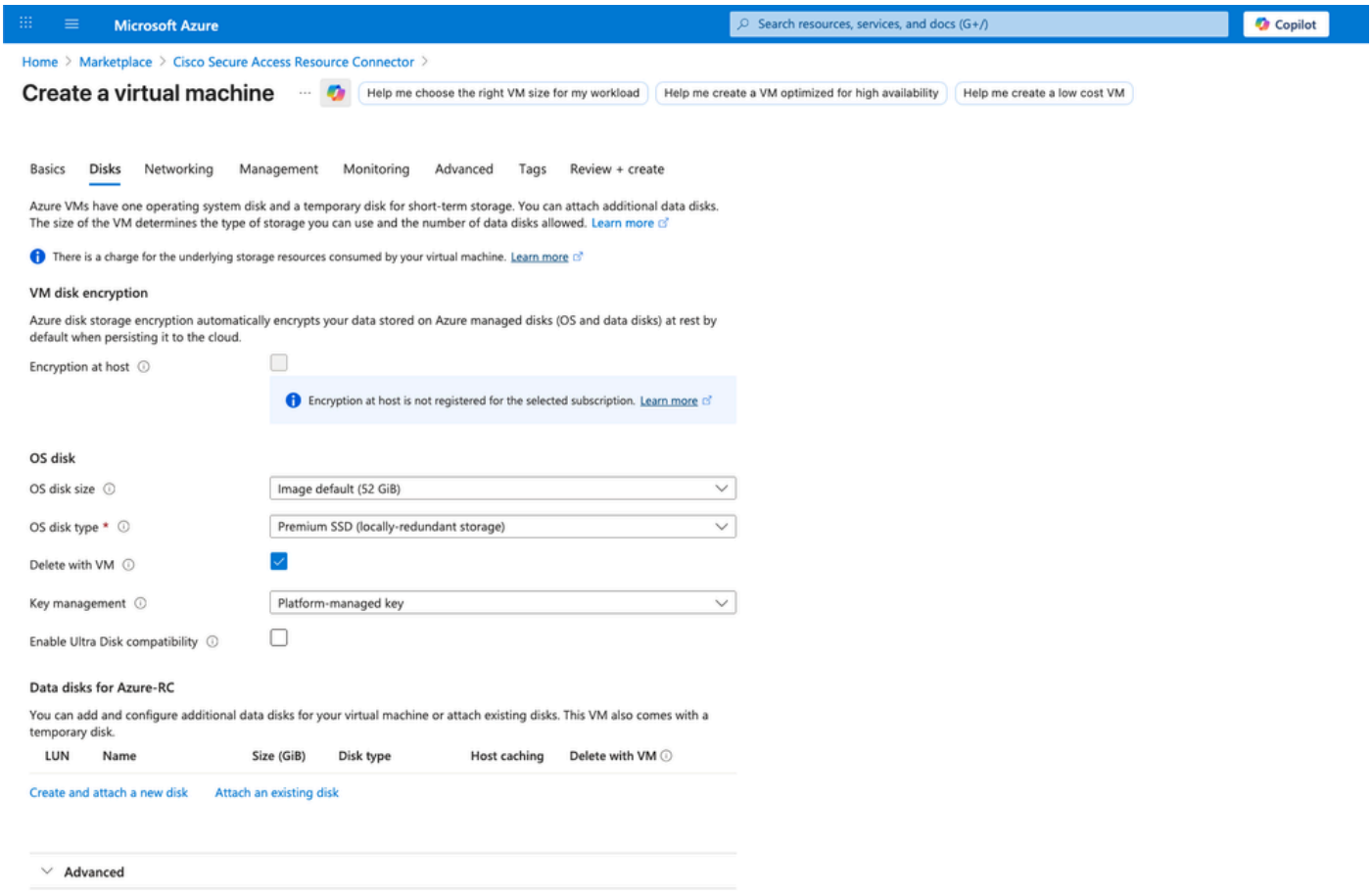
セキュアアクセス – Azureでのリソースコネクタの作成

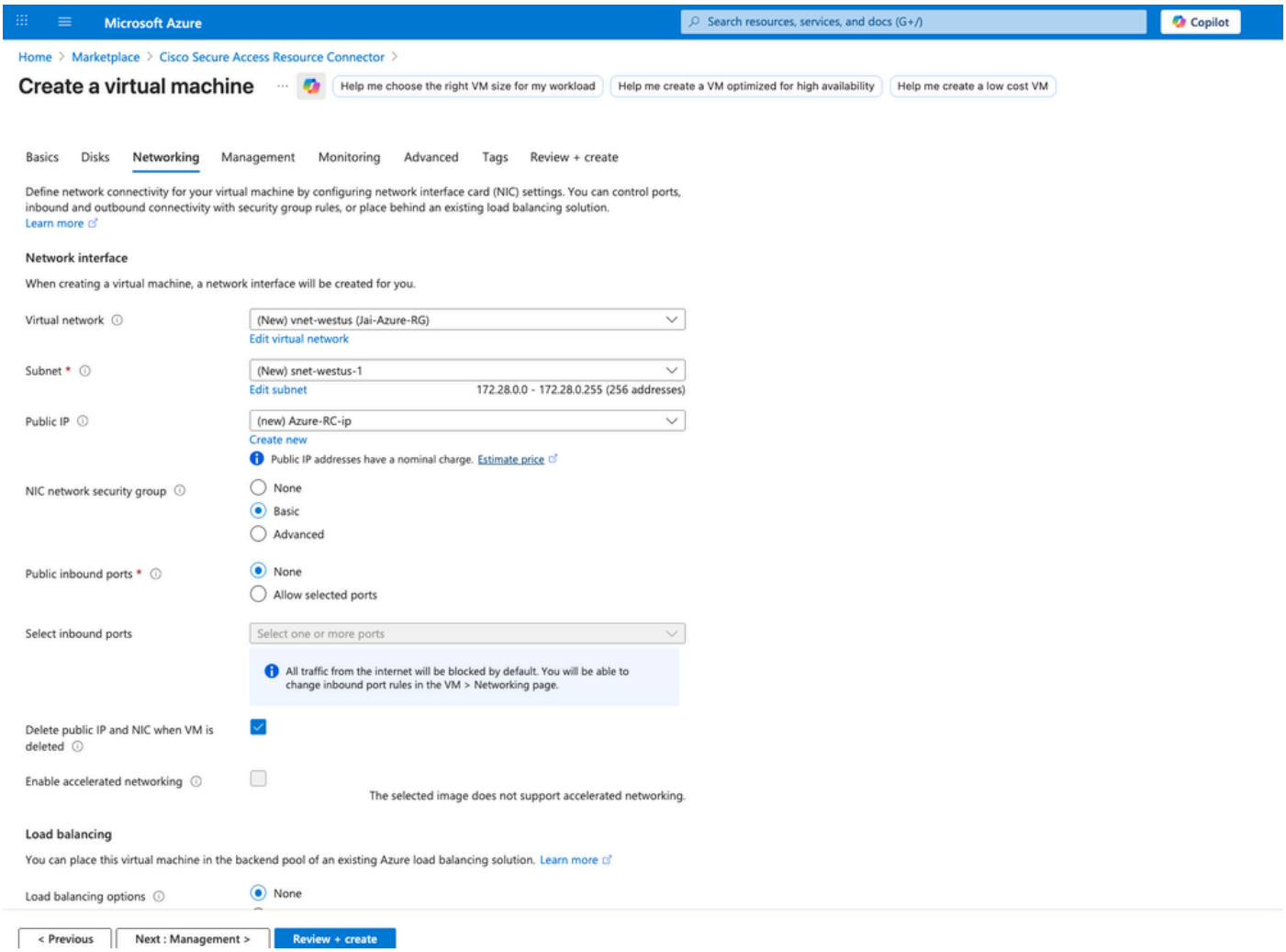
- ディスク、ネットワーキング、およびSSH公開キーの設定を確認します





⚠ 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。

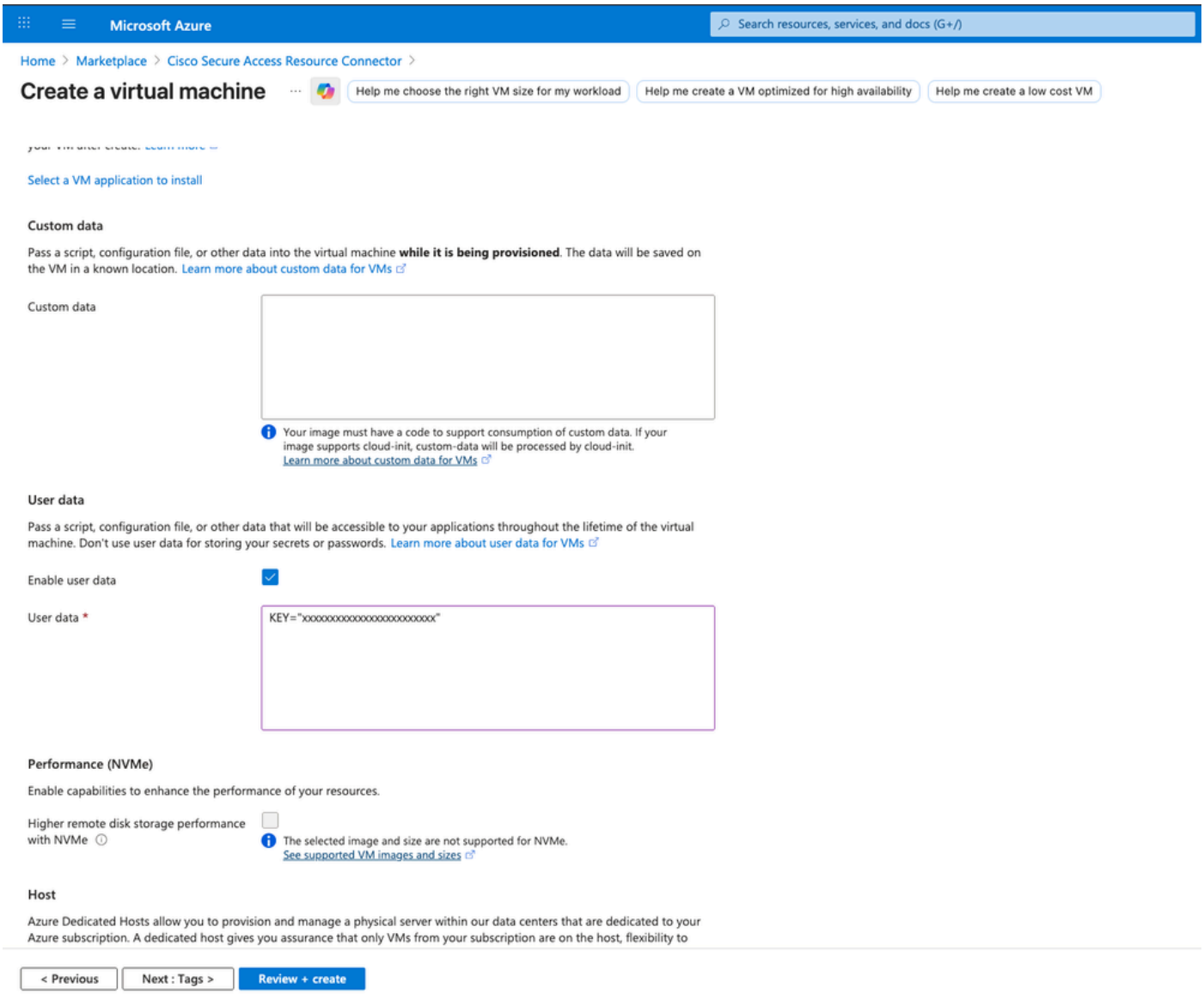

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Cisco Secure Access Resource Connector >
Create a virtual machine
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM
Basics Disks Networking 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
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
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



セキュアアクセス – Azureでのリソースコネクタの作成

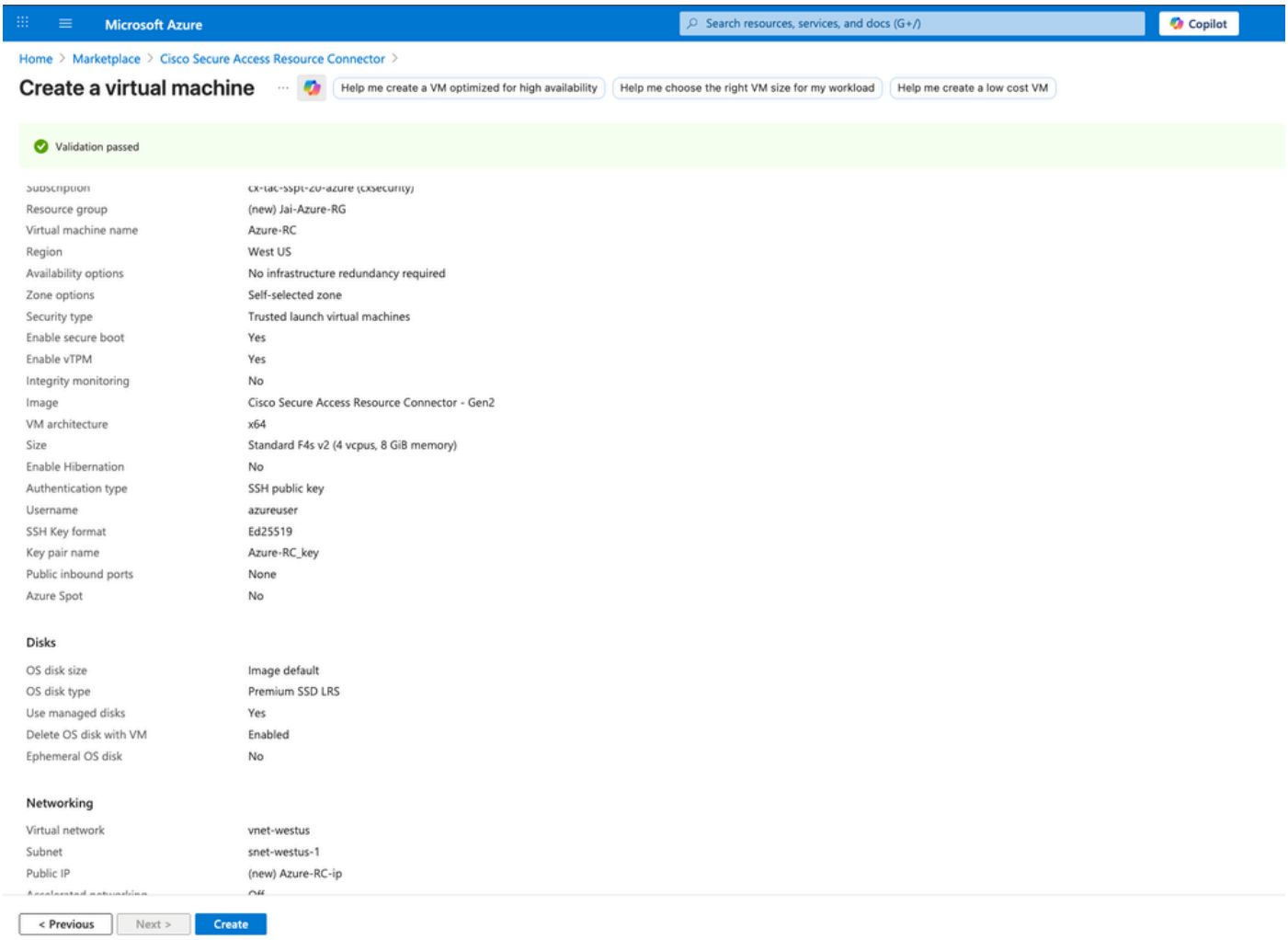
- Cisco Secure Accessからコピーされたプロビジョニングキーをユーザデータフィールドに貼り付けます

KEY=XXXXXXXXXXXXXXXXXXXXX



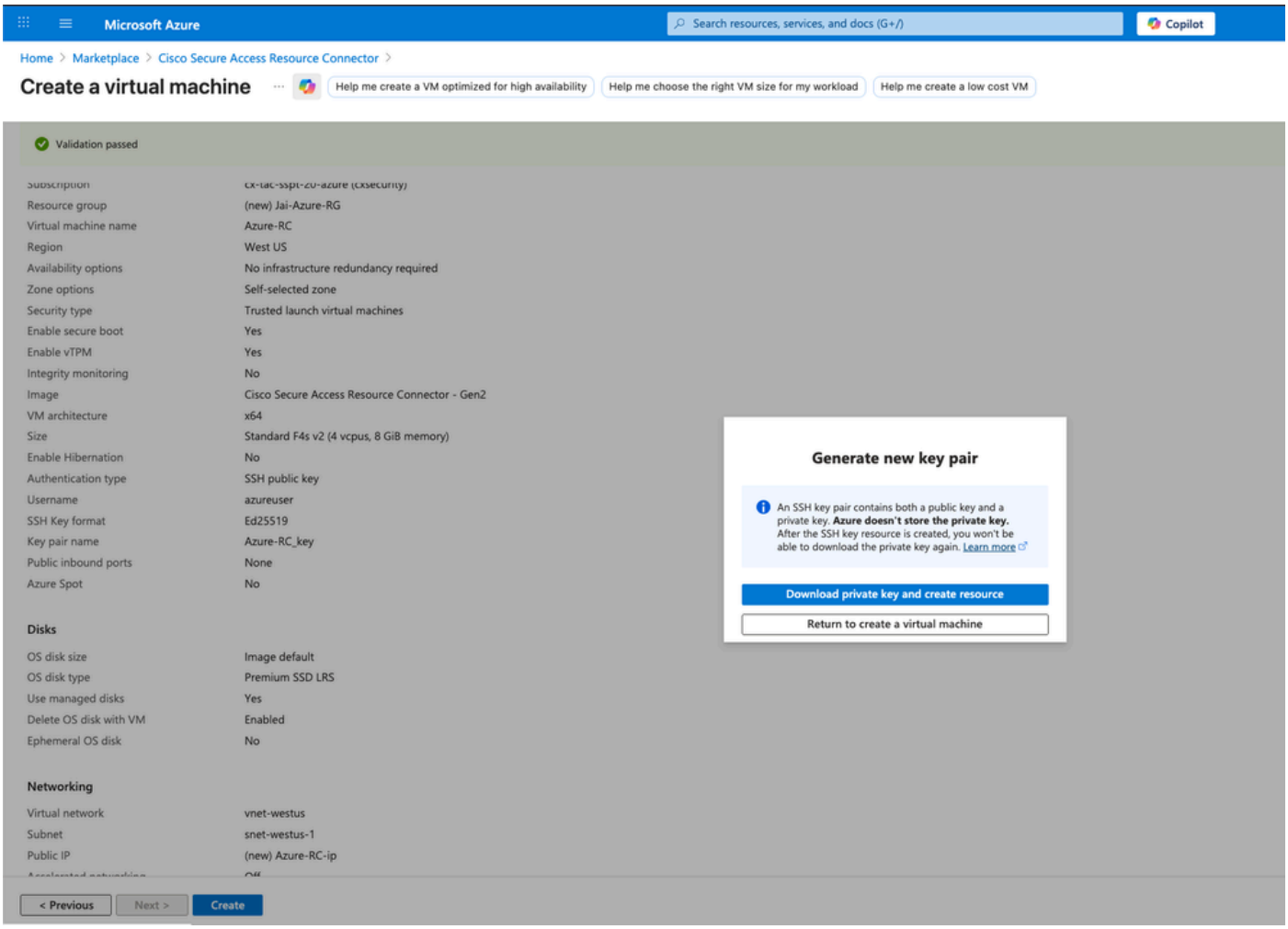
セキュアアクセス – Azureでのリソースコネクタの作成

- 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



セキュアアクセス – Azureでのリソースコネクタの作成

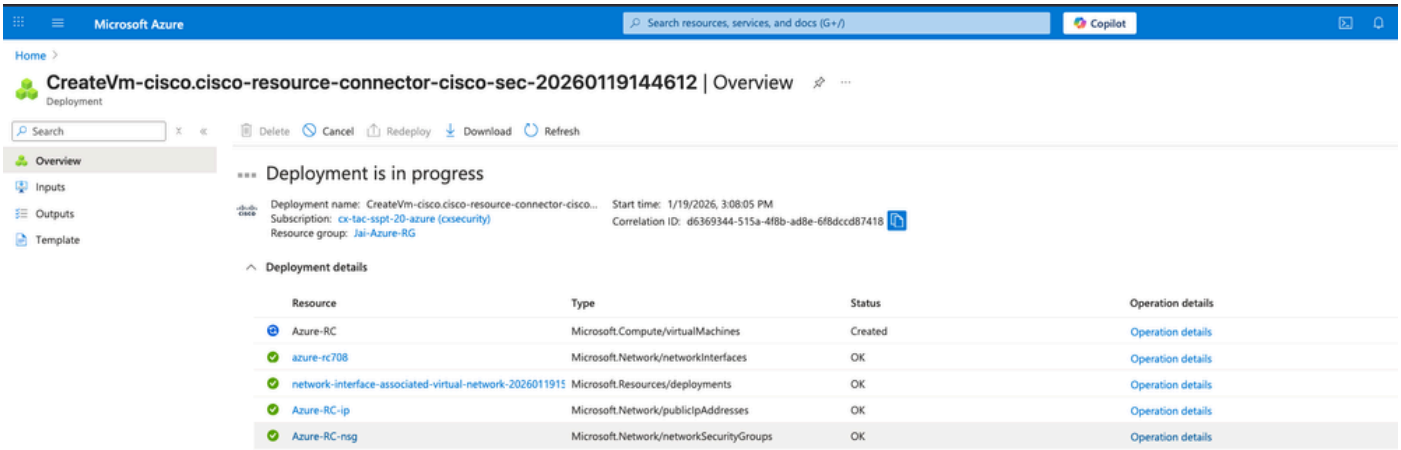
- Createをクリックすると、秘密キーをダウンロードするオプションが表示されます。Download private key and create resourceをクリックします



セキュアアクセス – Azureでのリソースコネクタの作成

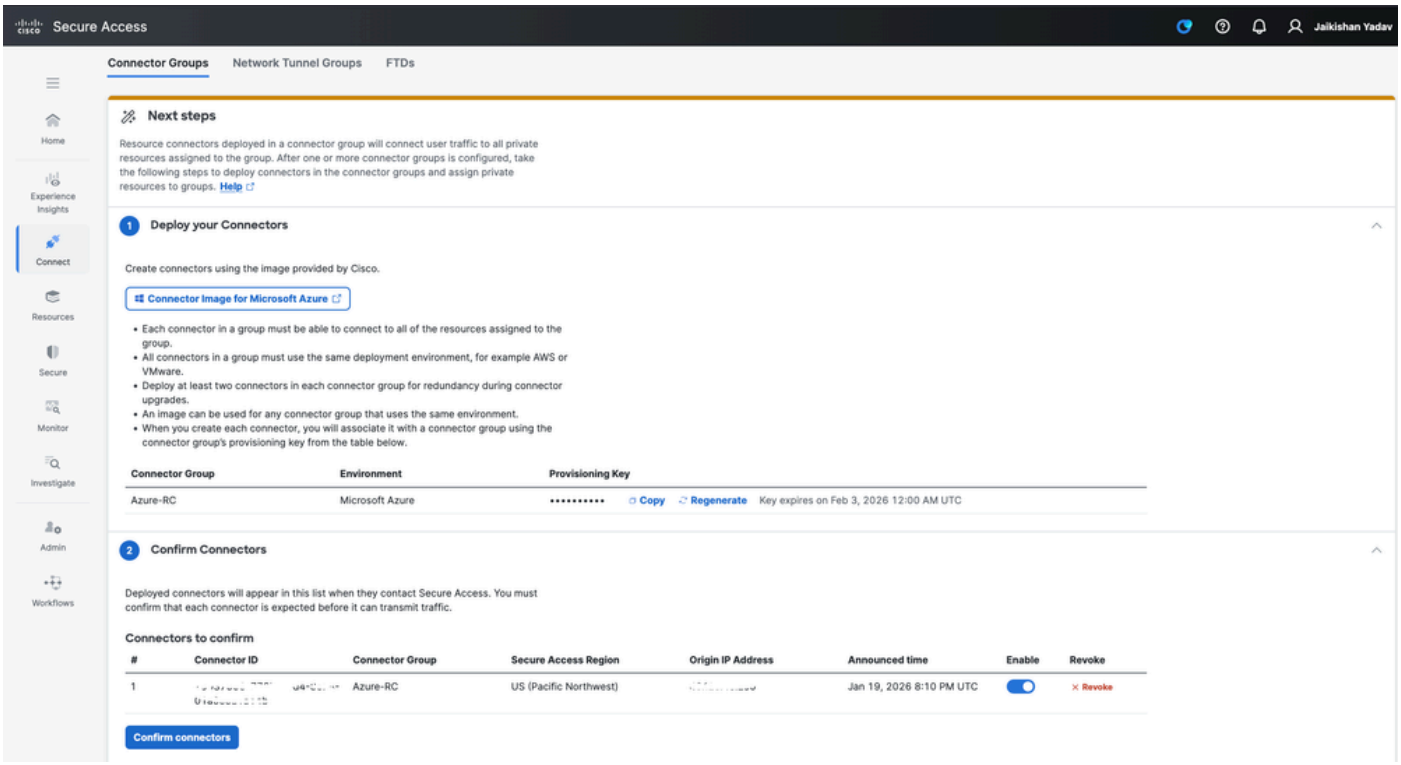
⚠ 注意：秘密SSHキーを失わないでください。失わないと、RC CLIにアクセスできず、トラブルシューティングのために再展開する必要があります。

- その後、リソースコネクタの進行状況を確認できます



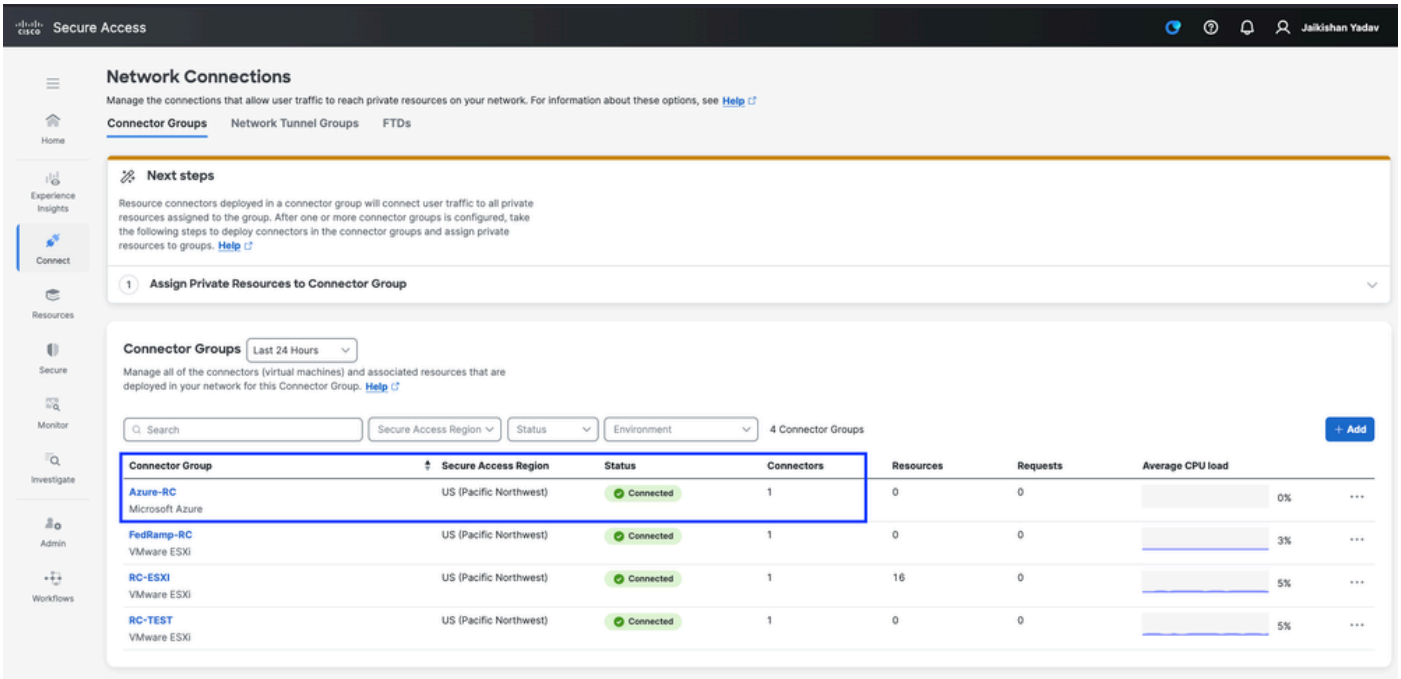
セキュアアクセス – Azureでのリソースコネクタの配置

- 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終了します



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。



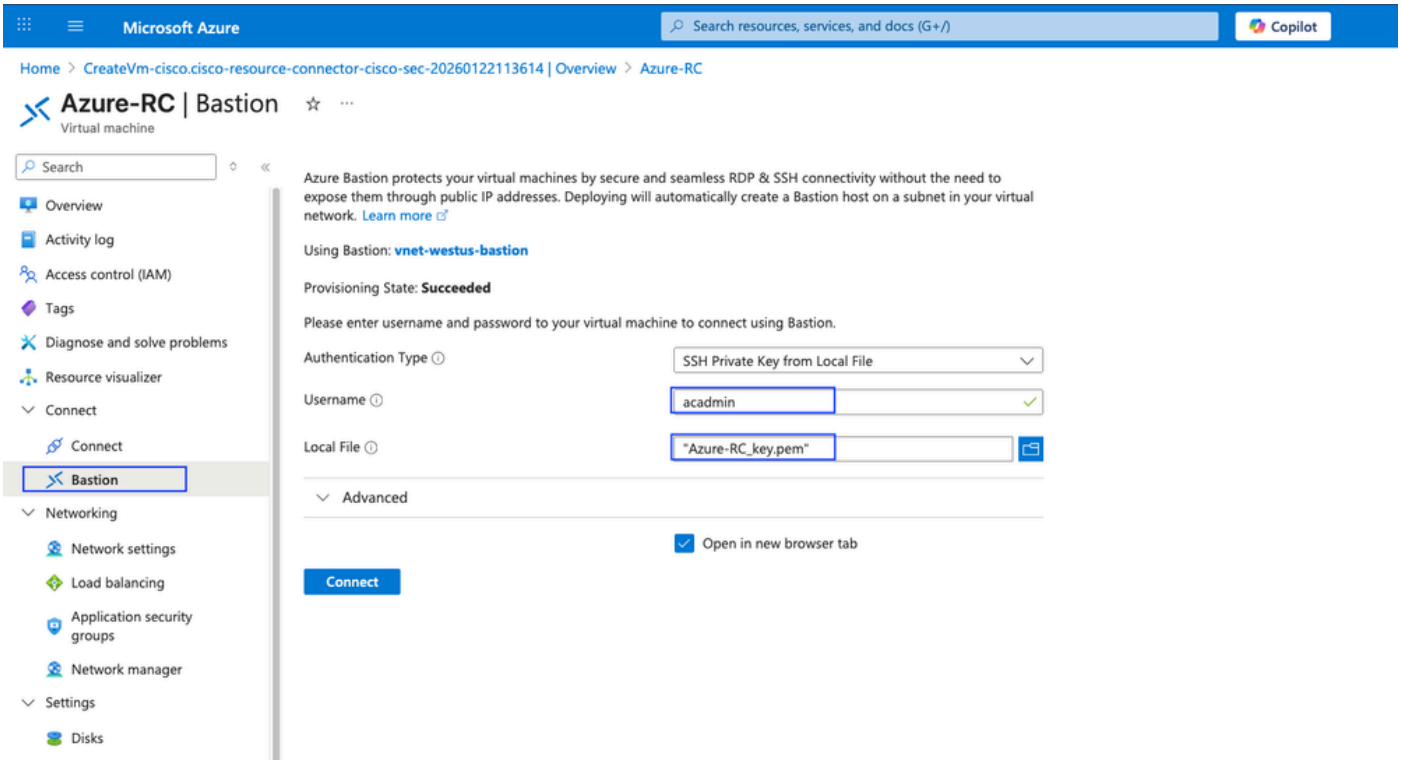
セキュアアクセス – リソースコネクタ

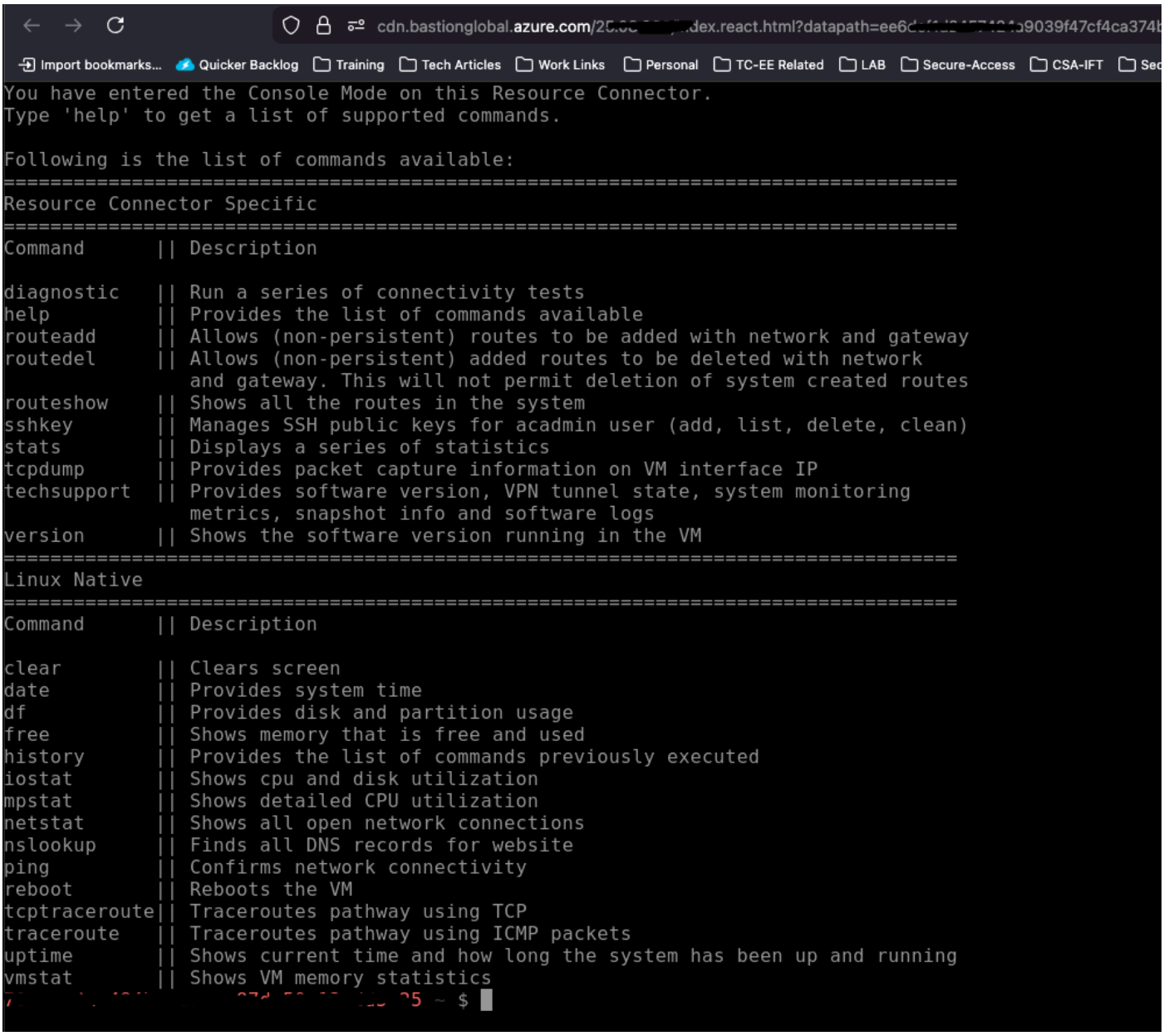
確認

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。

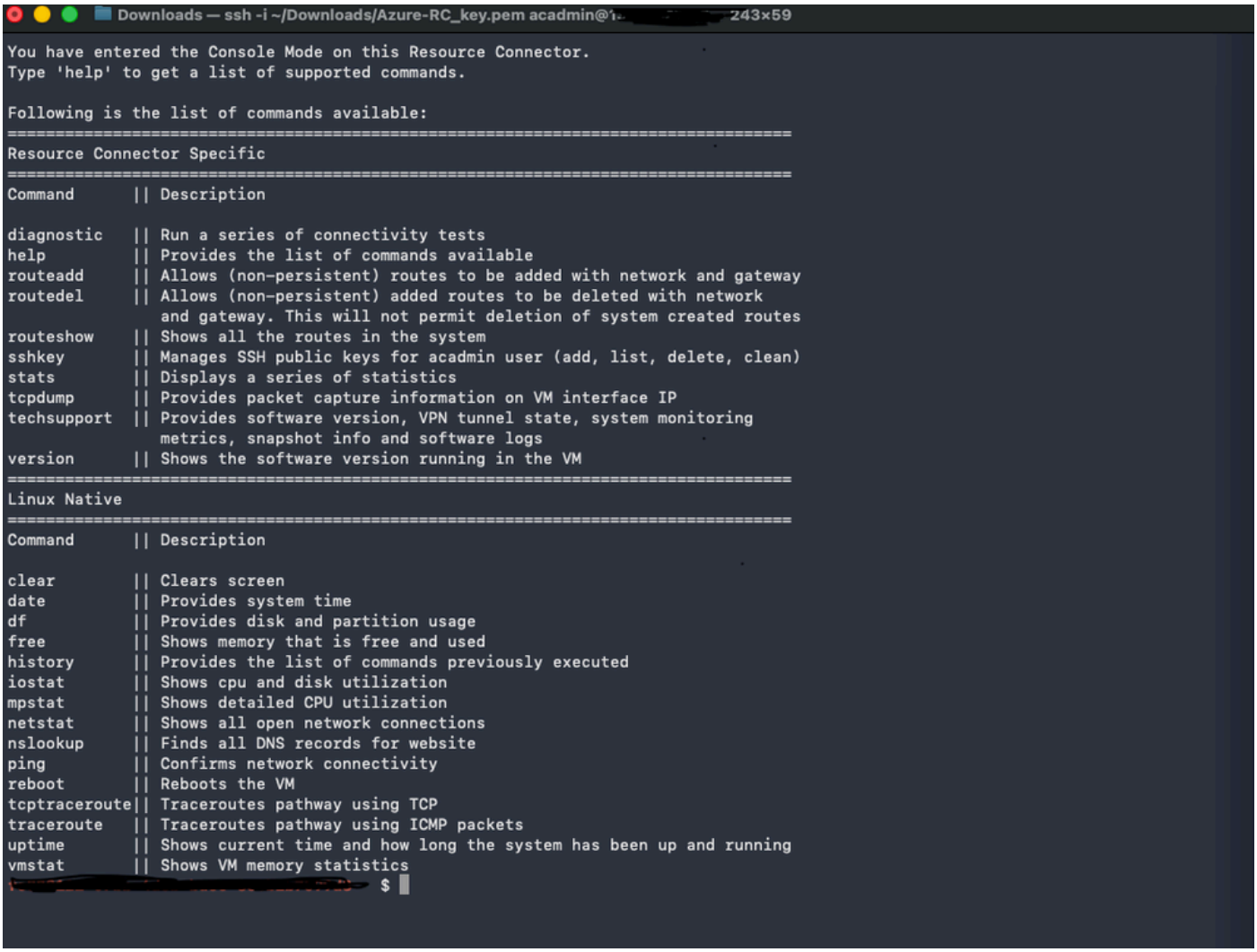




セキュアアクセス – リソースコネクタのコマンドラインへのアクセス

MAC-OS端末からのRCへのアクセス

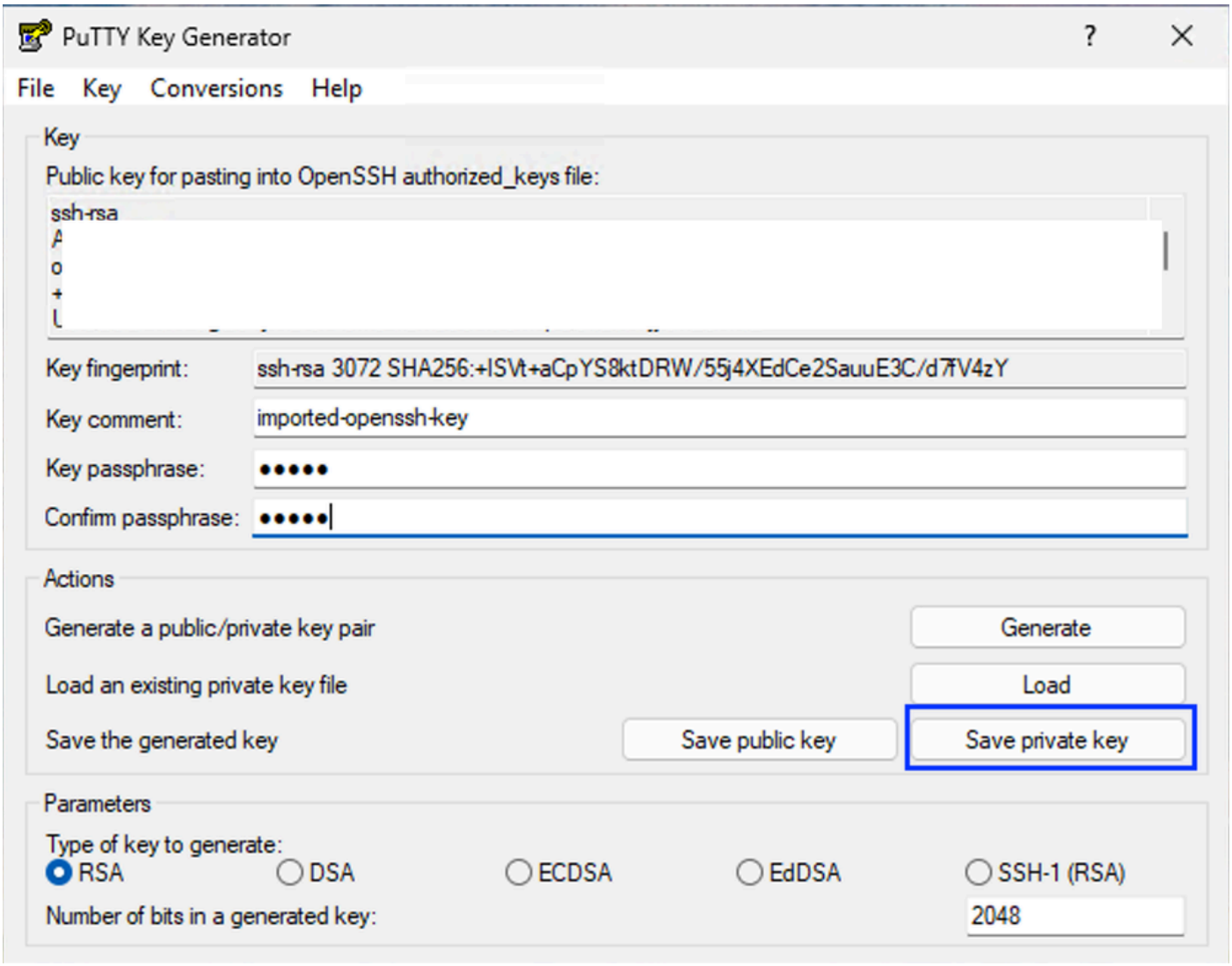
端末を開き、ssh -i <private-key-file-path> acadmin@x.x.x.x.xを使用して、リソースコネクタに接続します。



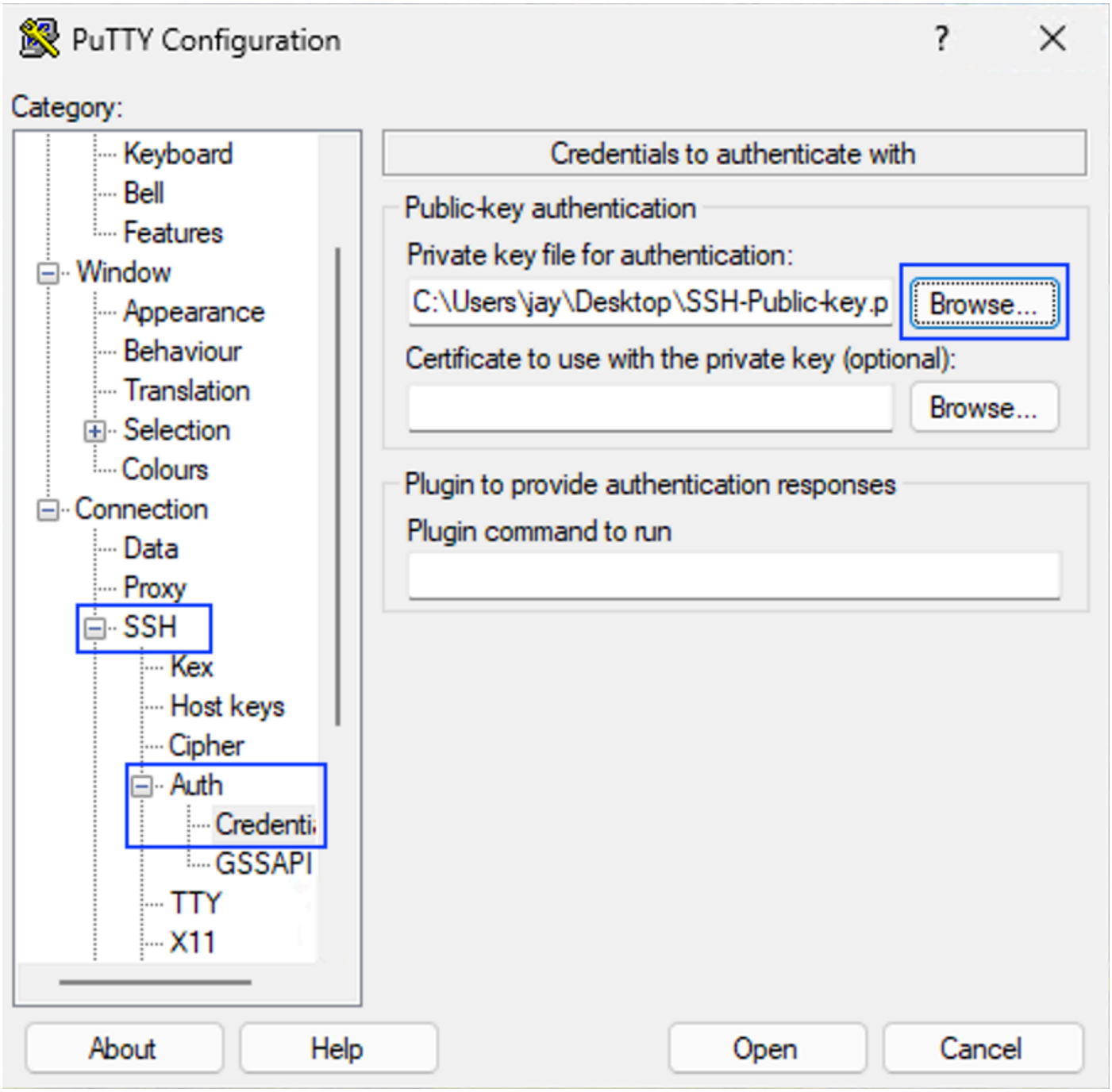
セキュアアクセス – リソースコネクタのコマンドラインへのアクセス

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
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
```

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。