Déployer Secure Access Resource Connector dans Azure

Table des matières

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

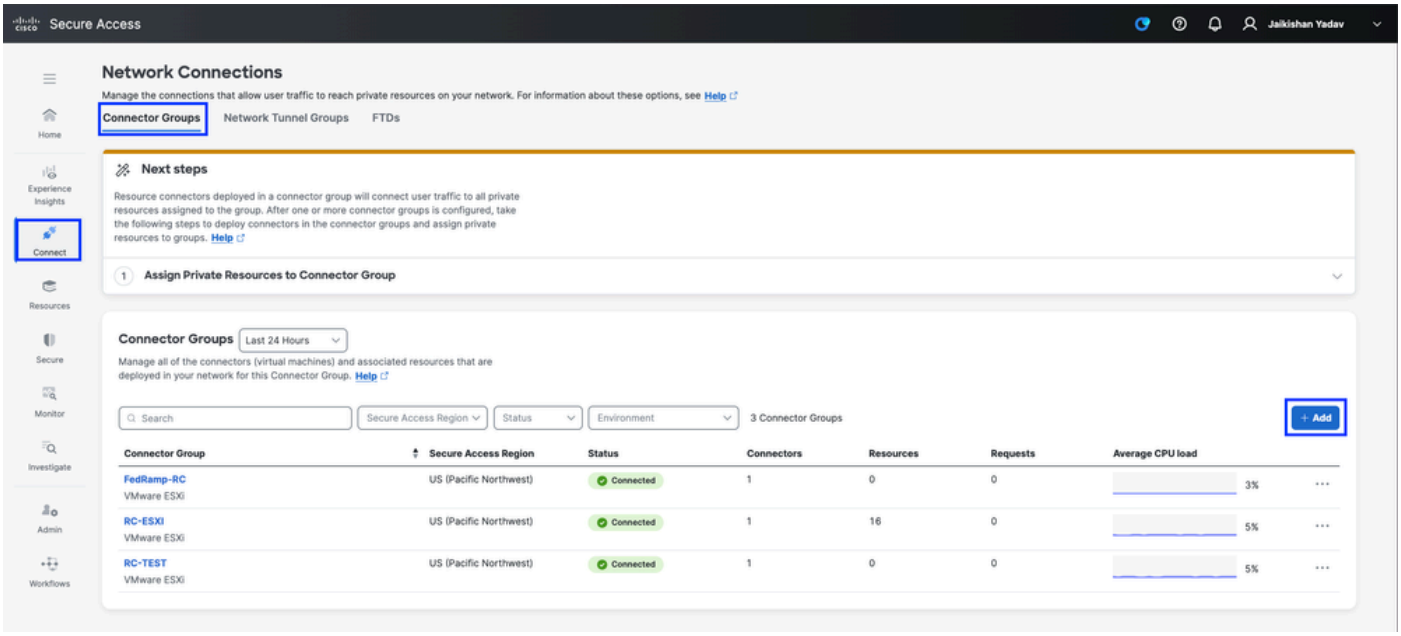
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Configurations dans Secure Access

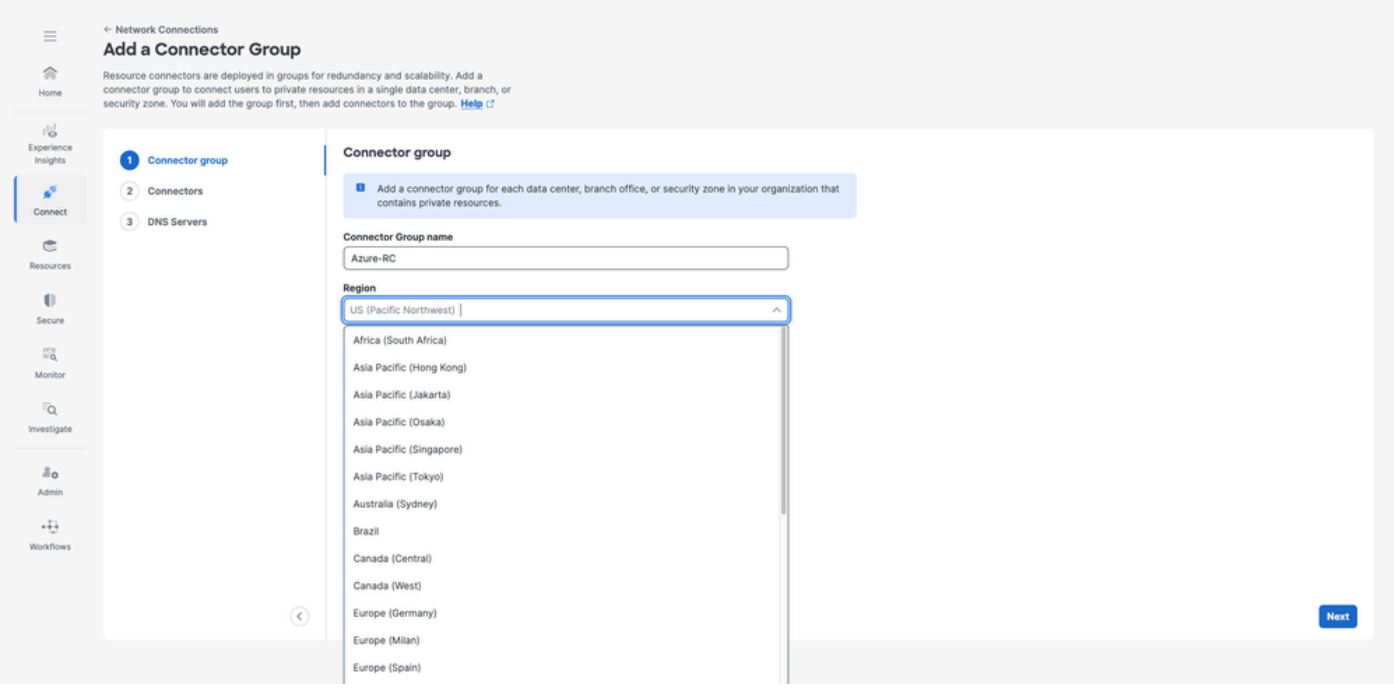
Connectez-vous au tableau de bord Secure Access et accédez à **Connect** > **Network Connections** > **Connector Groups**

- Cliquez sur add



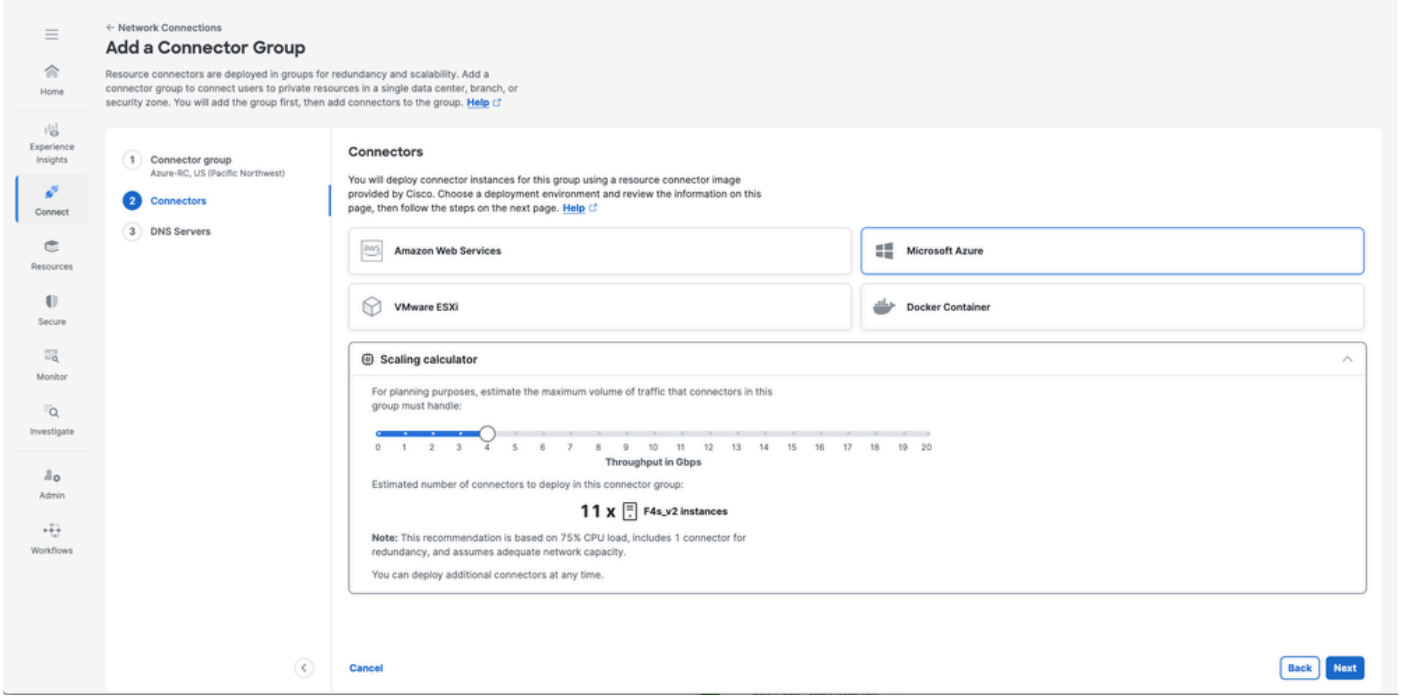
Accès sécurisé - Groupes de connecteurs

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



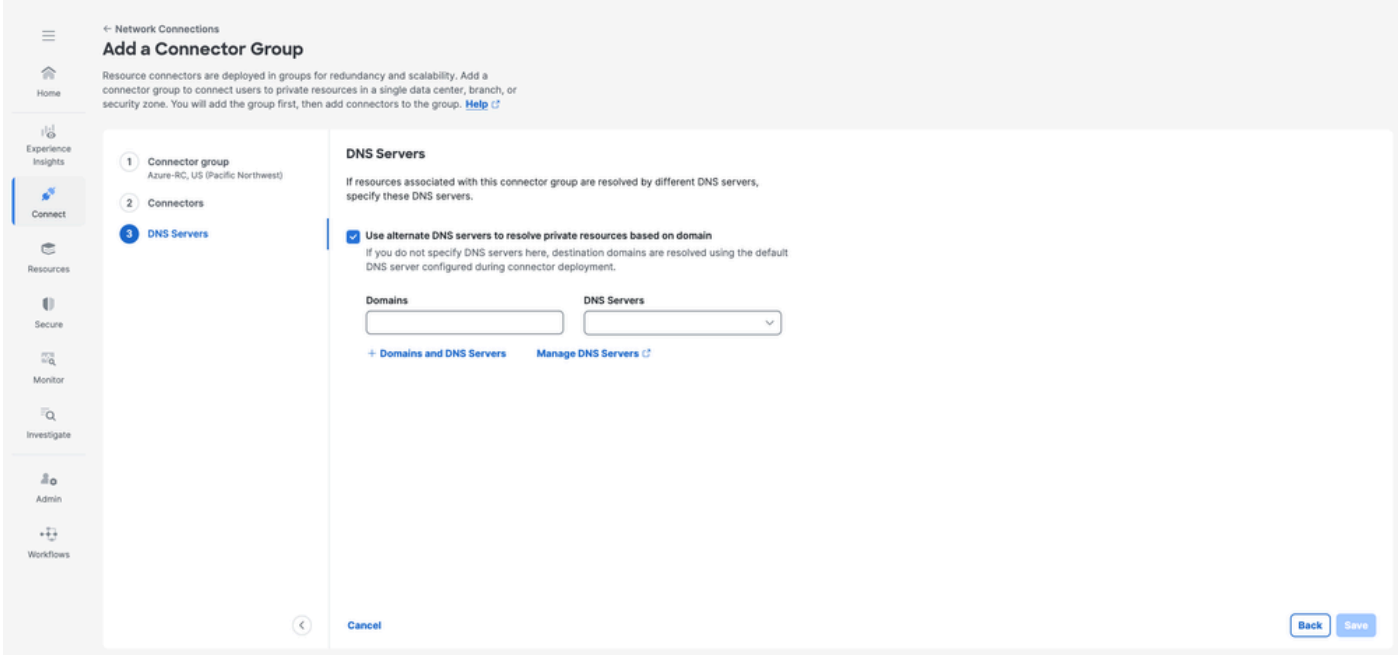
Accès sécurisé - Configuration des groupes de connecteurs

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



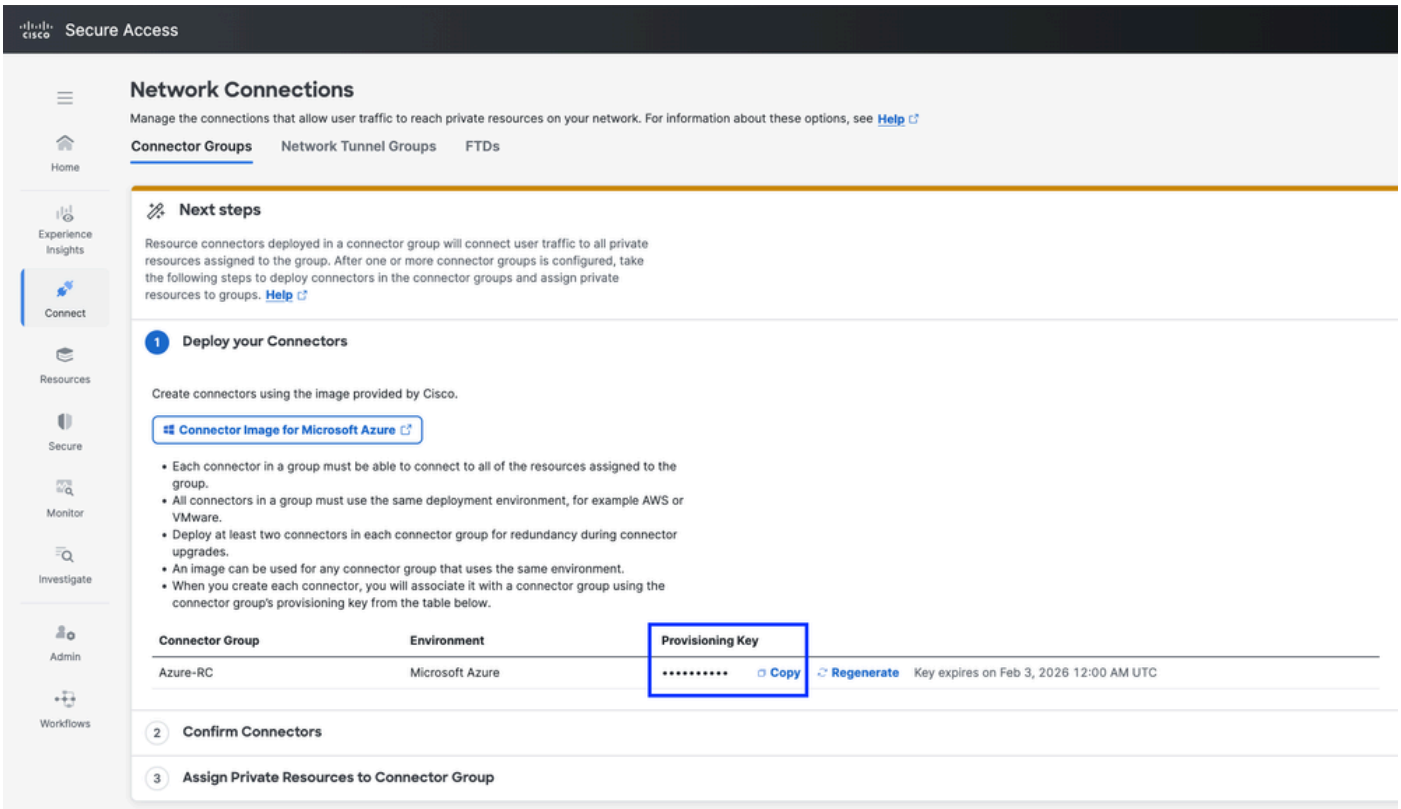
Accès sécurisé - Examen de la configuration du connecteur de ressources

- 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.

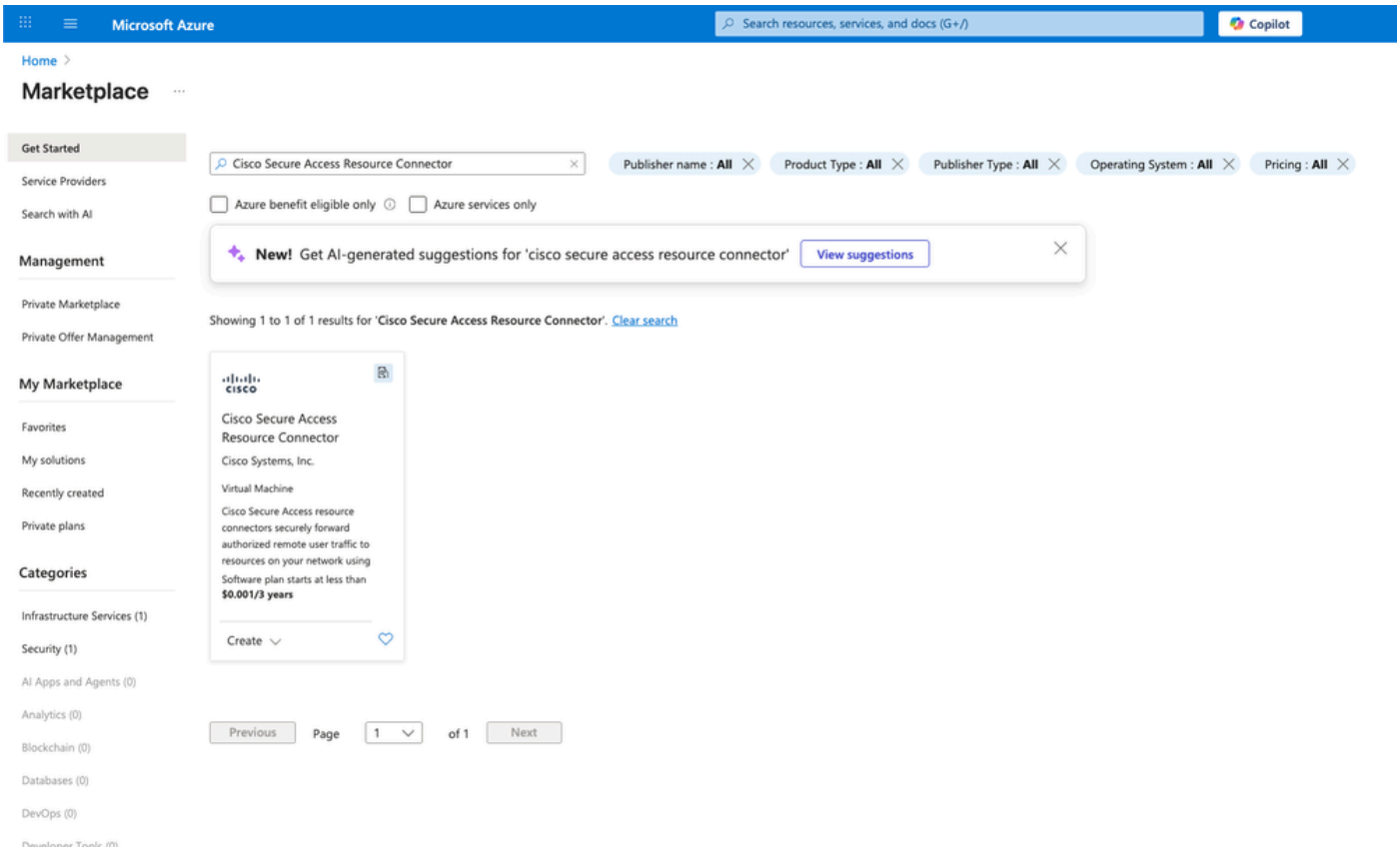


Accès sécurisé - Configuration du connecteur de ressources

Configurations dans Azure

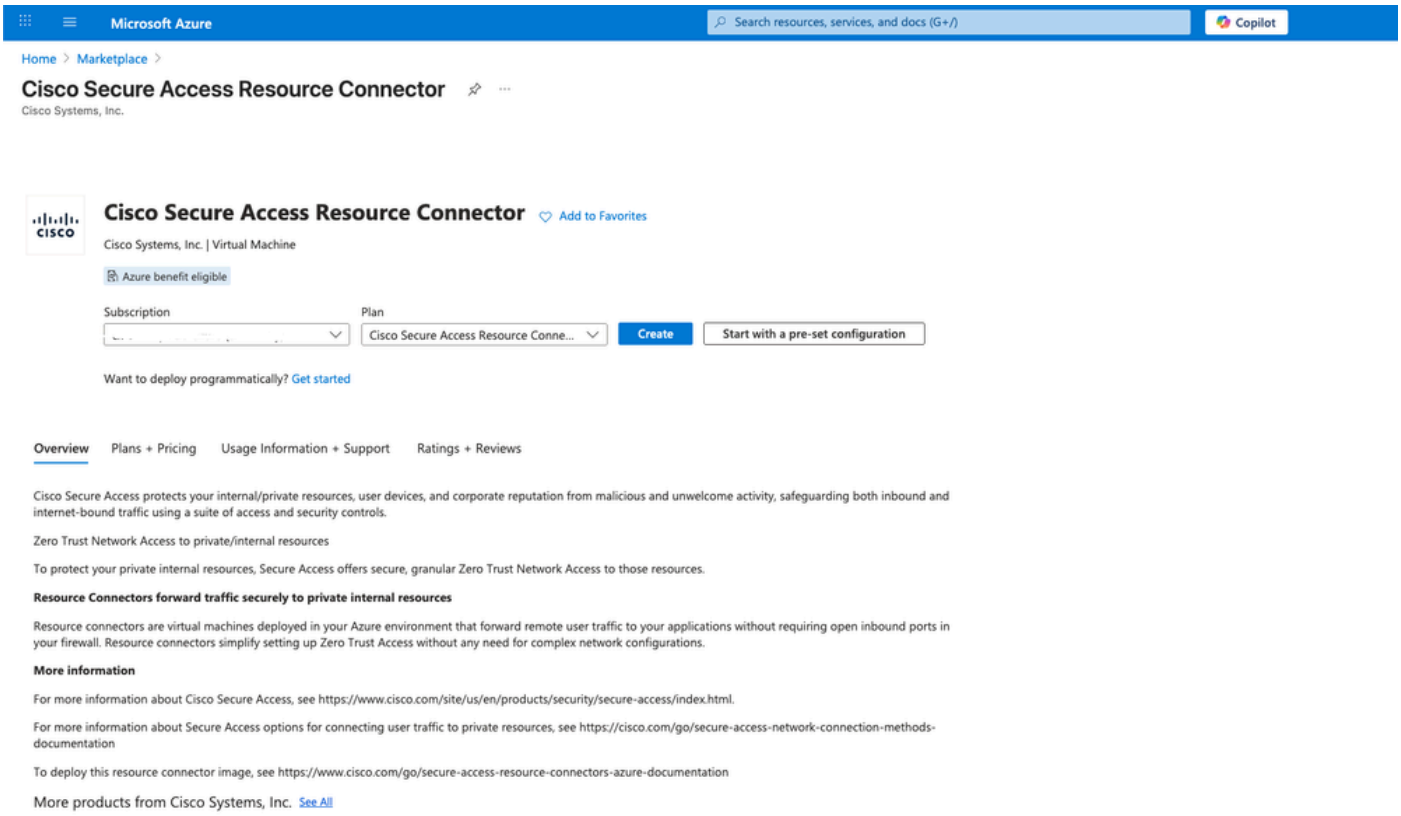
Accédez au portail Azure, puis à Microsoft Azure Marketplace et recherchez l'image Cisco Secure

Access Resource Connector :

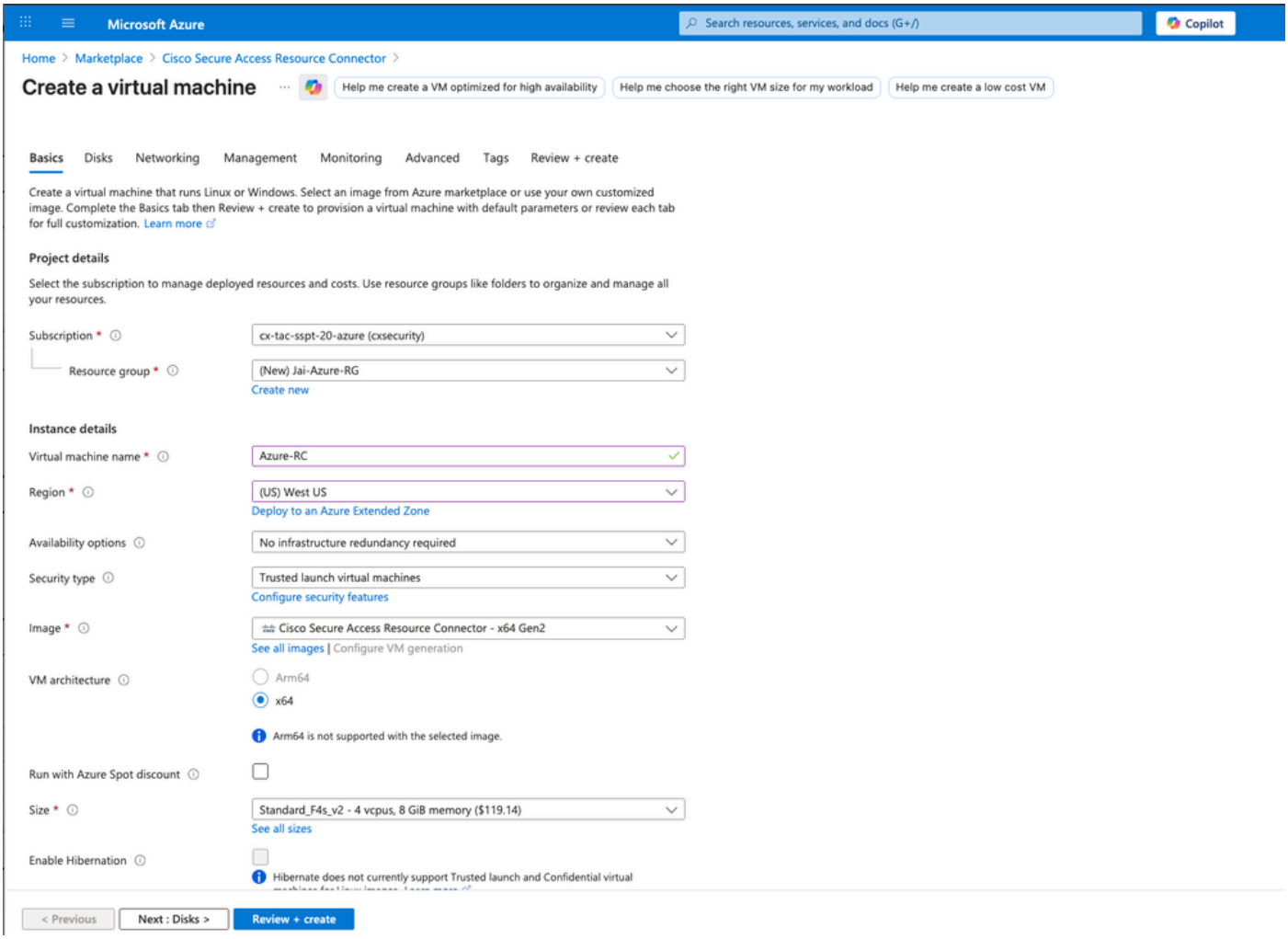


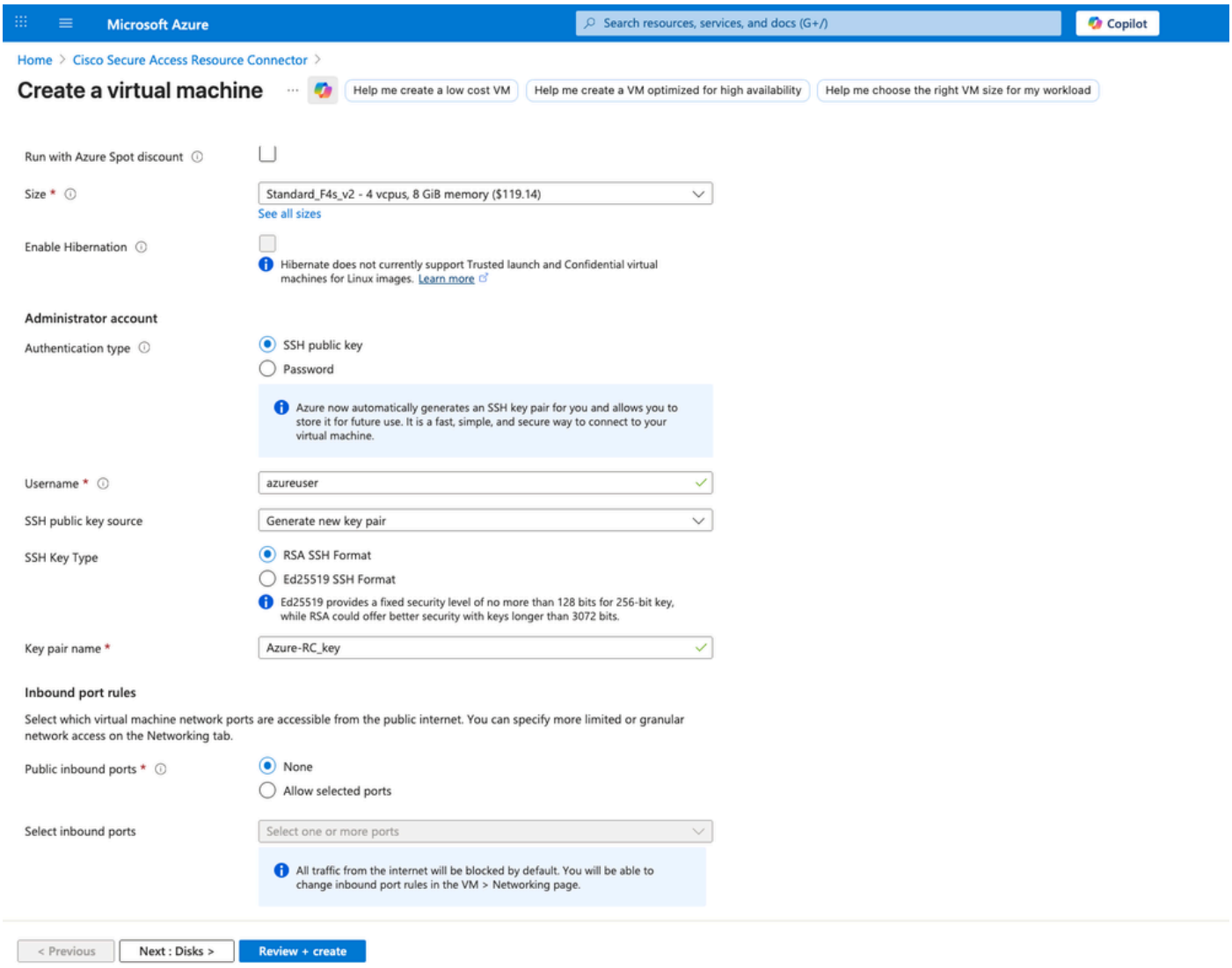
Accès sécurisé - Création du connecteur de ressources sur Azure

- Sélectionnez le Subscription approprié, puis Plan cliquez sur Create

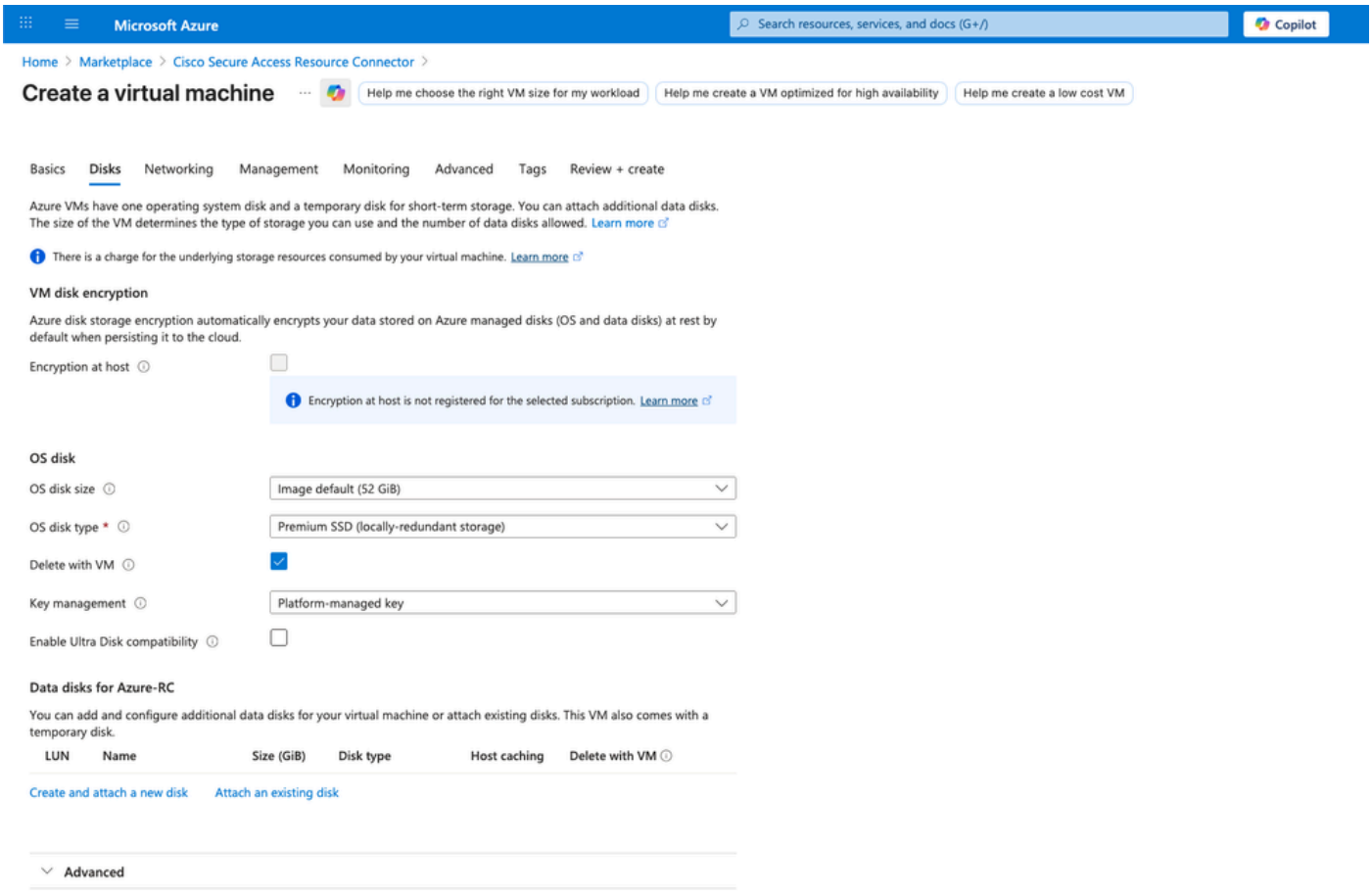


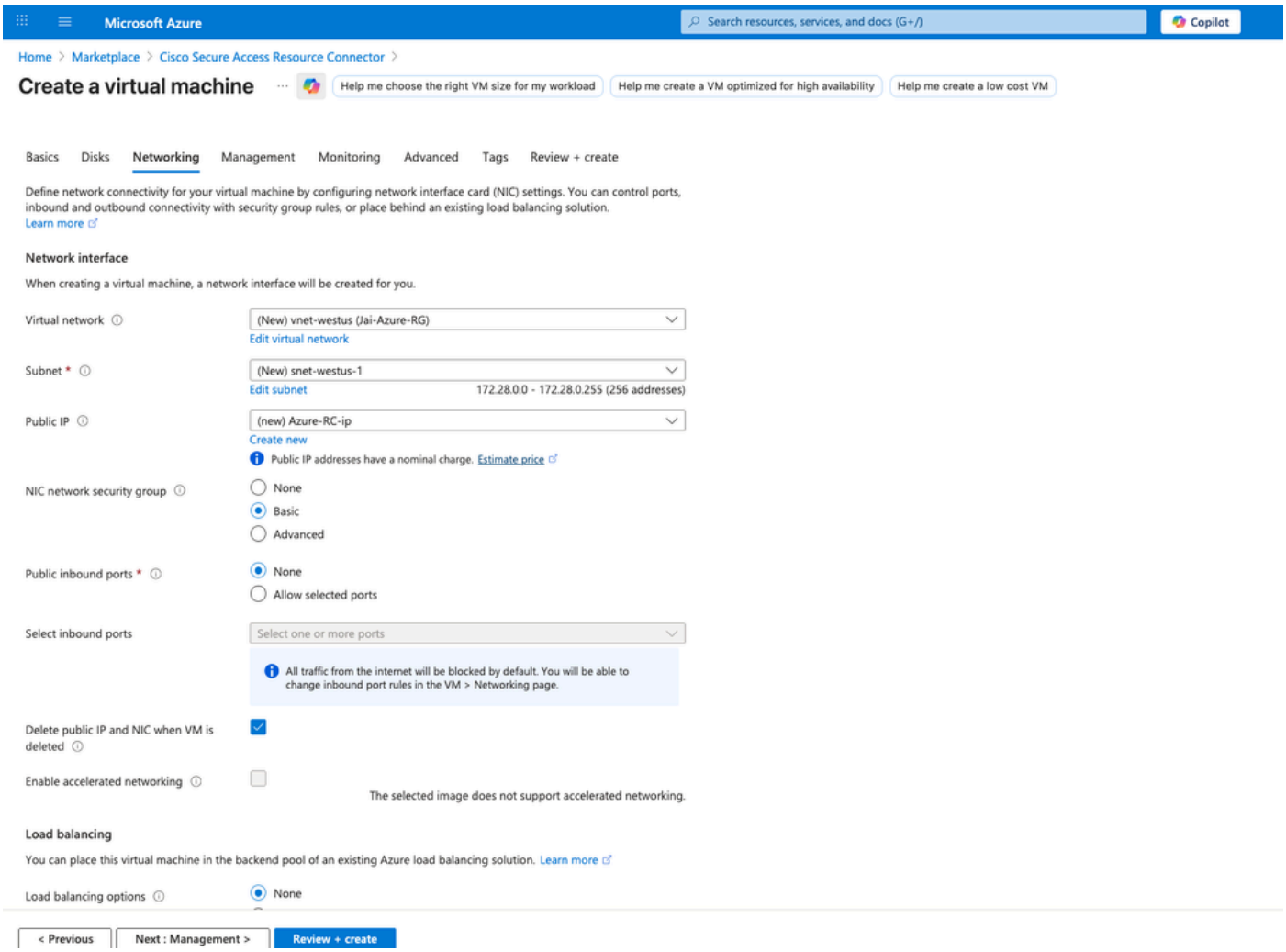
- Vérifiez la configuration de Disksetde la clé publique Networking SSH





⚠ 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.

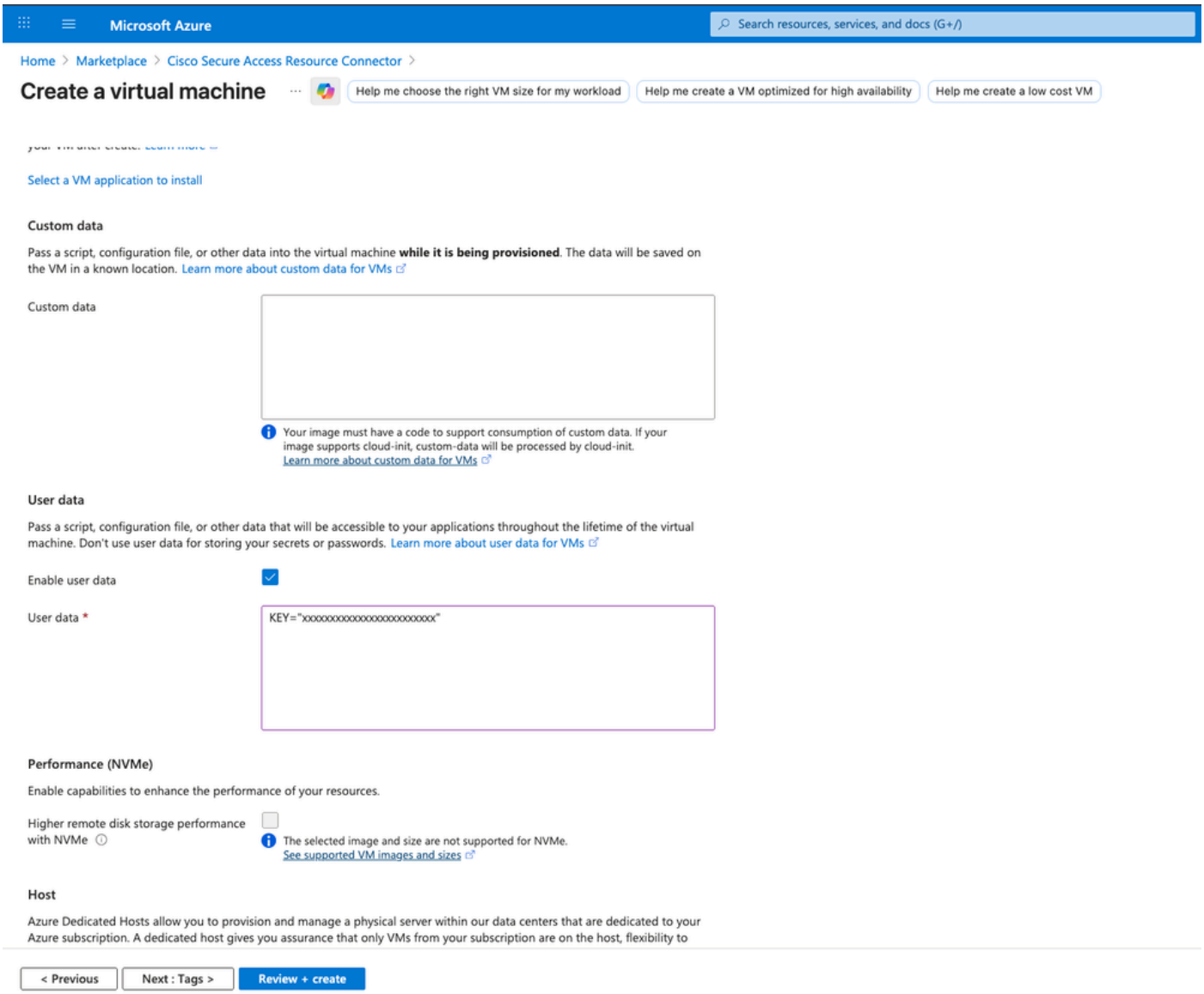

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Cisco Secure Access Resource Connector >
Create a virtual machine
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM
Basics Disks Networking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



Accès sécurisé - Création du connecteur de ressources sur Azure

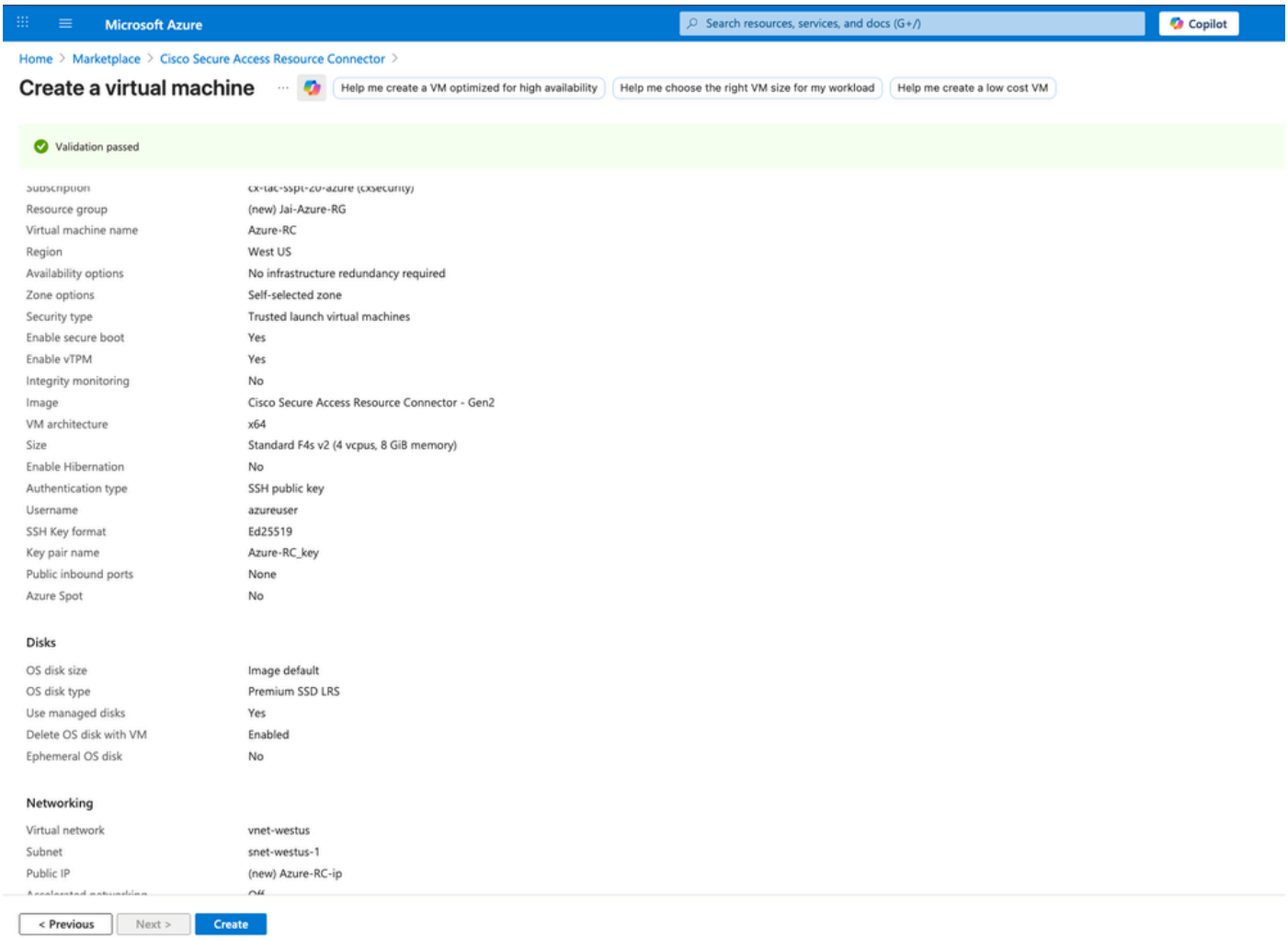
- Collez la copie Provisioning Key de Cisco Secure Access dans leUser datachamp

KEY=XXXXXXXXXXXXXXXXXXXXX



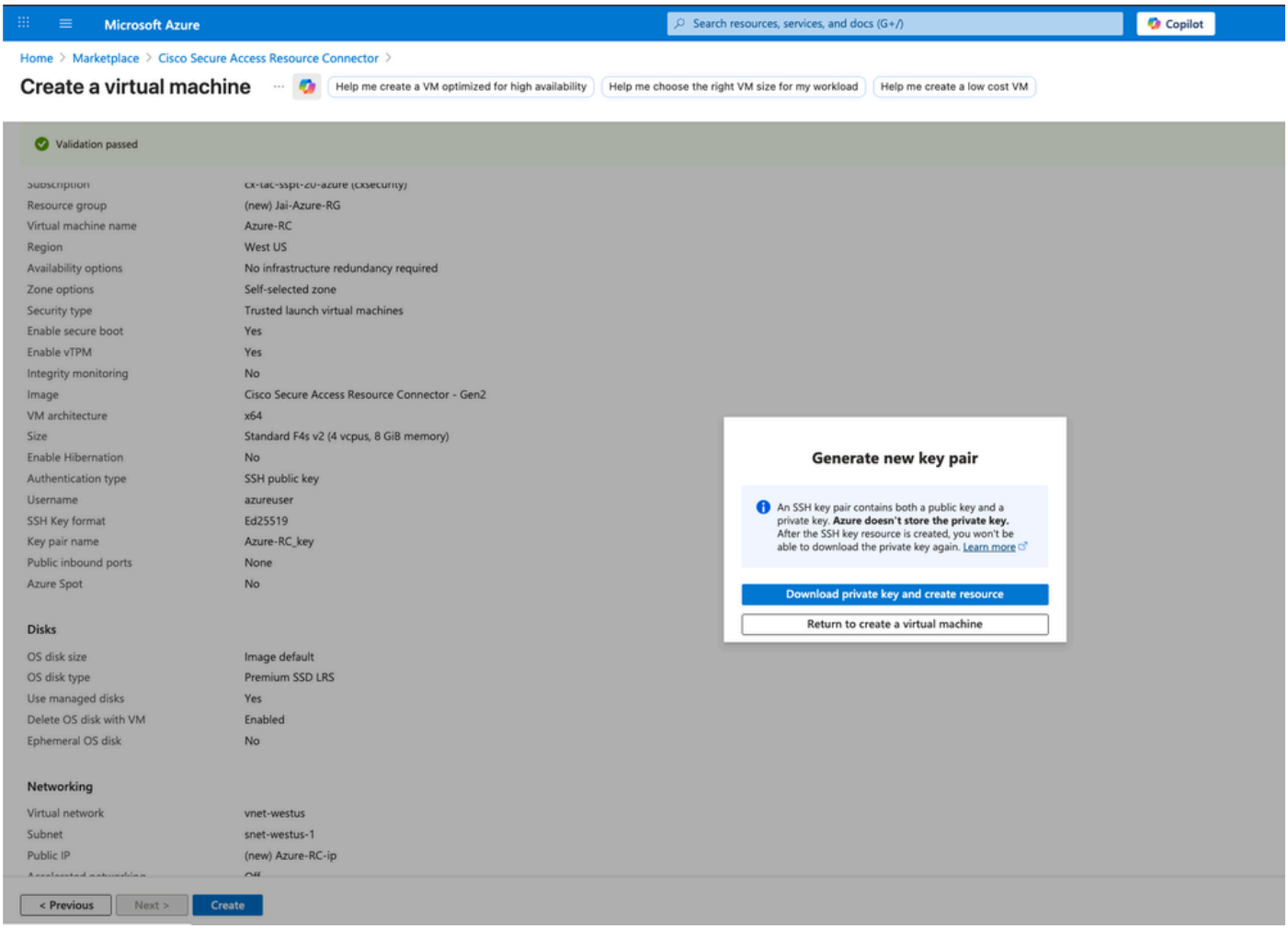
Accès sécurisé - Création du connecteur de ressources sur Azure

- Vérifiez et cliquez surCreateafin de poursuivre la création de votre Resource Connector



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

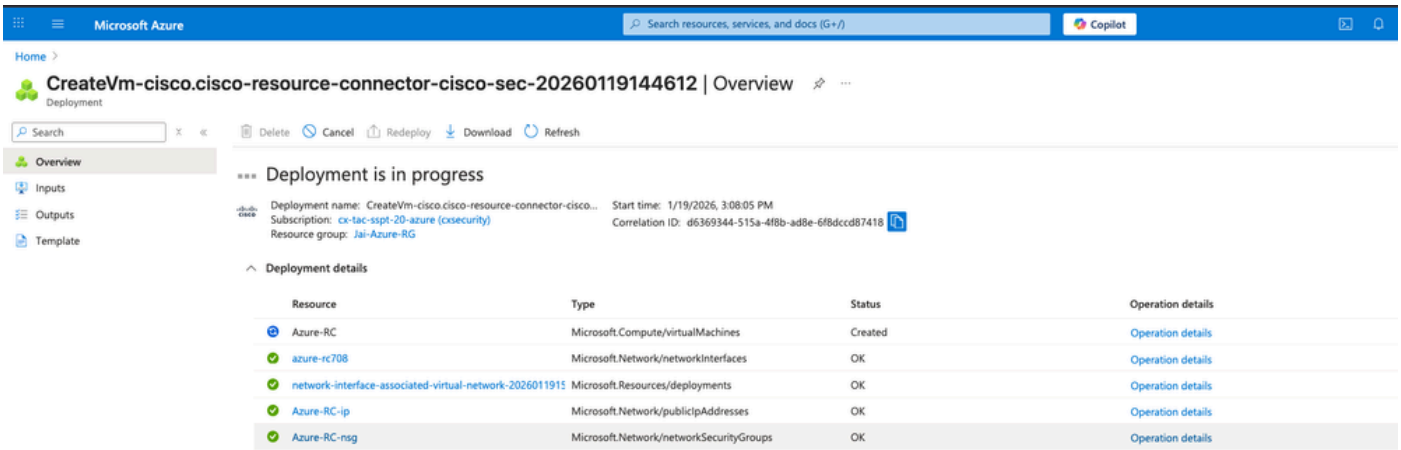


Accès sécurisé - Création du connecteur de ressources sur Azure

---

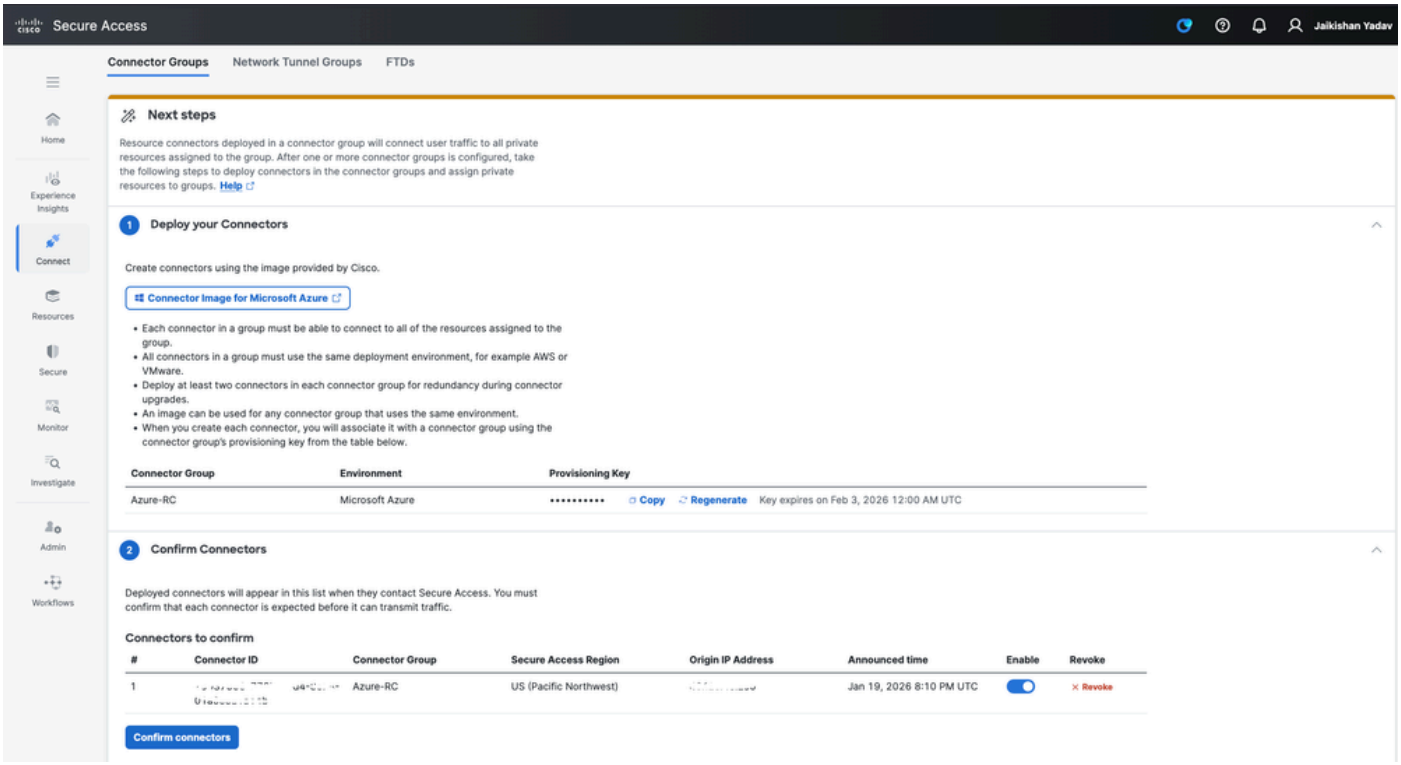
⚠ Mise en garde : Ne perdez pas la clé SSH privée ; sinon, vous ne pouvez pas accéder à l'interface de ligne de commande RC et devez la redéployer pour le dépannage.

- Après cela, vous pouvez voir la progression de votreResource Connector



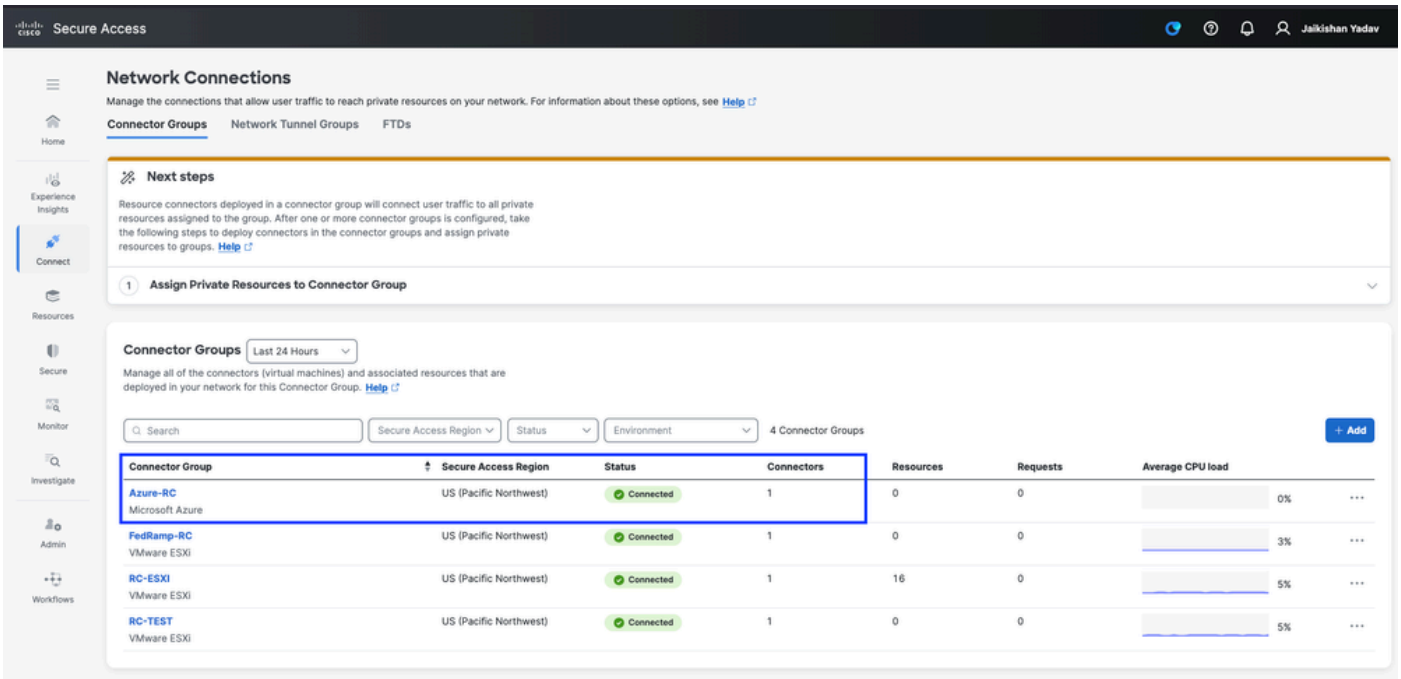
Accès sécurisé - Déploiement du connecteur de ressources sur Azure

- 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 surConfirm Connectorspour mettre fin au déploiement



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 :



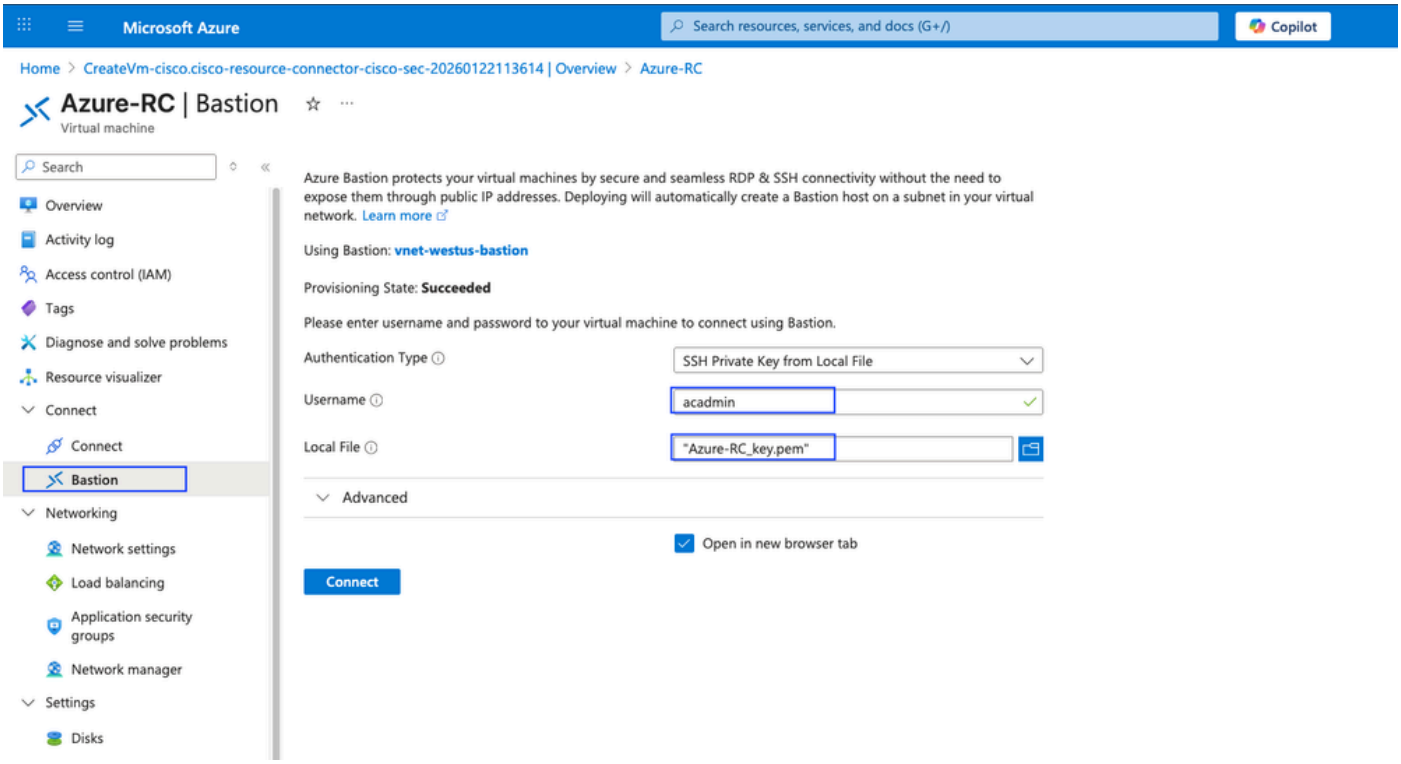
Accès sécurisé - Connecteur de ressources

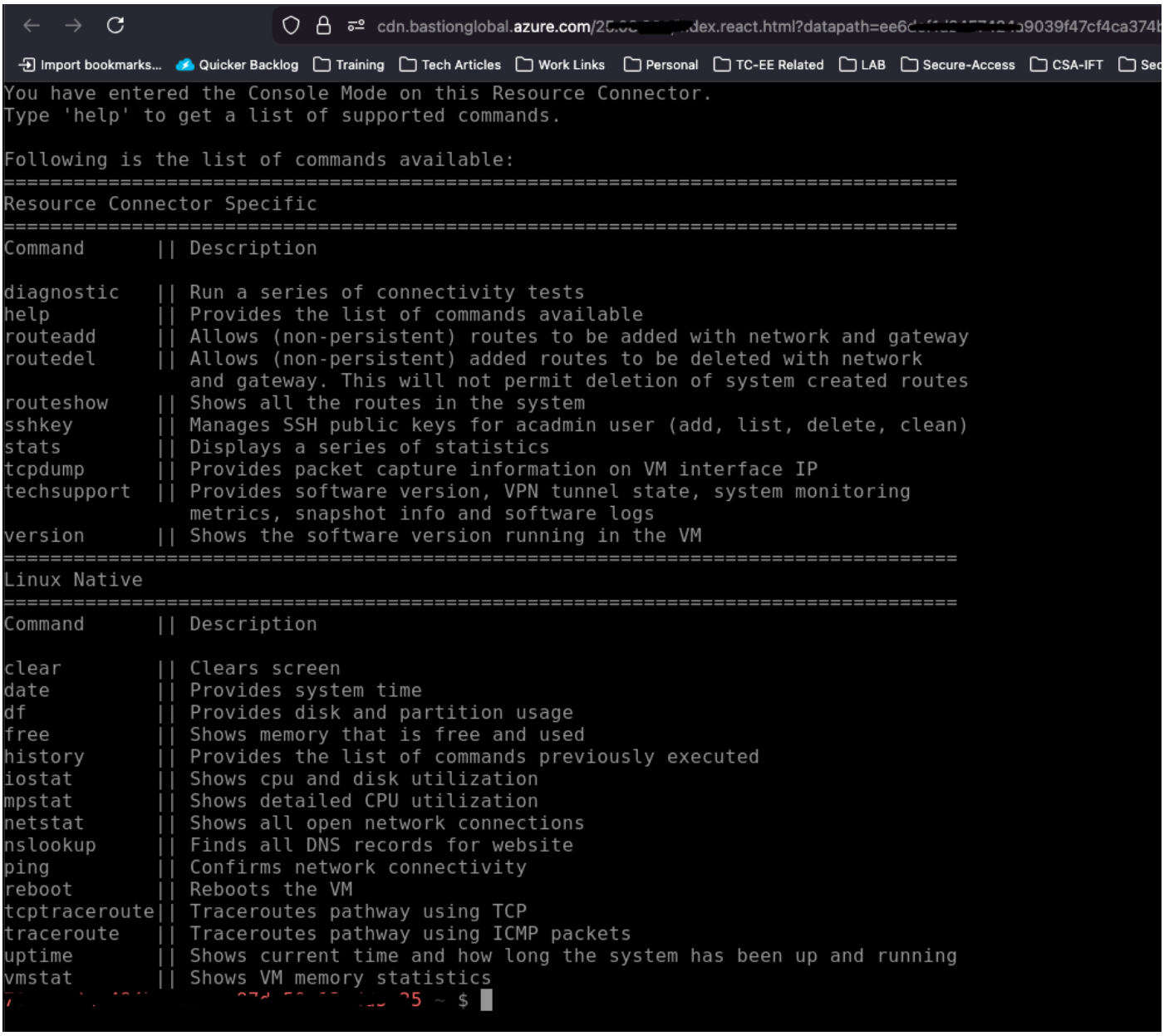
Vérifier

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

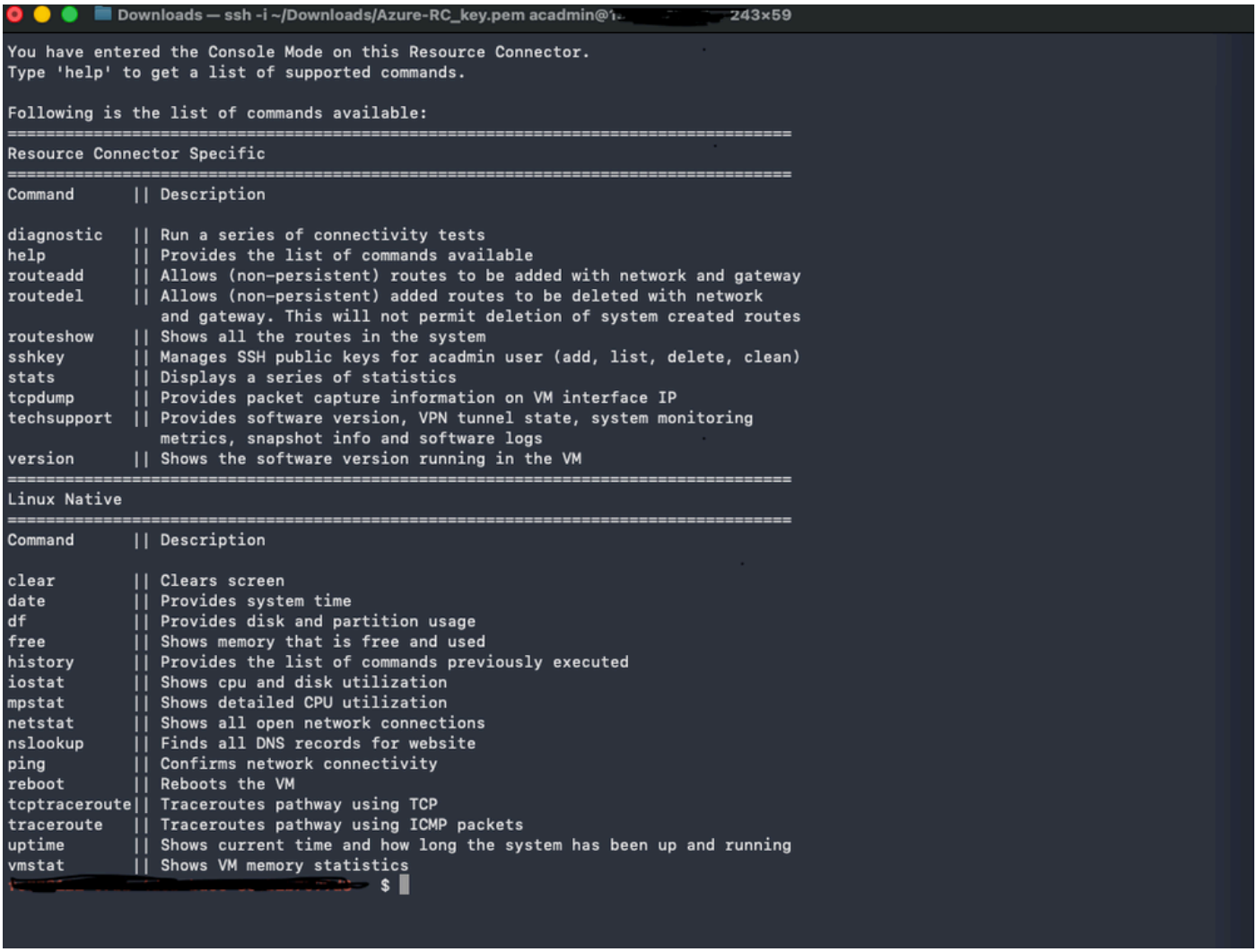




Accès sécurisé : accès à la ligne de commande du connecteur de ressources

Accès à RC à partir du terminal MAC-OS

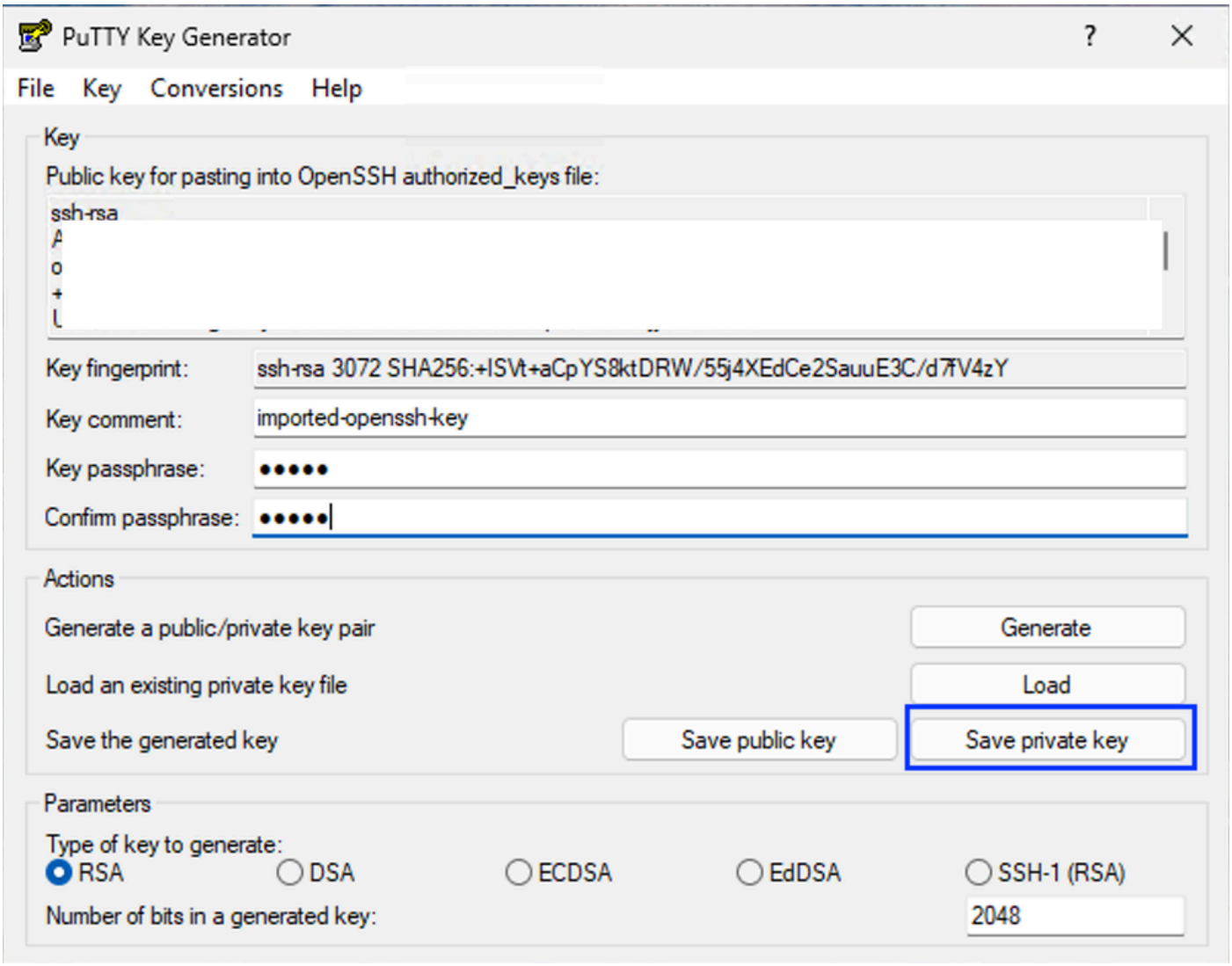
Ouvrez le terminal et utilisez ssh -i <chemin-fichier-clé-privée> acadmin@x.x.x.x.x afin de connecter à votre connecteur de ressources.



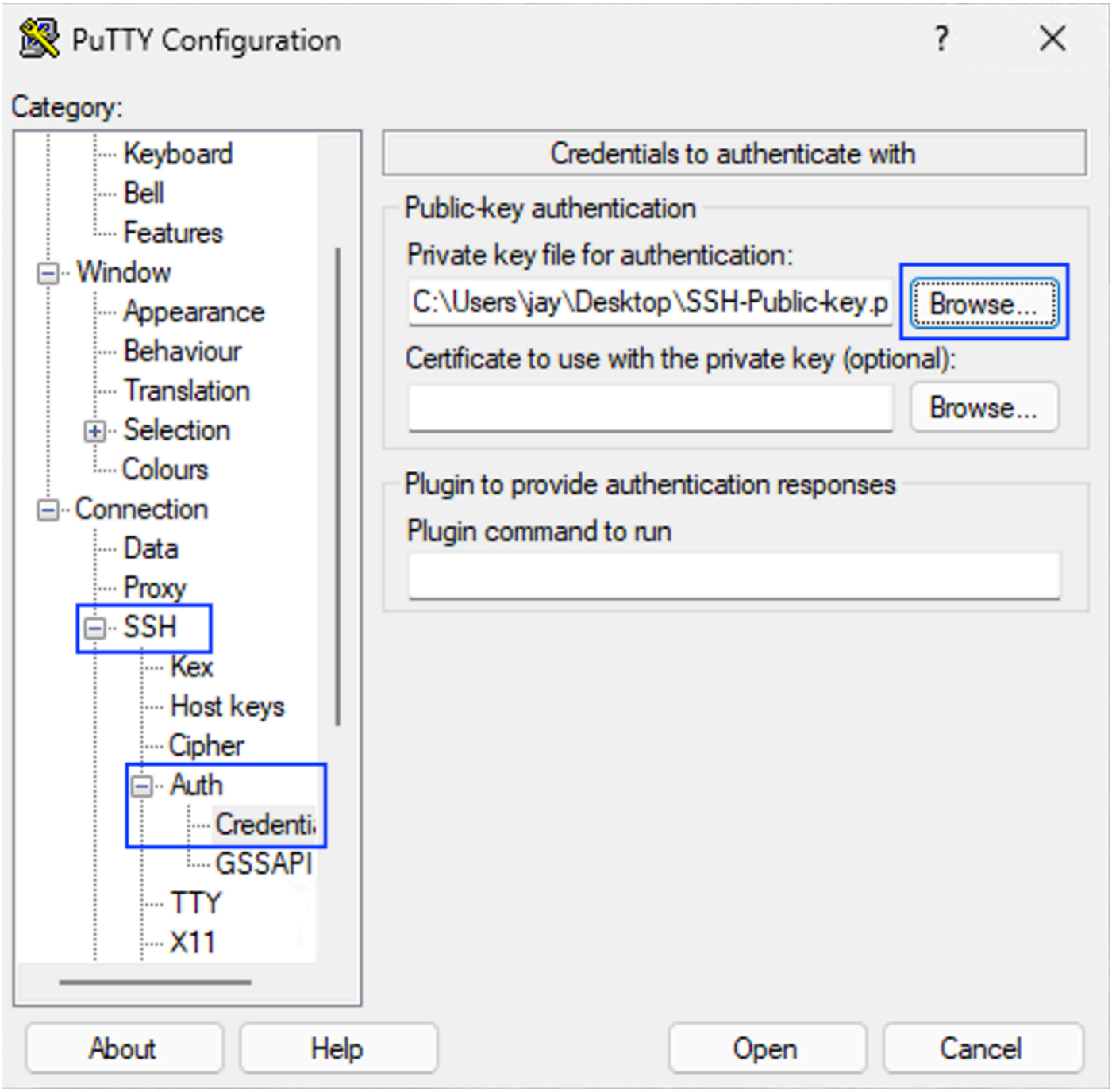
Accès sécurisé : accès à la ligne de commande du connecteur de ressources

Accès à partir de Windows - Putty

Afin d'utiliser la clé privée, vous devez convertir le SSH private key de à formart.pemen .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 Sessionl'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
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
```

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.