Bereitstellen von Secure Access Resource Connector in Azure

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen Ressourcenkonnektor Schritt für Schritt in Azure bereitstellen.

Voraussetzungen

Sammeln Sie die erforderlichen Informationen, und machen Sie sich mit den

- Rufen Sie das Steckverbinderbild ab.
  - Sie können das Image einmal herunterladen und für eine beliebige Anzahl von Anschlüssen in einer beliebigen Anschlussgruppe verwenden.
  - Wenn Sie ein zuvor heruntergeladenes Image verwenden, stellen Sie sicher, dass es sich um die neueste Version handelt.
  - Weitere Informationen finden Sie unter Abrufen des Connector-Images.
- Kopieren Sie den Bereitstellungsschlüssel für die jeweilige Connectorgruppe, für die Sie Connectors bereitstellen.
  Siehe Bereitstellungsschlüssel für Ressourcenkonnektoren.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Administratorzugriff auf das Cisco Secure Access Dashboard
- Azure-Portalzugriff

- Cisco Secure Client
- Windows-Maschine mit eingeschriebenem ZTA

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Test, der in einer Laborumgebung mit den folgenden Komponenten durchgeführt wurde:

- ZTNA-Client
- Sicherer Zugriff
- Azure
- Private Ressource

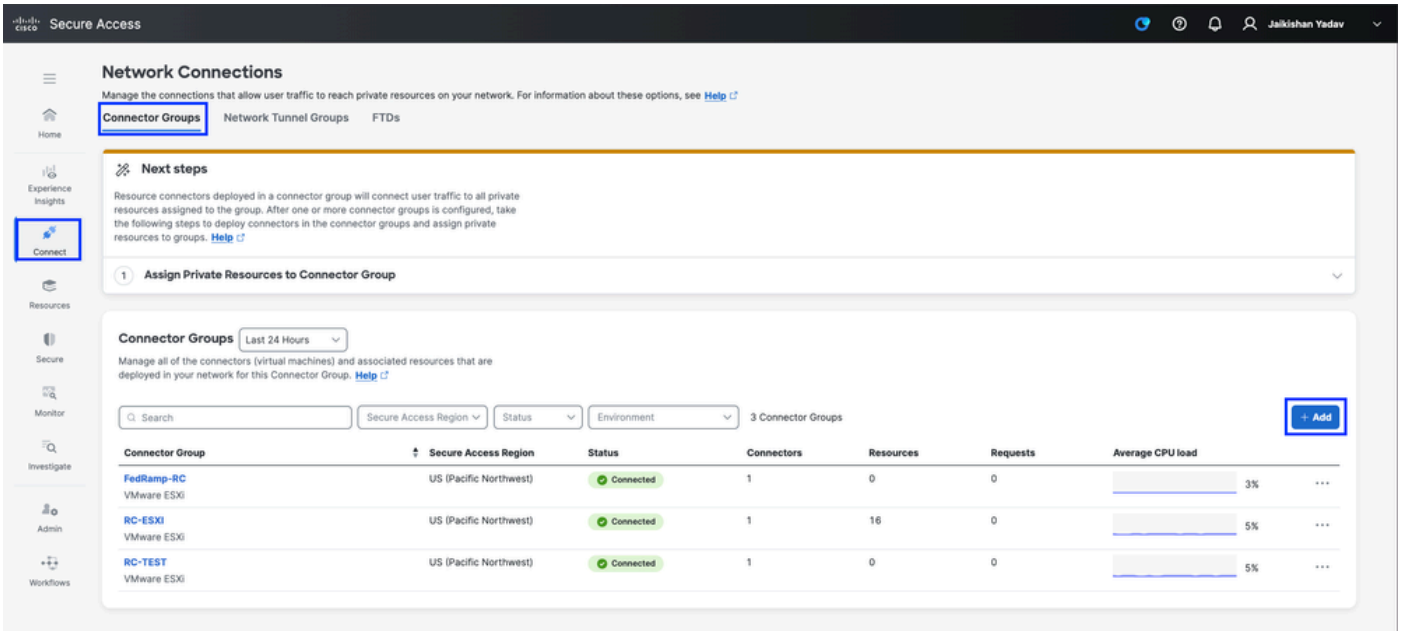
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Konfigurationen in sicherem Zugriff

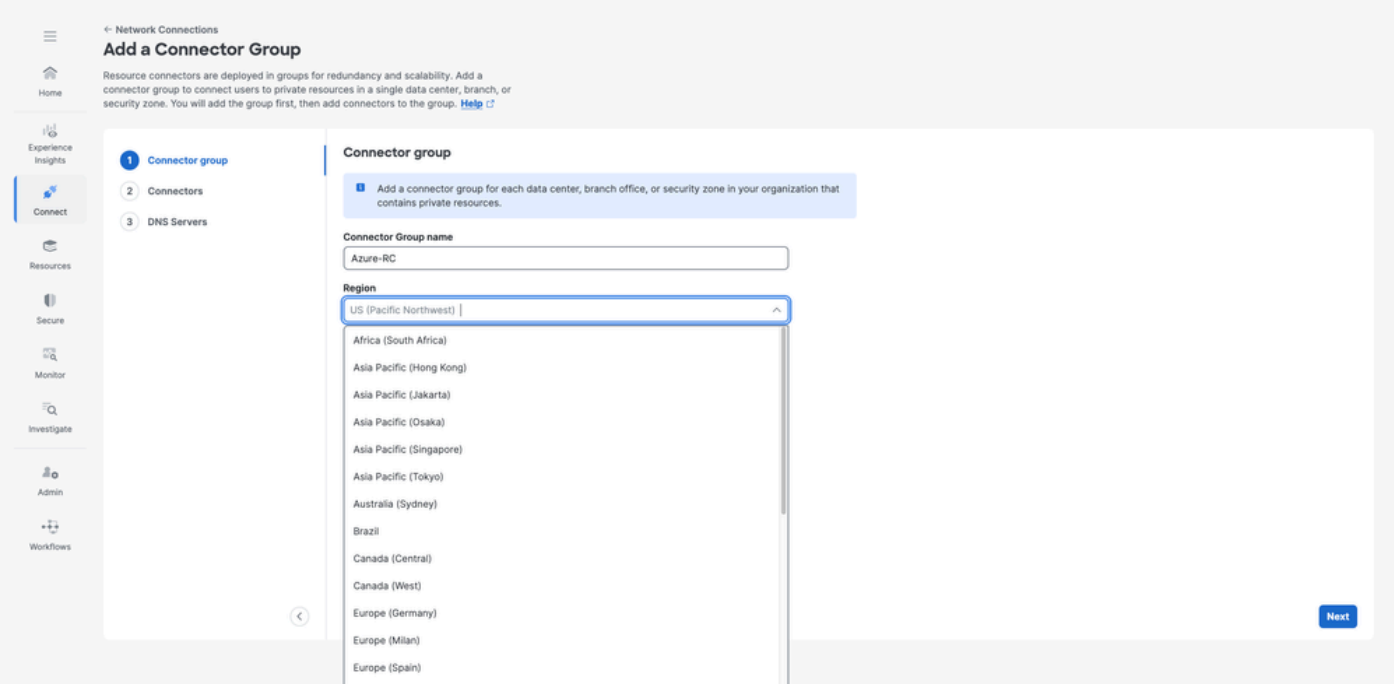
Melden Sie sich beim Secure Access Dashboard an, und navigieren Sie zu **Connect > Network Connections > Connector Groups**

- Klicken Sie add



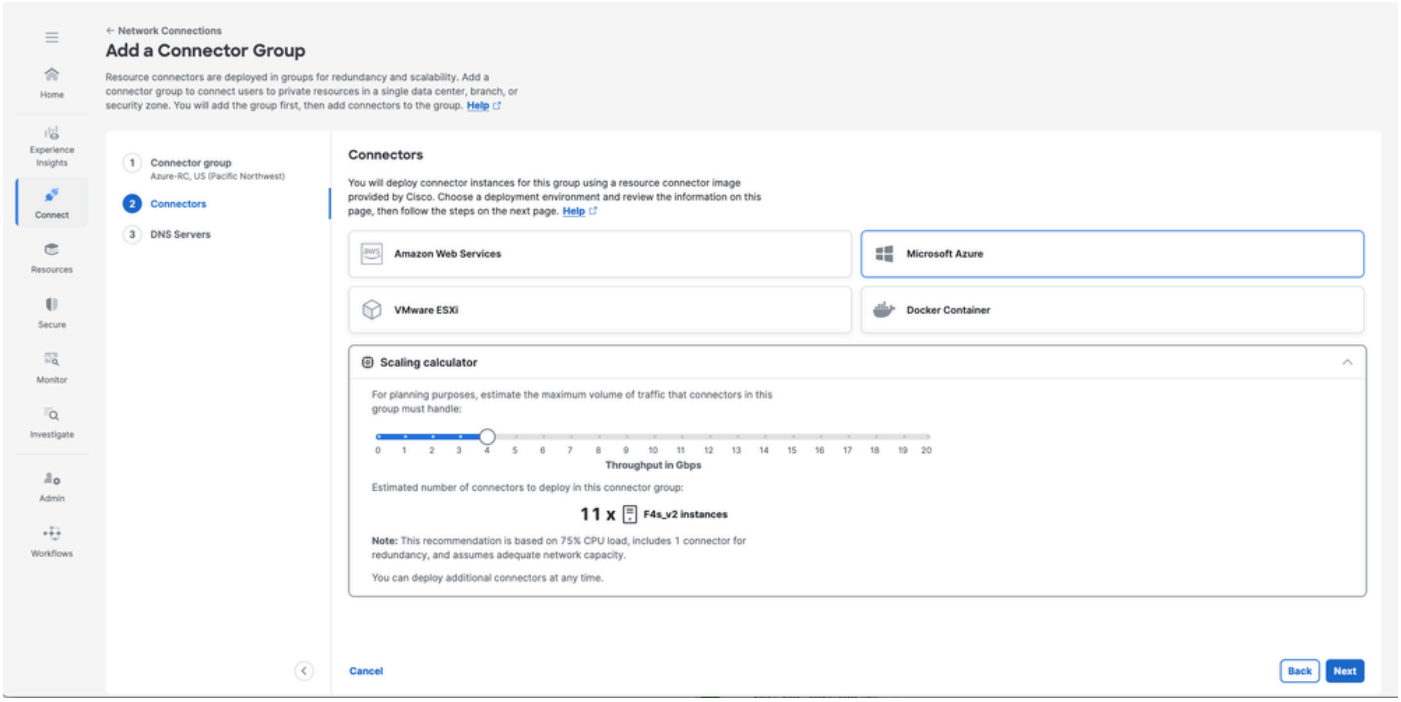
Sicherer Zugriff - Anschlussgruppen

- Geben Sie den Connector Group Name und den Region
- Klicken Sie auf Next



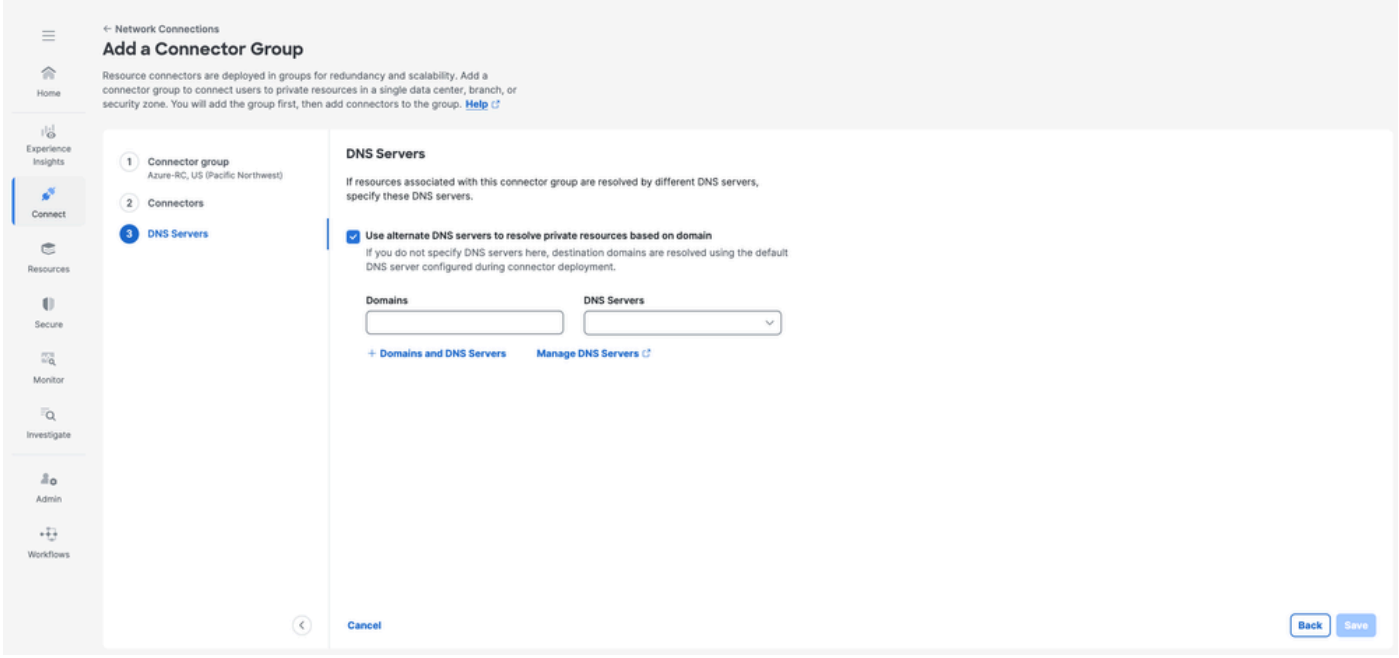
Sicherer Zugriff - Konfiguration von Anschlussgruppen

- Wählen Sie Microsoft Azure die erforderlichen Ressourcen aus, und bestimmen Sie die Scaling Calculator benötigten Ressourcen mithilfe des



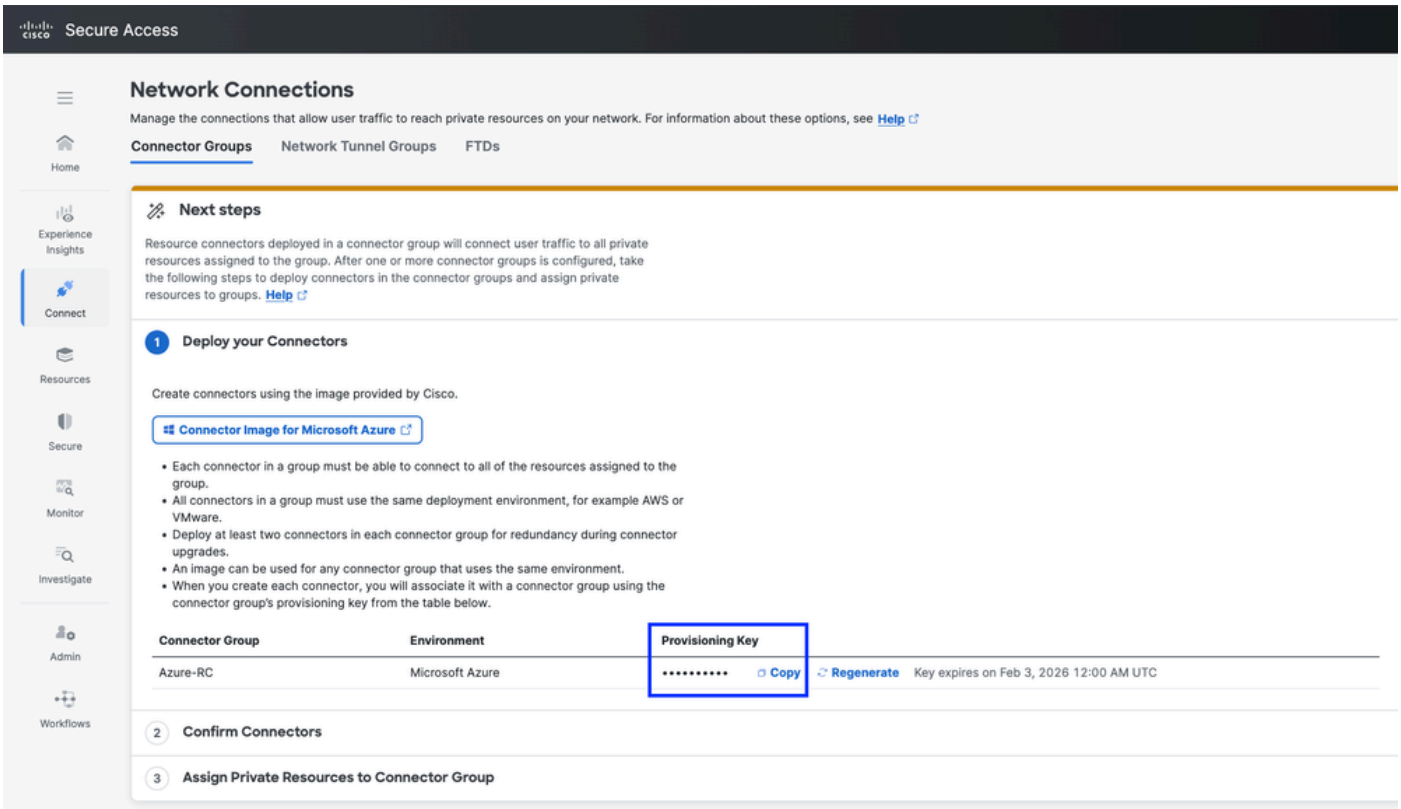
Sicherer Zugriff - Überprüfung der Resource Connector-Konfiguration

- Nutzung der DNS Servers Option zur Auflösung bestimmter Domänen über dedizierte DNS-Server. Dies gilt als Best Practice für Unternehmen mit mehreren internen Domänen.
- Klicken Sie auf Save



Sicherer Zugriff - Konfiguration des Ressourcenanschlusses

- Stellen Sie zu diesem Zeitpunkt sicher, dass Sie das Provisioning Keykopieren. Sie benötigen diese später in Azure während der Bereitstellung des Ressourcenkonnektors, um die Registrierung bei Ihrem sicheren Zugriffs-Tenant zu aktivieren.

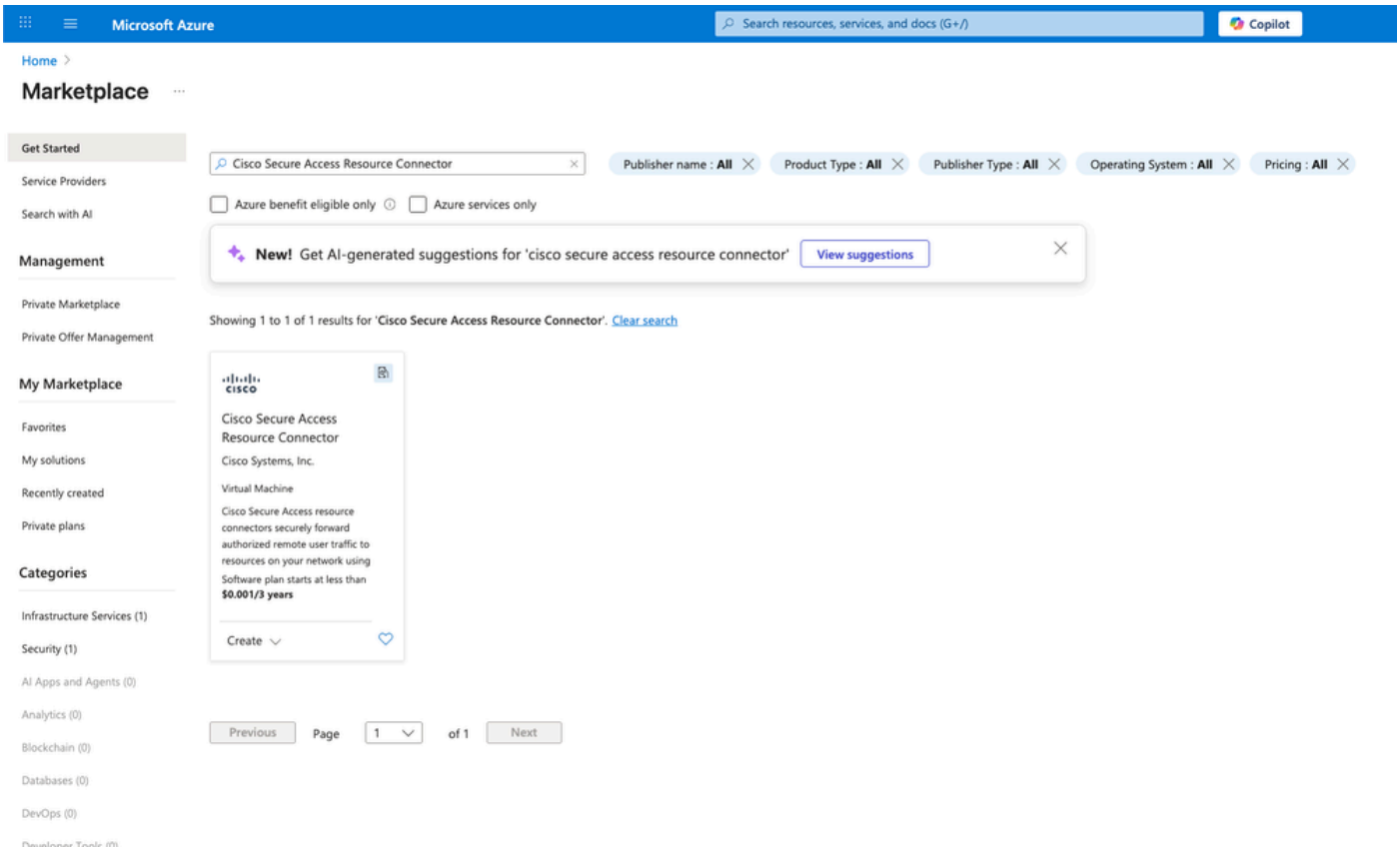


Sicherer Zugriff - Konfiguration des Ressourcenanschlusses

Konfigurationen in Azure

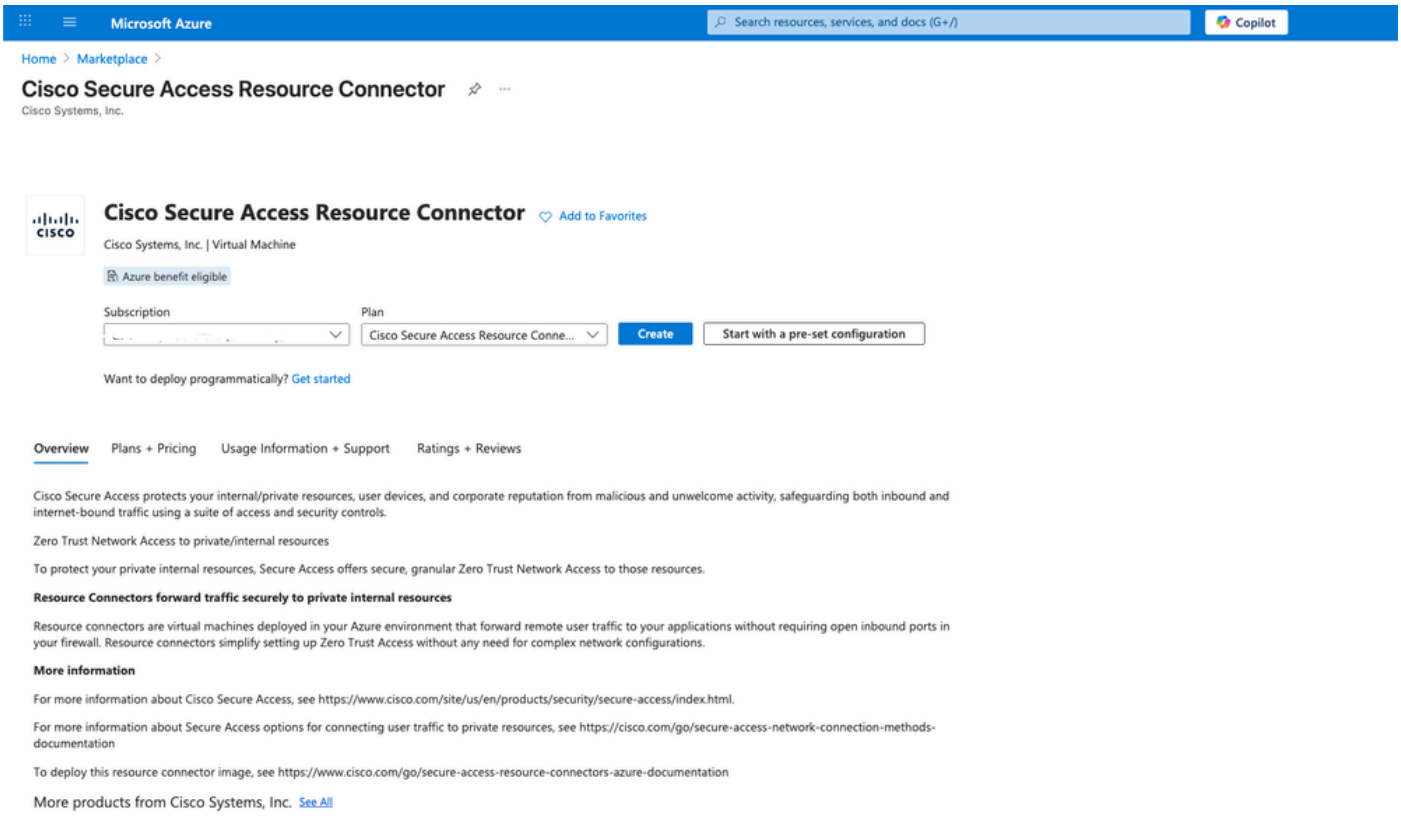
Navigieren Sie zum Azure-Portal, navigieren Sie zum Microsoft Azure Marketplace, und suchen

Sie nach dem Abbild Cisco Secure Access Resource Connector:

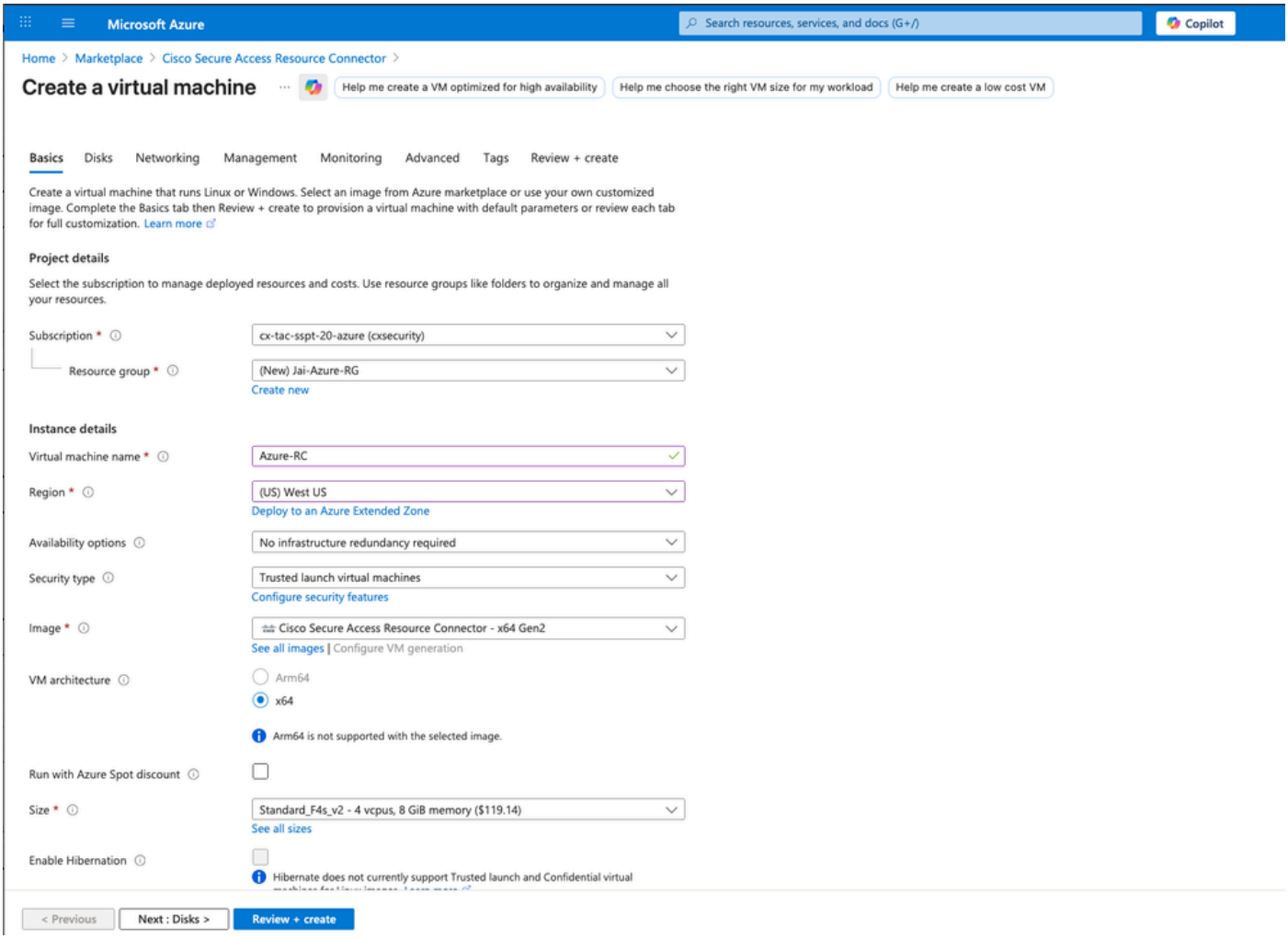


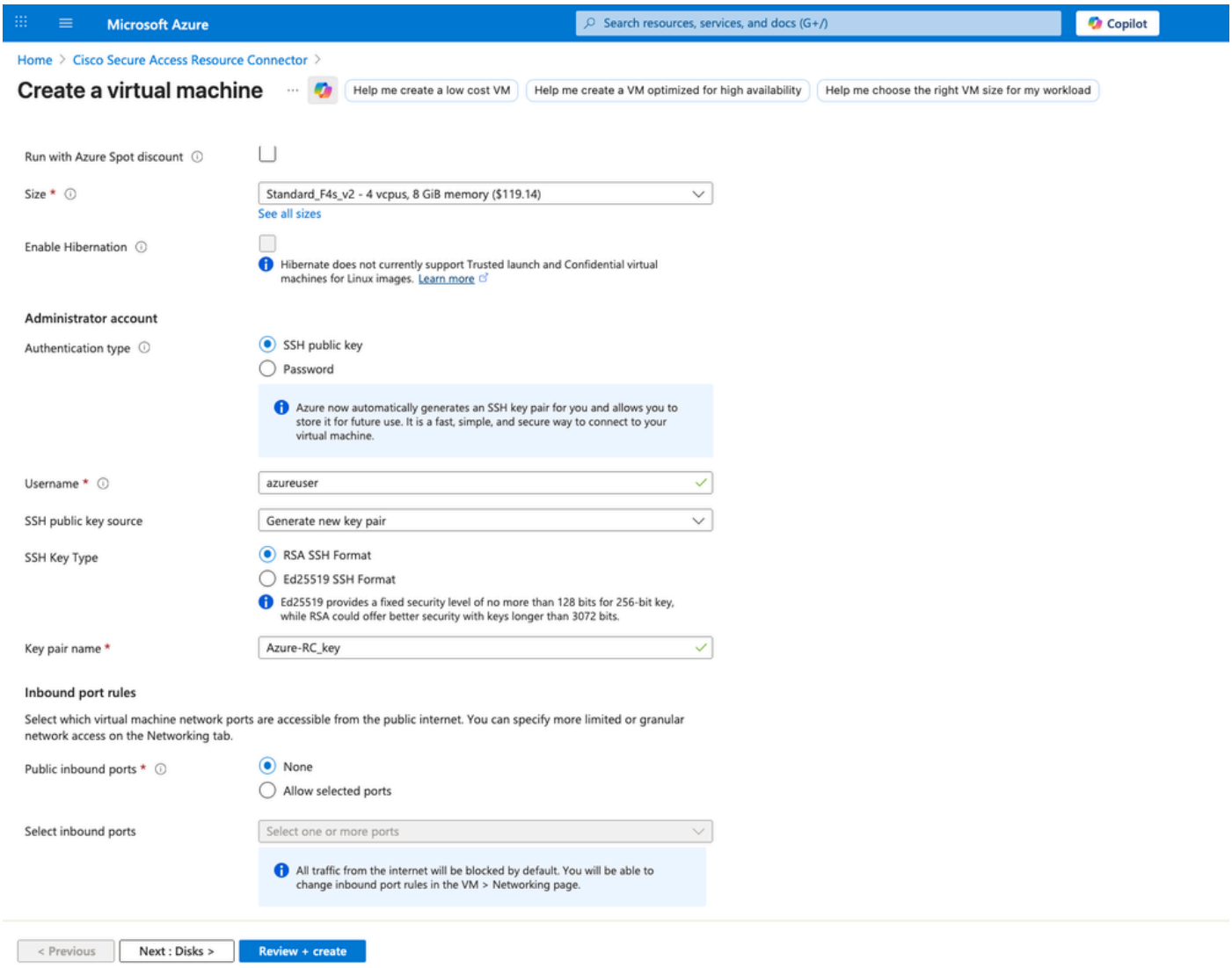
Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

- Wählen Sie die entsprechende Subscription und und klicken Sie dann Plan auf Create

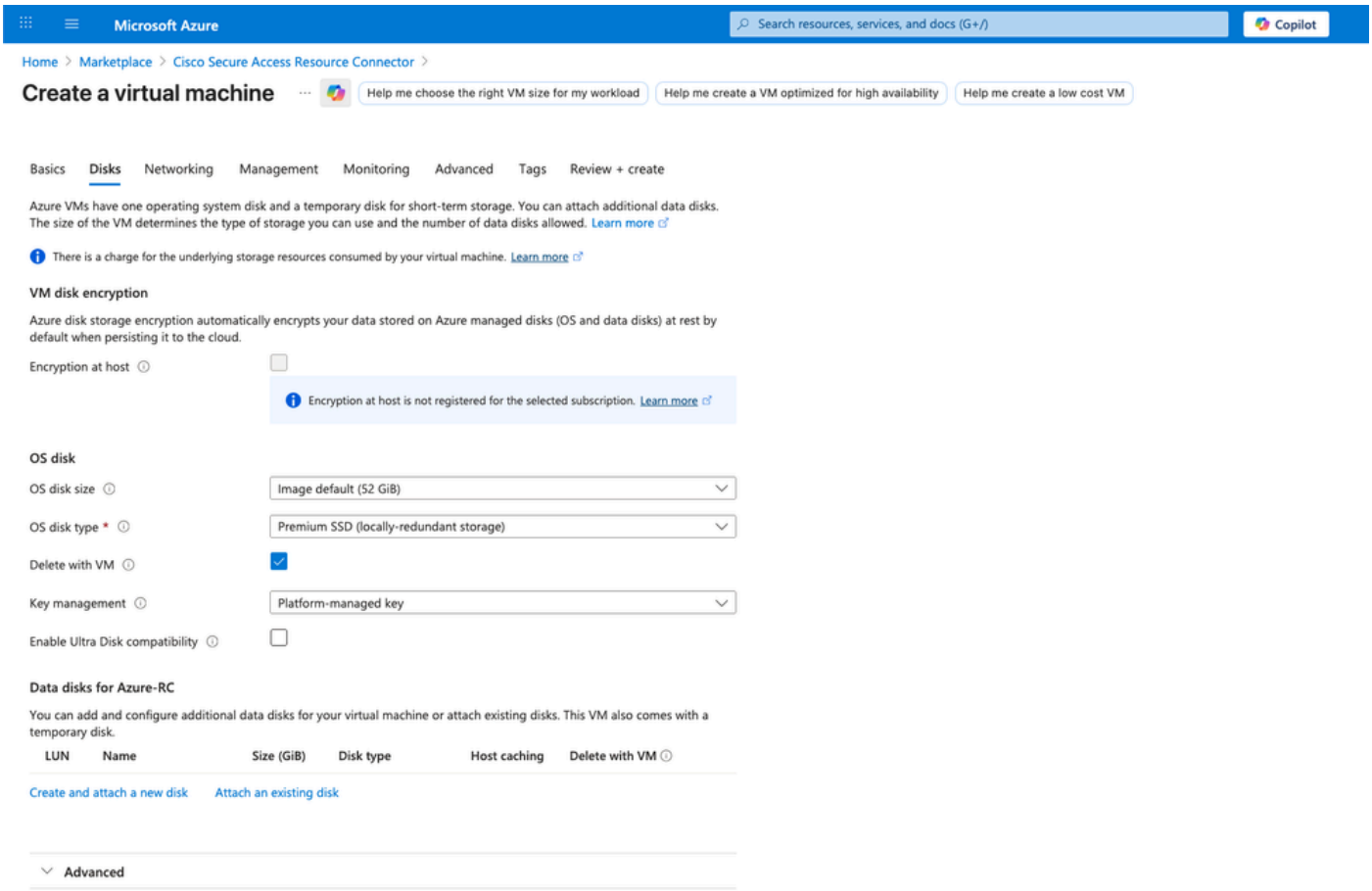


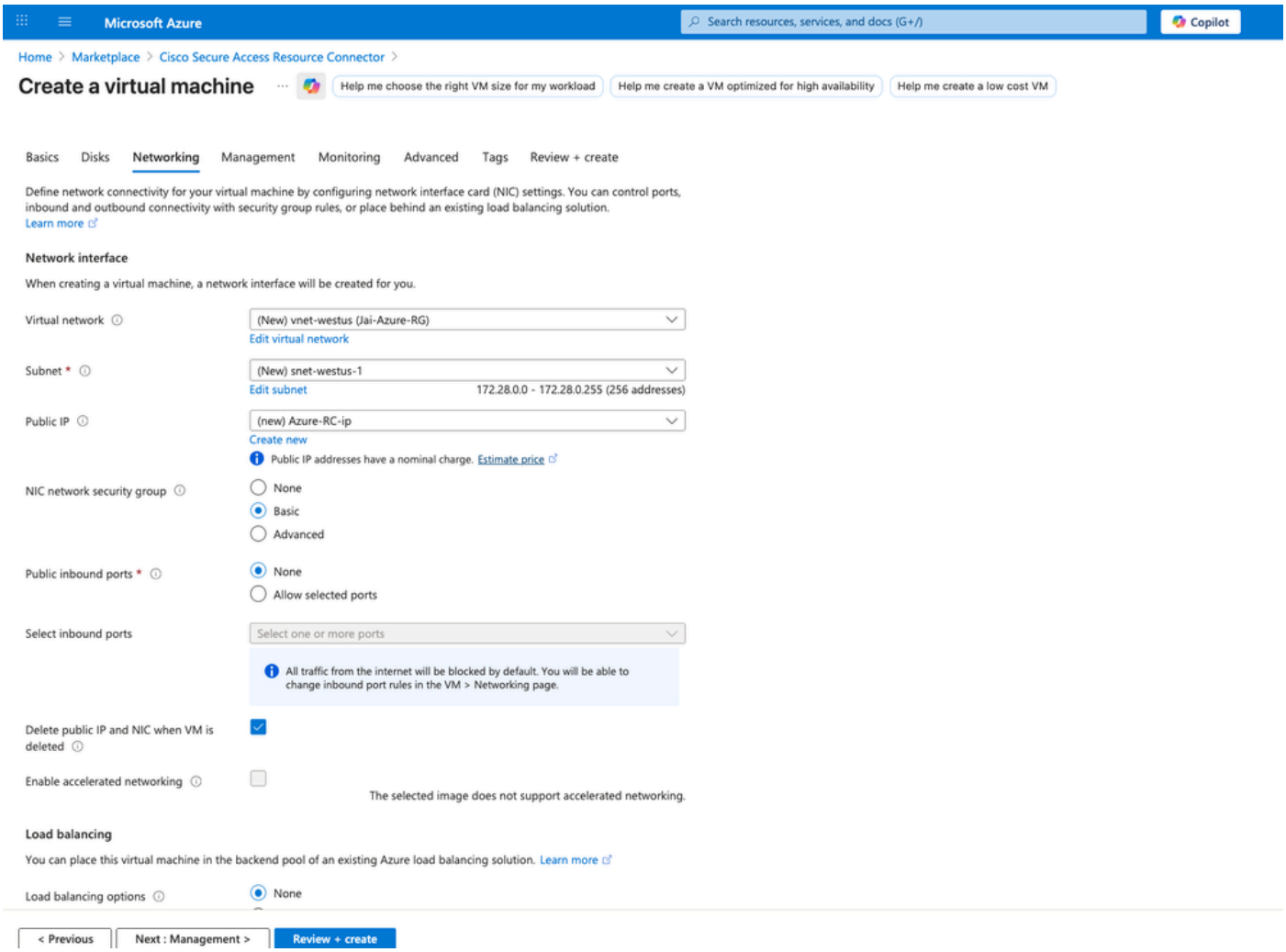
- Überprüfen der Konfiguration für Disks, Networking und den öffentlichen SSH-Schlüssel





⚠ Vorsicht: Verlieren Sie nicht den privaten SSH-Schlüssel. Andernfalls können Sie nicht auf die RC-CLI zugreifen und müssen diese zur Fehlerbehebung erneut bereitstellen.

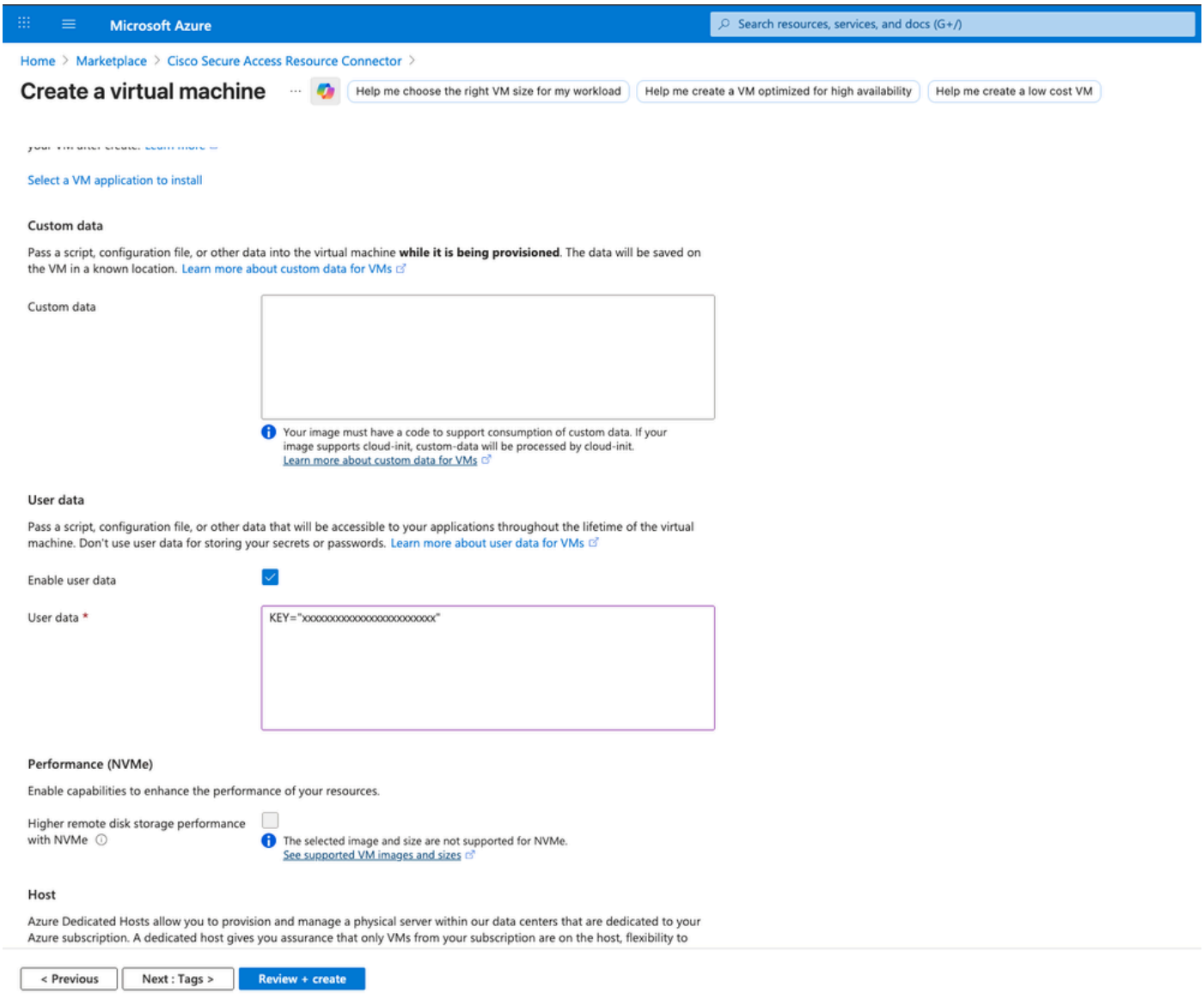

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Cisco Secure Access Resource Connector >
Create a virtual machine
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM
Basics Disks Networking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



Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

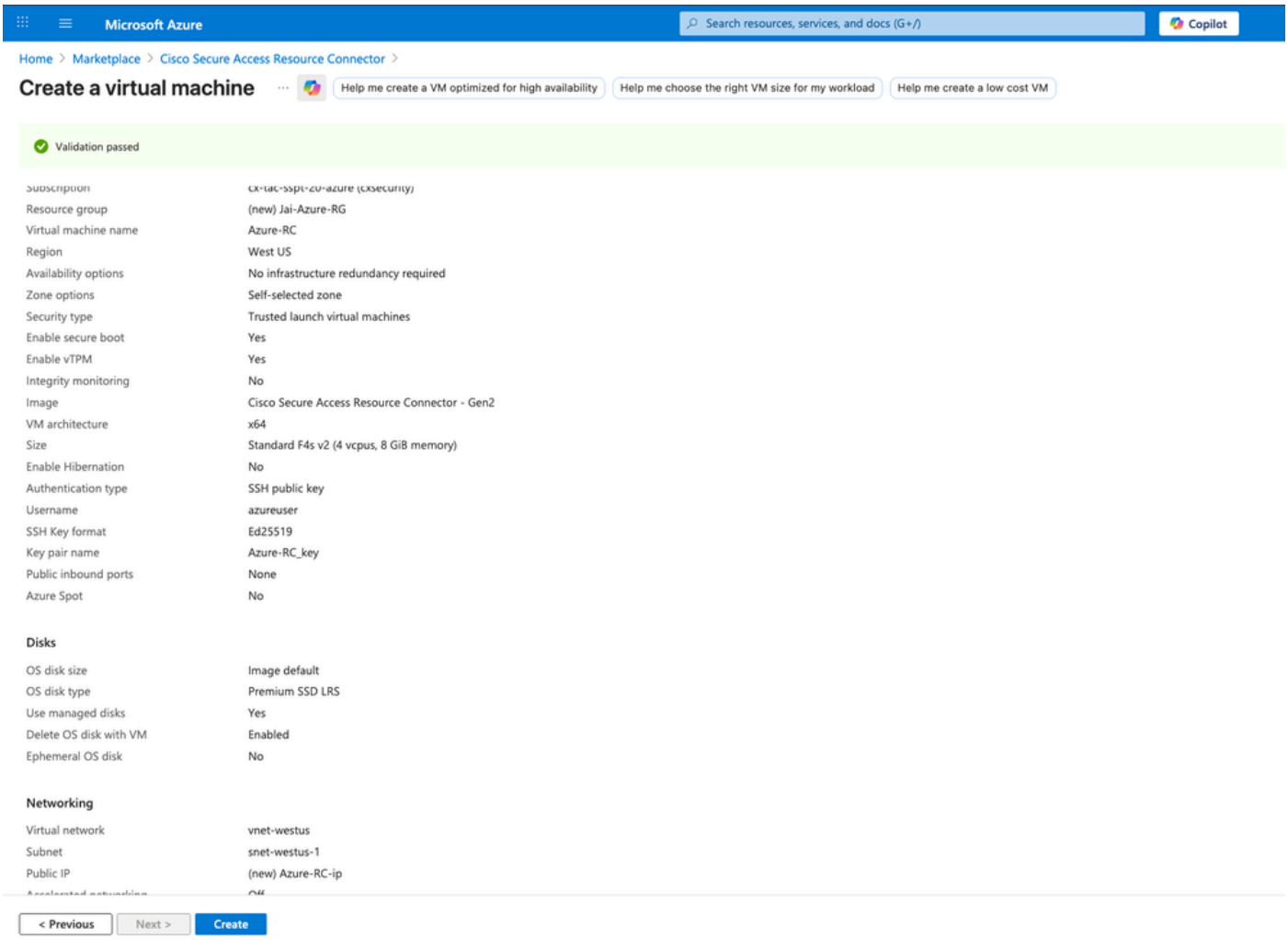
- Einfügen des Provisioning Key kopierten Dokuments aus Cisco Secure Access in dasUser dataFeld

KEY=XXXXXXXXXXXXXXXXXXXX



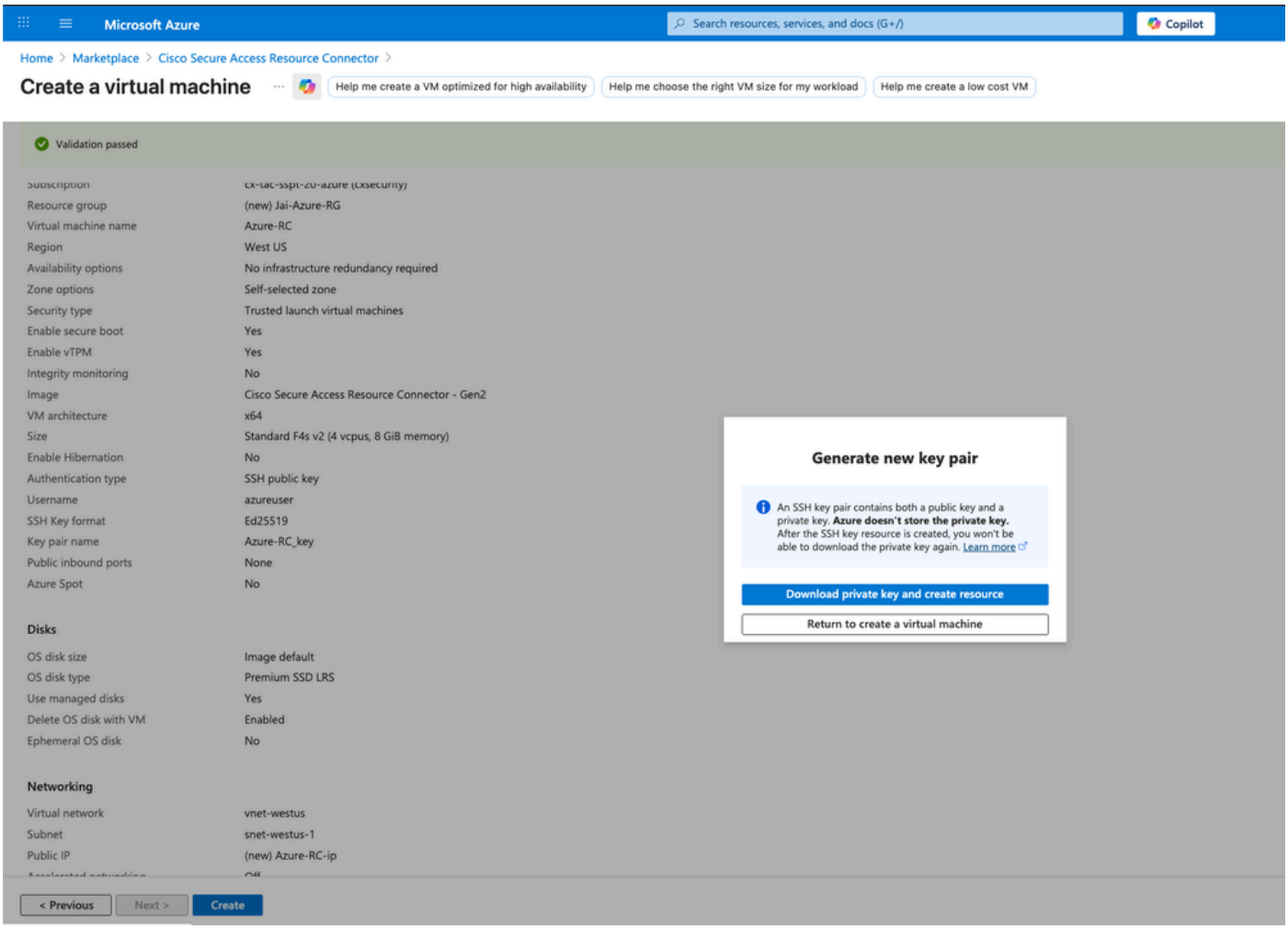
Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

- Klicken Sie auf, um mitCreateder Erstellung Ihres Resource Connector



Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

- Wenn Sie auf klickenCreate, wird eine Option zum Herunterladen des privaten Schlüssels angezeigt. Klicken Sie Download private key and create resource

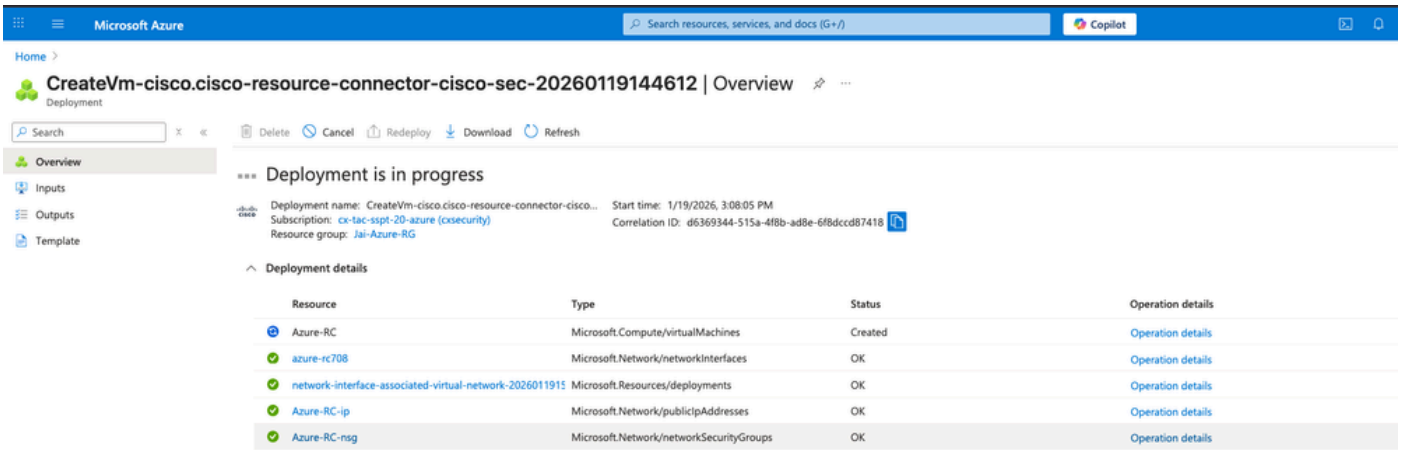


Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

---

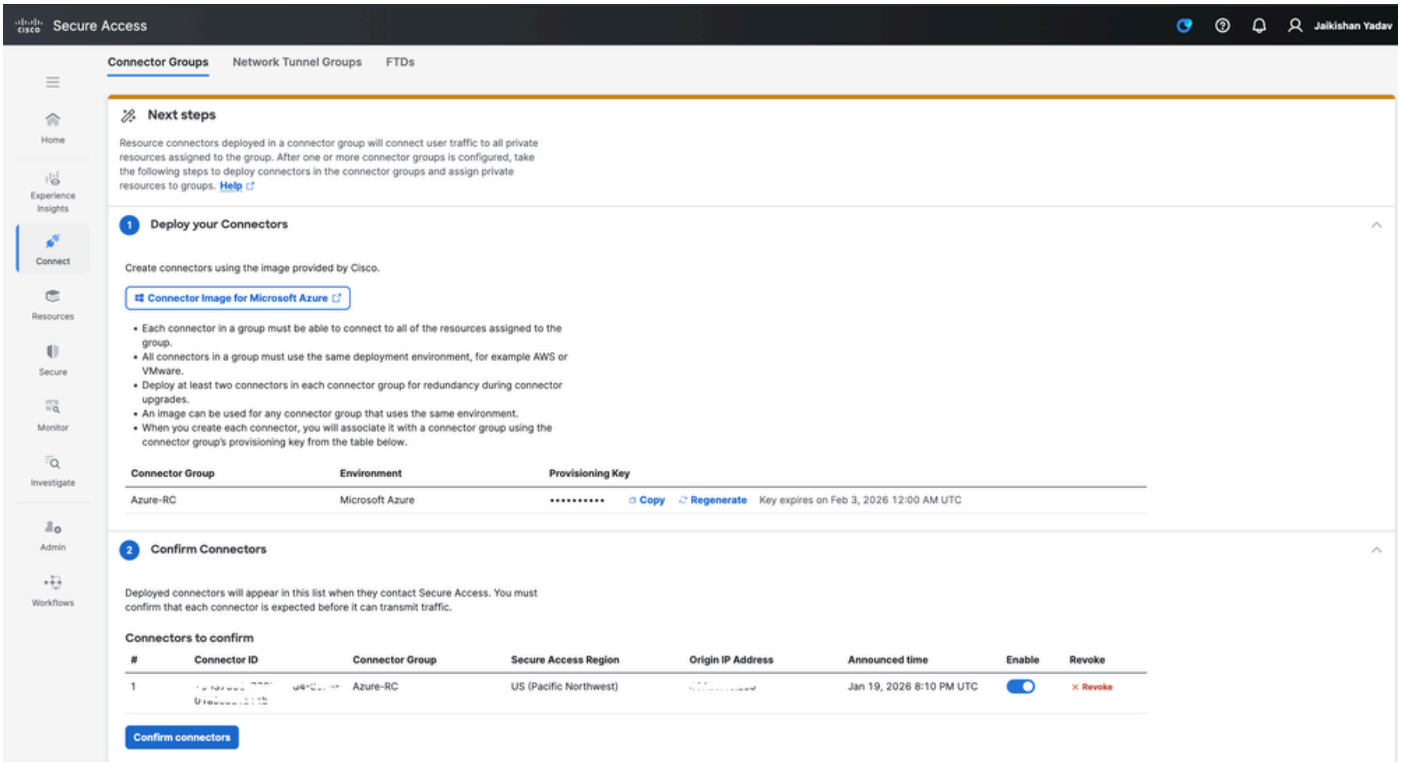
⚠ Vorsicht: Verlieren Sie nicht den privaten SSH-Schlüssel. Andernfalls können Sie nicht auf die RC-CLI zugreifen und müssen diese zur Fehlerbehebung erneut bereitstellen.

- Danach können Sie den Fortschritt IhresResource Connector



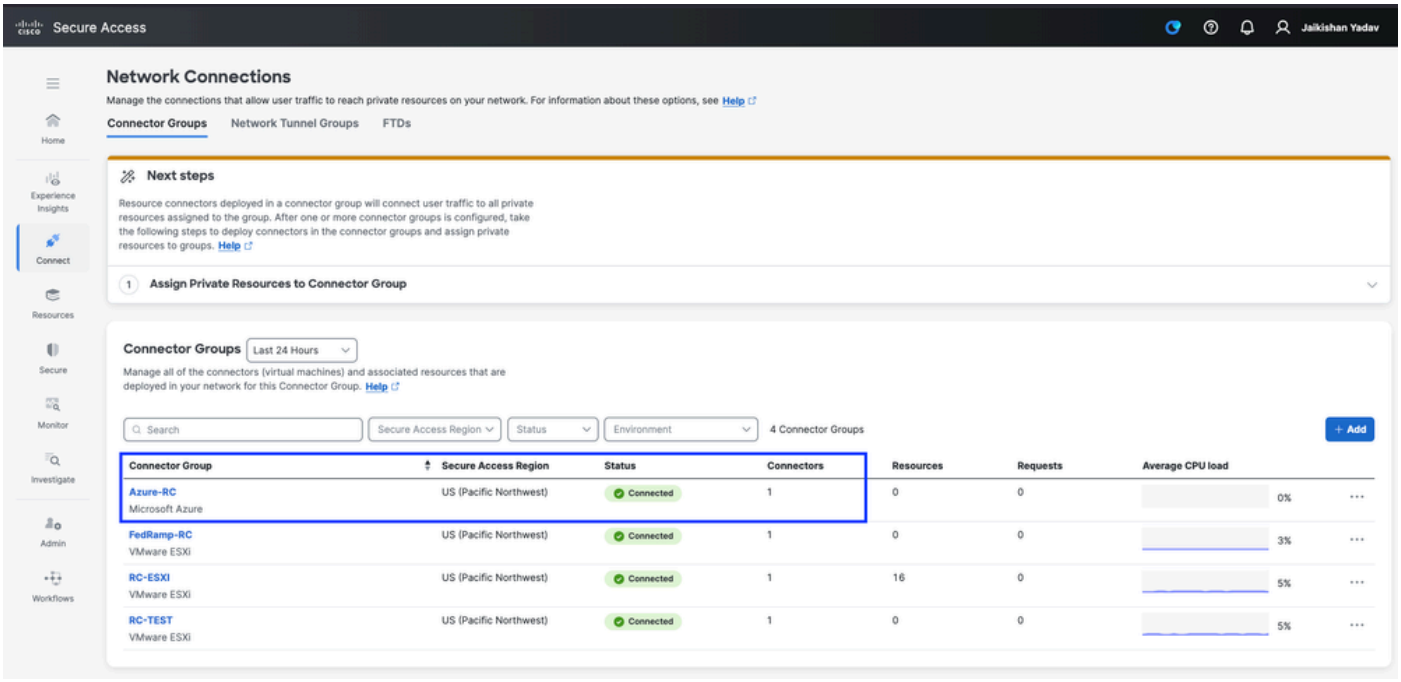
Sicherer Zugriff - Ressourcenkonnektorbereitstellung auf Azure

- Navigieren Sie anschließend zum Secure Access Dashboard, um die Verbindung und die Resource Connector erfolgreiche Bereitstellung in Ihrem Secure Access Tenant zu bestätigen.
- Klicken Sie **Connect** > **Network Connections** > **Connector Groups**
- Klicken Sie unter Option 2 Connectors bestätigen auf, um die BereitstellungConfirm Connectorszu beenden.



Sicherer Zugriff - Bestätigung des Ressourcenkonnektors

Jetzt können Sie sehen, wie der neue Resource Connector in Ihrem Secure Access-Tenant bereitgestellt und verbunden wird:

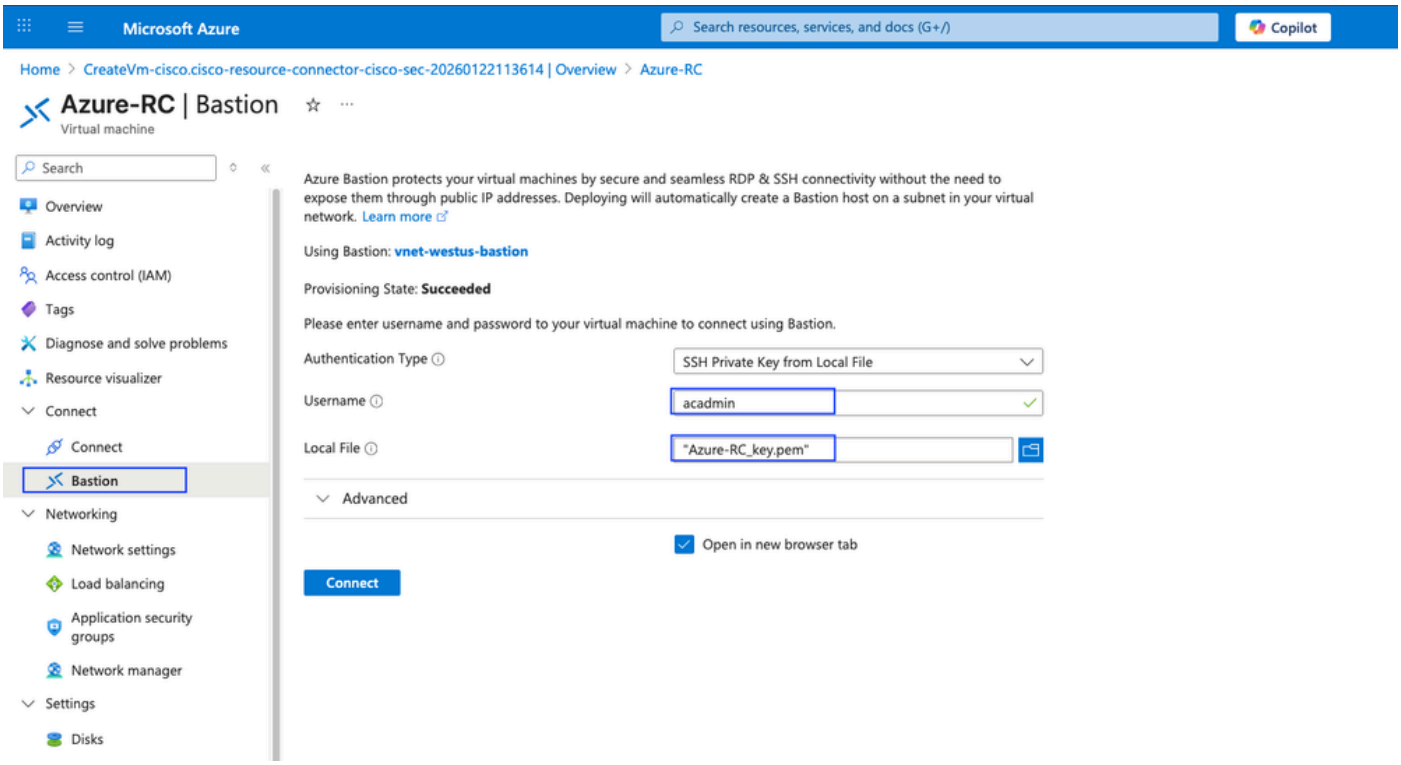


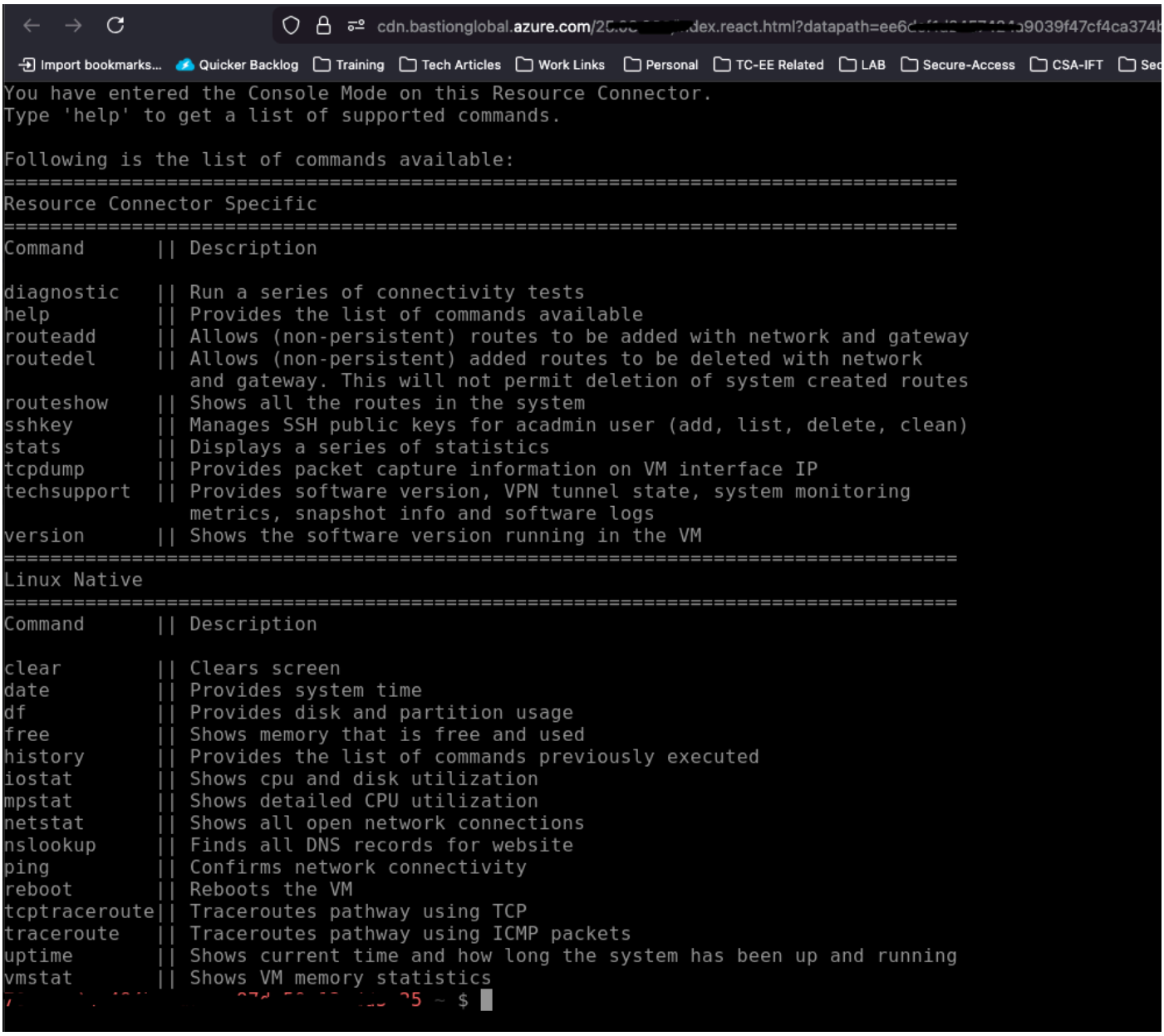
Überprüfung

Zugriff über die Kommandozeile der integrierten Bastion

Rufen Sie in Azure den Ressourcen-Connector auf, und klicken Sie auf Bastion:

- Authentication Type: Auswählen SSH Private key from Local File
- **Username**: Sie müssen acadmin
- **Local File**: Wählen Sie den private key zuvor heruntergeladenen

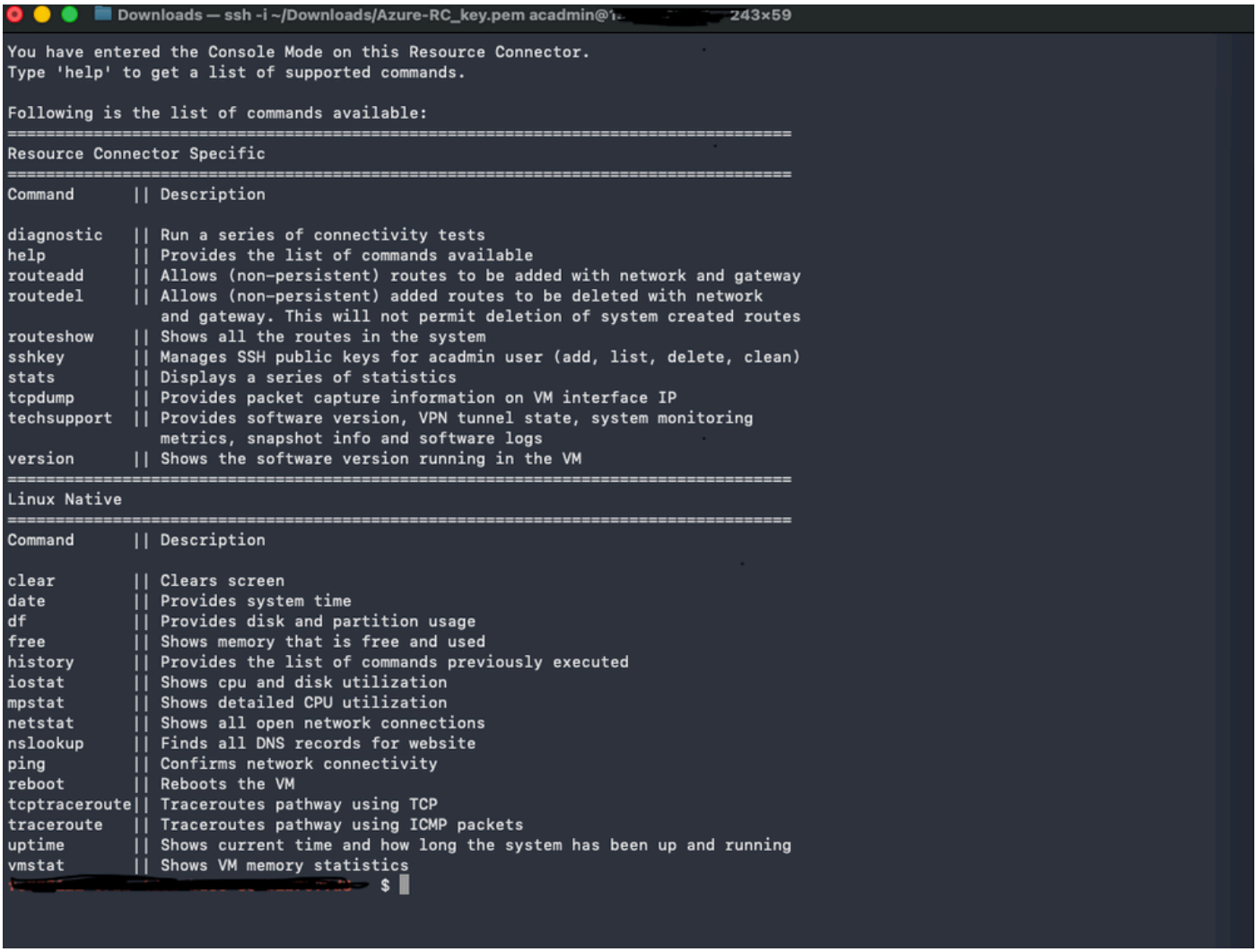




Sicherer Zugriff - Zugriff auf die Befehlszeile des Ressourcenkonnektors

Zugriff auf RC vom MAC-OS-Terminal

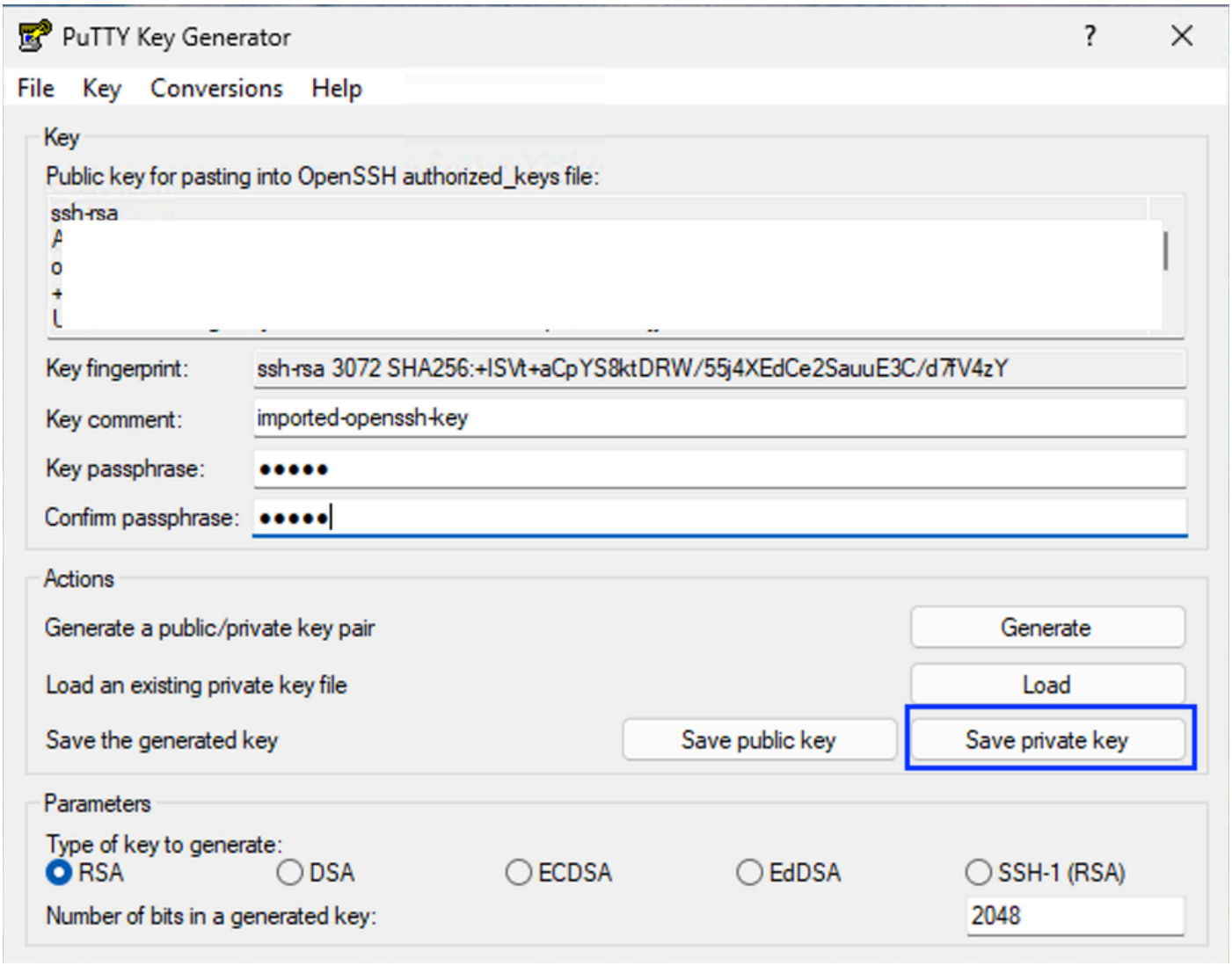
Öffnen Sie das Terminal, und verwenden Sie ssh -i <private-key-file-path> acadmin@x.x.x.x.x, um eine Verbindung mit dem Ressourcen-Connector herzustellen.



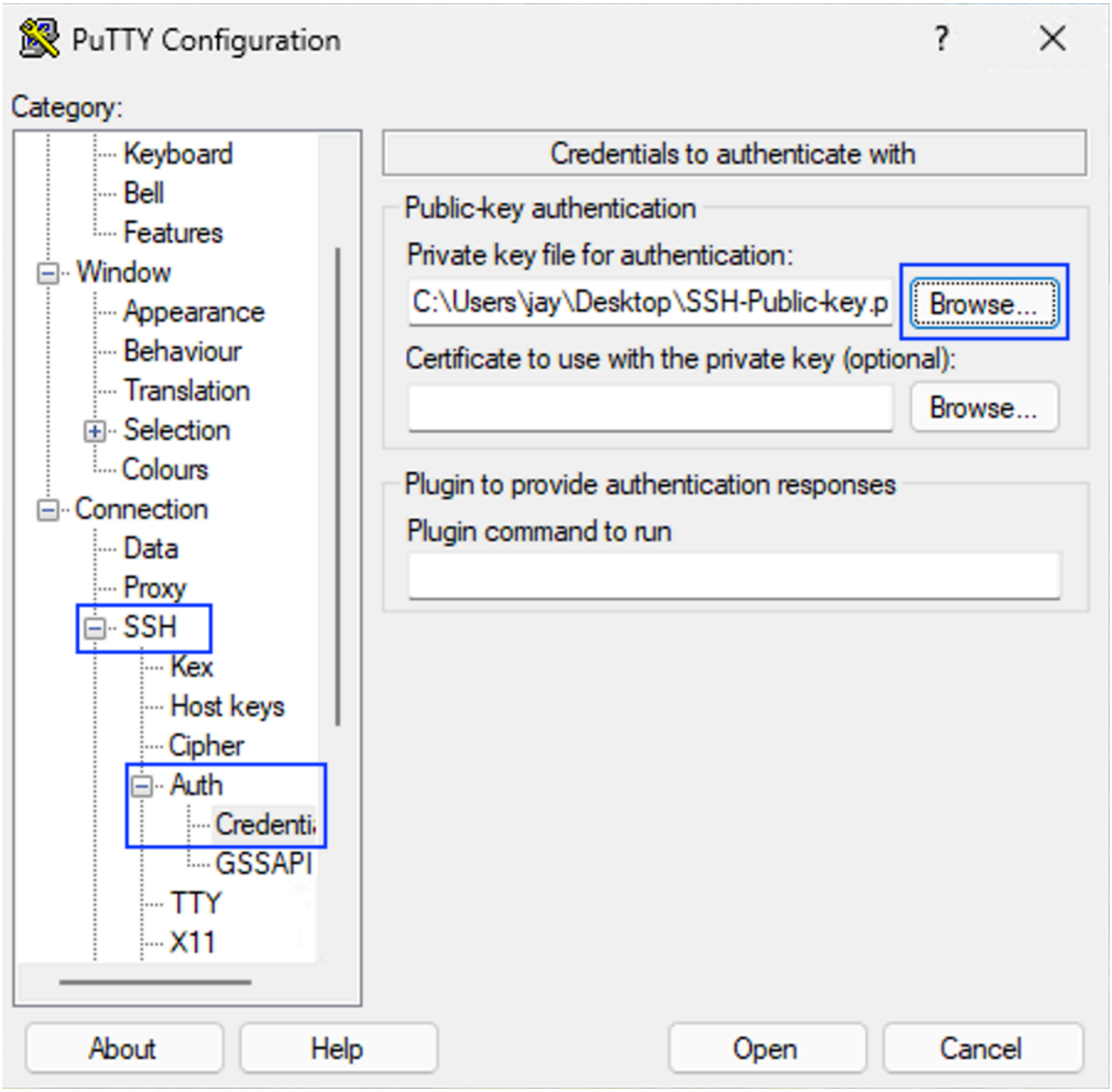
Sicherer Zugriff - Zugriff auf die Befehlszeile des Ressourcenkonnektors

Zugriff von Windows - Putt

Um den privaten Schlüssel zu verwenden, müssen Sie die SSH private key Form von.pemin .ppk Format konvertieren mit Puttygen:



- Den privaten Schlüssel im .ppk-Format speichern
- Starten Sie Kitt-Anwendung und navigieren Sie zu SSH > Auth > Credentials und durchsuchen Sie Ihre SSH private key in .ppk format



- Navigieren Sie zur IP-Adresse des Ressourcenkonnektors, Sessionund klicken Sie auf Open

Tipp: Benutzername: acadmin-Passphrase: Die Passphrase, die beim Konvertieren des privaten Schlüssels aus dem PEM- in das PPK-Format konfiguriert wurde.

```
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
```

Fehlerbehebung

Um auf den Fehlerbehebungsbefehl zuzugreifen, greifen Sie auf zu.

⚠ Vorsicht: Verlieren Sie nicht den privaten SSH-Schlüssel. Andernfalls können Sie nicht auf die RC-CLI zugreifen und müssen diese zur Fehlerbehebung erneut bereitstellen.

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- Weitere Dokumente für sicheren Zugriff

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.