نشر Secure Access Resource Connector في Azure

المحتويات

المقدمة

المتطلبات الأساسية

- المتطلبات
- المكونات المستخدمة

التكوين

- التكوينات في الوصول الآمن
- التكوينات في Azure

التحقق من الصحة

- الوصول من واجهة سطر الأوامر في InBuild Base
- الوصول إلى RC من الوحدة الطرفية لنظام التشغيل Mac-OS
- الوصول من Windows - Putty

استكشاف الأخطاء وإصلاحها

معلومات ذات صلة

المقدمة

يوضح هذا المستند كيفية نشر موصل المواراد في Azure خطوة بخطوة.

المتطلبات الأساسية

جمع المعلومات المطلوبة وفهم

- احصل على صورة الموصل.
  - يمكنك تنزيل الصورة مرة واحدة واستخدامها لأي عدد من الموصلات في أي مجموعة موصلات.
  - إذا كنت تستخدم صورة تم تنزيلها سابقا، فتأكد من أن الصورة هي أحدث إصدار.
  - للحصول على تفاصيل، راجع الحصول على صورة الموصل.
- انسخ مفتاح الإمداد لمجموعة الموصلات المحددة التي تقوم بنشر الموصلات لها. راجع توفير المفاتيح لموصلات المواراد.

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وصول مسؤول لوحة معلومات الوصول الآمن من Cisco
- الوصول إلى مدخل Azure

- Cisco Secure Client

- جهاز Windows مع ZTA مسجل

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الاختبار الذي تم إجراؤه في بيئة معملية باستخدام المكونات التالية:

- عميل ZTNA
- الوصول الآمن
- لازوردي
- مورد خاص

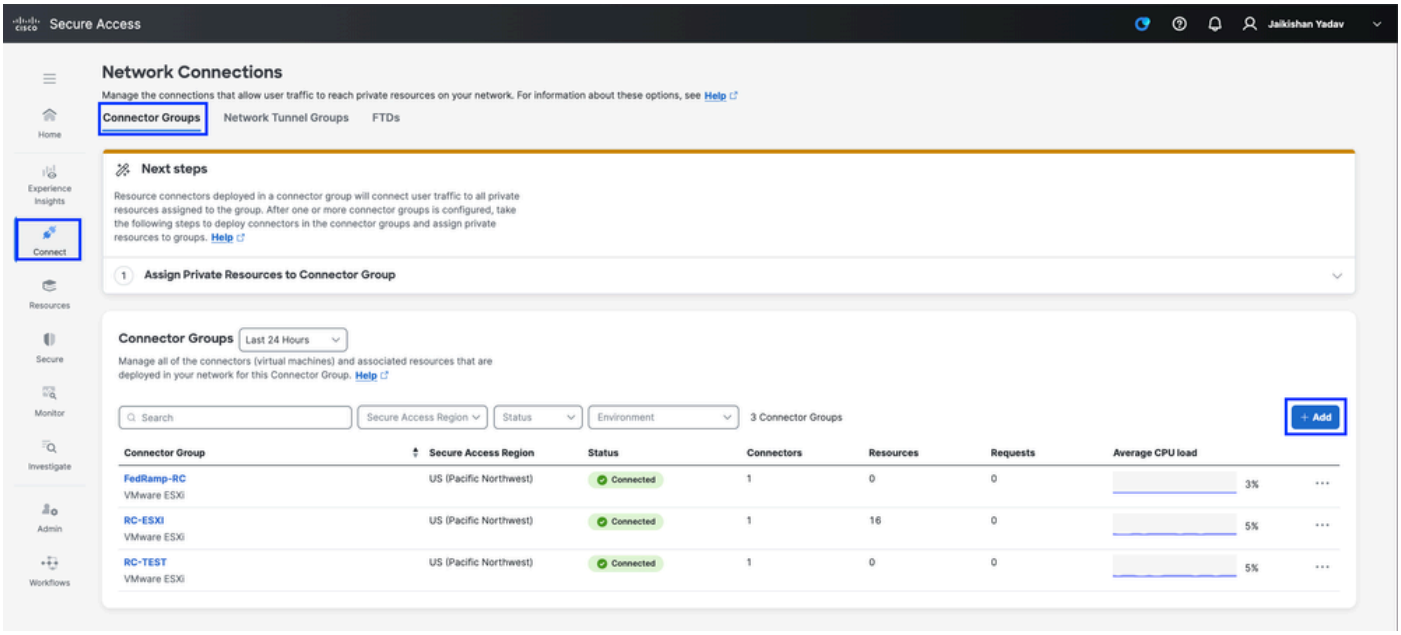
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

التكوينات في الوصول الآمن

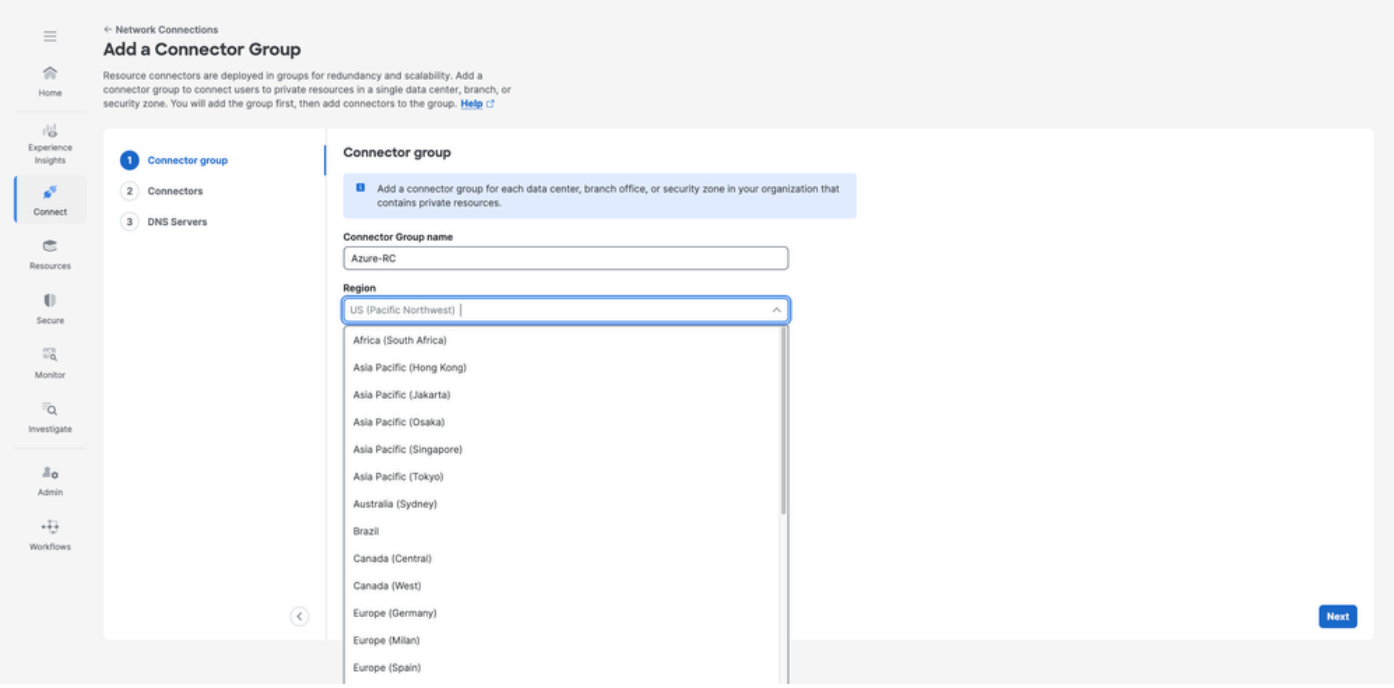
تسجيل الدخول إلى لوحة معلومات الوصول الآمن والانتقال إلى **Connect** > **Network Connections** > **Connector Groups**

- انقر فوق add



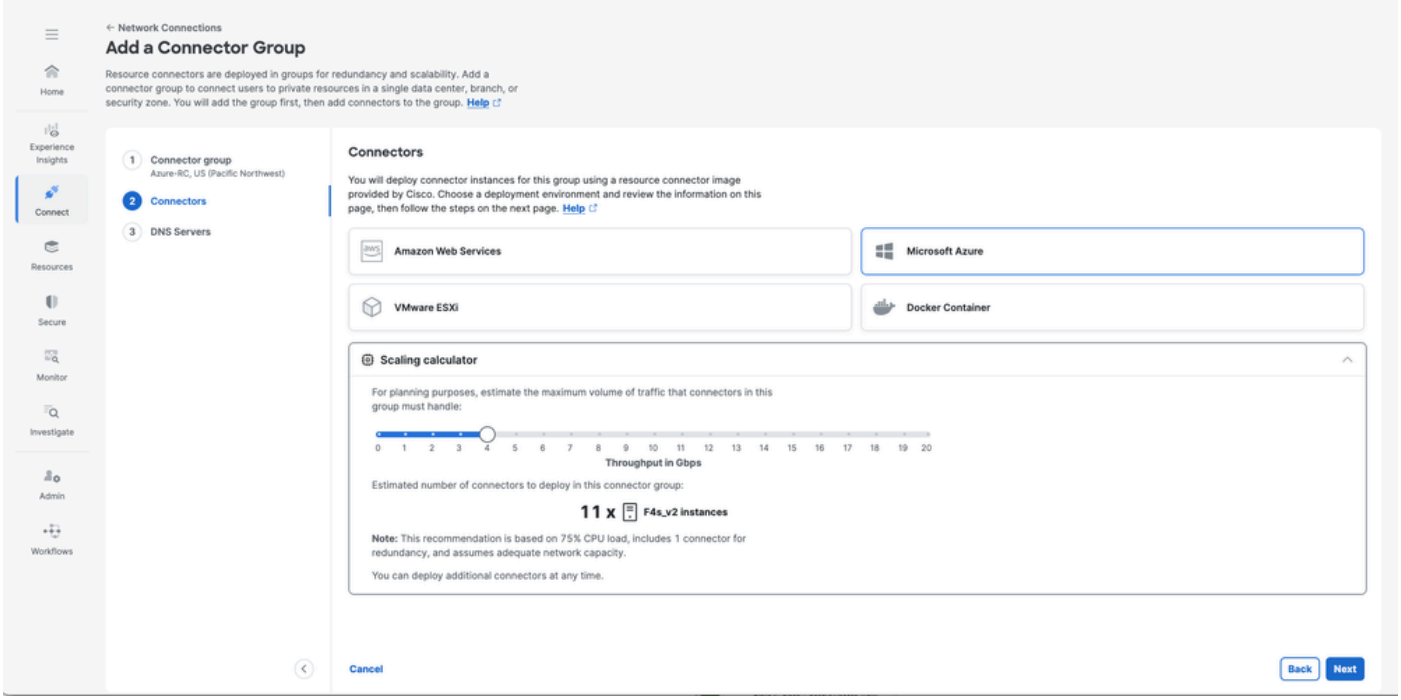
الوصول الآمن - مجموعات الموصلات

- حددConnector Group Nameو Region
- انقر Next



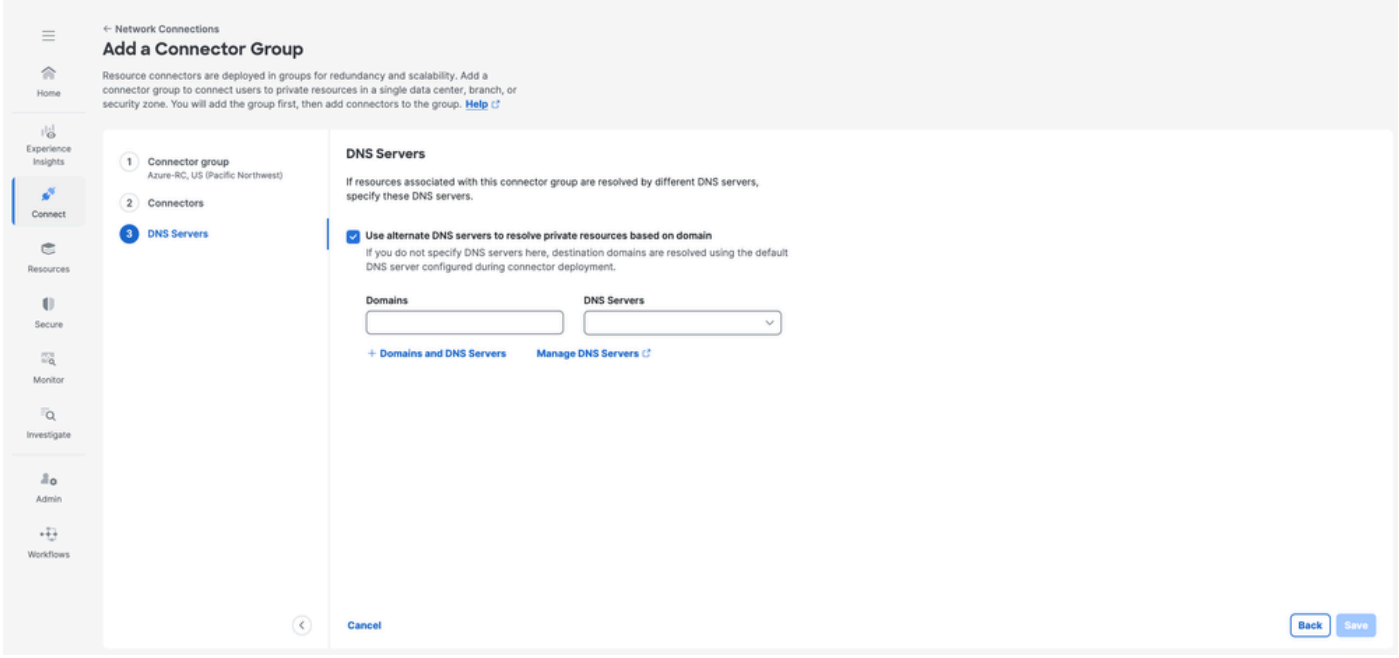
الوصول الآمن - تكوين مجموعات الموصلات

- إختيارMicrosoft AzureواستخدامScaling Calculatorلتحديد الموارد المطلوبة



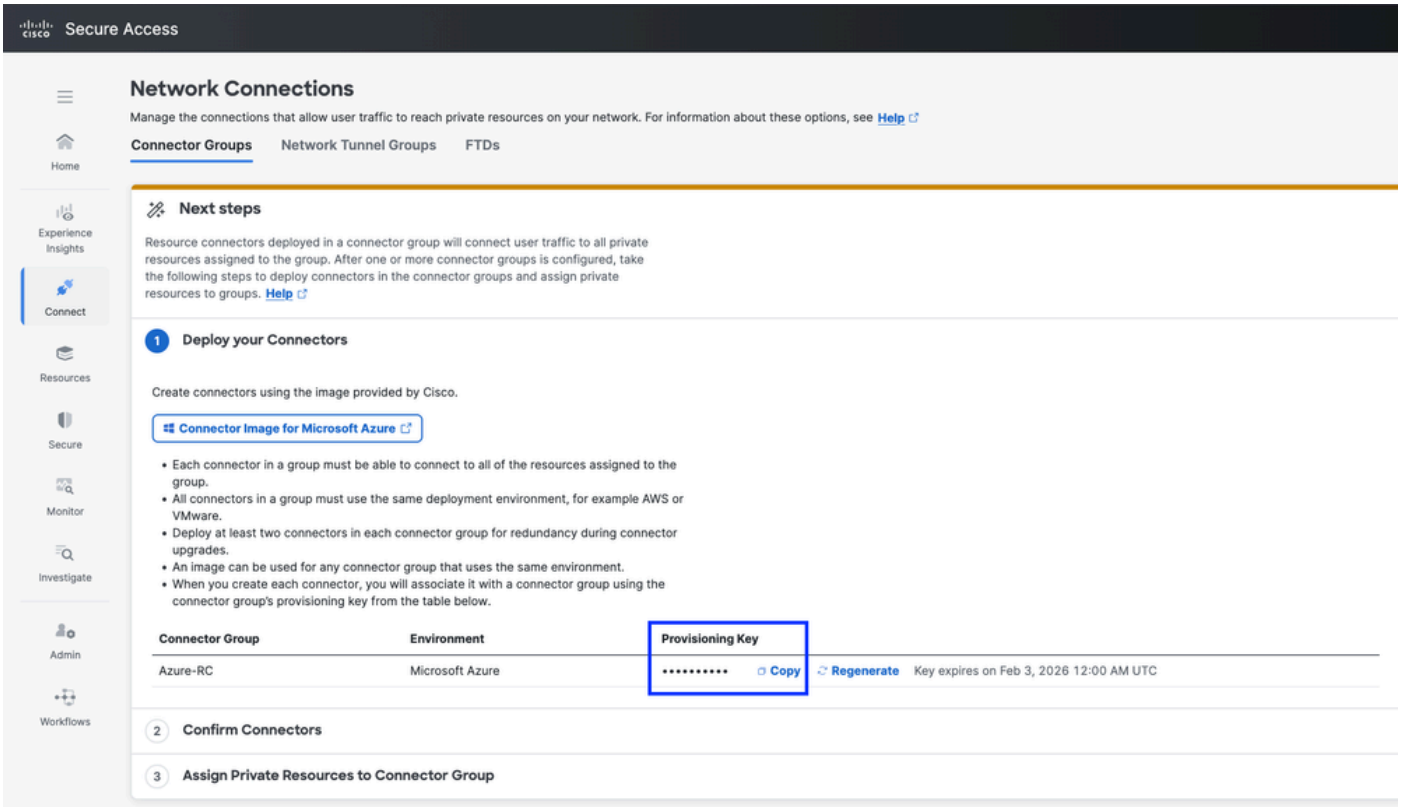
Secure Access - مراجعة تكوين موصل الموارد

- أستخدمDNS Serversالخيار لحل مجالات معينة من خلال خوادم DNS المخصصة. ويعتبر ذلك أفضل ممارسة للمنظمات ذات المجالات الداخلية المتعددة.
- انقر Save



الوصول الآمن - تكوين موصل الموارد

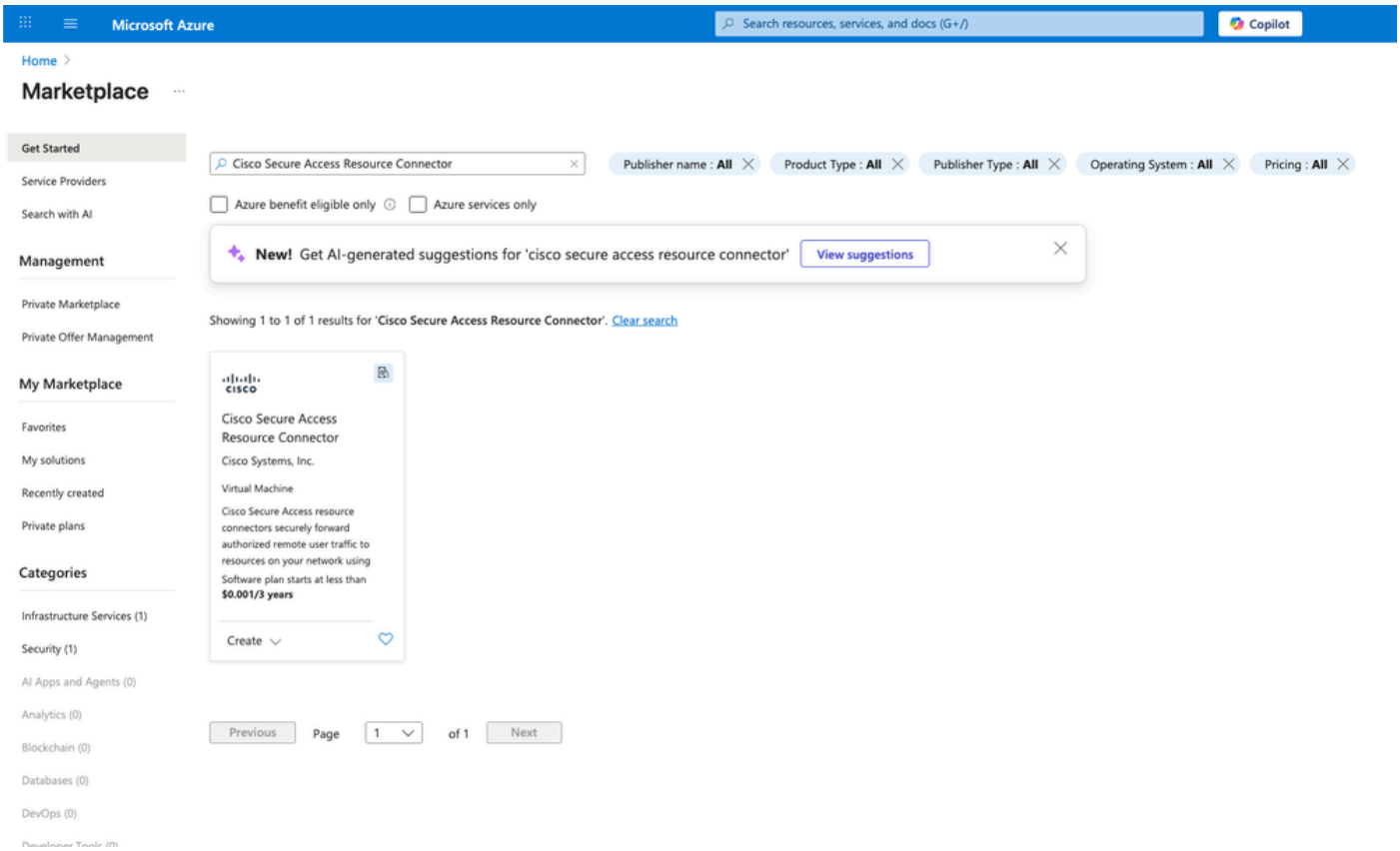
- في هذه المرحلة، تأكد من نسخProvisioning Key. تحتاج إليه لاحقا في Azure أثناء نشر Resource Connector لتمكين التسجيل مع مستأجر Secure Access.



الوصول الآمن - تكوين موصل الموارد

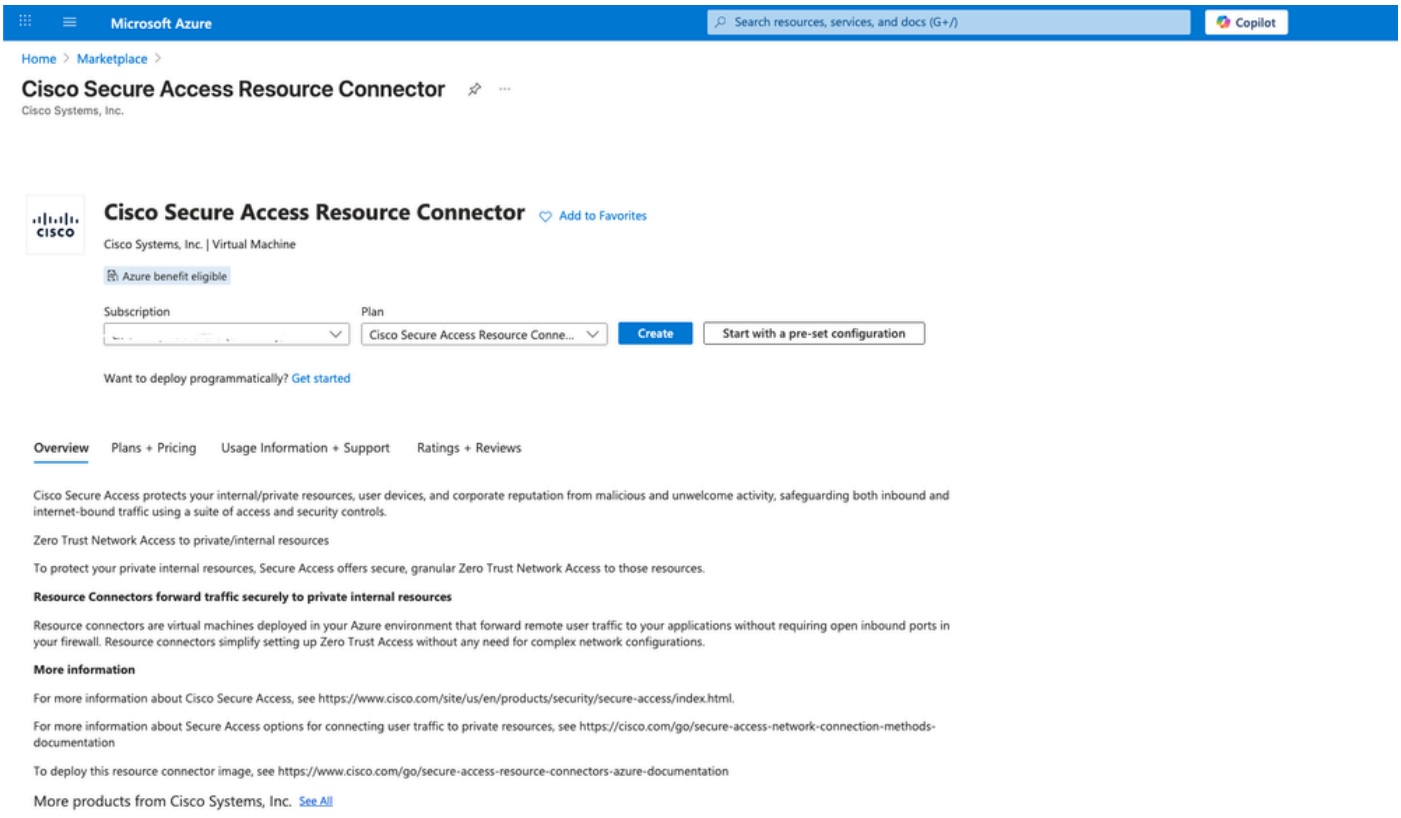
التكوينات في Azure

انتقل إلى مدخل Azure ثم انتقل إلى موقع تسوق Microsoft Azure وابحث عن صورة Cisco Secure Access Resource Connector:



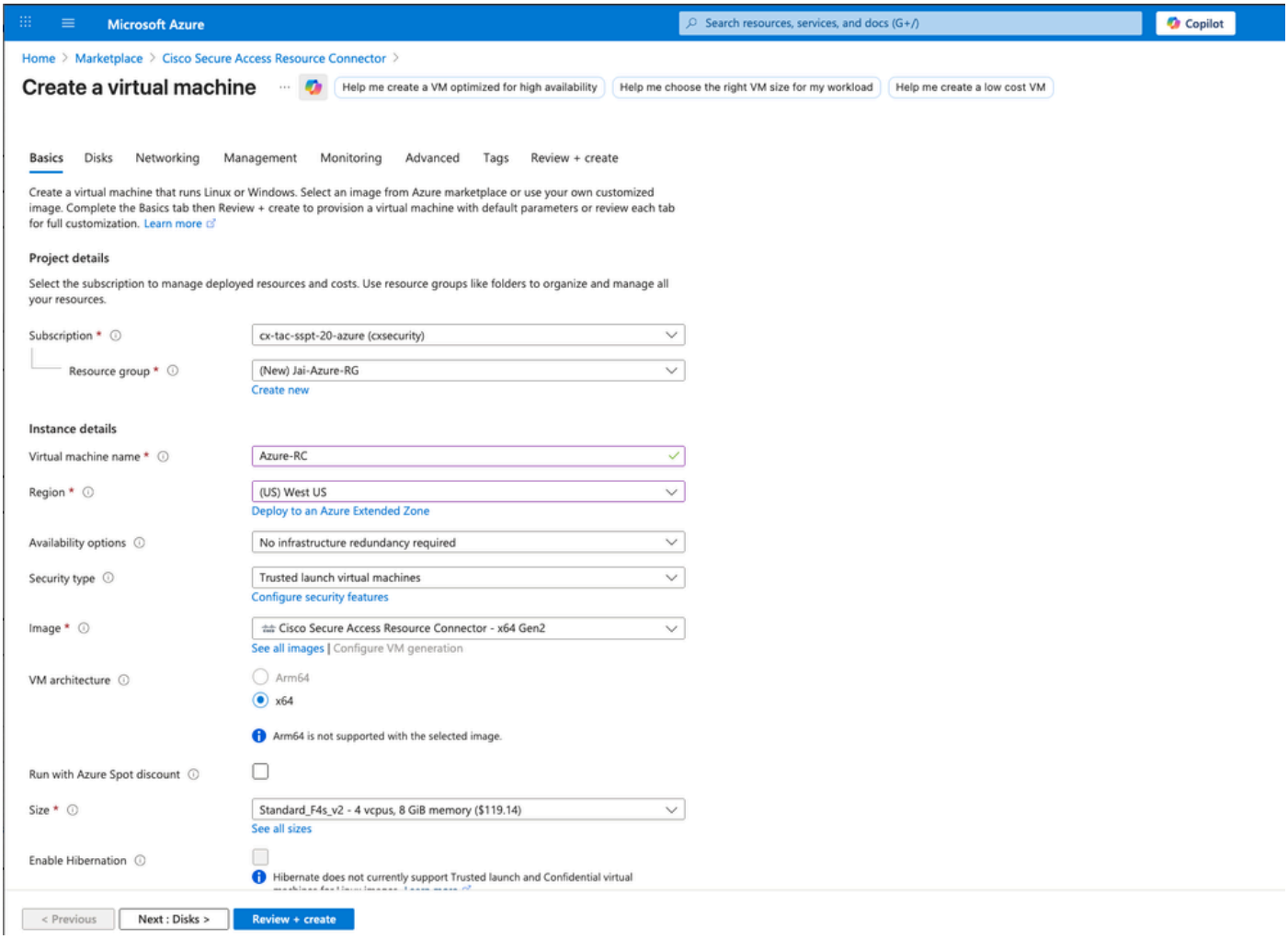
Secure Access - إنشاء موصل الموارد على Azure

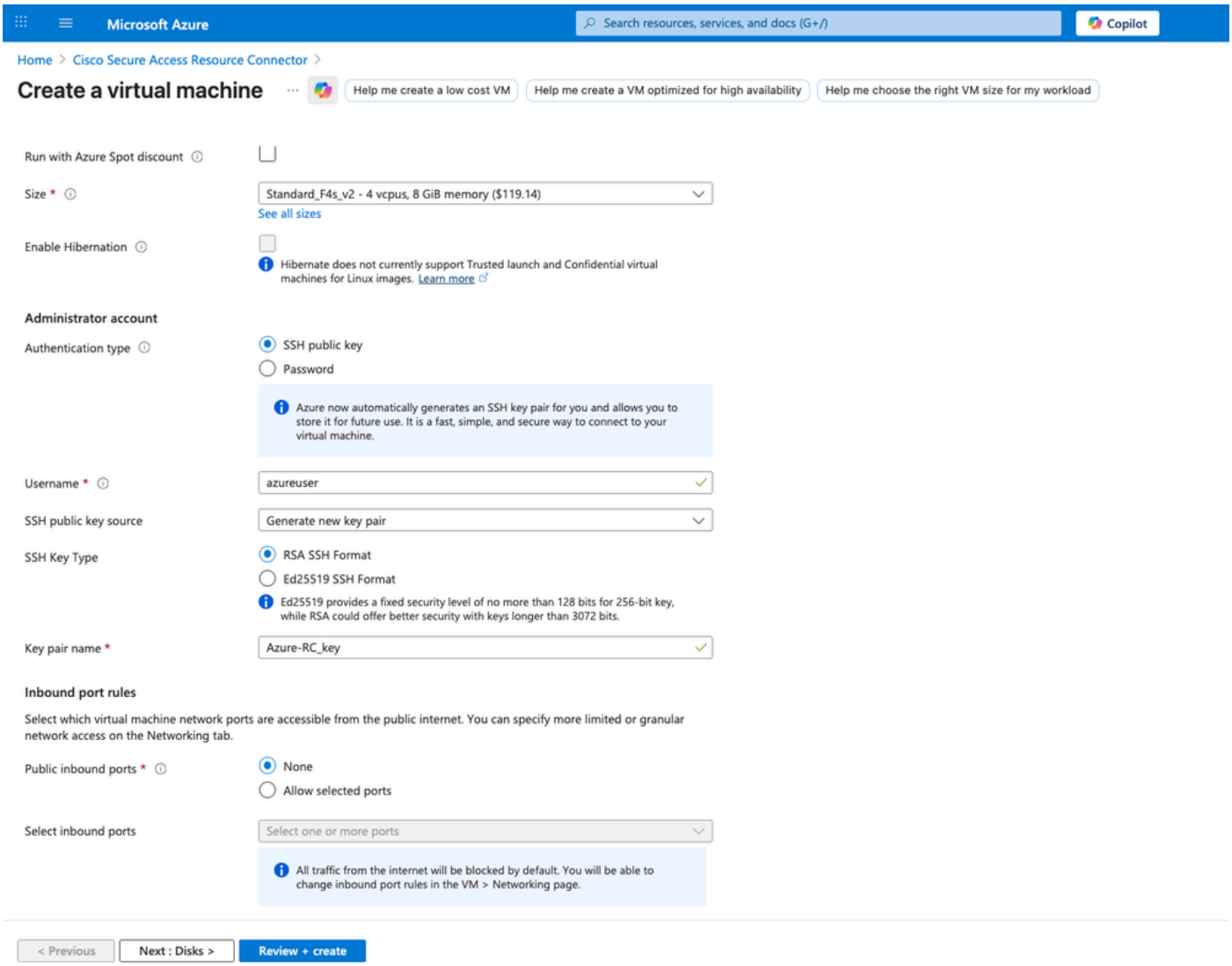
- أختر المناسبSubscription، ثمPlanانقر فوق Create



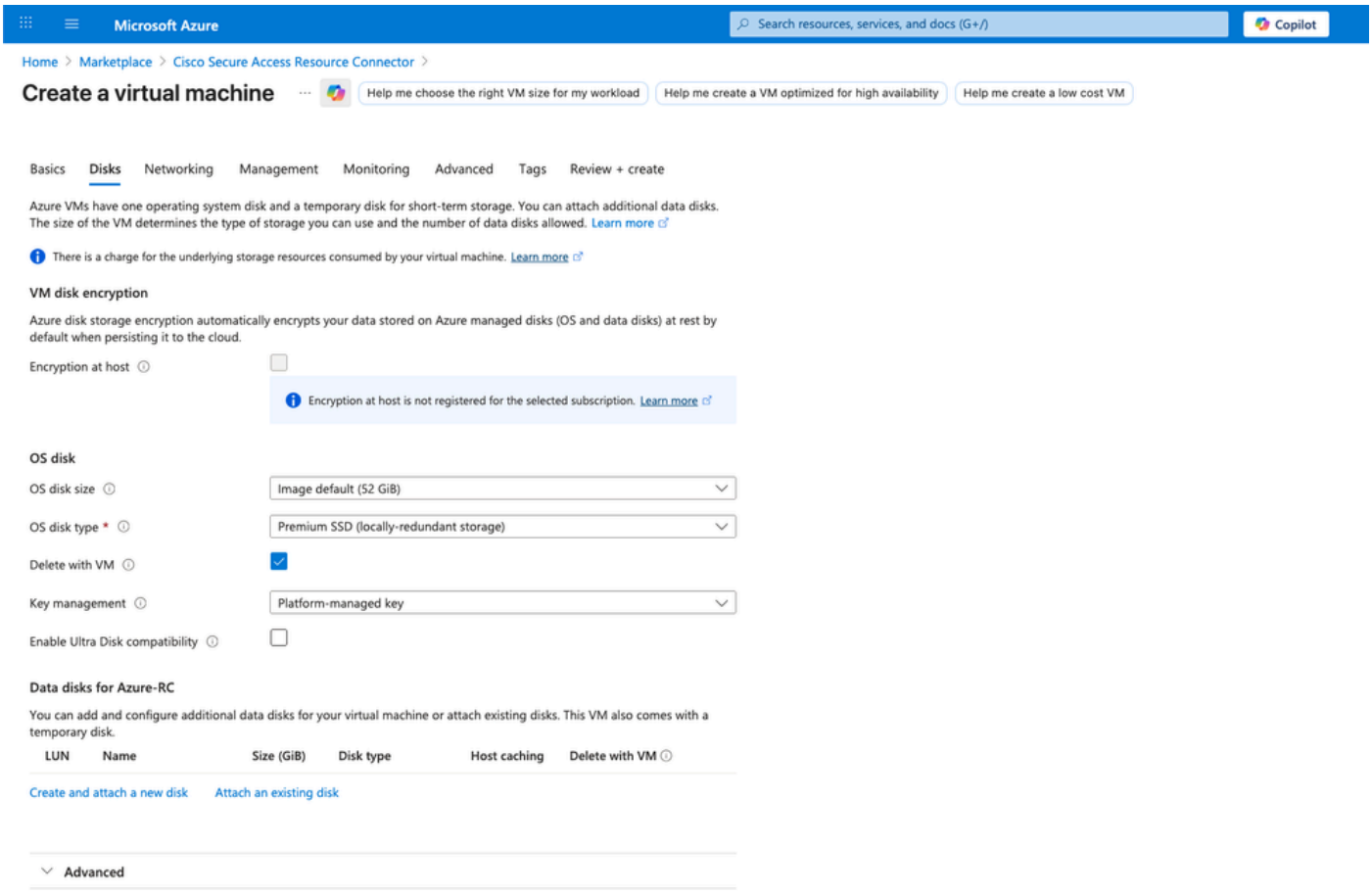
Secure Access - إنشاء موصل الموارد على Azure

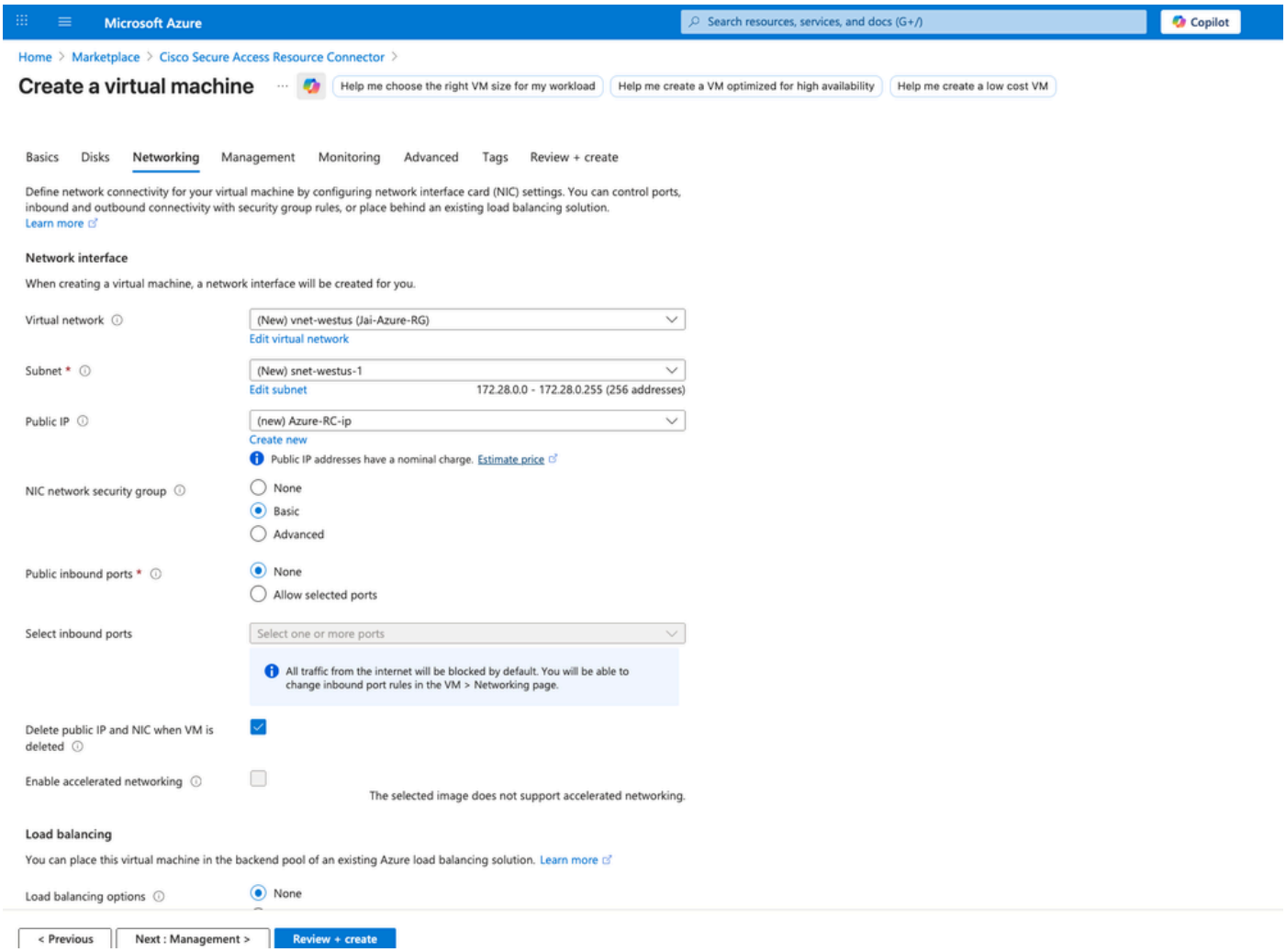
- راجع التكوين Disksلمفاتح SSH العام Networking و





⚠ تحذير: لا تفقد مفتاح SSH الخاص؛ وإلا، فلن يمكنك الوصول إلى واجهة سطر الأوامر (CLI) الخاصة بـ RC وسيجب عليك إعادة نشرها لاستكشاف الأخطاء وإصلاحها.

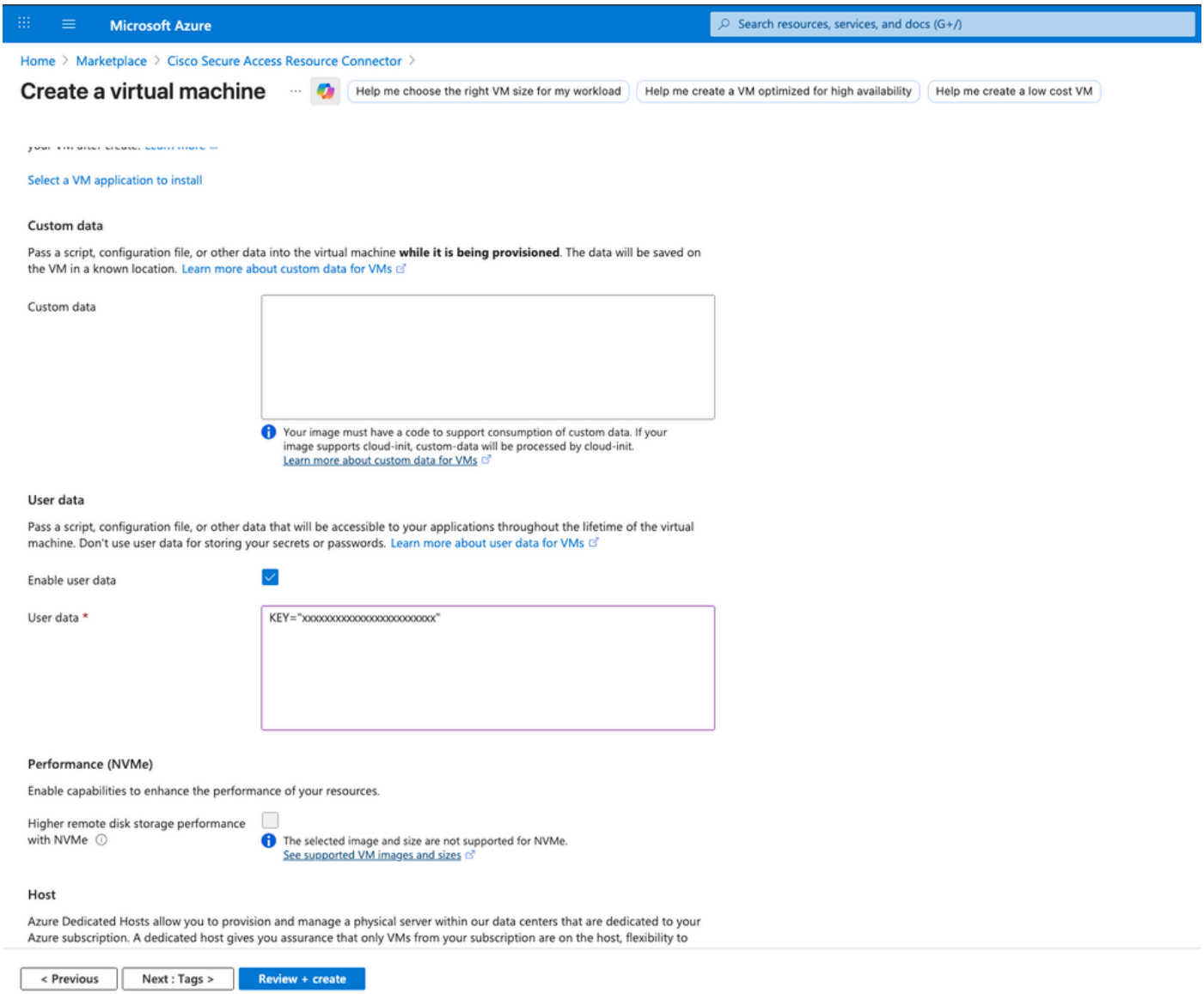

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Marketplace > Cisco Secure Access Resource Connector >
Create a virtual machine
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM
Basics Disks Networking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



Secure Access - إنشاء موصل الموارد على Azure

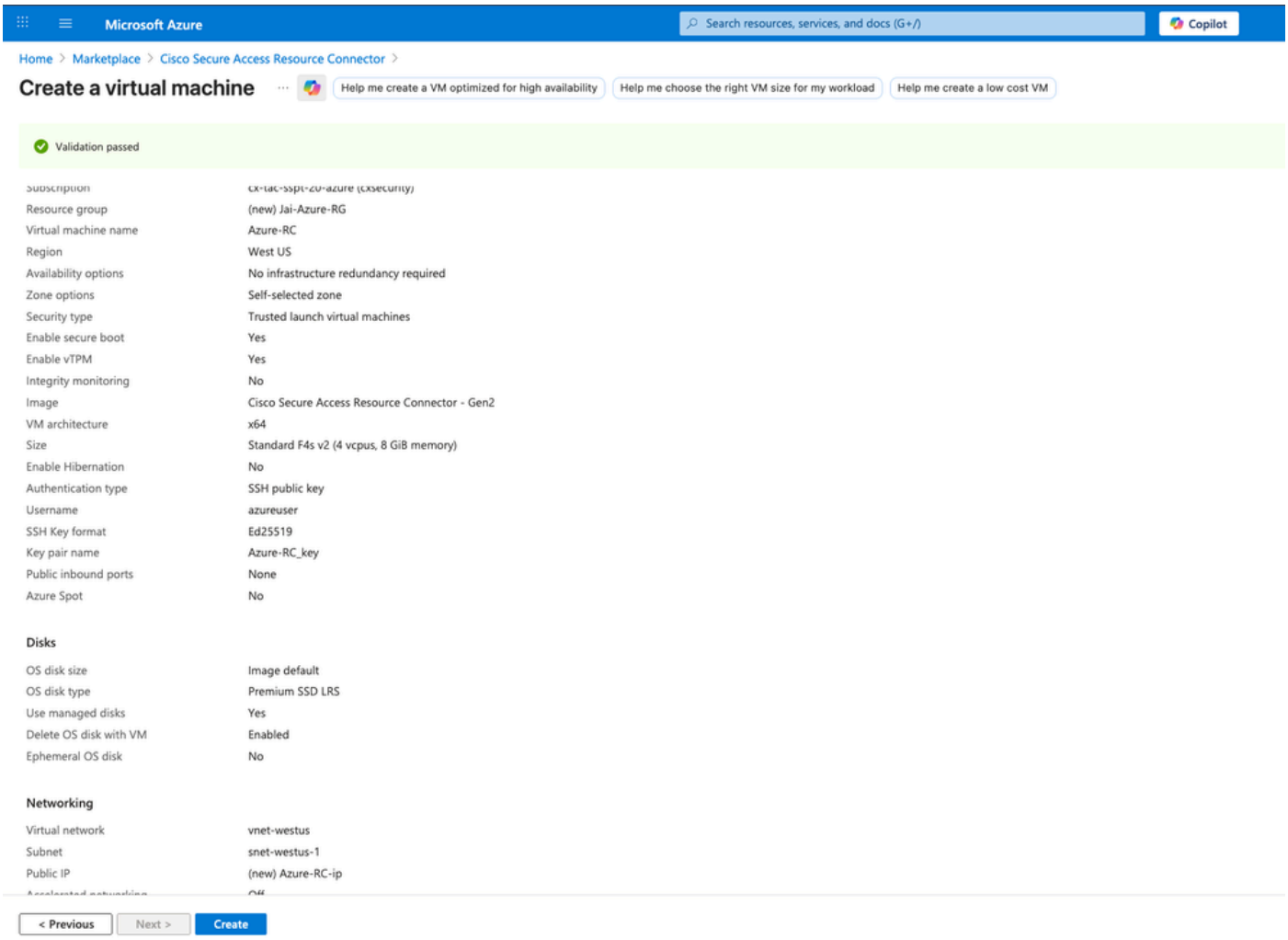
- القصProvisioning Keyالمنسوخ من Cisco Secure Access فيUser dataالحقل

KEY=XXXXXXXXXXXXXXXXXXXXX



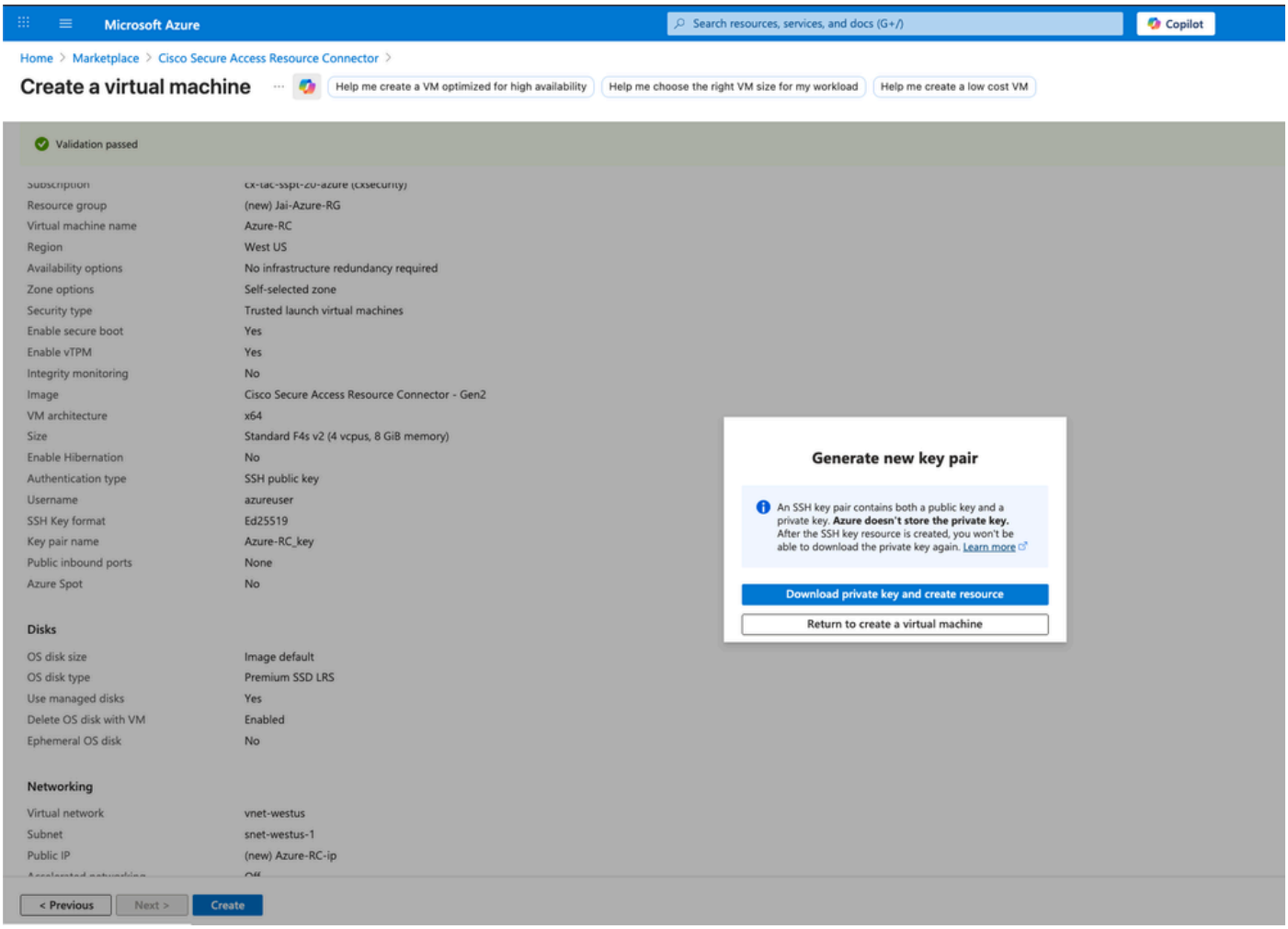
Secure Access - إنشاء موصل الموارد على Azure

- مراجعة وانقر فوقCreateلمتابعة إنشاء Resource Connector



Secure Access - إنشاء موصل الموارد على Azure

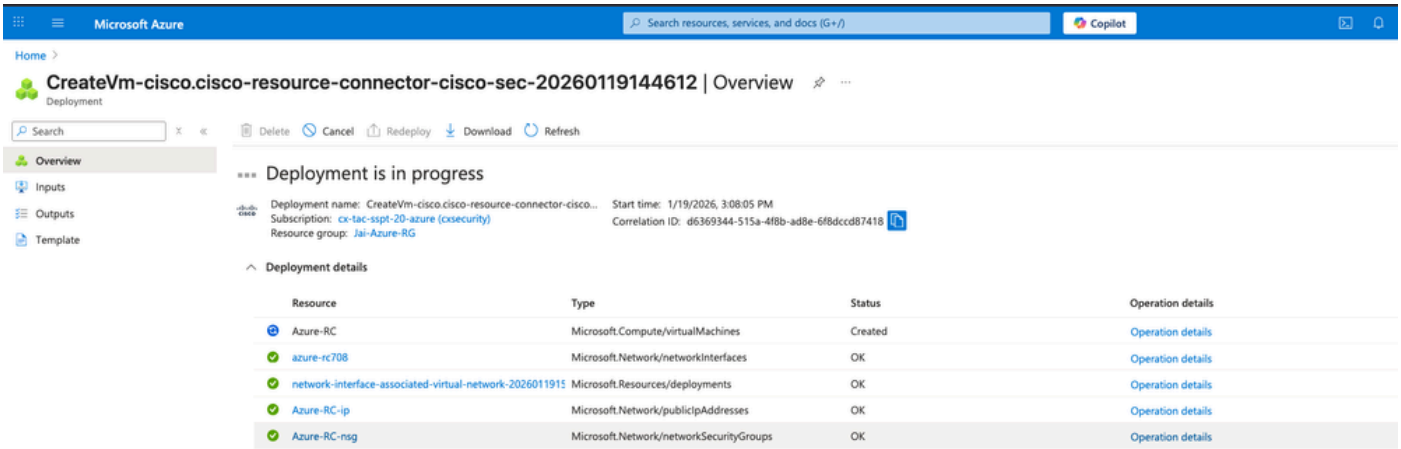
- بعد أن تنقرCreate، يظهر خيار لتنزيل المفتاح الخاص. انقر فوق Download private key and create resource



Secure Access - إنشاء موصل الموارد على Azure

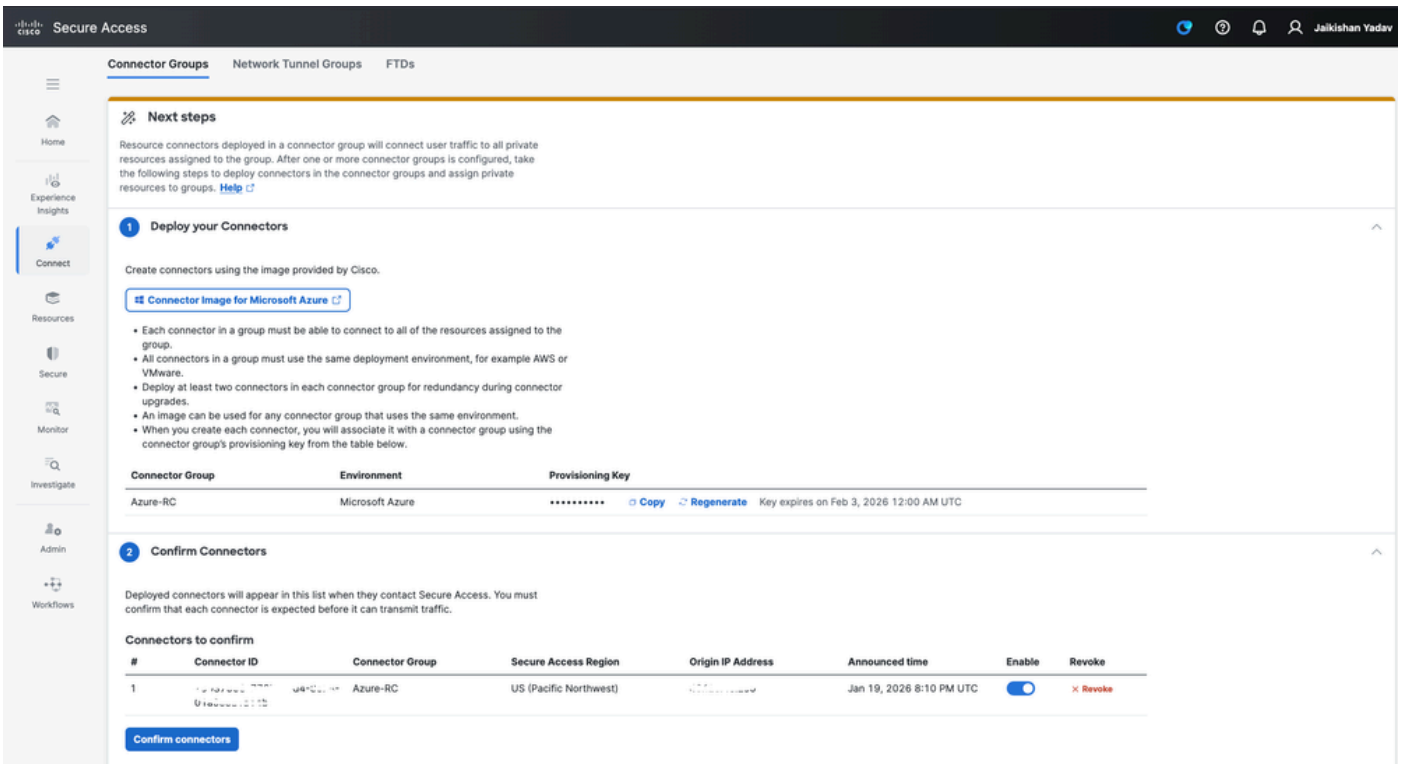
⚠ تحذير: لا تفقد مفتاح SSH الخاص؛ وإلا، فلن يمكنك الوصول إلى واجهة سطر الأوامر (CLI) الخاصة بـ RC ويجب عليك إعادة نشرها لاستكشاف الأخطاء وإصلاحها.

- بعد ذلك يمكنك رؤية تقدمResource Connector



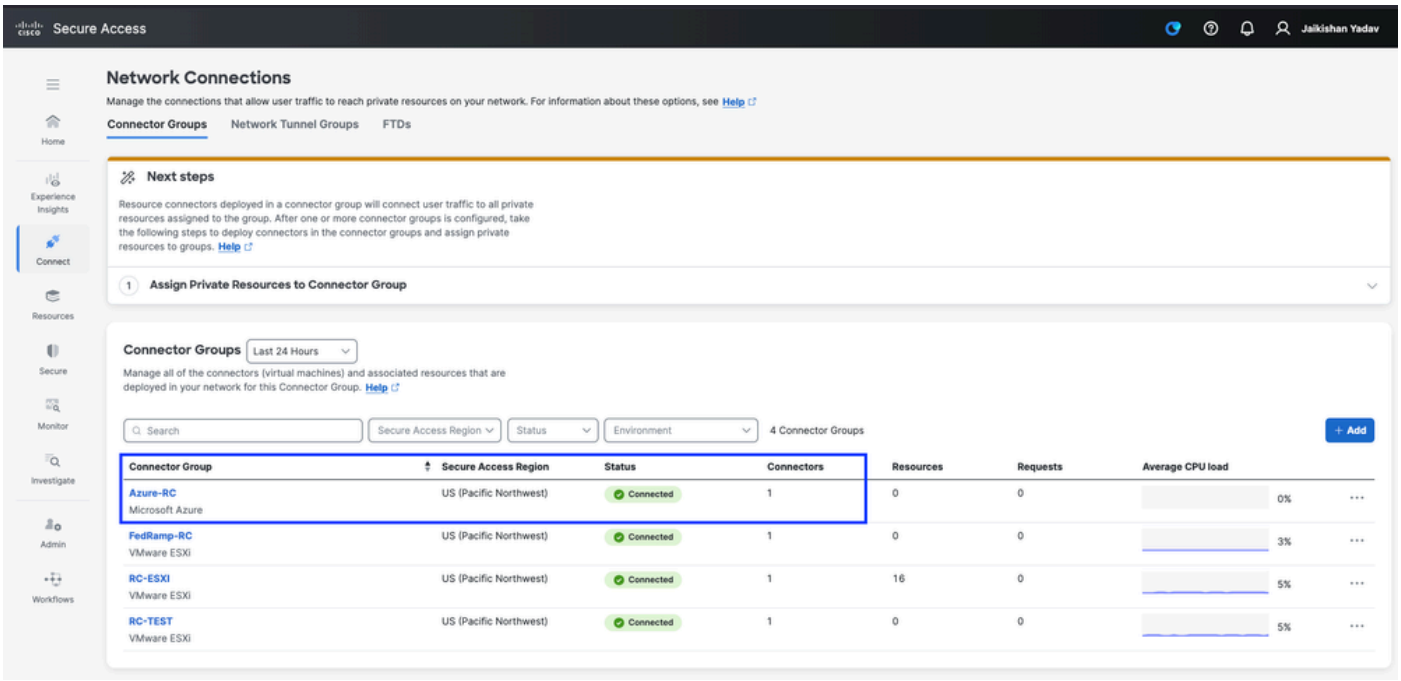
Secure Access - نشر موصل الموارد على Azure

- ثم انتقل إلى [لوحة معلومات الوصول الآمن](#) لتأكيدResource Connectorالاتصال والنشر الكامل في مستأجر Secure Access
- انقر فوق **Connect** > **Network Connections** > **Connector Groups**
- تحت الخيار 2 تأكد الموصلات انقرConfirm Connectorsلإنهاء النشر



الوصول الآمن - تأكيد موصل المواراد

يمكنك الآن رؤية "موصل المواراد" الجديد الذي قمت بنشره وتوصيله في مستأجر Secure Access الخاص بك:



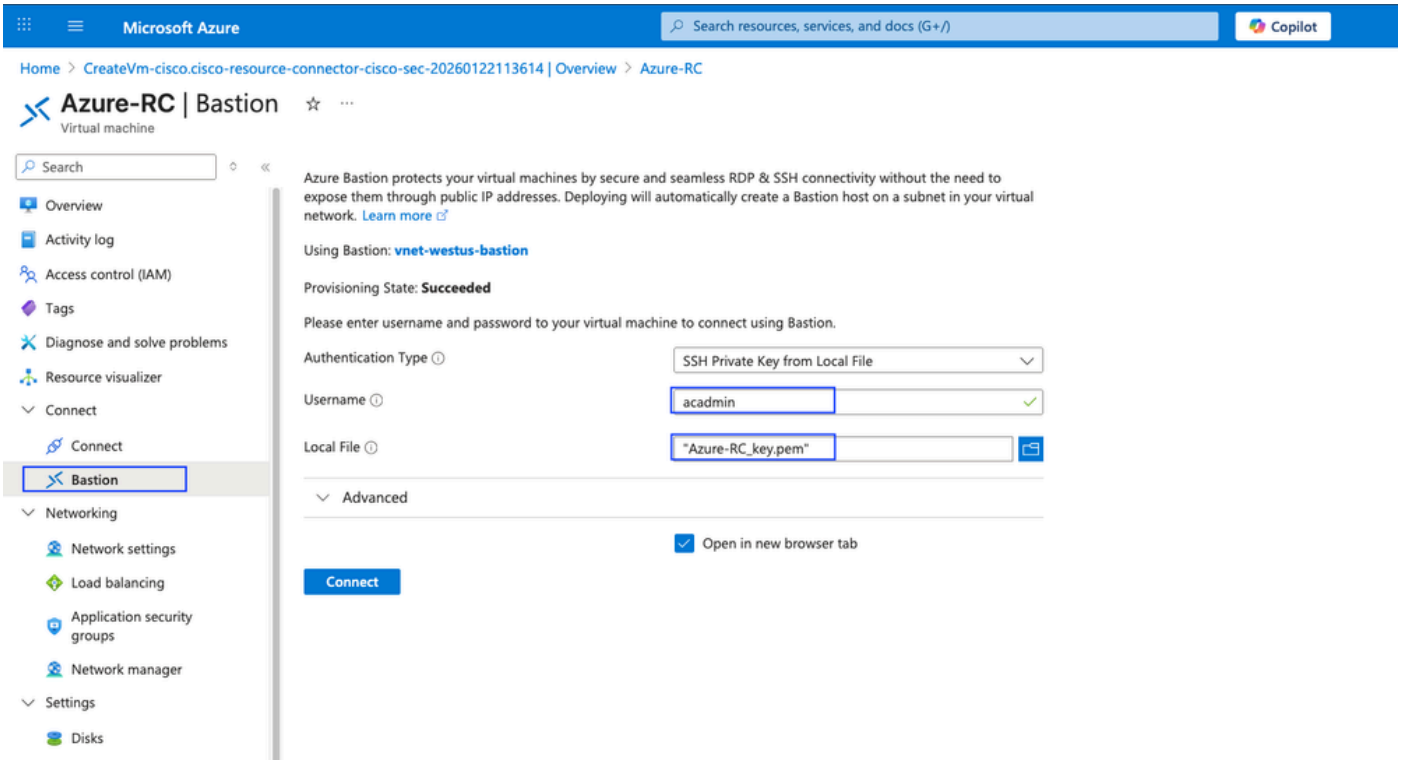
الوصول الآمن - موصل المواراد

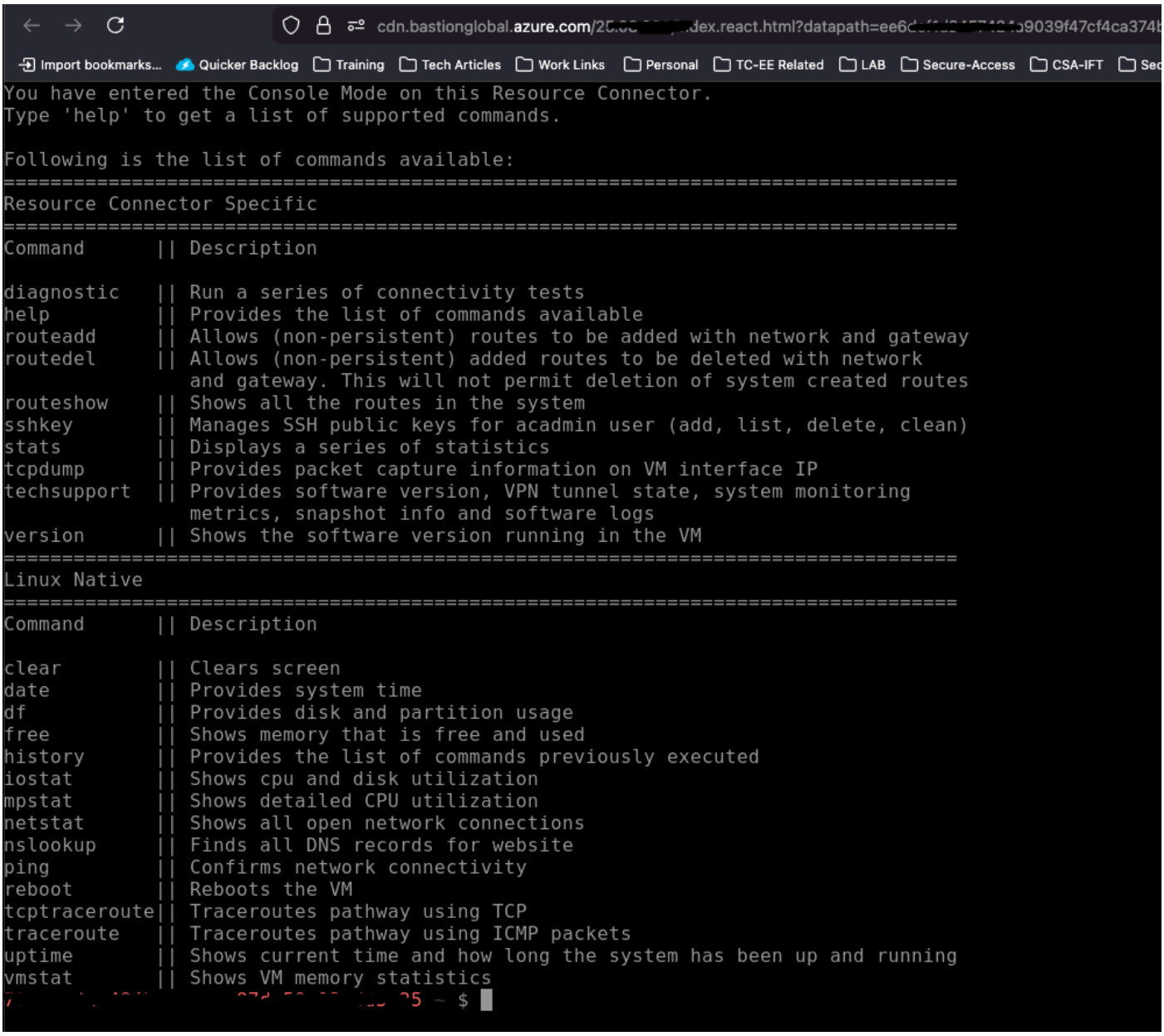
التحقق من الصحة

الوصول من واجهة سطر الأوامر في InBuild Base

في Azure، قم بالوصول إلى موصل الموارد وانقر فوقBastion:

- Authentication Type: اختَر SSH Private key from Local File
- **Username**: يجب عليك إستخدام acadmin
- **Local File**: أختر الذيprivate keyتم تنزيله سابقا

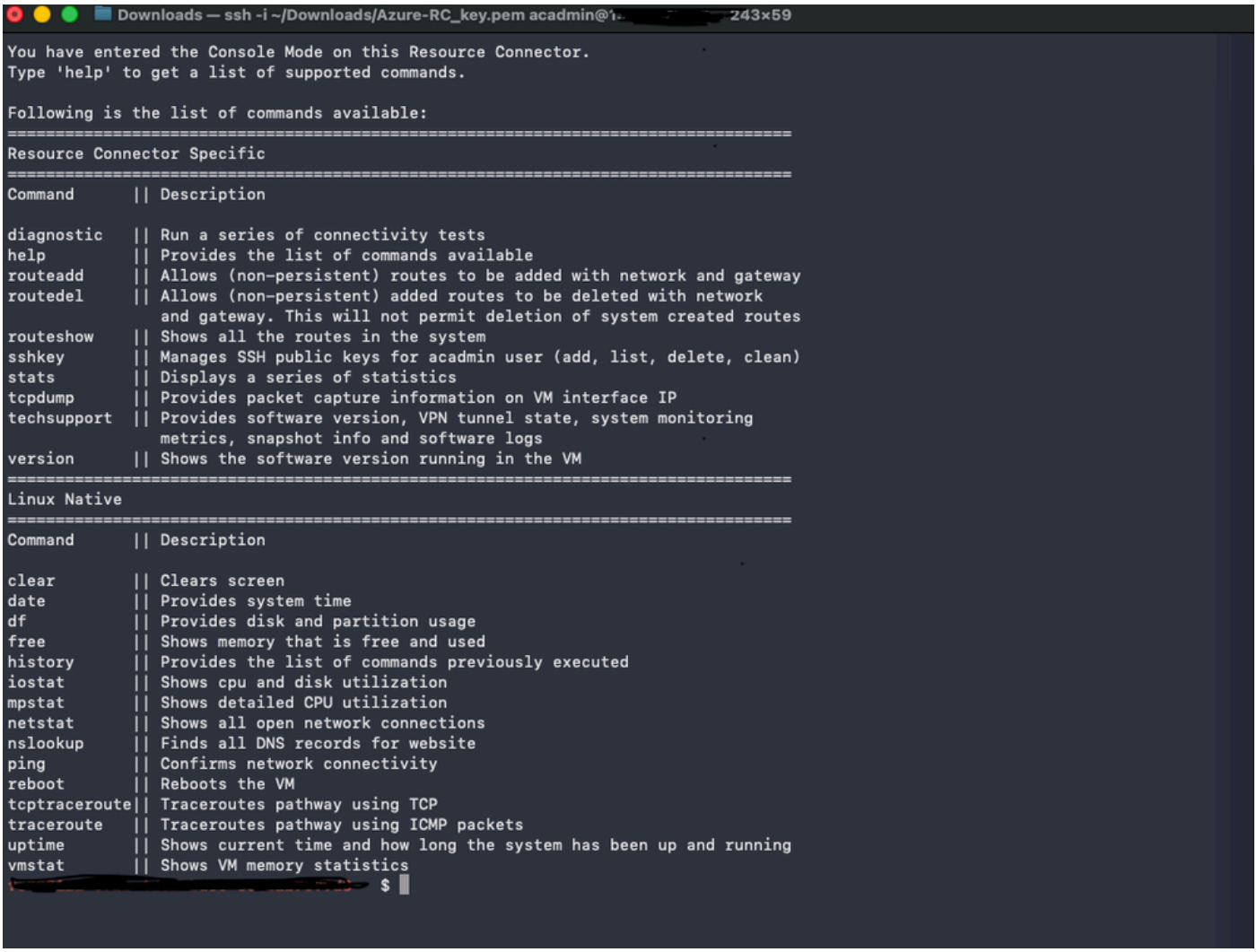




الوصول الآمن - الوصول إلى سطر الأوامر لموصل الموارد

الوصول إلى RC من الوحدة الطرفية لنظام التشغيل Mac-OS

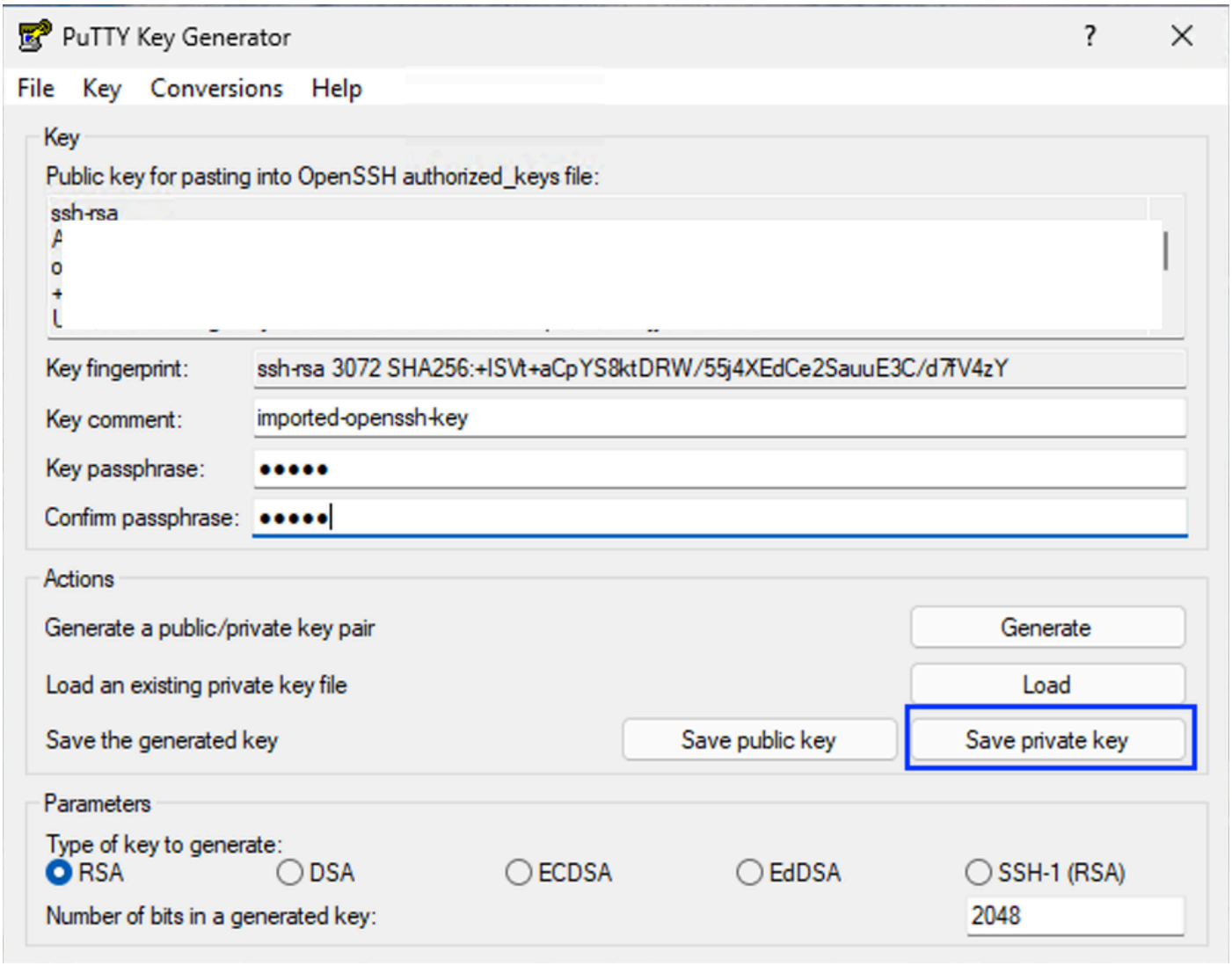
افتح الوحدة الطرفية واستخدم ssh -i <private-key-file-path> acadmin@x.x.x.x.x من أجل الموصل إلى موصل الموارد.



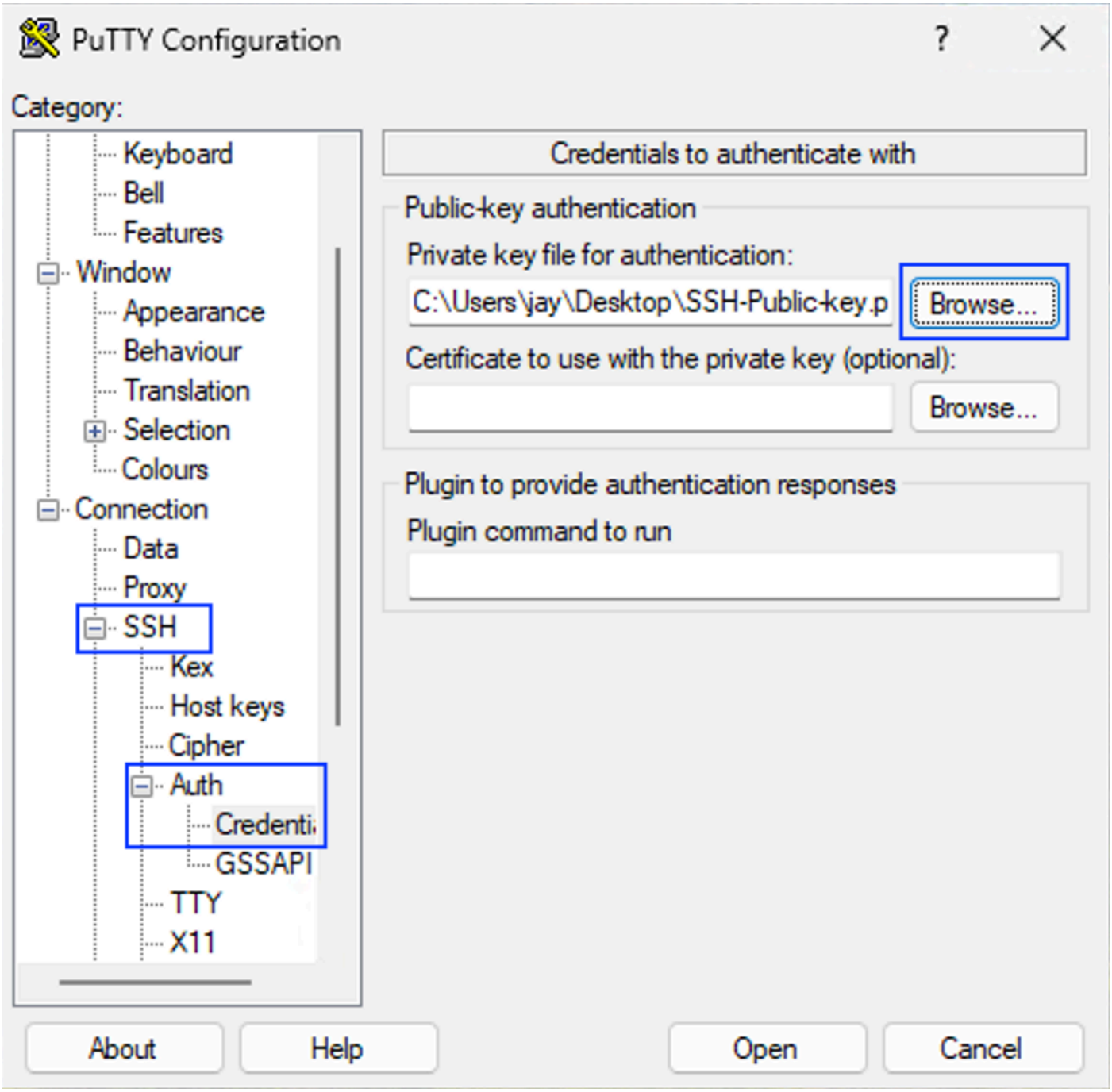
الوصول الآمن - الوصول إلى سطر الأوامر لموصل الموارد

الوصول من Windows - Putty

in order to استعملت المفتاح خاص، أنت ينبغي حولتSSH private keyمن.pemإلى.ppkصيغة يستعملPuttygen:



- حفظ المفتاح الخاص بتنسيق .ppk
- قم بتشغيل تطبيق PuTTY وتصفحSSH > Auth > Credentialsوتصفح دخولكSSH private key.ppk فورمات



- انتقل إلىSessionووضع عنوان IP الخاص بموصل الموارد وانقر Open

تلميح: username: عبارة مرور أكادميين : عبارة المرور التي تم تكوينها أثناء تحويل .ppk إلى .pem قم بتنسيق المفتاح الخاص من

```
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
```

استكشاف الأخطاء وإصلاحها

للوصول إلى الأمر أستكشاف الأخطاء وإصلاحها الذي يمكن الوصول إليه .

⚠ تحذير: لا تفقد مفتاح SSH الخاص؛ وإلا، فلن يمكنك الوصول إلى واجهة سطر الأوامر (CLI) الخاصة ب RC ويجب عليك إعادة نشرها لاستكشاف الأخطاء وإصلاحها.

معلومات ذات صلة

- الدعم الفني والتنزيلات من Cisco
- مستندات الوصول الآمن الأخرى

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).