

Bereitstellen von Secure Access Resource Connector in Azure

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen in sicherem Zugriff](#)

[Konfigurationen in Azure](#)

[Überprüfung](#)

[Zugriff über die Kommandozeile der integrierten Bastion](#)

[Zugriff auf RC vom MAC-OS-Terminal](#)

[Zugriff von Windows - Putt](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

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**

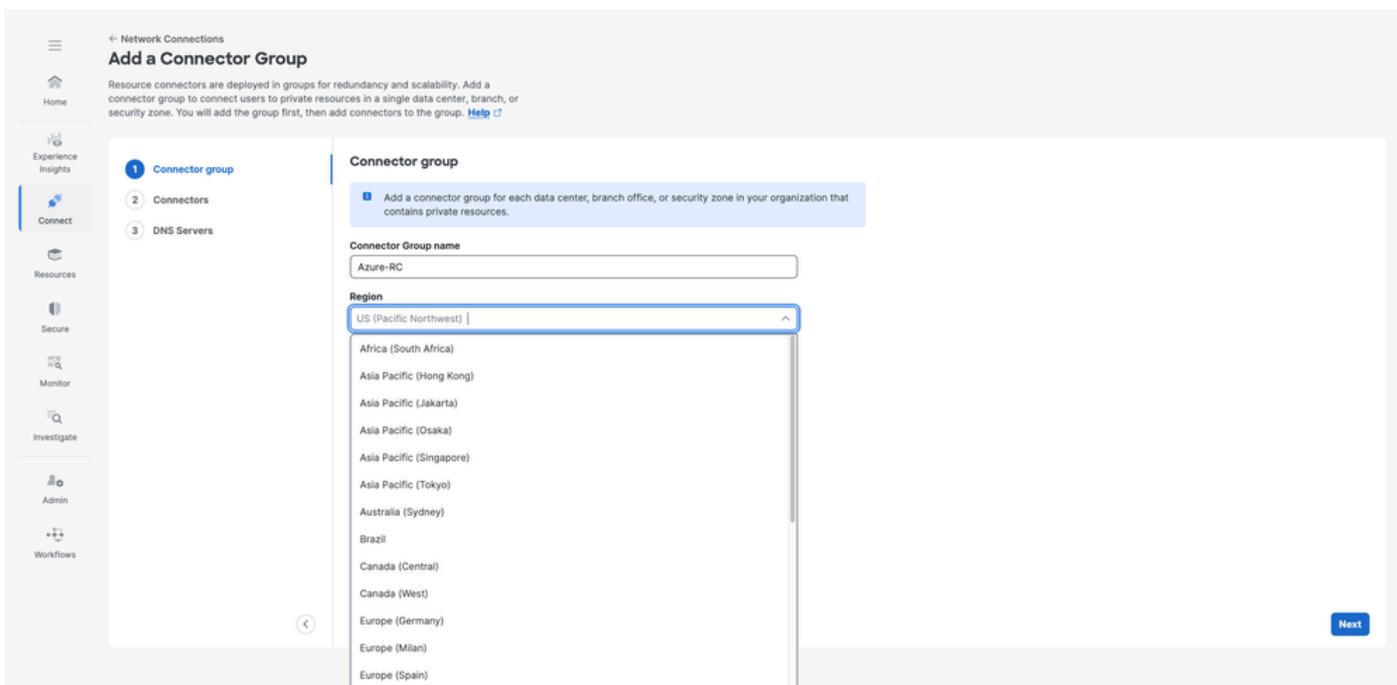
- Klicken Sie **add**

The screenshot shows the 'Network Connections' section of the Cisco Secure Access dashboard. The 'Connector Groups' tab is selected. Below the 'Next steps' section, there is a table of connector groups. The table has the following data:

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

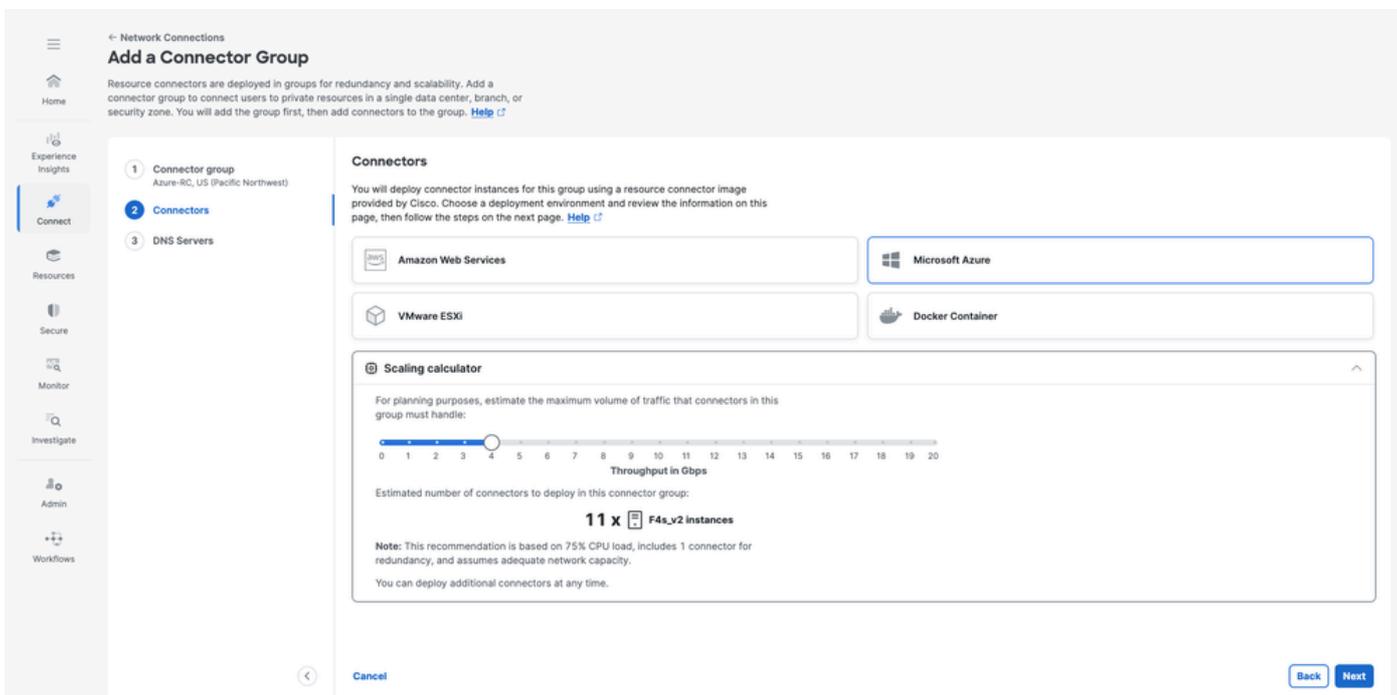
Sicherer Zugriff - Anschlussgruppen

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



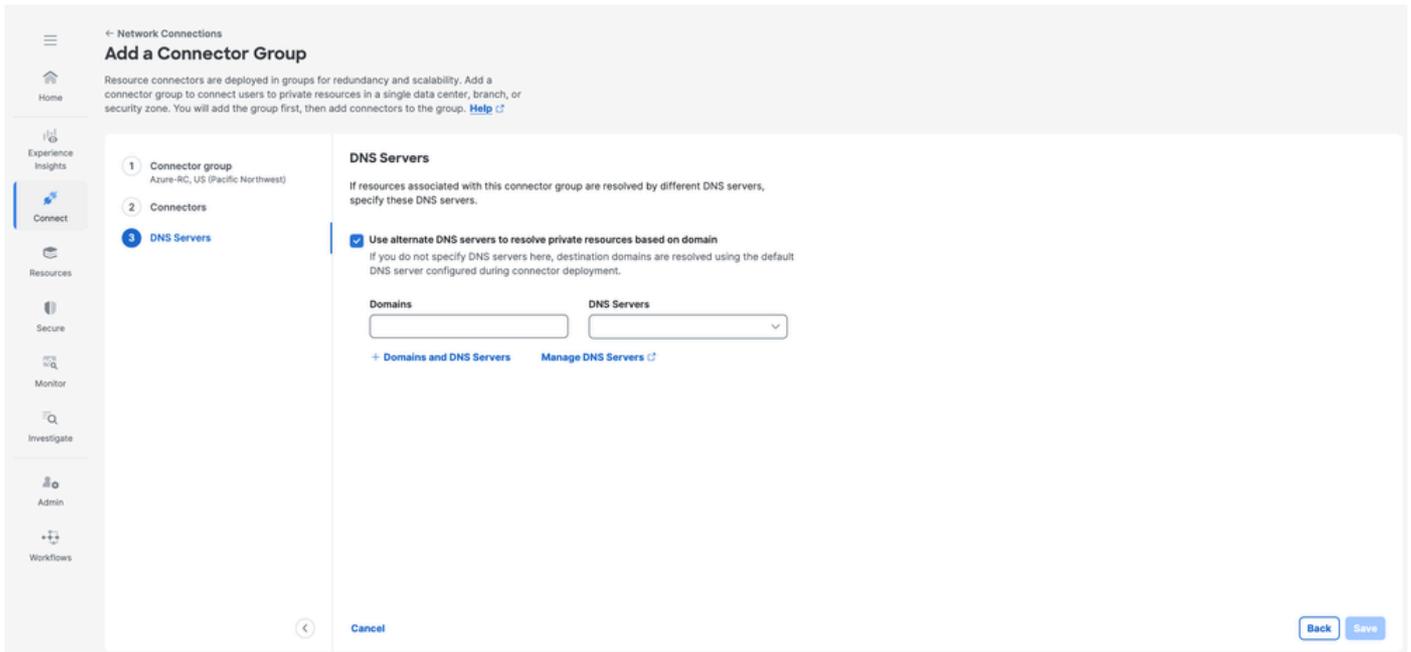
Sicherer Zugriff - Konfiguration von Anschlussgruppen

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



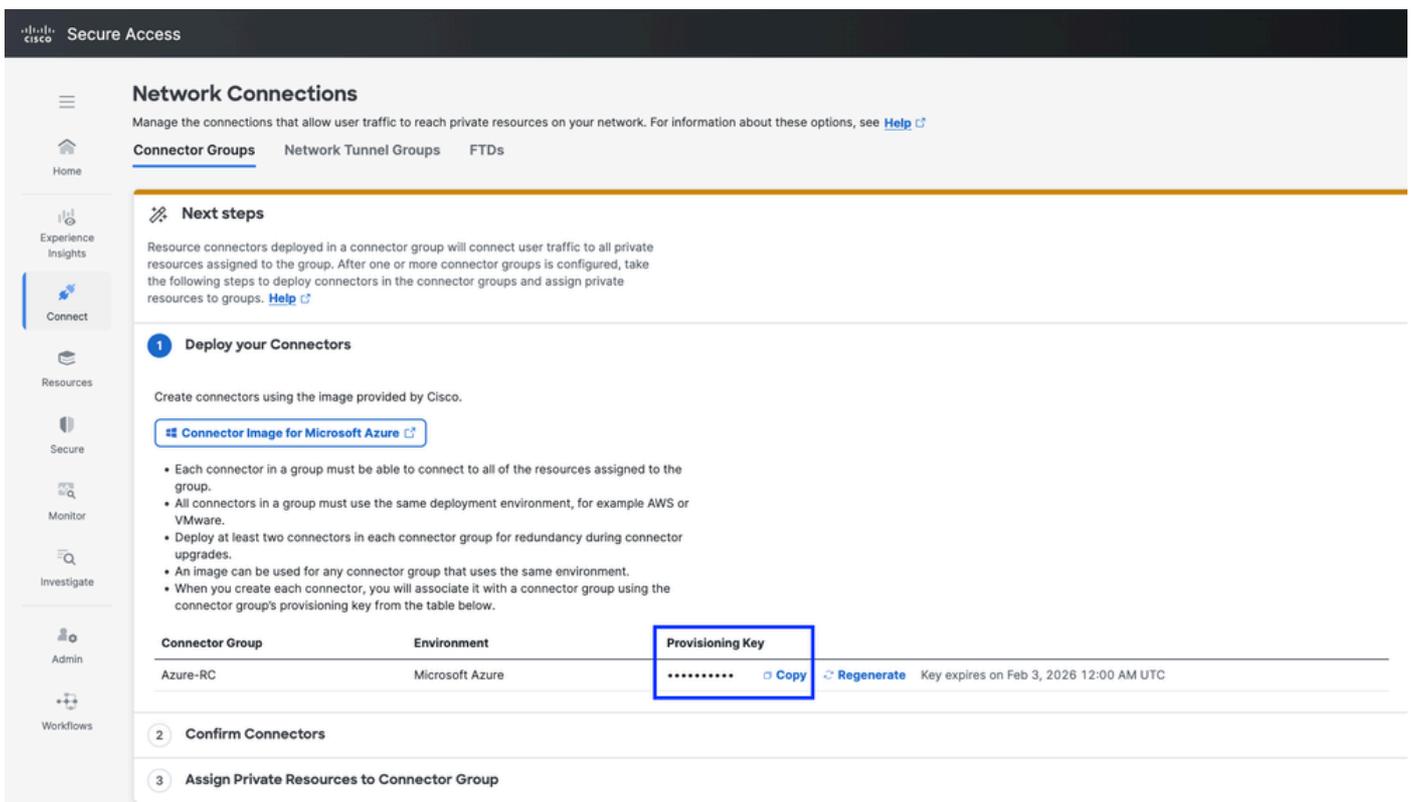
Sicherer Zugriff - Überprüfung der Resource Connector-Konfiguration

- 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 Key kopieren. 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:

The screenshot shows the Microsoft Azure Marketplace search interface. The search bar contains 'Cisco Secure Access Resource Connector'. The search results show one result: 'Cisco Secure Access Resource Connector' by Cisco Systems, Inc. The result card includes the Cisco logo, the product name, the publisher name, and a brief description: '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'. There is a 'Create' button and a heart icon for favorites. The left sidebar shows navigation options like 'Get Started', 'Management', and 'My Marketplace'. The top navigation bar includes the Microsoft Azure logo and a search bar.

Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

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

The screenshot shows the product page for 'Cisco Secure Access Resource Connector' in the Microsoft Azure Marketplace. The page header includes the Microsoft Azure logo and a search bar. The product name 'Cisco Secure Access Resource Connector' is prominently displayed, along with the publisher 'Cisco Systems, Inc.' and a 'Virtual Machine' category. Below the product name, there is a 'Subscription' dropdown menu and a 'Plan' dropdown menu. The 'Plan' dropdown is currently set to 'Cisco Secure Access Resource Conne...'. There is a 'Create' button and a 'Start with a pre-set configuration' button. The page also includes a 'Want to deploy programmatically? Get started' link. The main content area has tabs for 'Overview', 'Plans + Pricing', 'Usage Information + Support', and 'Ratings + Reviews'. The 'Overview' tab is selected, showing a description of the product: '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

Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

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

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** Hibernate does not currently support Trusted launch and Confidential virtual machines for this image. [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



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

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](#)

Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

- Einfügen des Provisioning Key kopierten Dokuments aus Cisco Secure Access in das `User data` Feld

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 after creation. Learn more >

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="xxxxxxxxxxxxxxxxxxxxxxxxxxxx"`

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

< Previous | Next : Tags > | **Review + create**

Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

- Klicken Sie auf, um mit `Create` der Erstellung Ihres 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-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

< Previous Next > Create

Sicherer Zugriff - Erstellen von Ressourcenkonnektoren auf Azure

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

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-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

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](#)

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**

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 Ihres Resource Connector

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-sspt-zu-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	Operation details
azure-rc708	Microsoft.Network/networkInterfaces	OK	Operation details
network-interface-associated-virtual-network-2026011915	Microsoft.Resources/deployments	OK	Operation details
Azure-RC-ip	Microsoft.Network/publicIPAddresses	OK	Operation details
Azure-RC-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

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 Bereitstellung Confirm Connectors zu beenden.

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	***** Copy Regenerate 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"/>	X Revoke

[Confirm connectors](#)

Sicherer Zugriff - Bestätigung des Ressourcenkonnektors

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

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

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

The screenshot shows the Azure portal interface for configuring a Bastion host. The top navigation bar includes the Microsoft Azure logo, a search bar, and the Copilot icon. The breadcrumb trail indicates the path: Home > CreateVm-cisco.cisco-resource-connector-cisco-sec-20260122113614 | Overview > Azure-RC. The main heading is 'Azure-RC | Bastion' with a star icon and a menu icon. Below the heading is a search bar and a left-hand navigation pane with options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Bastion (highlighted), Networking, Network settings, Load balancing, Application security groups, Network manager, Settings, and Disks. The main content area provides information about Azure Bastion and the current configuration. It states: 'Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. Deploying will automatically create a Bastion host on a subnet in your virtual network. Learn more'. It specifies 'Using Bastion: vnet-westus-bastion' and 'Provisioning State: Succeeded'. A message asks to 'Please enter username and password to your virtual machine to connect using Bastion.' The configuration fields are: Authentication Type (SSH Private Key from Local File), Username (acadmin), and Local File ('Azure-RC_key.pem'). There is an 'Advanced' section with a checkbox for 'Open in new browser tab' which is checked. A blue 'Connect' button is located at the bottom of the configuration area.

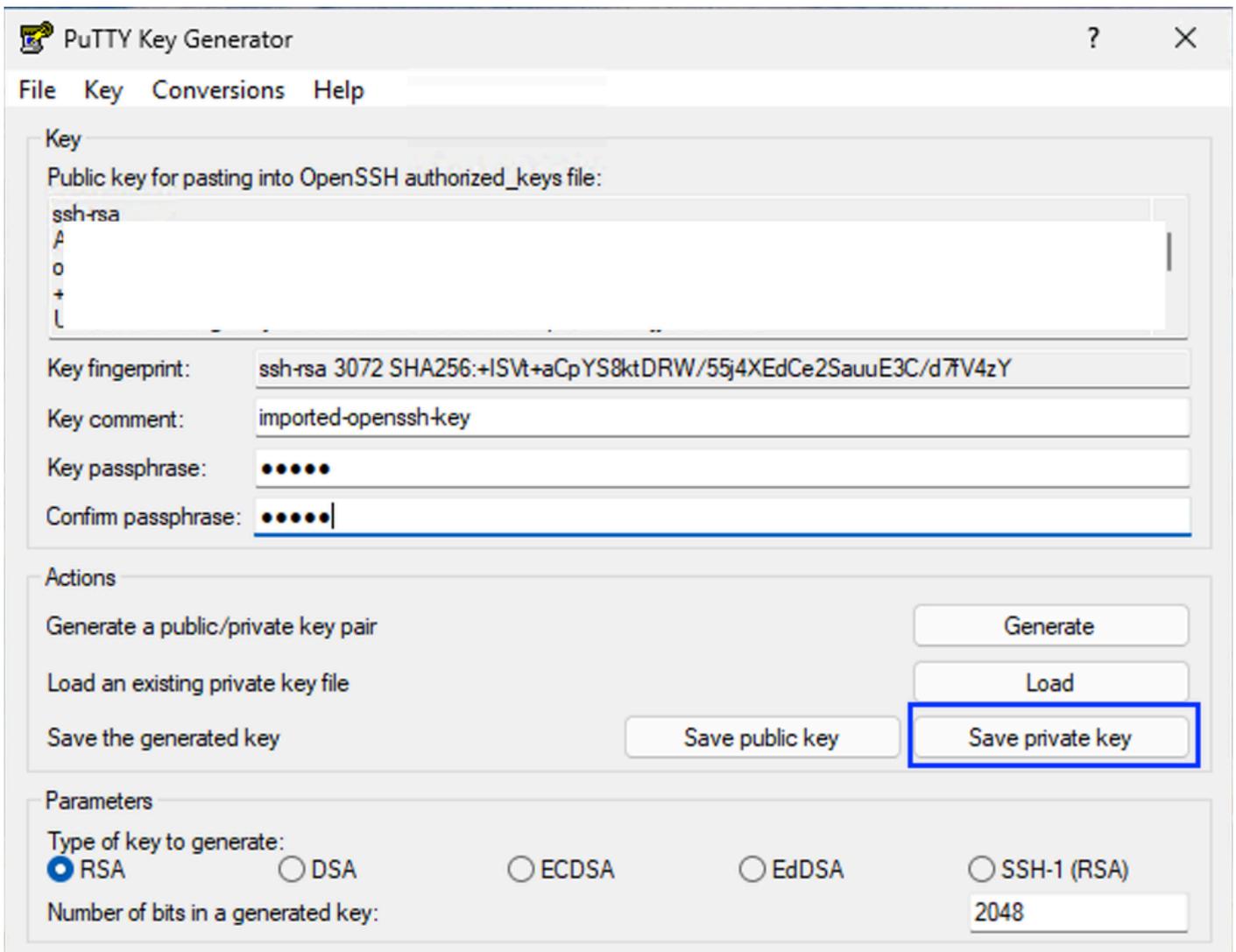

```
Downloads — ssh -i ~/Downloads/Azure-RC_key.pem acadmin@i-... 243x59
You have entered the Console Mode on this Resource Connector.
Type 'help' to get a list of supported commands.

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
=====
$
```

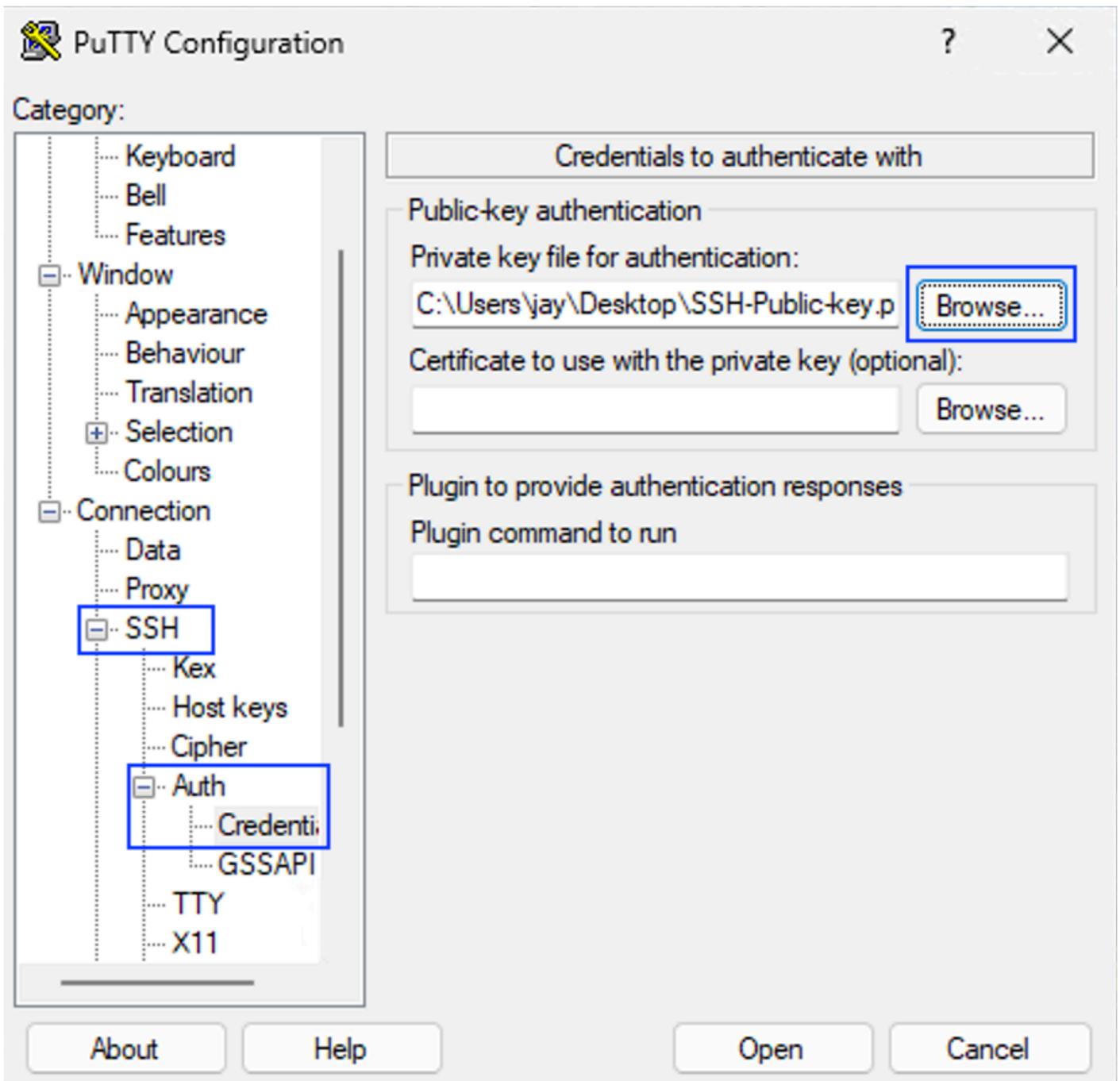
Sicherer Zugriff - Zugriff auf die Befehlszeile des Ressourcenkonnektors

Zugriff von Windows - Putt

Um den privaten Schlüssel zu verwenden, müssen Sie die SSH private key Form von .pem in .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, *Session* und 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
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

```

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.