

在Azure云服务上安装ISE

目录

[简介](#)

[先决条件](#)

[使用的组件](#)

[思科ISE支持的Azure VM大小](#)

[Microsoft Azure云服务中Cisco ISE的限制](#)

[配置](#)

[连接到Azure云的ISE部署示例](#)

[配置](#)

[下一步操作](#)

[安装后任务](#)

[在Azure云上恢复和重置密码](#)

1. [通过串行控制台重置Cisco ISE GUI密码](#)

2. [为SSH访问创建新的公钥对](#)

简介

本文档介绍如何使用Azure虚拟机安装Cisco ISE IOS实例。思科ISE IOS可用于Azure云服务。

先决条件

- 订阅和资源组。

导航到所有服务>订阅。确保存在具有与Microsoft达成企业协议的活动订阅的Azure帐户。使用Microsoft PowerShell Azure模块CLI执行命令以保留空间：(请参阅[<如何安装Azure PowerShell>](#)以了解如何安装Power Shell和相关包)。

```
Connect-AzAccount -TenantID <Tenant-ID>  
Register-AzResourceProvider -ProviderNamespace Microsoft.AVS |  
Register-AzResourceProvider -ProviderNamespace Microsoft.Batch
```



注意：用实际租户ID替换租户ID

有关更多详细信息，请完成为Azure VMware解决方案预申请的[atRequest host quota](#)。

在正确订阅后创建资源组，导航到所有服务>资源组。单击 Add。输入资源组名称。

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ

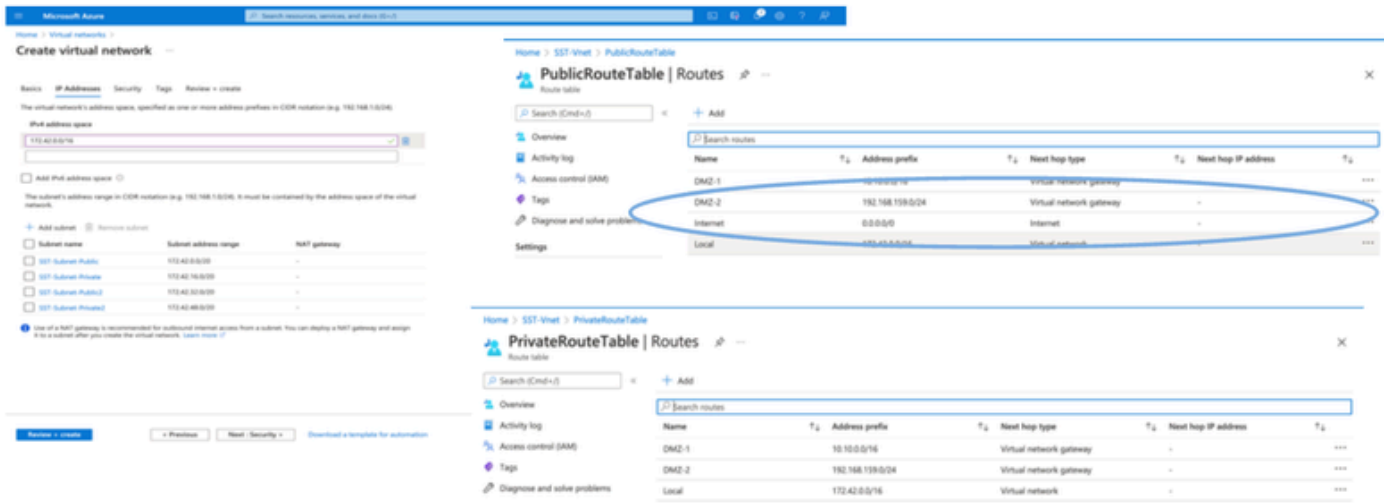
Resource group * ⓘ

Resource details

Region * ⓘ

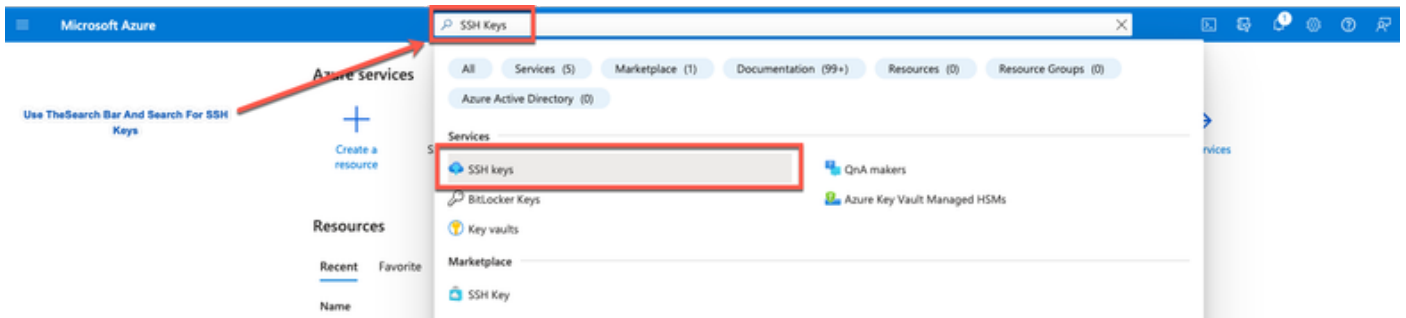
- 虚拟网络和安全组。

需要Internet可达性的子网必须将路由表配置为使用下一跳作为Internet。请参阅公共子网和专用子网示例。具有公共IP的PAN让离线源和在线源更新都工作，具有私有IP的PAN需要依赖离线源更新。

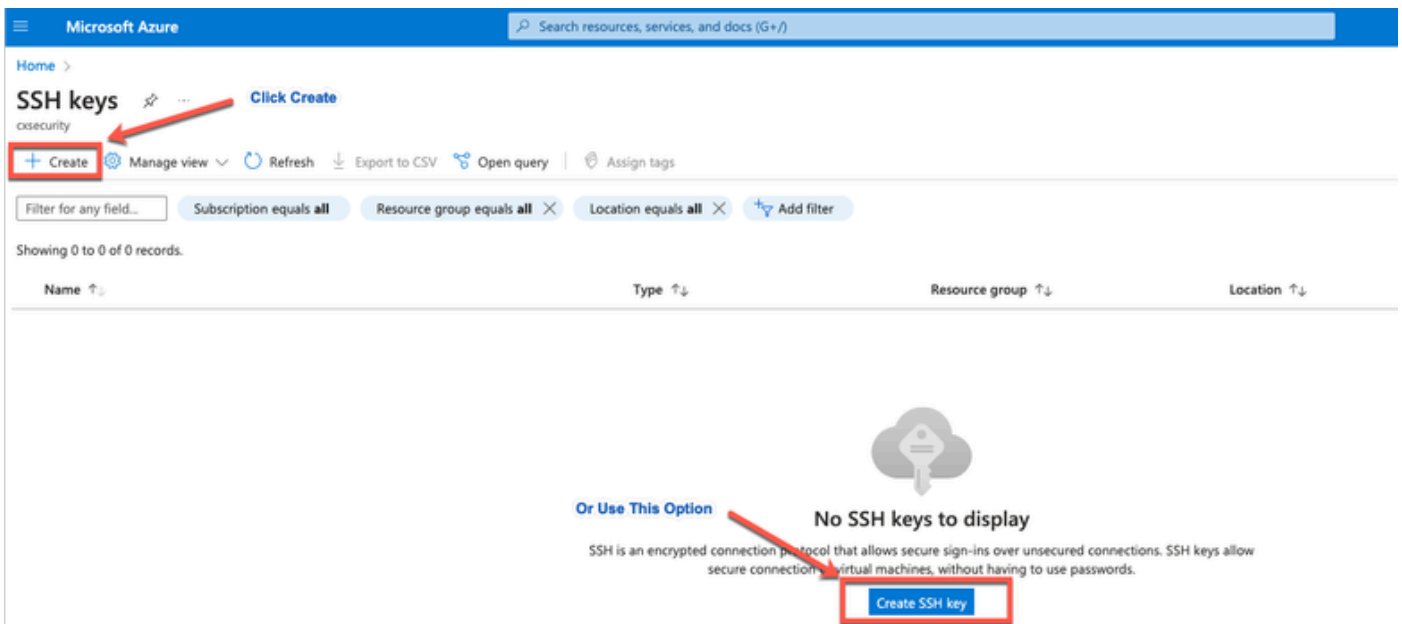


- 创建SSH密钥对。

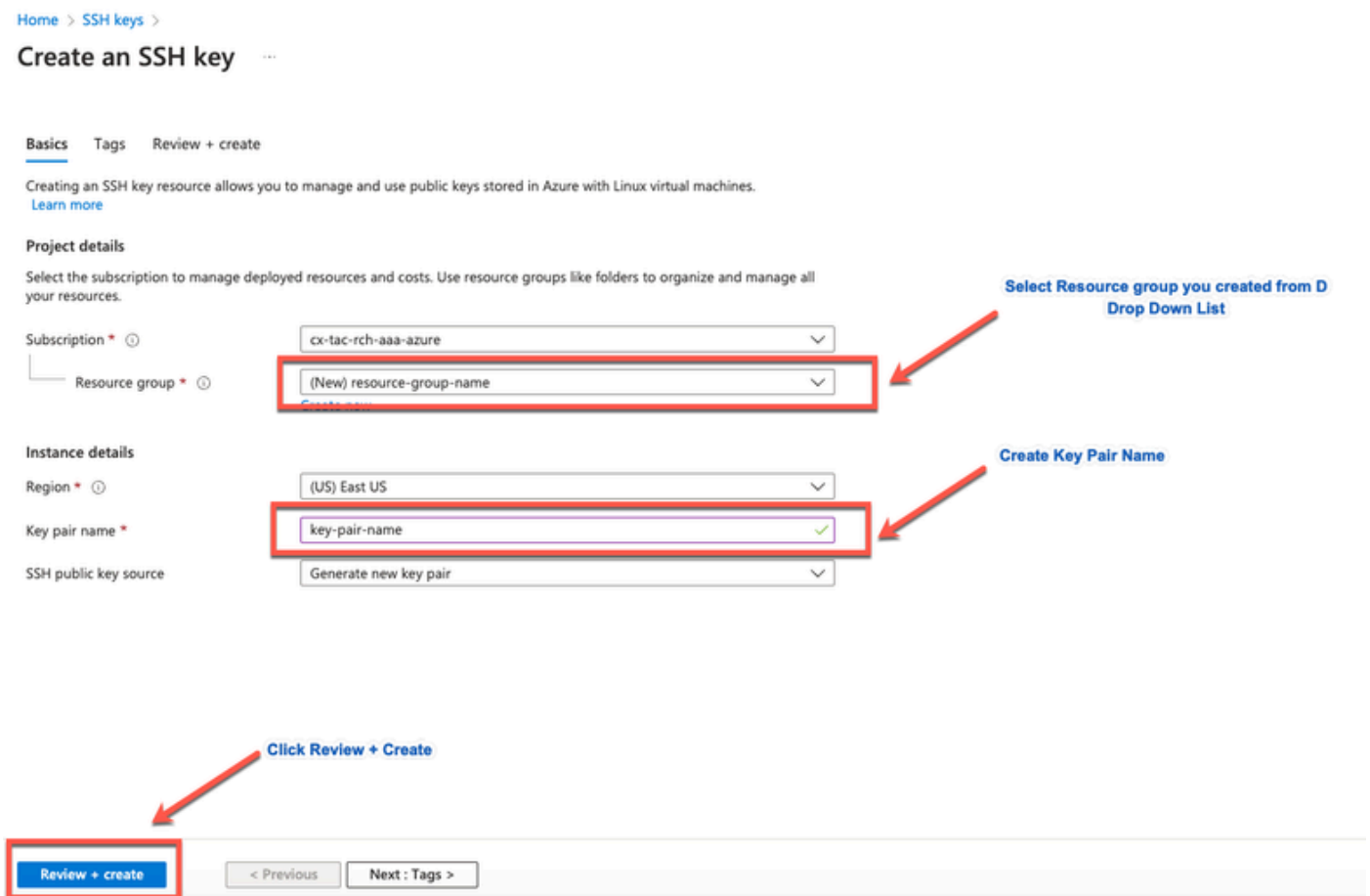
a.使用Azure Web Portal主页上的搜索栏并搜索SSH密钥。



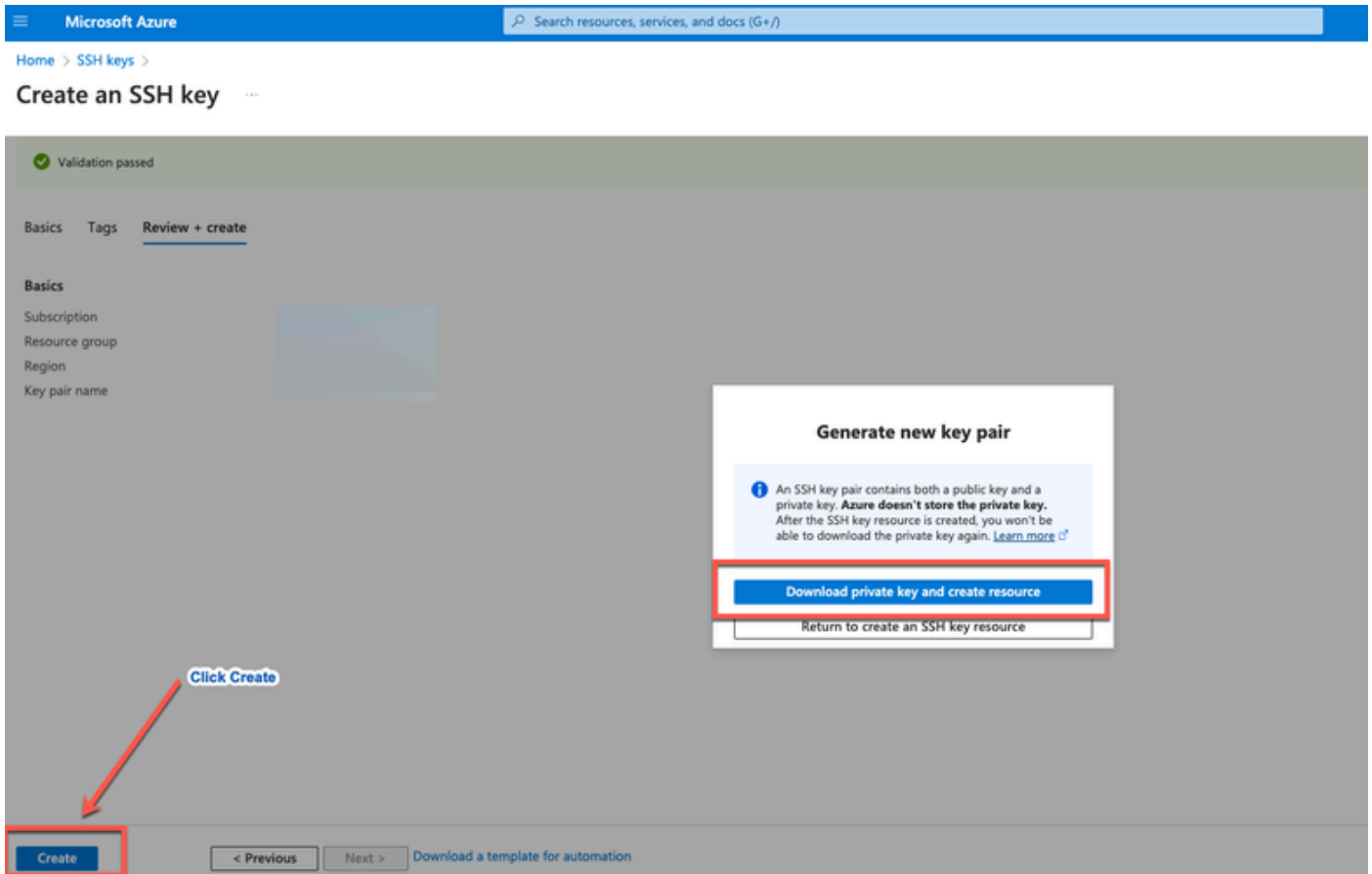
b.在下一个窗口中，单击创建。



c.从下一个窗口中选择资源组和密钥名称。然后单击Review + Create。



d.在下一个窗口中，单击Create和Download Private Key。



使用的组件

本文档的内容基于这些软件和云服务。

- 思科ISE版本3.2。
- Microsoft Azure云服务

本文档中的信息是在特定实验环境中的设备上创建的。用于本文的所有设备始于初始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

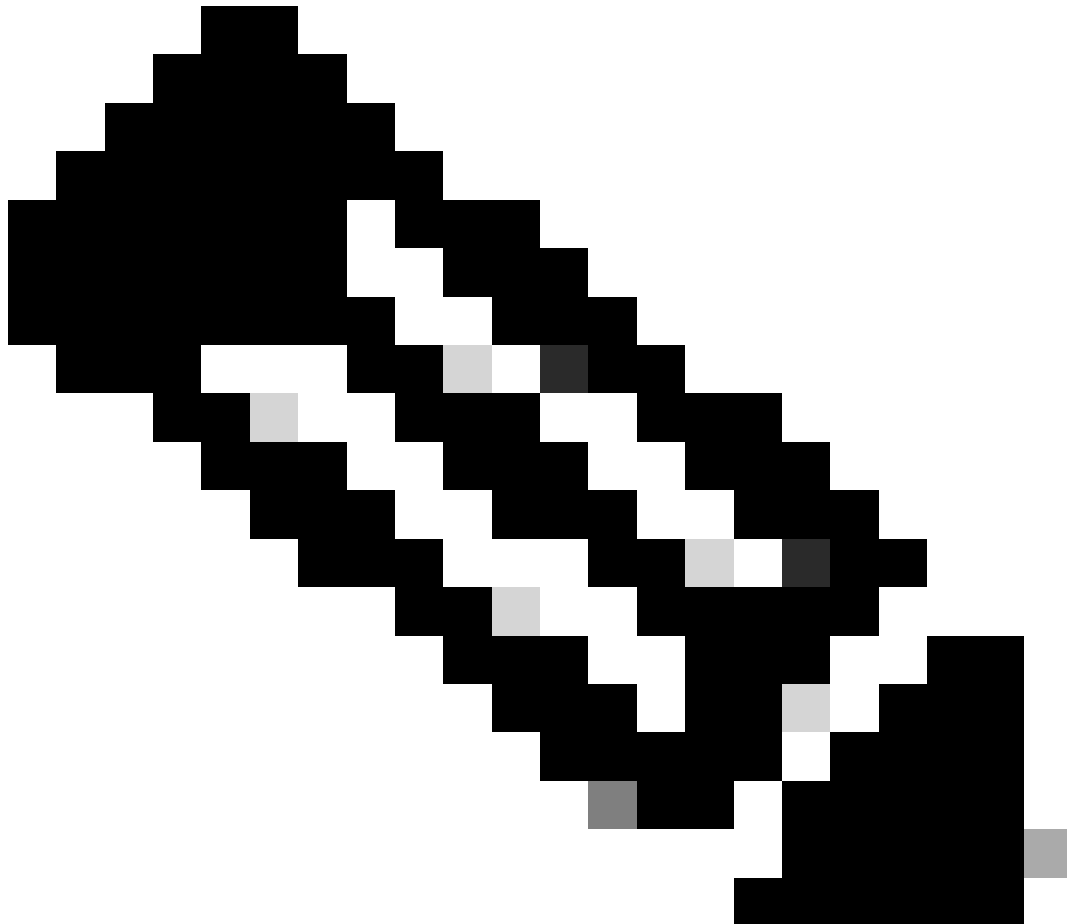
思科ISE支持的Azure VM大小

Azure VM Sizes	vCPU	RAM (in GB)
Standard_D4s_v4 (This instance supports the Cisco ISE evaluation use case. 100 concurrent active endpoints are supported.)	4	16
Standard_D8s_v4	8	32
Standard_F16s_v2	16	32
Standard_F32s_v2	32	64
Standard_D16s_v4	16	64
Standard_D32s_v4	32	128
Standard_D64s_v4	64	256

- Fsv2系列Azure VM大小经过计算优化，最适合用作计算密集型任务和应用的PSN。

- Dsv4系列是通用的Azure VM大小，最适合用作PAN或MnT节点或两者，用于数据处理任务和数据库操作。

如果将通用实例用作PSN，则性能数值低于作为PSN的计算优化实例的性能。Standard_D8s_v4 VM大小只能用作额外的小型PSN。



注意：请勿克隆现有Azure云映像以创建思科ISE实例。这样做会在创建的ISE机器中导致随机和意外故障。

Microsoft Azure云服务中Cisco ISE的限制

- 如果[使用Azure虚拟机](#)创建[思科ISE](#)，默认情况下，Microsoft Azure通过DHCP服务器将私有IP地址分配给VM。在Microsoft Azure上创建思科ISE部署之前，必须使用Microsoft Azure分配的IP地址更新转发和反向DNS条目。

或者，在安装Cisco ISE后，通过更新Microsoft Azure中的网络接口对象将静态IP地址分配到VM：

1. 停止虚拟机。
 2. 在VM的“专用IP地址设置”区域的“分配”区域中，点击静态。
 3. 重新启动虚拟机。
 4. 在思科ISE串行控制台中，将IP地址分配为Gi0。
 5. 重新启动Cisco ISE应用服务器。
- 只有两个NIC支持双NIC -千兆以太网0和千兆以太网1。要在您的思科ISE实例中配置辅助NIC，您必须首先在Azure中创建网络接口对象，关闭您的思科ISE实例，然后将此网络接口对象附加到思科ISE。在Azure上安装并启动Cisco ISE后，使用Cisco ISE CLI手动将网络接口对象的IP地址配置为辅助NIC。
 - 思科ISE升级工作流程在Microsoft Azure上的思科ISE中不可用。仅支持全新安装。但是，您可以执行配置数据的备份和恢复。
 - 公共云仅支持第3层功能。Microsoft Azure上的Cisco ISE节点不支持依赖第2层功能的Cisco ISE功能。例如，通过Cisco ISE CLI使用DHCP SPAN分析器探针和CDP协议功能是当前不支持的功能。
 - 当您执行配置数据的恢复和备份功能时，备份操作完成后，首先通过CLI重新启动Cisco ISE。然后，从Cisco ISE GUI启动恢复操作。
 - Azure中不支持使用基于密码的身份验证对思科ISE CLI进行SSH访问。您只能通过密钥对访问思科ISE CLI，并且必须安全地存储此密钥对。如果使用私钥（或PEM）文件并且丢失文件，您将无法访问Cisco ISE CLI。

不支持使用基于密码的身份验证方法访问Cisco ISE CLI的任何集成，例如Cisco DNA Center 2.1.2版及更早版本。

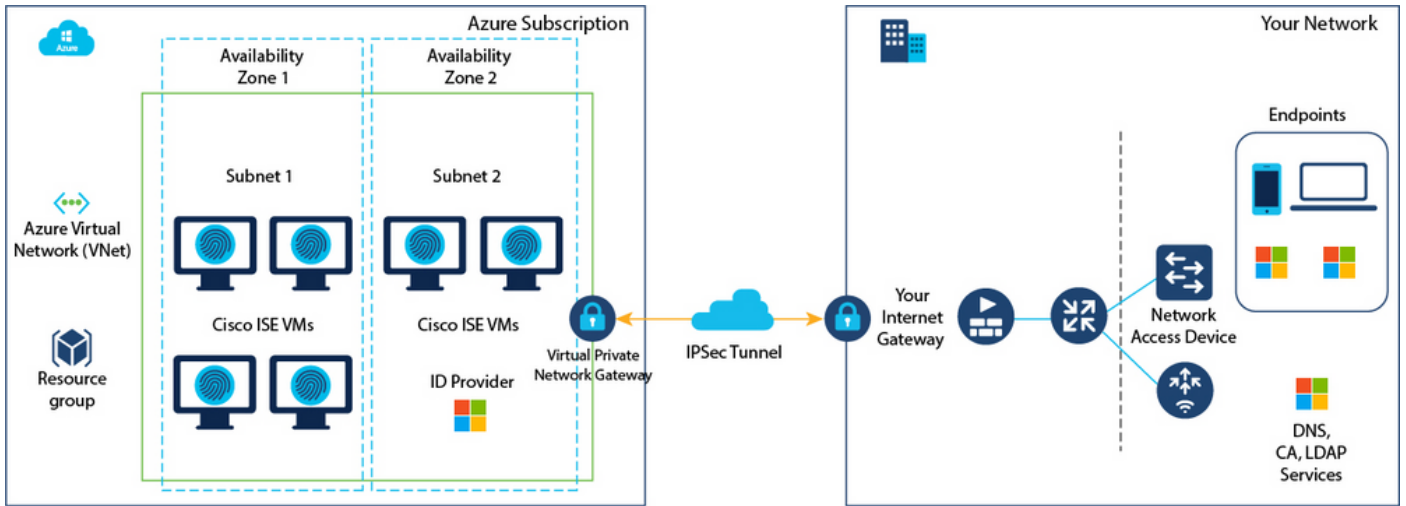
- Azure上的Cisco ISE IOS部署通常利用动态多点虚拟专用网络(DMVPN)和软件定义的广域网(SD-WAN)等VPN解决方案，其中IPSec隧道开销可能导致MTU和分段问题。在这种情况下，思科ISE IOS不会收到完整的RADIUS数据包，并且身份验证失败不会触发故障错误日志。

一种可能的解决方法是寻求Microsoft技术支持以探索Azure中允许无序碎片传递到目标而不是被丢弃的任何解决方案。

- CLI管理员用户必须是“iseadmin”。

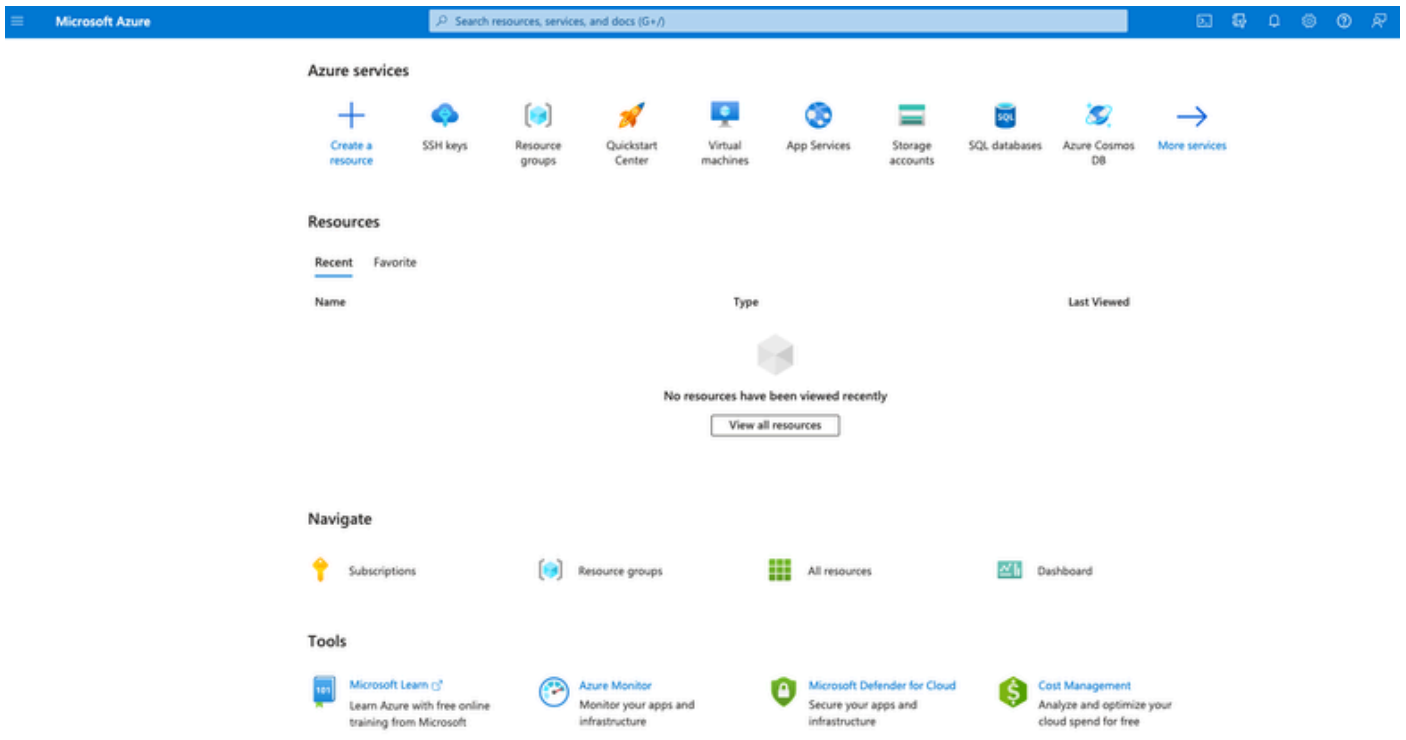
配置

连接到Azure云的ISE部署示例

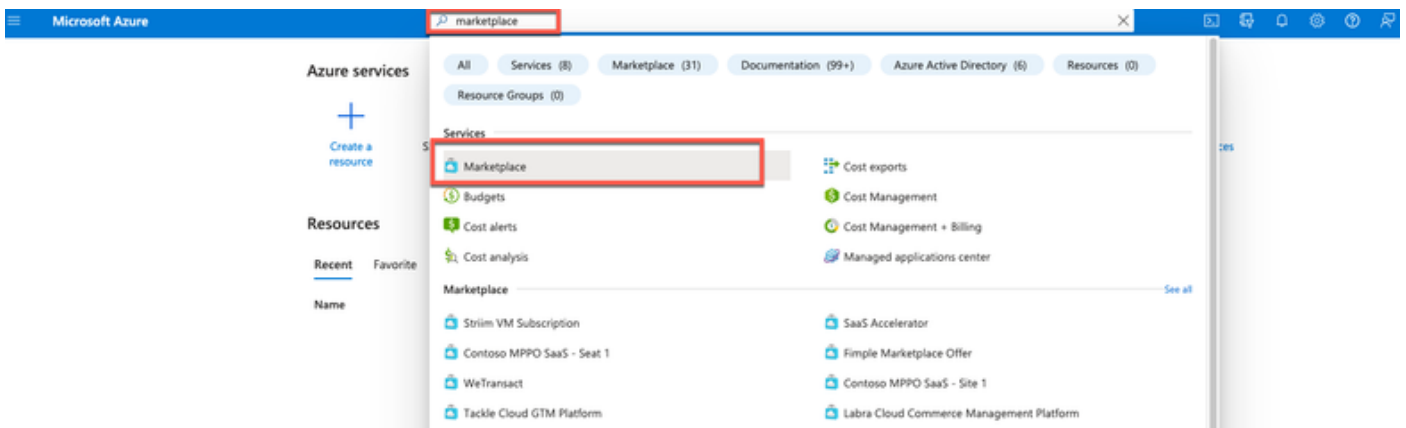


配置

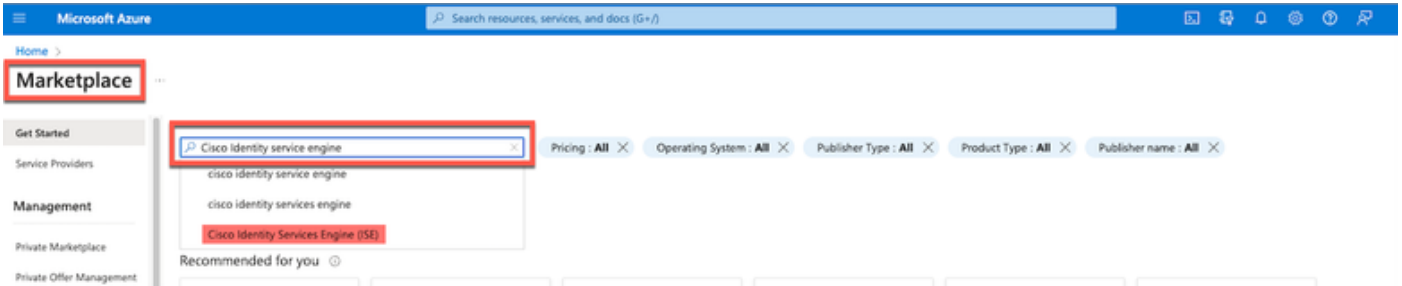
- 第(1)步：转到[Azure门户](#)并登录你的Microsoft Azure帐户。



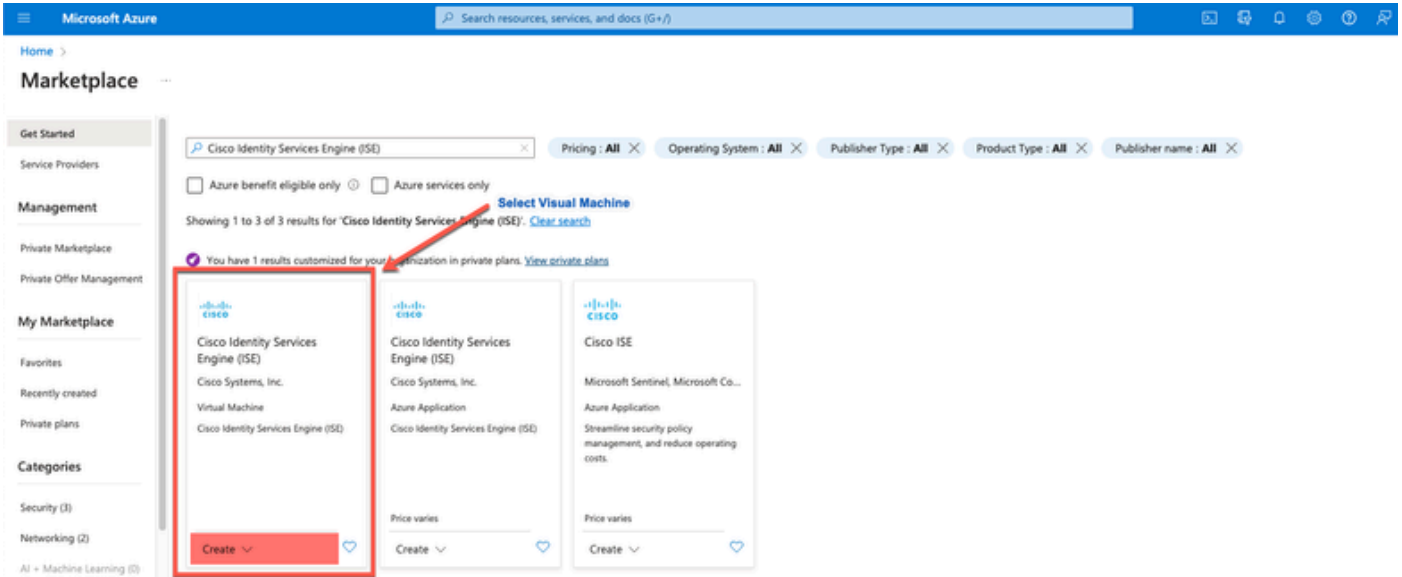
- 第(2)步：使用窗口顶部的搜索字段搜索市场。



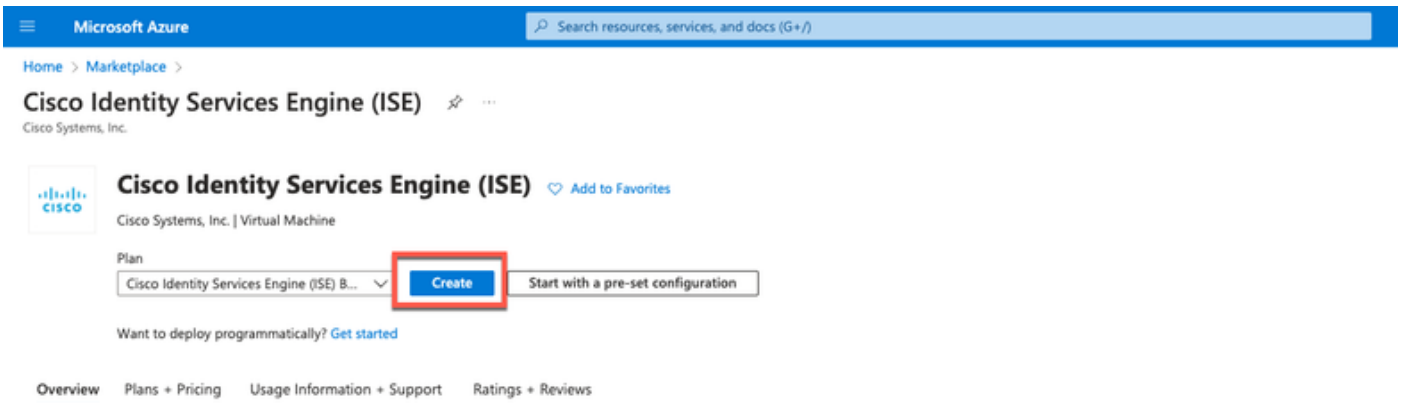
- 第(3)步：使用搜索Marketplace搜索字段搜索思科身份服务引擎(ISE)。



- 第(4)步：点击虚拟机。



- 第(5)步：在显示的新窗口中，单击创建。



- 第(6)步：在基础信息选项卡中：

- a.在项目详细信息区域，从订用和资源组下拉列表中选择所需的值。
- b.在实例详细信息区域，在虚拟机名称字段中输入值。
- c.从Image下拉列表中选择Cisco ISE映像。
- d.从Size下拉列表中，选择要用于安装思科ISE的实例大小。选择思科ISE支持的实例，如

Azure云表中所列

Cisco ISE支持的实例，在[Azure云上的Cisco ISE](#)部分。

- e. 在Administrator account > Authentication type区域中，单击SSH Public Key单选按钮。
- f. 在用户名字段中输入iseadmin。
- g. 从SSH Public Key Source下拉列表中，选择Use existing key stored in Azure。
- h. 从Stored keys下拉列表中，选择作为此任务前提条件而创建的密钥对。
- j. 在Inbound port rules区域中，单击Allow selected ports单选按钮。
- k. 在Licensing区域中，从Licensing type下拉列表中选择Other。

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[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 *

[Select Your Subscription](#)

Resource group *

[Resource Group You Created](#)[Create new](#)

Instance details

Virtual machine name *

ise-vm-name

Region *

(US) East US

Availability options

Availability zone

Availability zone *

Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type

Standard

Image *

Cisco Identity Services Engine (ISE) BYOL 3.2 - x64 Gen1

[See all images](#) | [Configure VM generation](#)

VM architecture

 Arm64 x64

Arm64 is not supported with the selected image.

[Click Here To Select ISE Image](#)

Run with Azure Spot discount

Size *

Standard_D32s_v4 - 32 vcpus, 128 GiB memory (\$863.59/month)

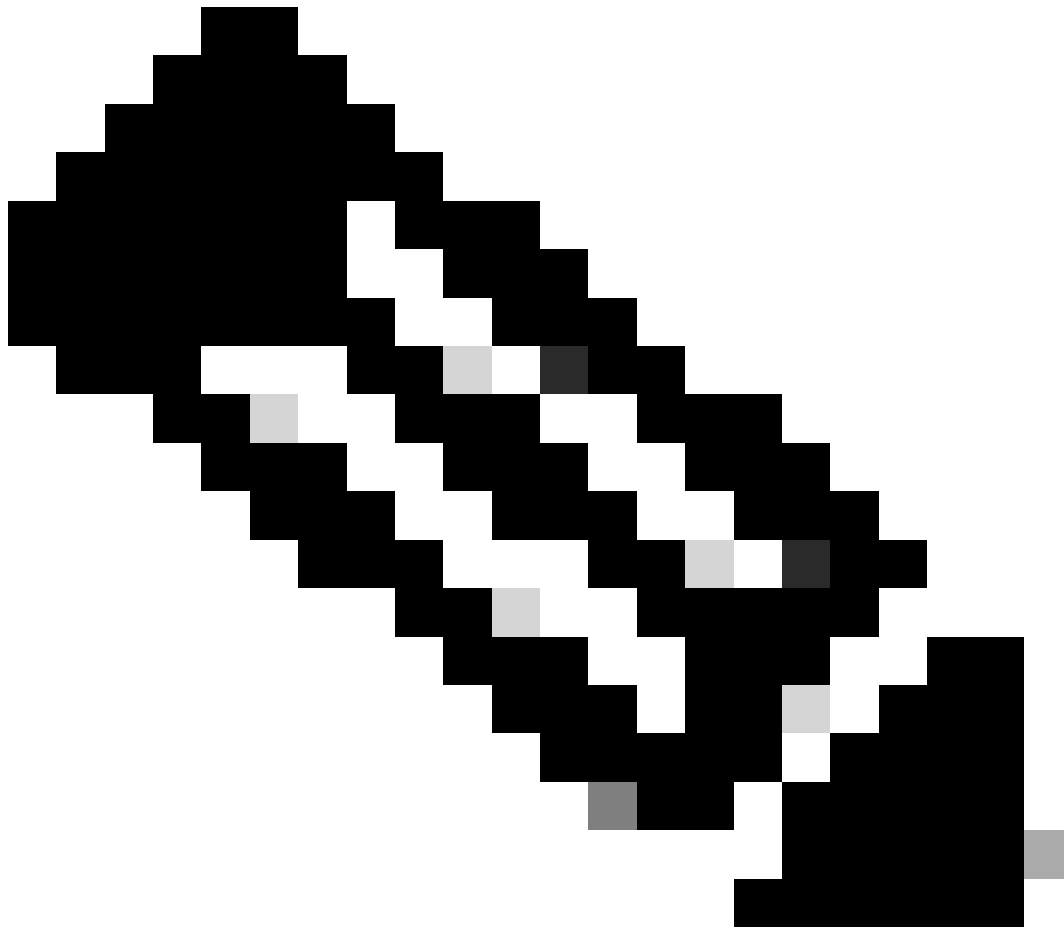
[See all sizes](#)

Administrator account

Authentication type

 SSH public key Password[Click Here To Select ISE Template](#)

Azure now automatically generates an SSH key pair for you and allows you to



注意：对于磁盘类型，可从下拉列表中选择更多选项。您可以选择符合您需求的解决方案。对于生产和性能敏感型工作负载，推荐使用高级SSD。

-
- 第(9)步：在Network Interface区域中，从Virtual network、Subnet和Configure network security group下拉列表中，选择您创建的虚拟网络和子网。



注意：具有公共IP地址的子网接收在线和离线状态源更新，而具有专用IP地址的子网仅接收离线状态源更新。

Create a virtual machine ...

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. [Virtual Network You created Or Click Create New](#)
[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [Create new](#)

Subnet *

Public IP [Create new](#)

NIC network security group None
 Basic
 Advanced [Select Security Group You Created Or Click Create New](#)

Configure network security group * [Create new](#)

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](#)

[Review + create](#) [< Previous](#) [Next : Management >](#)

- 第(10)步：点击下一步：管理。

Delete public IP and NIC when VM is deleted

Enable accelerated networking The selected image does not support accelerated networking.

[Review + create](#) [< Previous](#) [Next : Management >](#)

- 第(11)步：在管理选项卡中，保留必填字段的默认值并点击下一步：高级。



Home > Virtual machines >

Create a virtual machine ...

“Click Next on This Page > Monitoring > Advanced”

Basics Disks Networking Management Monitoring Advanced Tags Review + create


Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)


 Your subscription is protected by Microsoft Defender for Cloud basic plan.

Identity

Enable system assigned managed identity 

Azure AD

Login with Azure AD 

 This image does not support Login with Azure AD.

Auto-shutdown

Enable auto-shutdown 

Create a virtual machine ...

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Premium SSD "Recommended Type For Production"

Alerts

Enable recommended alert rules

Diagnostics

Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

Review + create

< Previous

Next : Advanced >

- 第(12)步：在用户数据区域中，选中启用用户数据复选框。

在用户数据字段中，填写以下信息：

hostname=<Cisco ISE的主机名>

primarynameserver=<IPv4地址>

dnsdomain=<域名>

ntpserver=<IPv4地址或NTP服务器的FQDN>

timezone=<timezone>

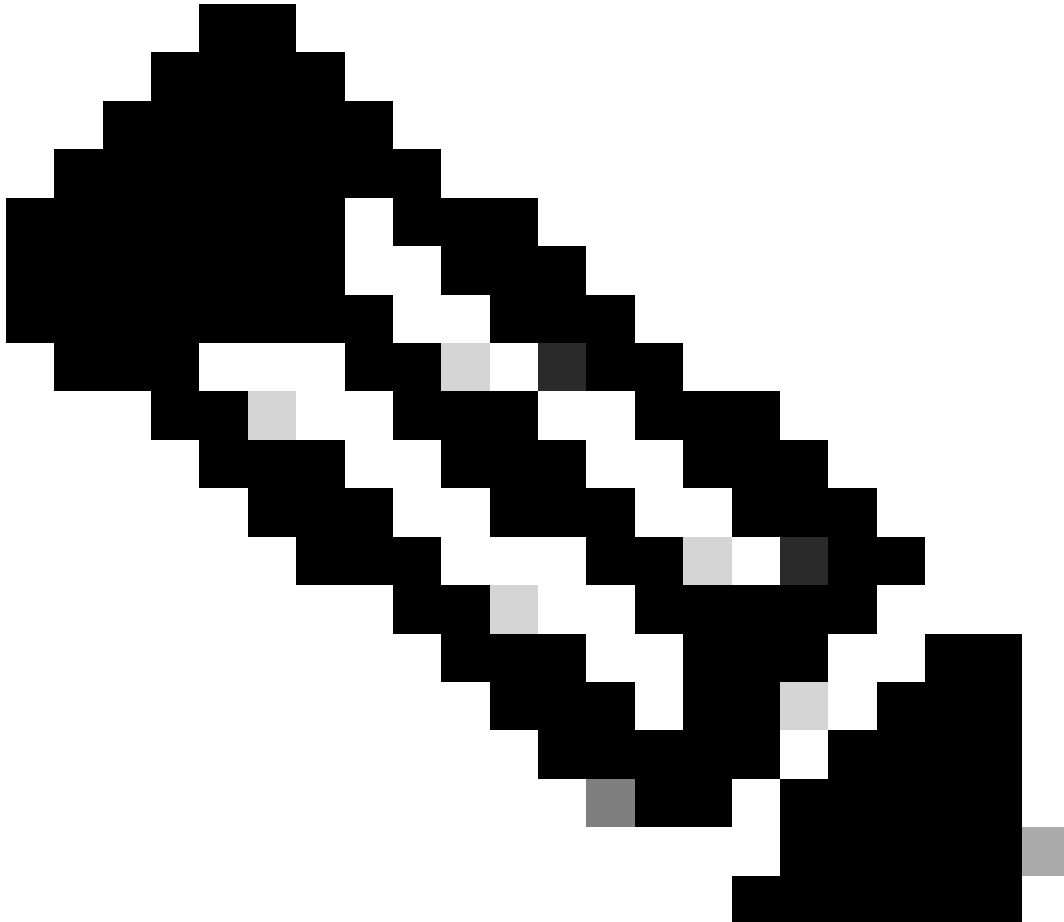
password=<password>

ersapi=<yes/no>

openapi=<yes/no>

pxGrid=<是/否>

pxgrid_cloud=<yes/no>



注意：对于通过用户数据条目配置的每个字段，必须使用正确的语法。输入时，您在“用户数据”字段中输入的信息不会经过验证。如果使用错误的语法，当您启动映像时，思科ISE服务不会出现。

有关必须通过User Data字段提交的配置，请参阅准则：

a.主机名：输入仅包含字母数字字符和连字符(-)的主机名。主机名的长度不能超过19个字符，并且不能包含下划线(_)。

b.主名称服务器：输入主名称服务器的IP地址。仅支持IPv4地址。

在此步骤中只能添加一个DNS服务器。您可以在安装后通过Cisco ISE CLI添加其他DNS服务器。

c. dnsdomain : 输入DNS域的FQDN。条目可以包含ASCII字符、数字、连字符(-)和句点(.)。

d. ntpserver : 输入必须用于同步的NTP服务器的IPv4地址或FQDN。

在此步骤中只能添加一个NTP服务器。您可以在安装后通过Cisco ISE CLI添加其他NTP服务器。使用有效且可访问的NTP服务器，因为ISE操作需要此服务器。

e.时区 : 输入时区，例如Etc/UTC。我们建议您将所有思科ISE节点设置为协调世界时(UTC)时区，特别是如果您的思科ISE节点安装在分布式部署中。此过程可确保来自部署中各个节点的报告和日志的时间戳始终同步。

f.密码 : 为基于GUI的登录思科ISE配置密码。您输入的密码必须符合Cisco ISE密码策略。密码必须包含6到25个字符，并至少包含一个数字、一个大写字母和一个小写字母。密码不能与用户名相同，或其反向 (iseadmin或nimdaesi)、cisco或ocsic。允许的特殊字符为@~*!, +=_-。请参阅[Cisco ISE管理员指南](#)的“基本设置”一章中的“用户密码策略”一节了解您的版本。

g. ersapi : 输入yes启用ERS，或输入no禁止ERS。

h. openapi : 输入yes启用OpenAPI，或输入no禁止OpenAPI。

i. pxGrid : 输入yes启用pxGrid，或输入no禁用pxGrid。

j. pxgrid_cloud : 输入yes启用pxGrid云，或输入no禁用pxGrid云。要启用pxGrid云，必须启用pxGrid。如果禁用pxGrid，但启用pxGrid云，则在启动时不启用pxGrid云服务。

Create a virtual machine

Select This

Enable user data

User data *

```
hostname=isehostname  
primarynameserver=primary sever ip address  
dnsdomain=domain fqdn  
ntpserver=ntp server ip address  
timezone=America/Chicago  
username= iseadmin  
password=passworded  
ersapi=yes  
openapi=yes  
pxGrid=no  
pxgrid_cloud=no
```

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 choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group

No host groups found

Capacity reservations

Capacity reservations allow you to reserve capacity for your virtual machine needs. You get the same SLA as normal virtual machines with the security of reserving the capacity ahead of time. [Learn more](#)

Review + create

< Previous

Next : Tags >

用户数据部分

- 第(13)步：点击下一步：标记。

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe ⓘ

ⓘ The selected image and size are not supported for NVMe. [See supported VM images and sizes](#) ⓘ

Review + create

< Previous

Next : Tags >

- 第(14)步：要创建允许您对资源进行分类的名称-值对，以及合并多个资源和资源组，请在名称和值字段中输入值。

[Home](#) > [Virtual machines](#) >

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) ⓘ

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
<input type="text" value="Tag Name"/>	<input type="text" value="Value Name"/>	13 selected ▾

- 第(15)步：点击下一步：审核+创建。

Review + create

< Previous

Next : Review + create >

- 第(16)步：查看您目前提供的信息，然后点击创建。

显示Deployment is in progress窗口。创建并可以使用思科ISE实例大约需要30分钟。Cisco ISE VM实例显示在

“虚拟机”窗口（使用主搜索字段查找窗口）。

Create a virtual machine



Preferred e-mail address

Preferred phone number

Basics

Subscription

Resource group

Virtual machine name

Region

Availability options **Availability zone**

Availability zone **1**

Security type **Standard**

Image **Cisco Identity Services Engine (ISE) BYOL 3.2 - Gen1**

VM architecture **x64**

Size **Standard D16s v4 (16 vcpus, 64 GiB memory)**

Authentication type **SSH public key**

Username **iseuser**

Key pair name

Azure Spot **No**

Disks

[Download a template for automation](#)

CreateVm-cisco.cisco-ise-virtual-cisco-ise_3_2-20230926145056 | Overview

Search

- Overview
- Inputs
- Outputs
- Template

Deployment is in progress

Deployment name: CreateVm-cisco.cisco-ise-virtual-cisco-ise_3_2-2... Start time: 9/26/2023, 4:06:05 PM
Subscription: Correlation ID:

Deployment details

Resource	Type	Status	Operation details
	Microsoft.Compute/virtualMachines	Created	Operation details
	Microsoft.Network/networkInterfaces	Created	Operation details
	Microsoft.Network/virtualNetworks	OK	Operation details
	Microsoft.Network/publicIpAddresses	OK	Operation details
	Microsoft.Network/networkSecurityGroups	OK	Operation details

Give feedback
[Tell us about your experience with deployment](#)

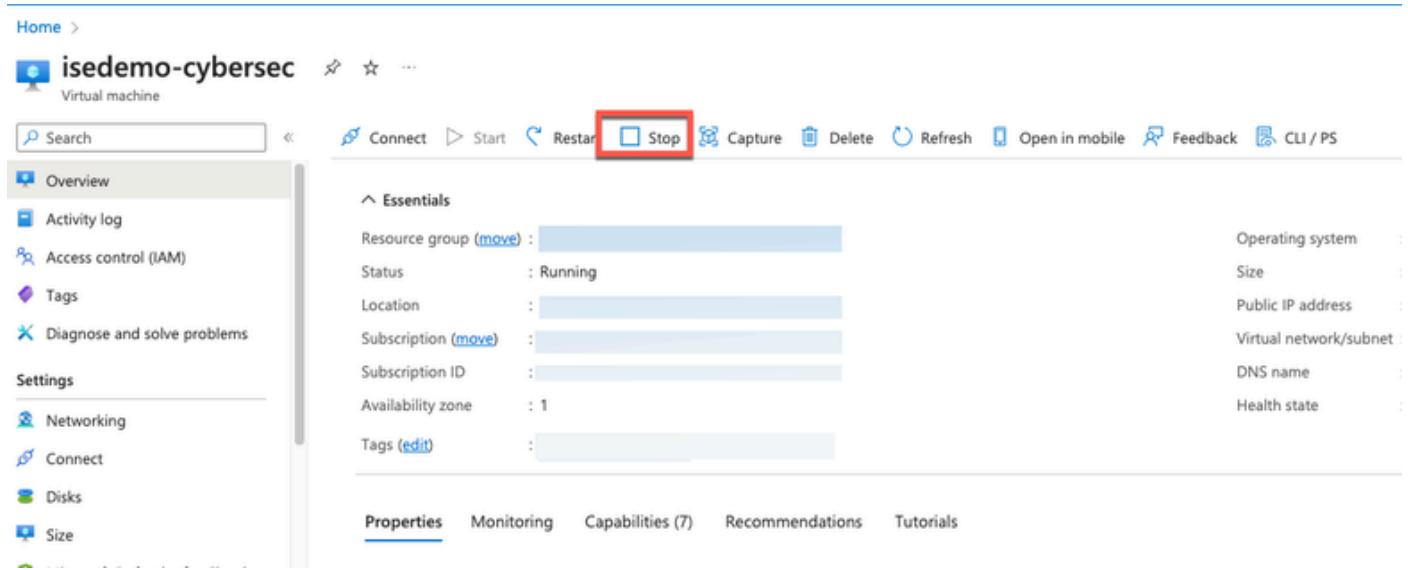
下一步操作

由于Microsoft Azure默认设置，您创建的思科ISE VM仅配置为300 GB磁盘大小。Cisco ISE节点通常需要超过300 GB的磁盘大小。当您首次从Microsoft Azure启动Cisco ISE时，您可以看到Insufficient Virtual Memory警报。

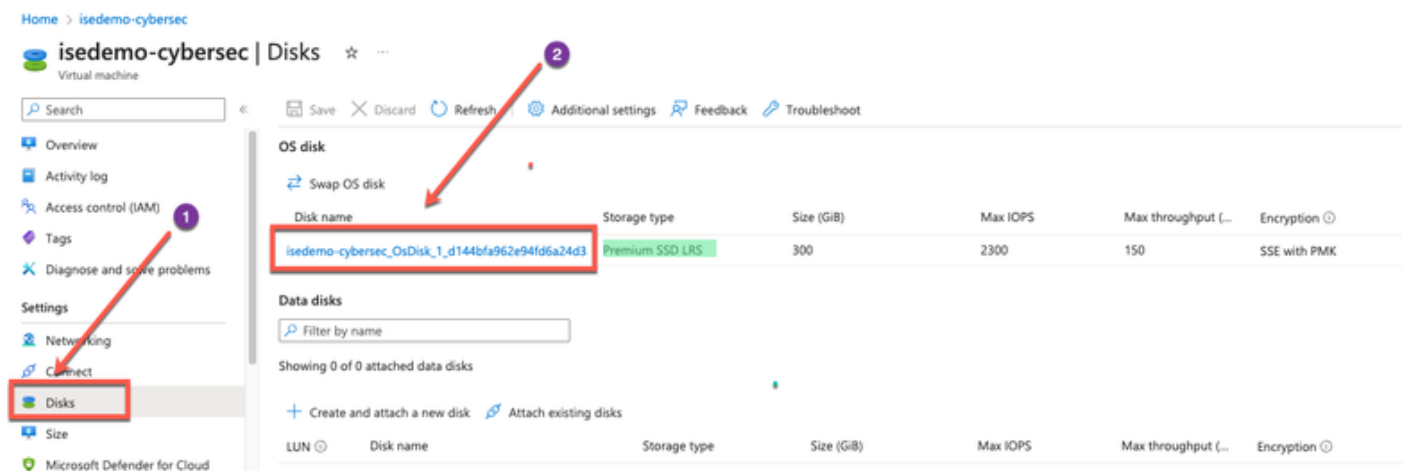
在Cisco ISE VM创建完成后，请登录Cisco ISE管理门户验证Cisco ISE已设置。然后，在Microsoft

Azure门户中，在虚拟机窗口中执行并完成以下步骤以编辑磁盘大小：

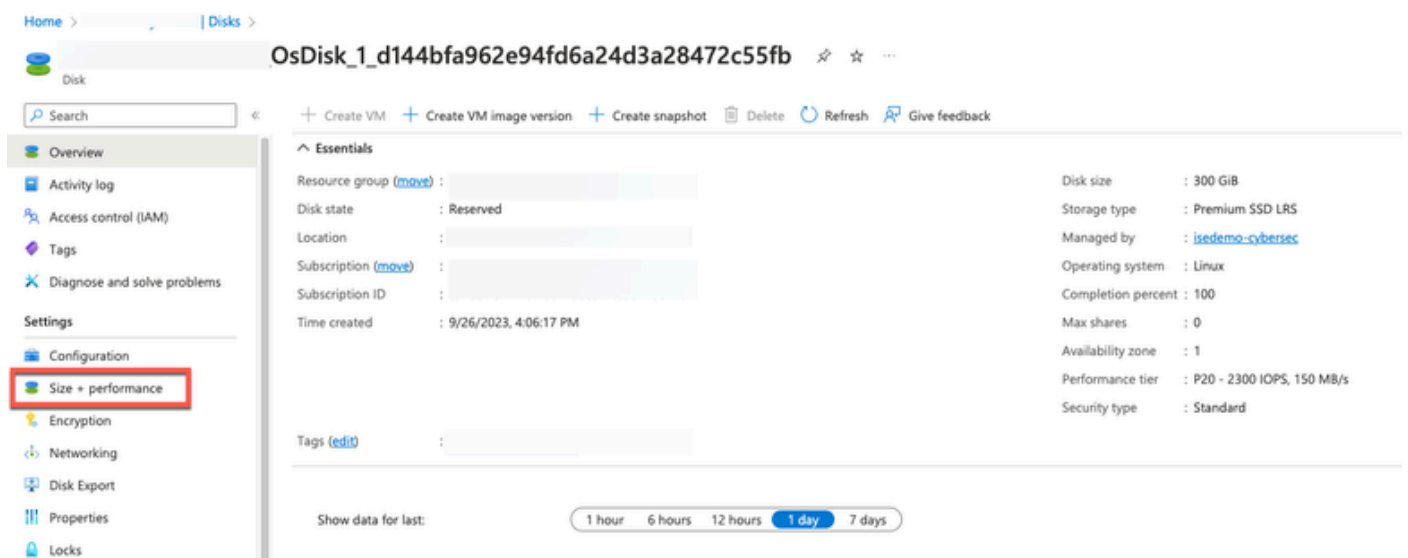
1. 停止Cisco ISE实例。



2. 在左侧窗格中单击Disk，然后单击您用于思科ISE的磁盘。



3. 单击左侧窗格中的Size + performance。



4. 在自定义磁盘大小字段中，以GiB格式输入所需的磁盘大小。

Size	Disk tier	Provisioned IOPS	Provisioned throughput	Max Shares
4 GiB	P1	120	25	3
8 GiB	P2	120	25	3
16 GiB	P3	120	25	3
32 GiB	P4	120	25	3
64 GiB	P6	240	50	3
128 GiB	P10	500	100	3
256 GiB	P15	1100	125	3
512 GiB	P20	2300	150	3
1024 GiB	P30	5000	200	5
2048 GiB	P40	7500	250	5
4096 GiB	P50	7500	250	5
8192 GiB	P60	16000	500	10
16384 GiB	P70	18000	750	10
32767 GiB	P80	20000	900	10

安装后任务

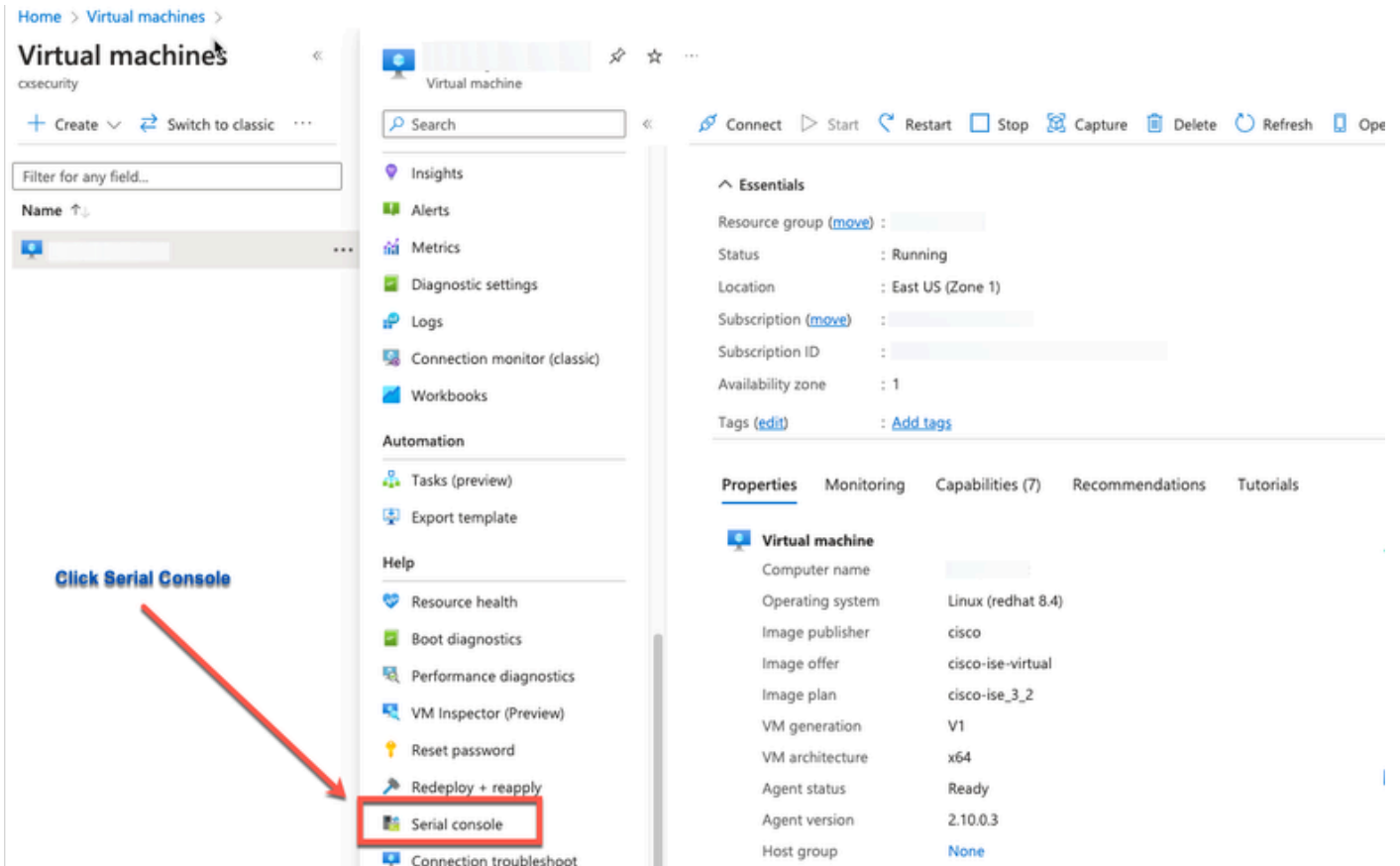
有关成功创建Cisco ISE实例后必须执行的安装后任务的信息，请参阅您的Cisco ISE版本的[Cisco ISE安装指南](#)中的“安装验证和安装后任务”一章。

在Azure云上恢复和重置密码

完成有助于重置或恢复您的Cisco ISE虚拟机密码的任务。选择您需要的任务，并执行详细步骤。

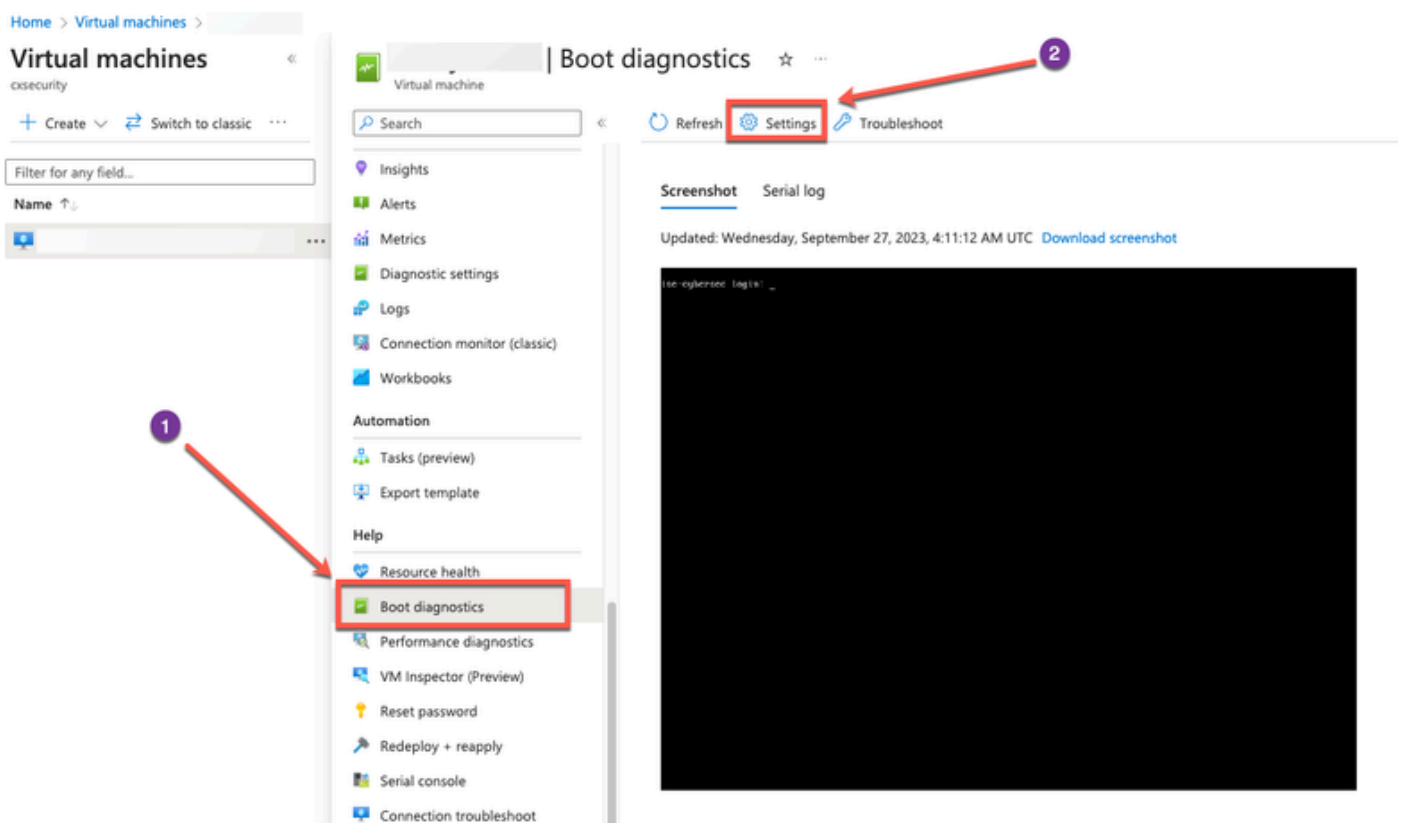
1. 通过串行控制台重置Cisco ISE GUI密码

- 第(1)步：登录到Azure云并选择包含思科ISE虚拟机的资源组。
- 第(2)步：从资源列表中，点击要重置密码的思科ISE实例。
- 第(3)步：在左侧菜单中，从支持+故障排除部分，单击串行控制台。

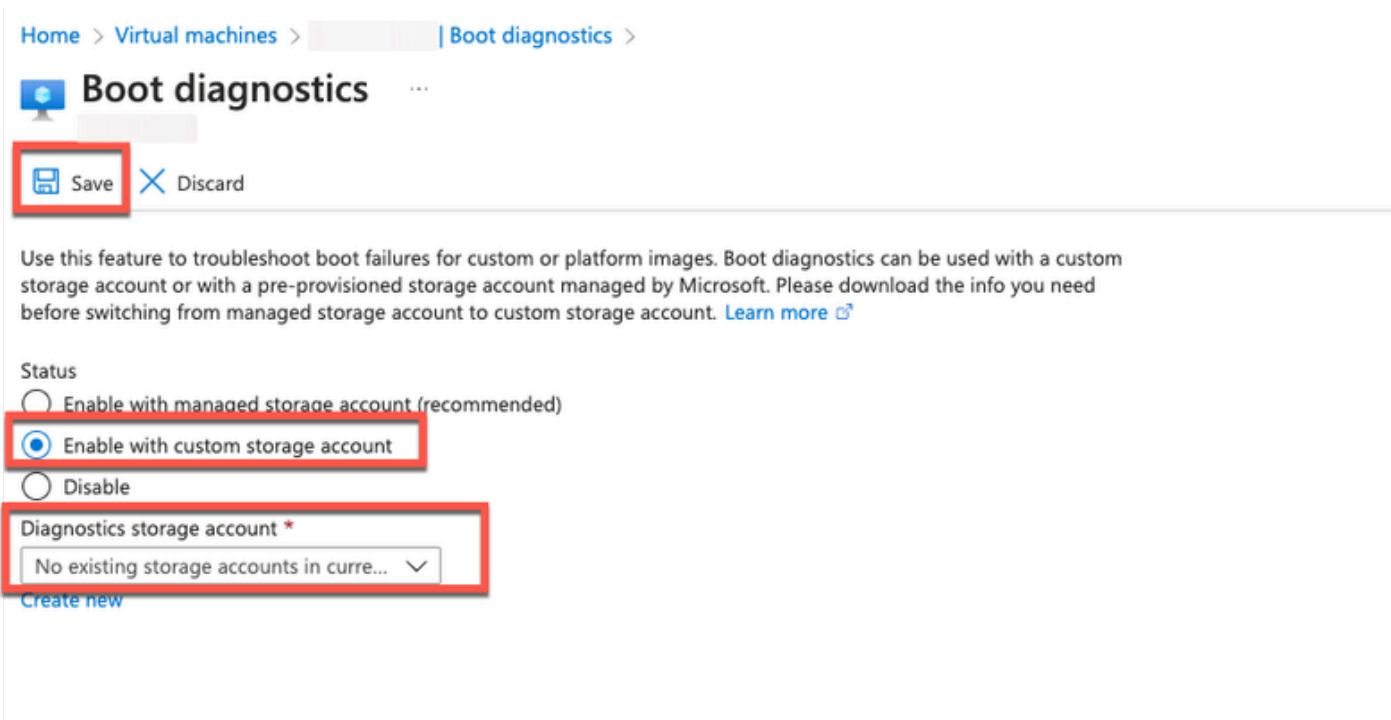


- 第(4)步：如果在此处查看错误消息，则必须通过执行并完成以下步骤来启用引导诊断：

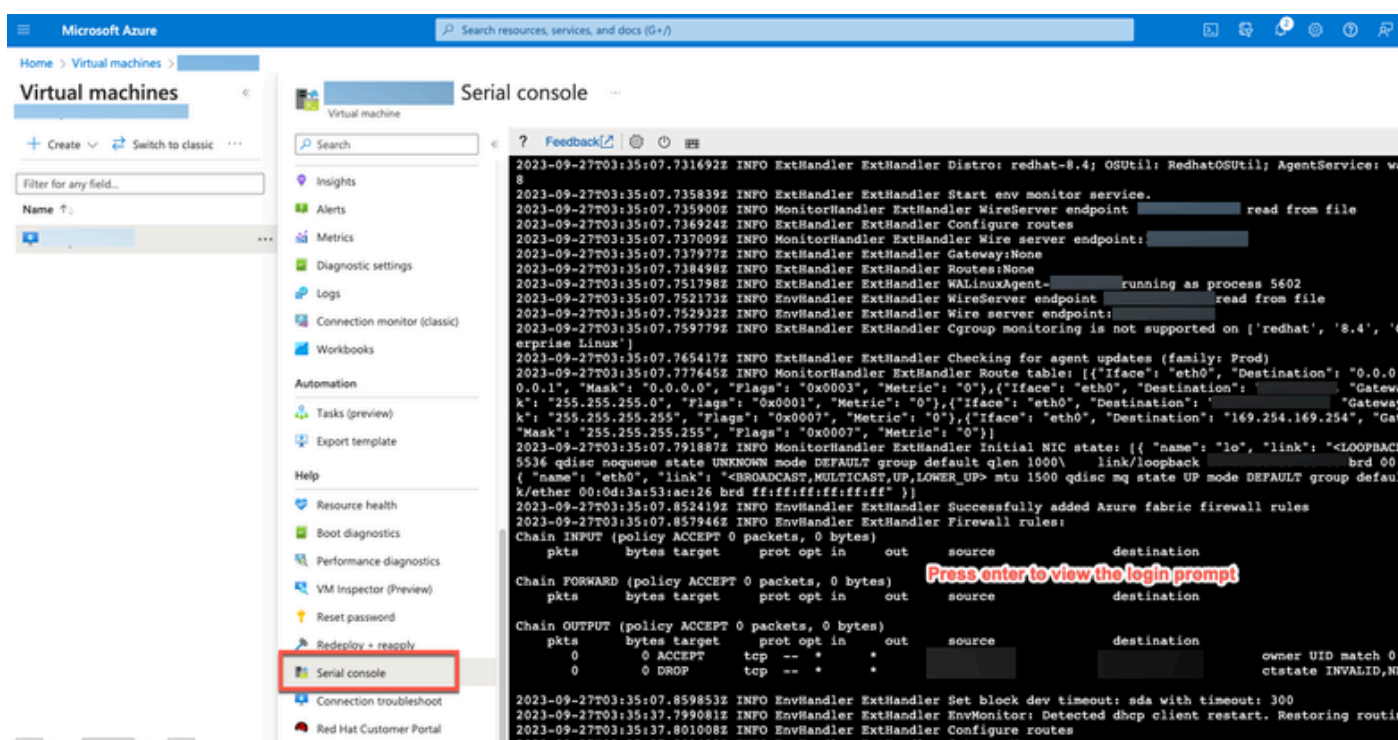
a. 从左侧菜单中单击Boot diagnostics。



b. 单击Enable with custom storage account。然后单击保存。



- 第(5)步：在左侧菜单中，从支持+故障排除部分，单击串行控制台。 Azure Cloud Shell将显示在新窗口中。如果屏幕是黑色的，请按Enter查看登录提示。



- 第(8)步：登录到串行控制台。要登录到串行控制台，您必须使用安装实例时配置的原始密码。
- 第(9)步：使用application reset-password iseadmin命令为iseadmin帐户配置新的GUI密码。

2. 为SSH访问创建新的公钥对

通过此任务，可以向存储库中添加其他密钥对。在Cisco ISE实例配置时创建的现有密钥对不会替换

为您创建的新公钥。

- 第(1)步：在Azure云中创建新公钥。

[Home](#) > [SSH keys](#) >

Create an SSH key ...

[Basics](#) [Tags](#) [Review + create](#)

Creating an SSH key resource allows you to manage and use public keys stored in Azure with Linux virtual machines.

[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 * ⓘ

(New) resource-group-name

Select Resource group you created from D Drop Down List

Instance details

Region * ⓘ

(US) East US

Key pair name *

key-pair-name

Create Key Pair Name

SSH public key source

Generate new key pair

Click Review + Create


Review + create

< Previous

Next: Tags >

您将看到一个弹出窗口，用于选择Download private key和create resource，通过此窗口可下载SSH密钥作为.pem文件。

Generate new key pair

i 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 an SSH key resource](#)

- 第(2)步：要创建新存储库以将公钥保存到，请参阅[Azure Repos文档](#)。

如果已经拥有可通过CLI访问的存储库，请跳到步骤3。

- 第(3)步：要导入新的公钥，请使用命令`crypto key import <public key filename> repository <repository name>`。
- 第(4)步：导入完成后，您可以使用新的公钥通过SSH登录思科ISE。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。