在Azure云服务上安装ISE

目录

简介

先决条件

- 要求
- 使用的组件

步骤

- 虚拟网络和安全组
- 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

下一步工作

安装后任务

Azure云上的密码恢复和重置

- 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

要求

Cisco 建议您了解以下主题：

- 订用和资源组

使用的组件

本文档中的信息基于思科ISE版本3.2和Microsoft Azure云服务。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（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。

步骤

1.定位至所有服务>订用。确保存在一个具有有效订阅的Azure帐户以及与Microsoft的企业协议。

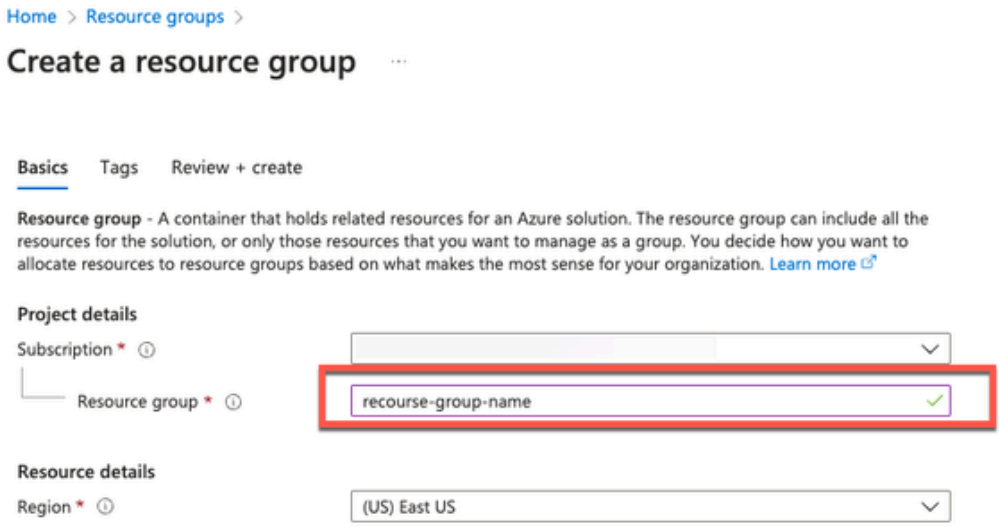
2.使用Microsoft PowerShell Azure模块CLI执行命令以保留空间。请参阅如何安装Azure PowerShell，以安装Power Shell和相关包。

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

注意：使用实际租户ID替换租户ID。

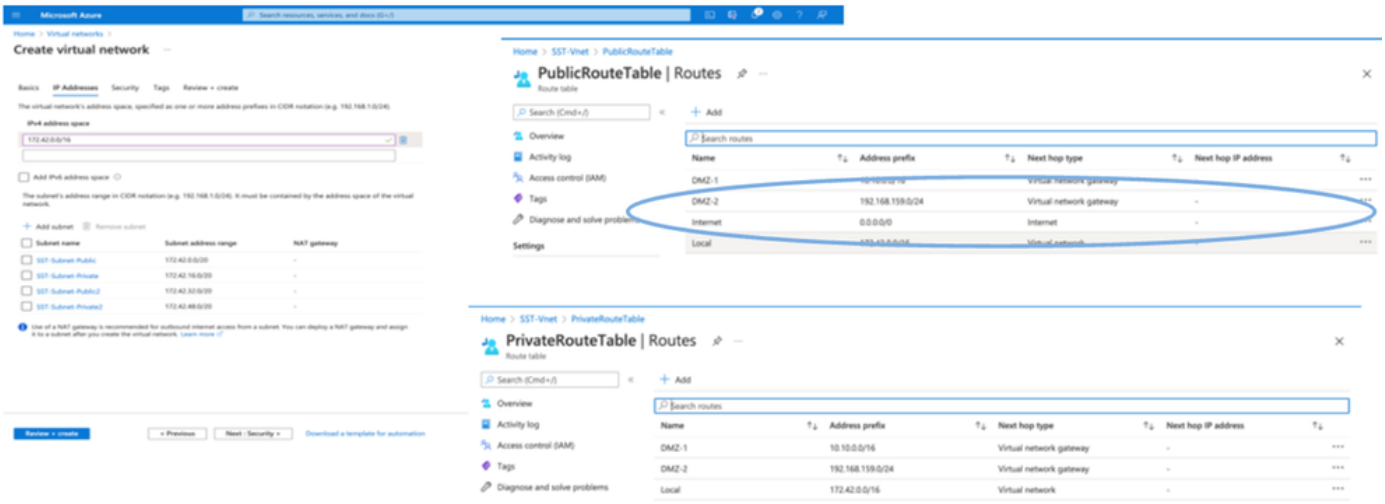
3.在申请Azure VMware解决方案的主机配额时完成必备条件 了解更多信息。

4.在订阅后立即创建资源组。导航到所有服务>资源组。单击 Add。输入资源组名称。



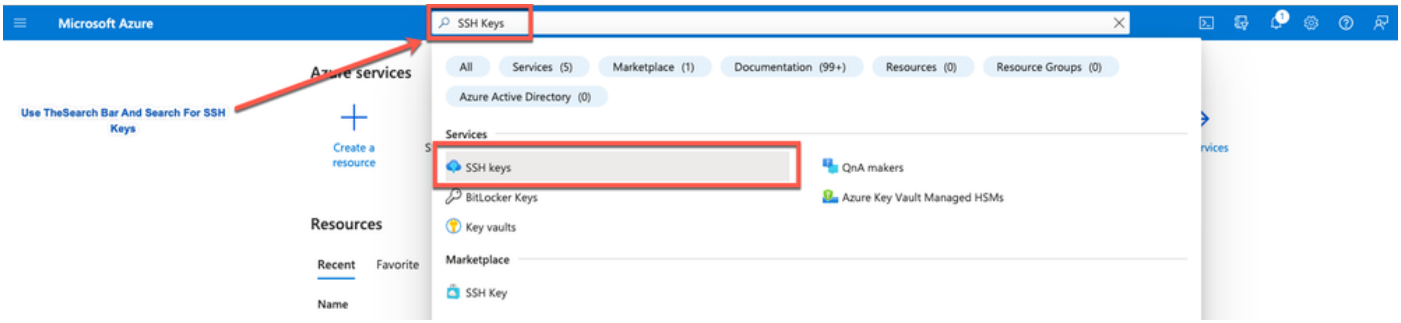
虚拟网络和安全组

需要Internet可达性的子网必须将下一跳路由表配置为Internet。请参阅公共子网和专用子网示例。具有公有IP的PAN同时运行离线源和在线源更新，而具有私有IP的PAN必须依赖于离线源更新。

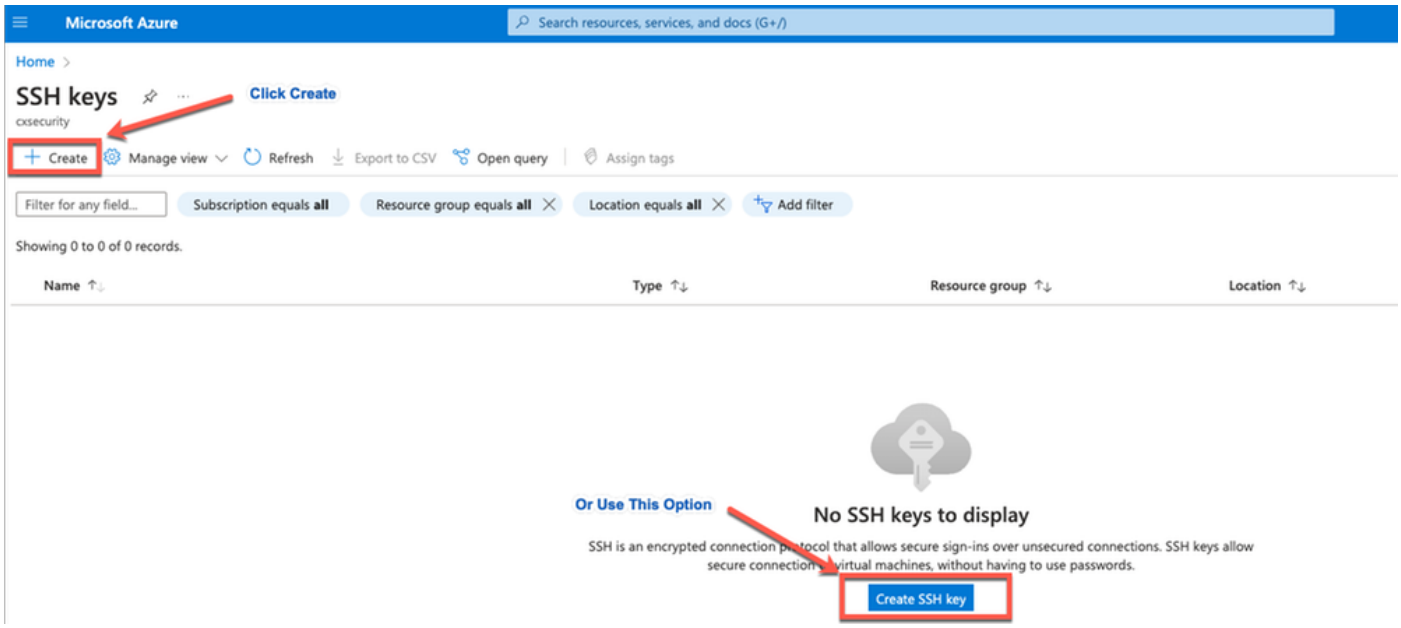


创建SSH密钥对

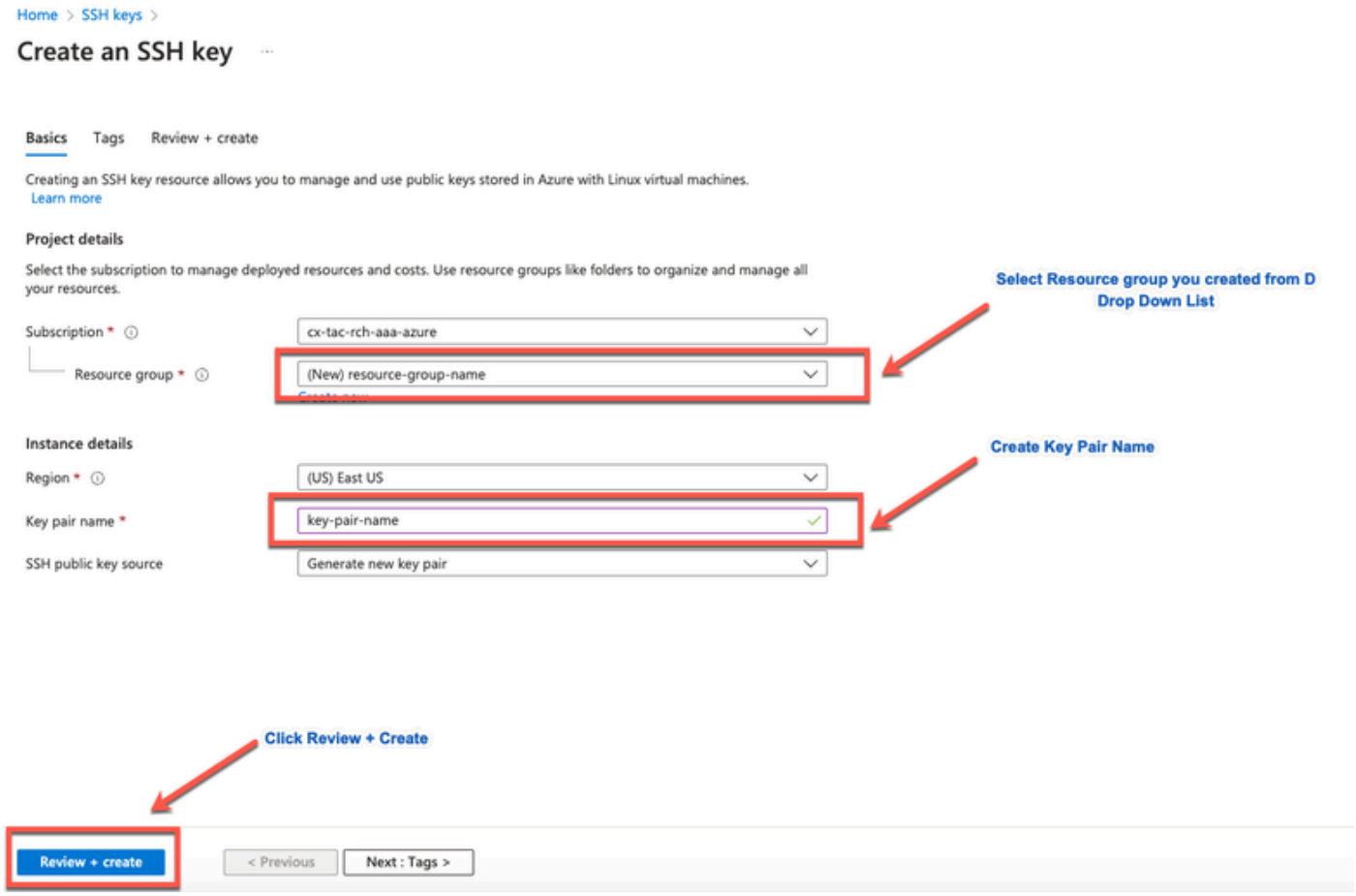
1.使用Azure Web Portal主页的搜索栏搜索SSH密钥。



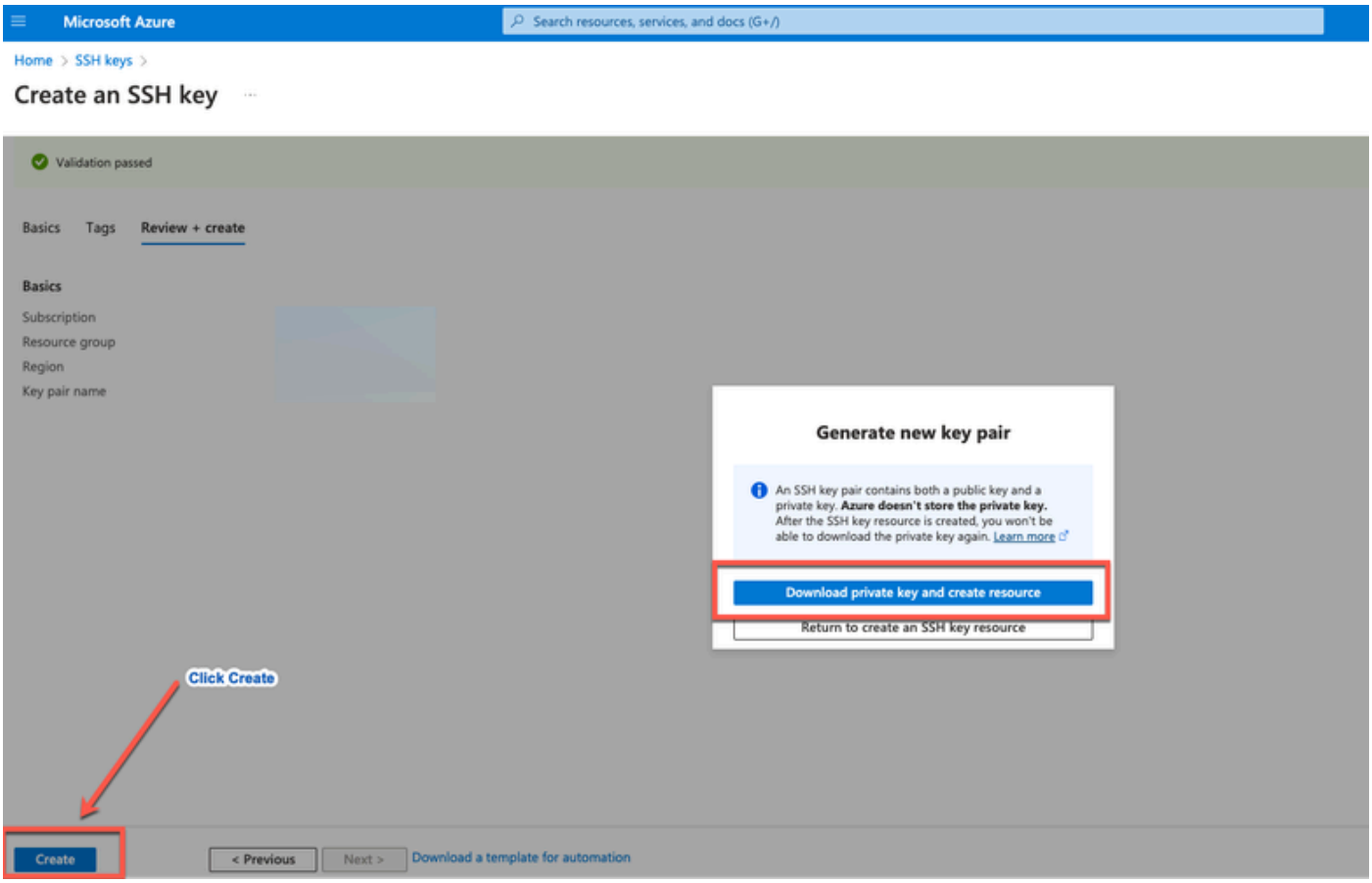
2.单击创建。



3.选择资源组和密钥名称。然后，单击Review + Create。



4.然后单击Create并下载私钥。



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，则性能数值比计算优化实例用作PSN的性能要低。Standard_D8s_v4 VM大小只能用作额外的小型PSN。

注意：不要克隆现有Azure云映像以创建思科ISE实例。这样做会导致所创建的ISE机器出现随机和意外故障。

Microsoft Azure云服务中Cisco ISE的限制

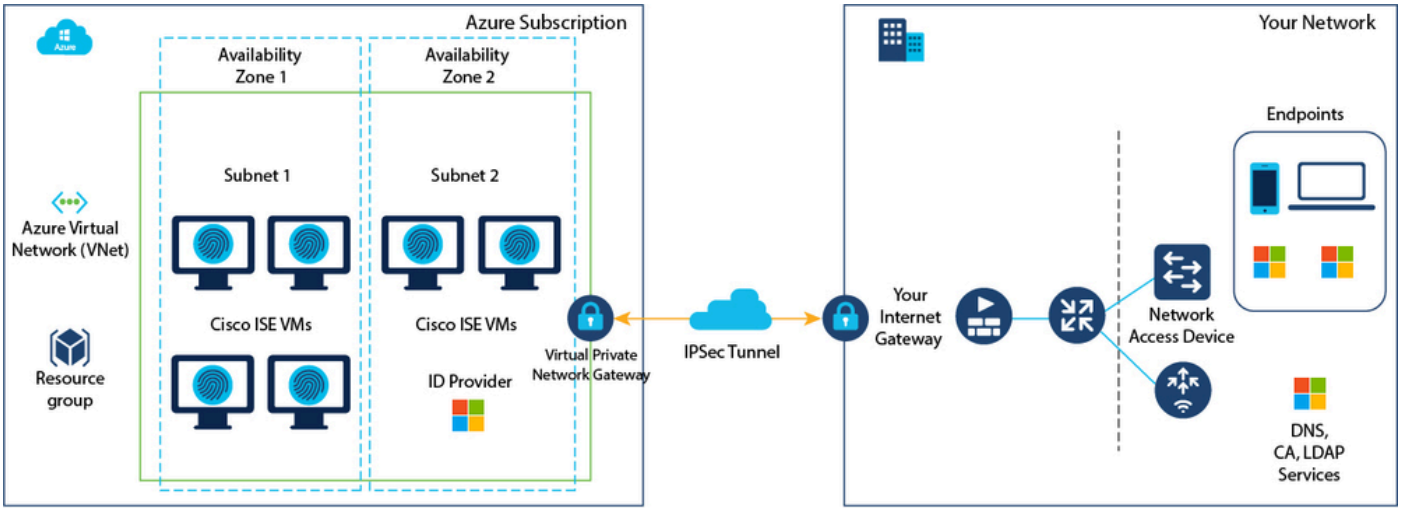
- 如果您使用Azure虚拟机创建Cisco ISE，默认情况下，Microsoft Azure通过DHCP服务器将专用IP地址分配给VM。在Microsoft Azure上创建Cisco ISE部署之前，必须使用Microsoft Azure分配的IP地址更新转发和反向DNS条目。
- 或者，在安装Cisco ISE后，通过更新Microsoft Azure中的网络接口对象将静态IP地址分配到VM:
    1. 停止虚拟机。
    2. 在VM的Private IP address settings（专用IP地址设置）区域的Assignment（分配）区域中，单击Static。
    3. 重新启动虚拟机。
    4. 在Cisco 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，关闭思科ISE实例电源，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，您可以对配置数据进行备份和恢复。
- 公共云仅支持第3层功能。Microsoft Azure上的思科ISE节点不支持依赖第2层功能的思科ISE功能。例如，通过Cisco ISE CLI使用DHCP SPAN分析器探针和CDP协议功能是当前不受支持的功能。
- 当您执行配置数据的还原和备份功能时，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，则无法访问思科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（Cisco DNA Center 2.1.2版及更低版本）。
- 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。

- 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”。

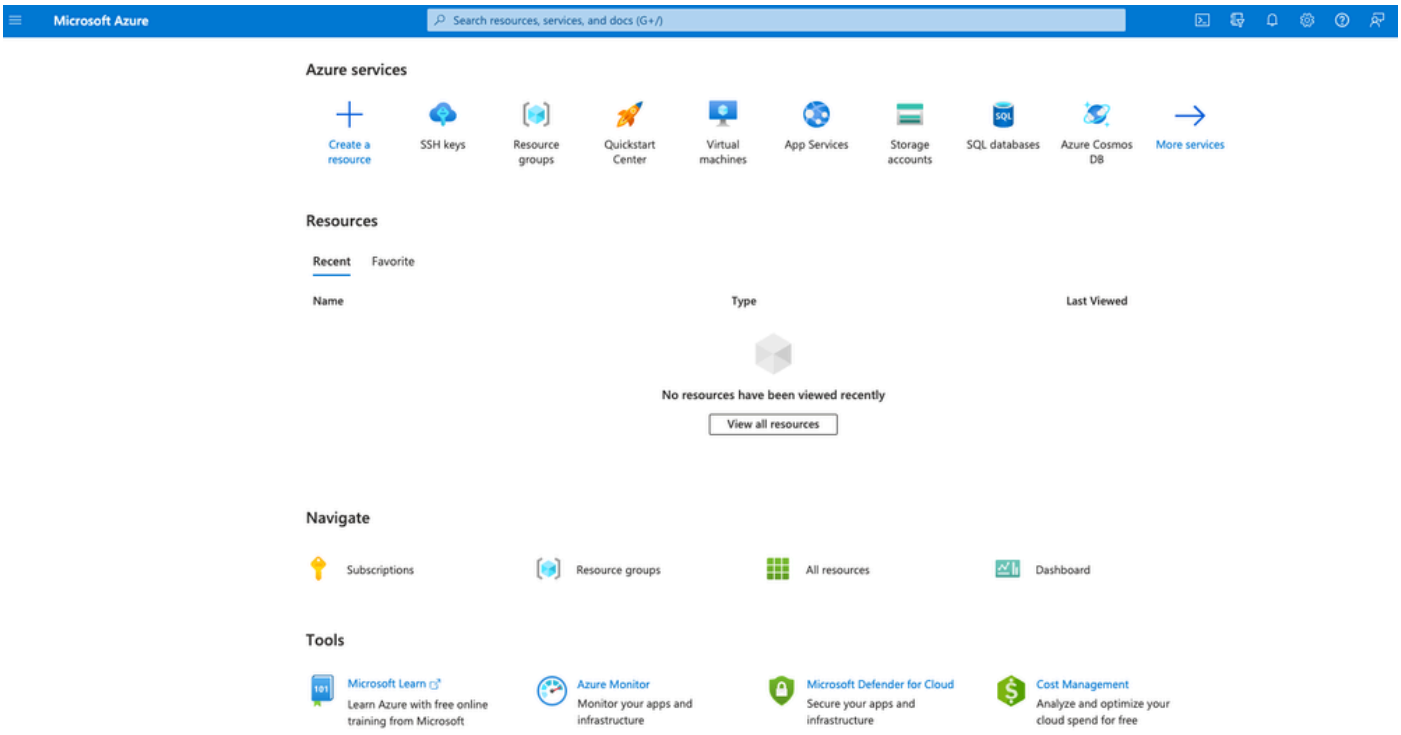
配置

连接到Azure云的ISE部署示例

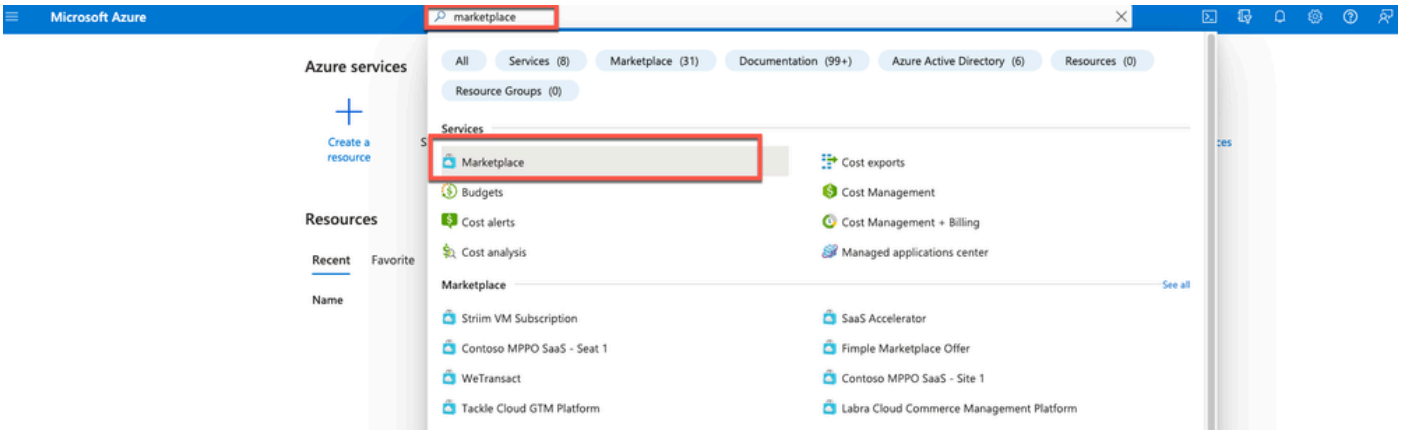


配置

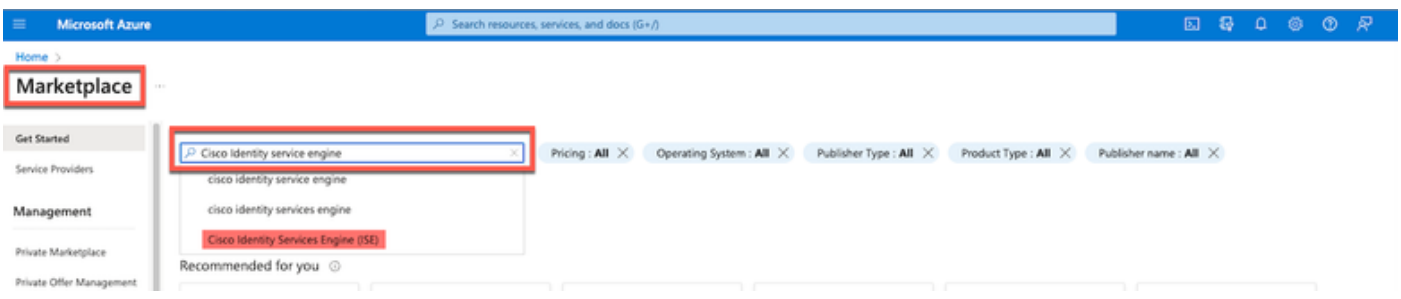
1.导航到Azure Portal并登录到您的Microsoft Azure帐户。



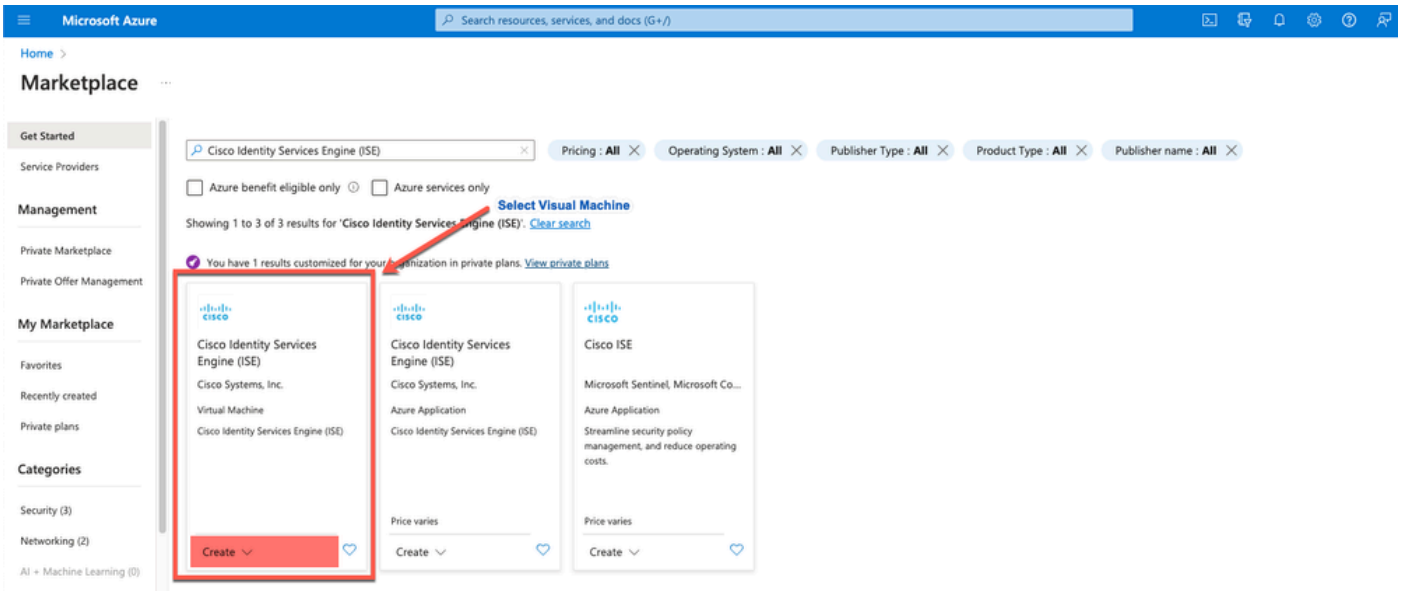
2.使用窗口顶部的搜索字段搜索Marketplace。



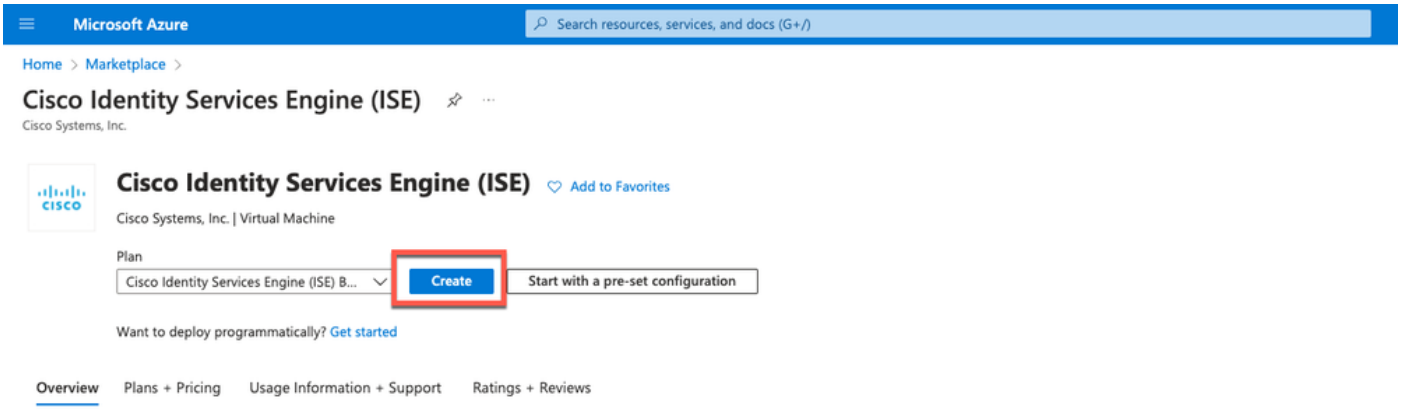
3.使用Search the Marketplace搜索字段搜索思科身份服务引擎(ISE)。



4.单击Virtual Machine。



5.在新窗口中，单击创建。



6.在基础知识选项卡中：

- 在Project details区域中，从Subscription和Resource Group下拉列表中选择所需的值。
- 在实例详细信息区域中，在虚拟机名称字段中输入值。
- 从Image下拉列表中，选择Cisco ISE Image。
- 从Size下拉列表中，选择要安装思科ISE的实例大小。选择思科ISE支持的实例，如标题为Azure Cloud的表所列。

思科ISE支持的实例列在Azure云上的思科ISE部分。

e.在Administrator Account > Authentication type区域中，单击SSH Public Key单选按钮。

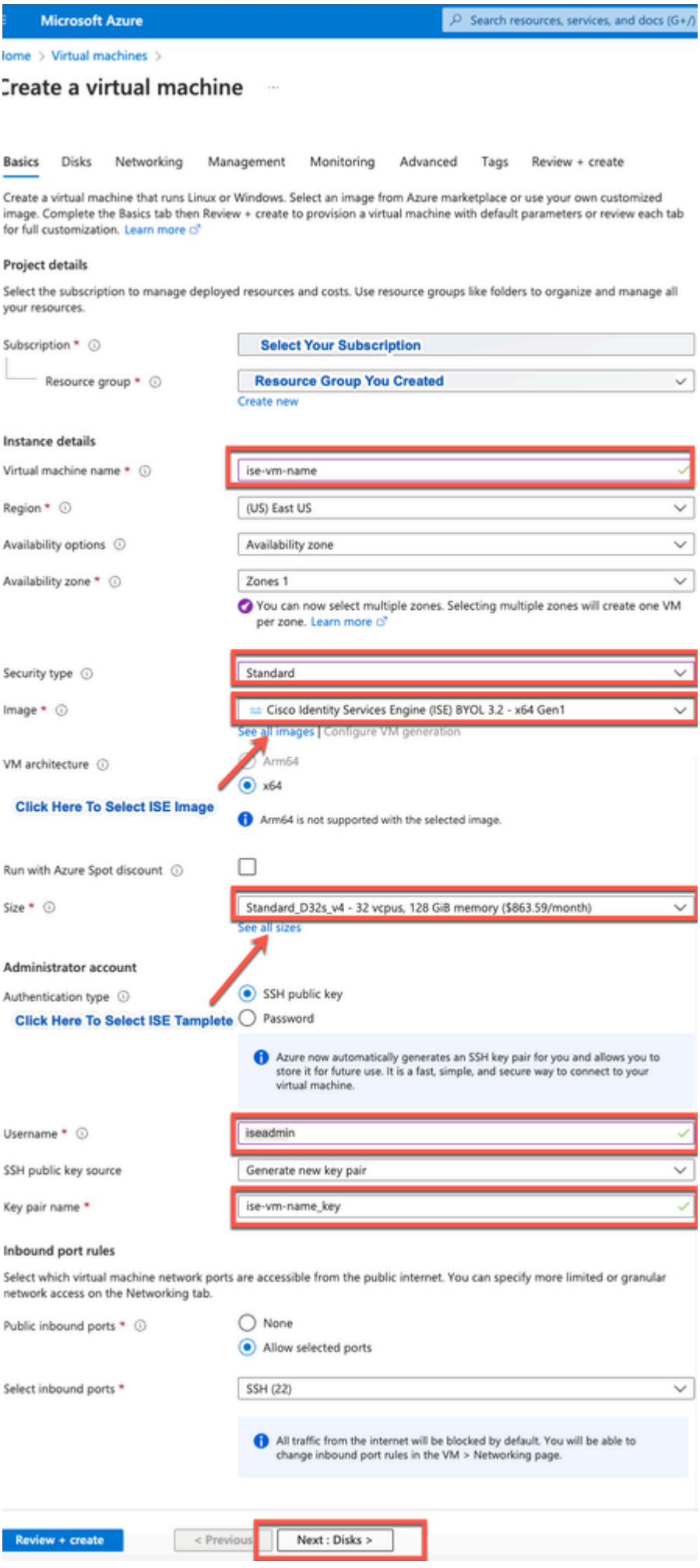
f. 在Username字段中，输入iseadmin。

g.从SSH公钥源下拉列表中，选择使用存储在Azure中的现有密钥。

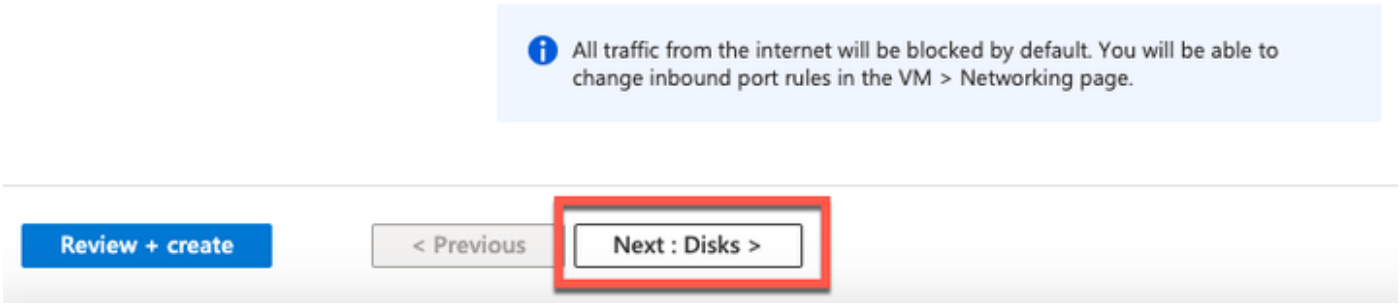
h.从Stored keys下拉列表中，选择您创建作为此任务前提条件的密钥对。

j. 在Inbound port rules区域中，点击Allow selected ports单选按钮。

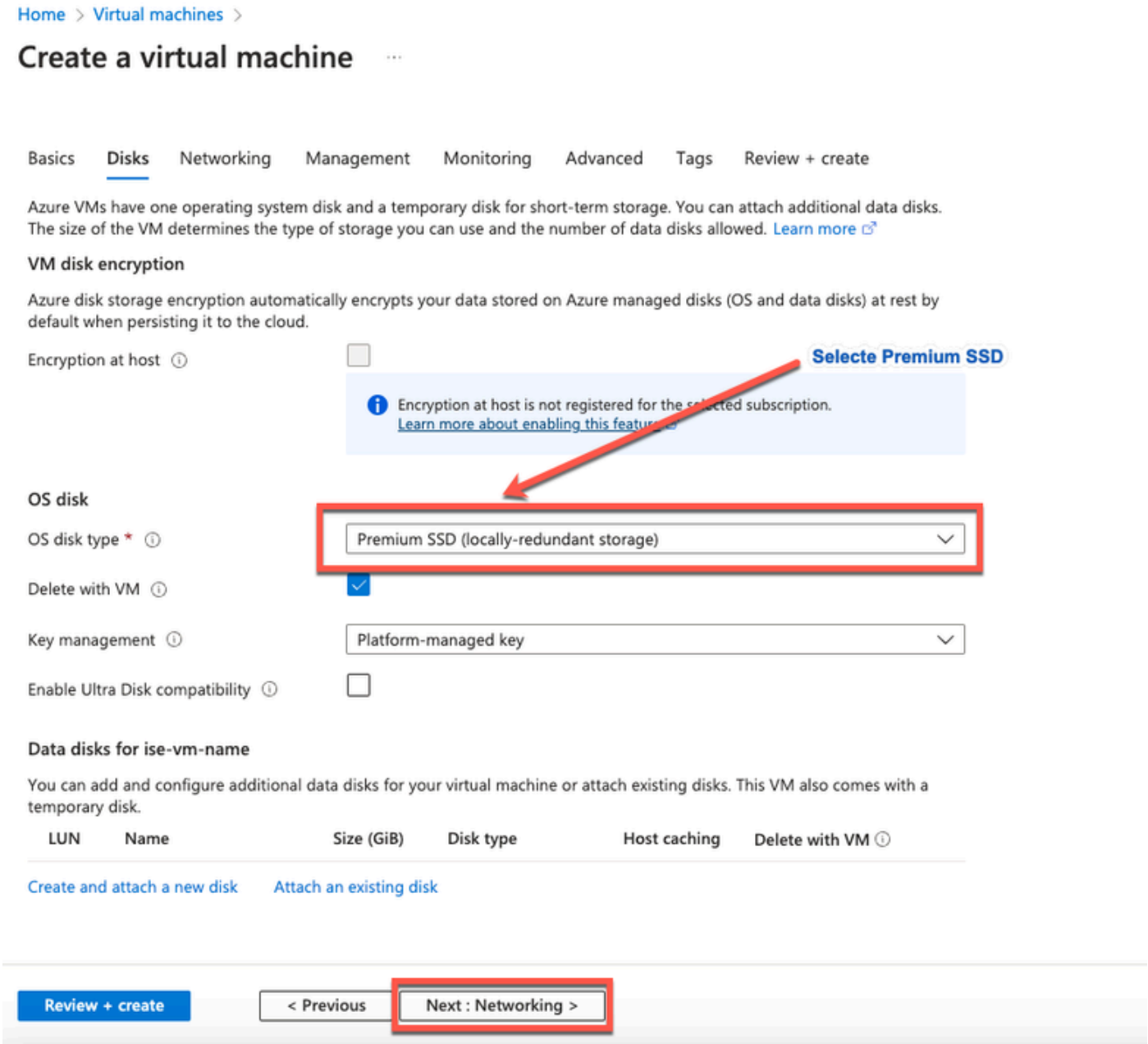
k.在Licensing区域中，从Licensing type下拉列表中选择Other。


Microsoft Azure
Search resources, services, and docs (G+/)
lome > 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
Click Here To Select ISE Image
Arm64 is not supported with the selected 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 Tamplete
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 *
iseadmin
SSH public key source
Generate new key pair
Key pair name *
ise-vm-name_key
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 *
SSH (22)
All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.
Review + create
< Previous
Next : Disks >

7.单击下一步：磁盘。



8.在磁盘选项卡中，保留必填字段的默认值，然后单击下一步：网络.

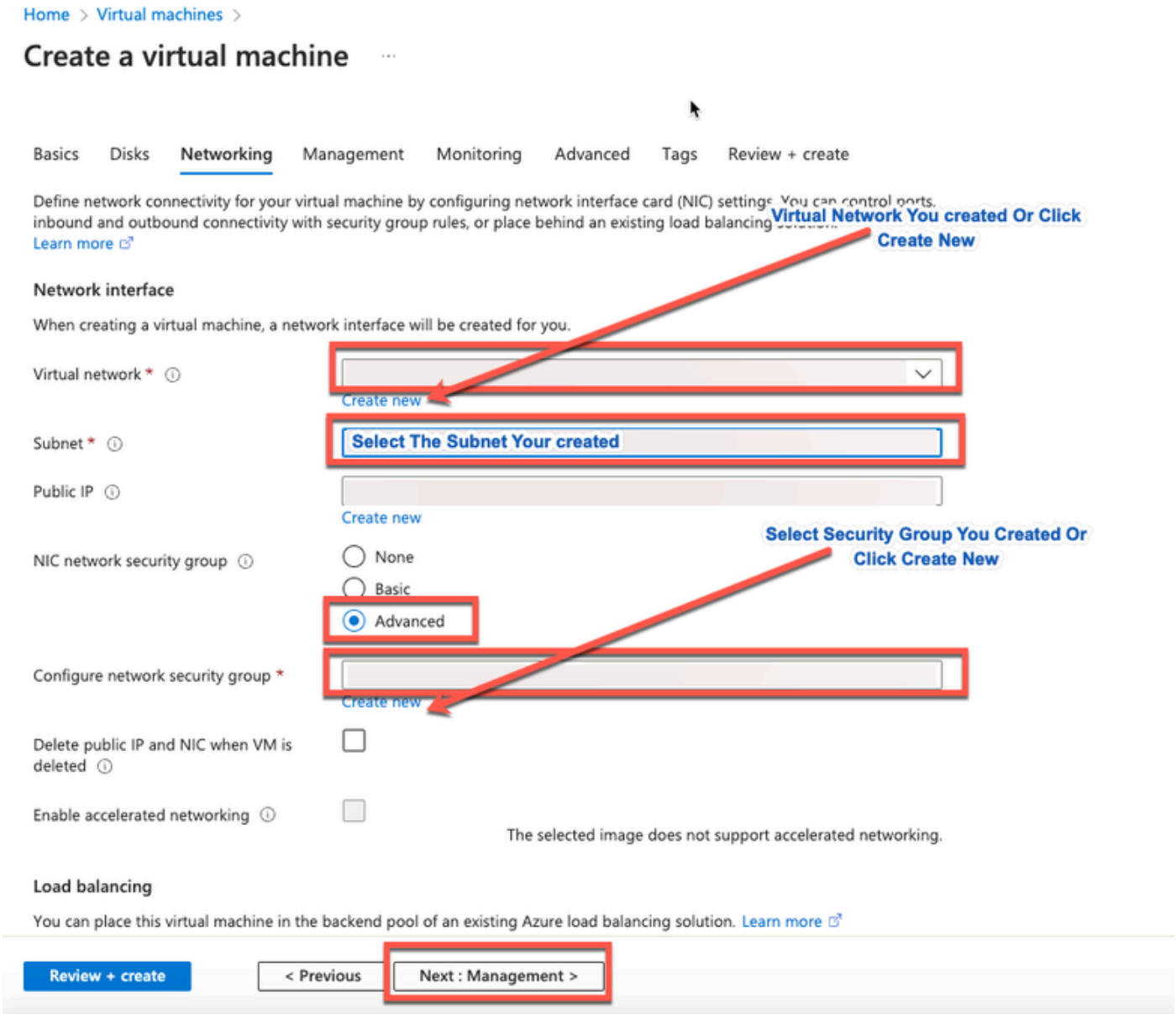


注意：对于“磁盘类型”(Disk Type)，可从下拉列表中选择更多选项。您可以选择符合您需求的产品。对于生产和性能敏感型工作负载，推荐使用高级SSD类型。

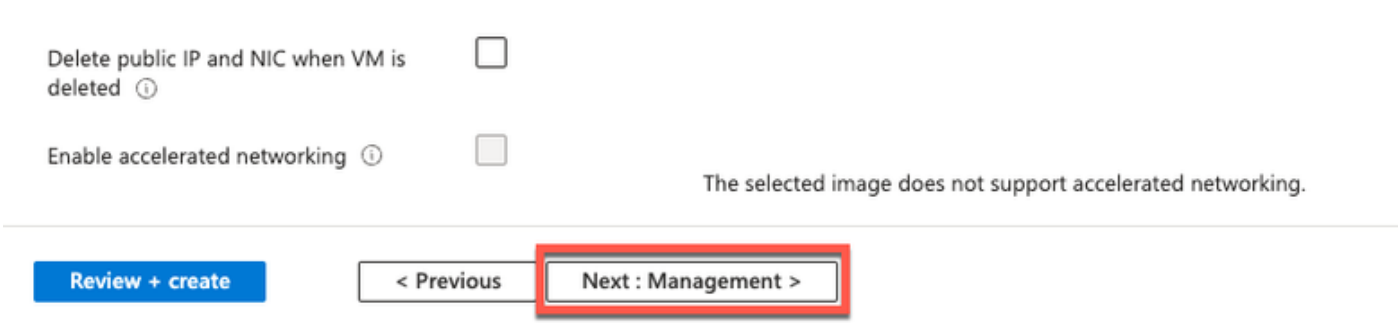
9.在Network Interface区域中，从Virtual Network、Subnet和Configure Network Security Group下拉列表中选择创建的虚拟网络和子网。

注意：具有公有IP地址的子网接收在线和离线状态源更新，而具有私有IP地址的子网仅接收

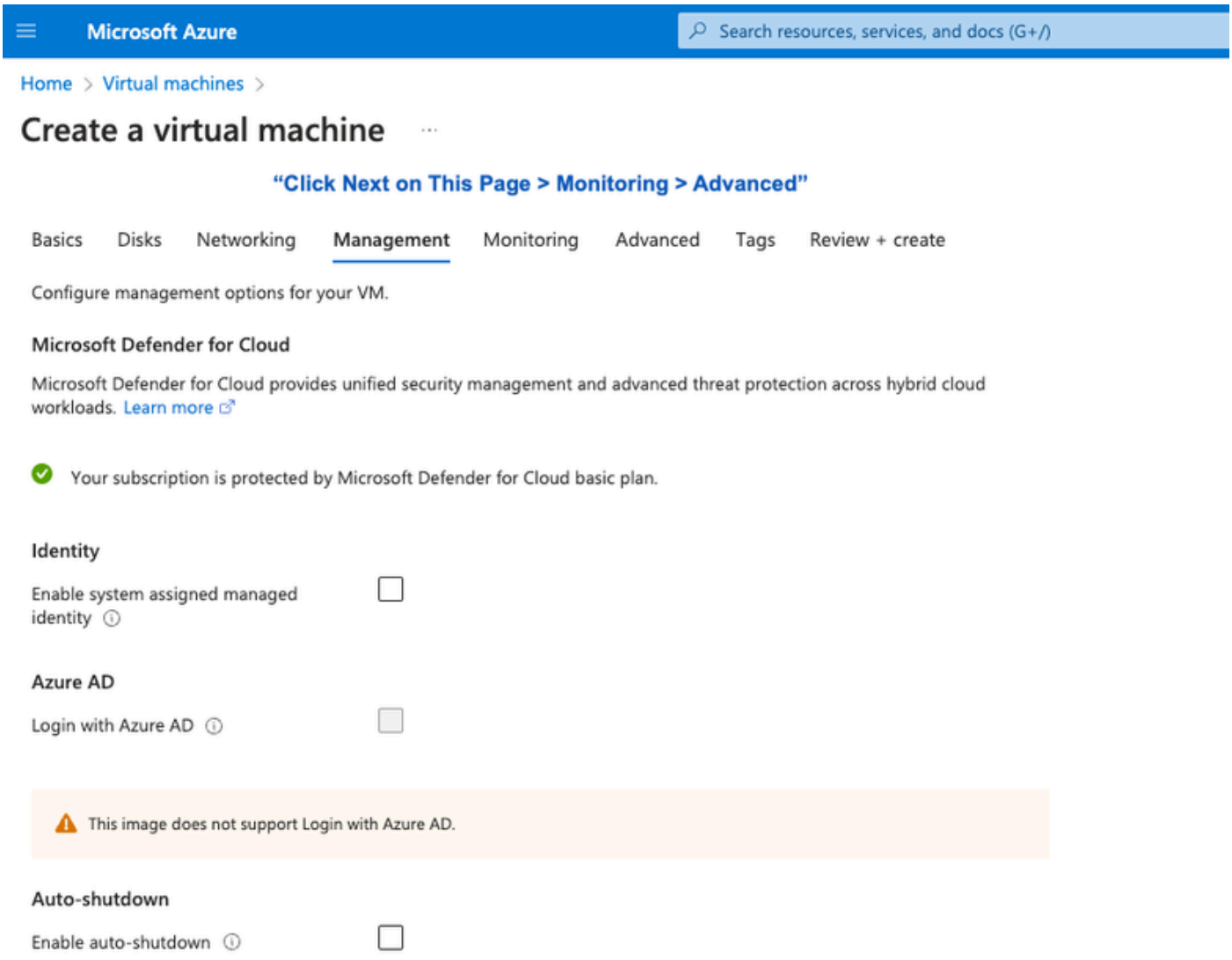
离线状态源更新。

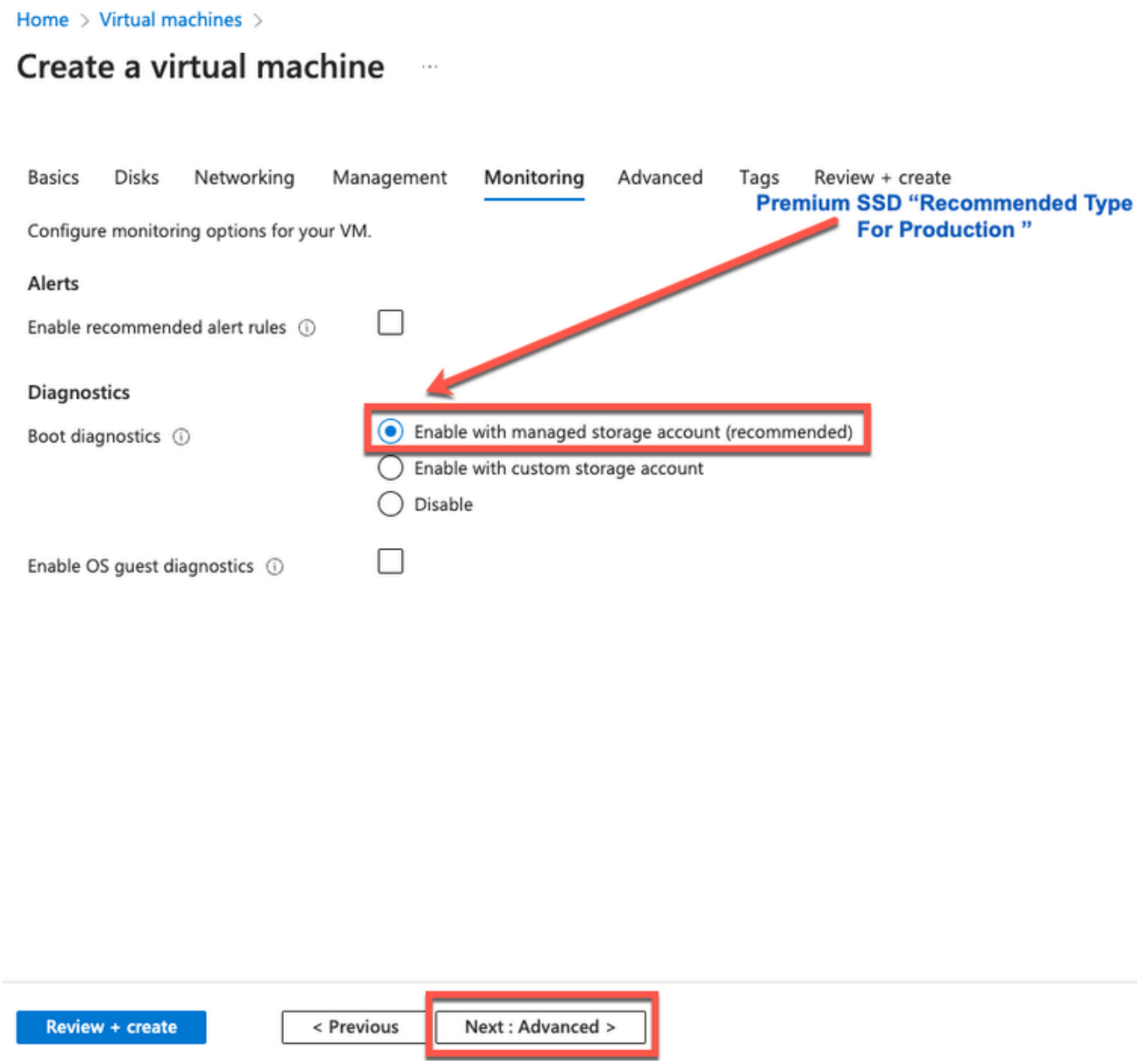


10.单击下一步：管理.



11.在管理选项卡中，保留必填字段的默认值，然后点击下一步：高级.





12.在User Data区域中，选中Enable User Data复选框。

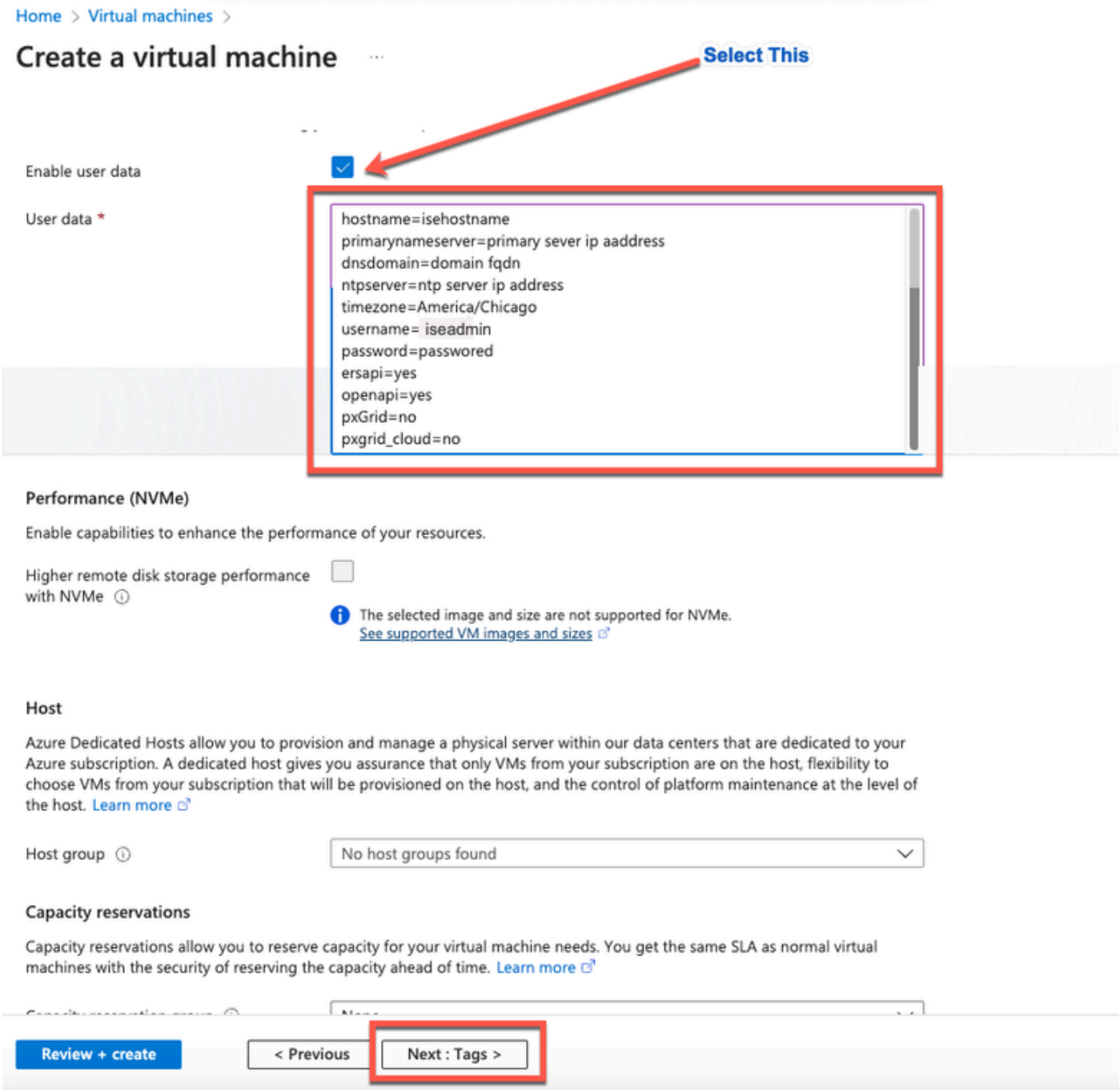
- 在用户数据字段中，填写以下信息：
  - hostname=<Cisco ISE的主机名>
  - primarynameserver=<IPv4地址>
  - dnsdomain=<域名>
  - ntpserver=<IPv4地址或NTP服务器的FQDN>
  - timezone=<timezone>
  - password=<password>
  - ersapi=<是/否>
  - openapi=<yes/no>
  - pxGrid=<yes/no>
  - pxgrid_cloud=<yes/no>

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。您在“用户数据”字段中输入的信息在输入时不经过验证。如果您使用错误的语法，思科ISE服务在您启动映像时不会加载。

从Cisco ISE版本3.4,ntpserver字段名称更改为primaryntpserver。如果使用ntpserver，思科ISE服务无法启动。默认情况下，OpenAPI处于启用状态，因此openapi=<yes/no>字段不是必填项。如果将secondarynameserver字段留空且仅使用tertiarynameserver字段，则思科ISE服务无法启动。如果将secondaryntpserver字段留空且仅使用tertiaryntpserver字段，则思科ISE服务无法启动。

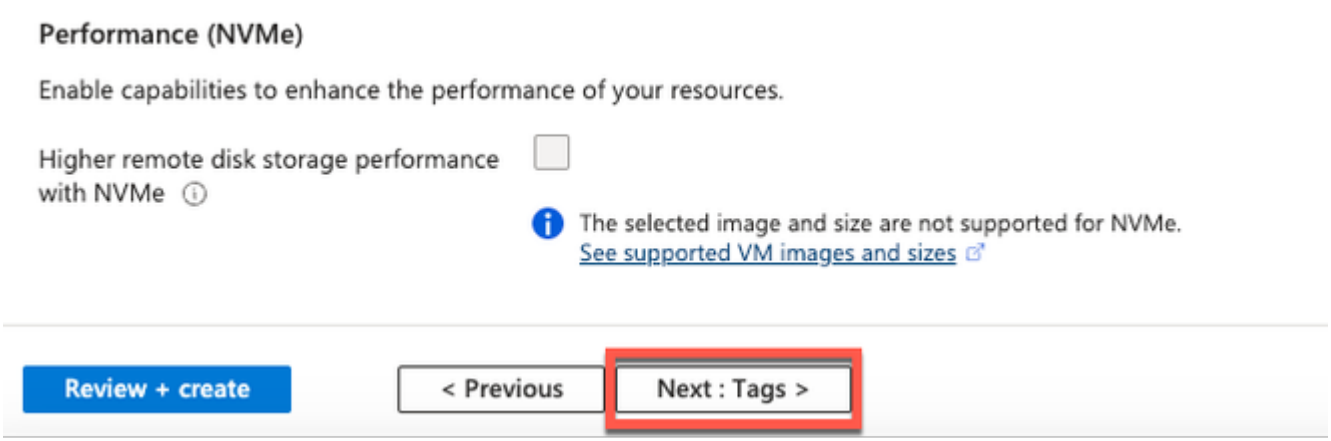
有关必须通过user data字段提交的配置，请参阅准则:

- 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，且不能包含下划线(_)。
- 主名称服务器：输入主域名服务器的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。
- dnsdomain:输入DNS域的FQDN。条目可以包含ASCII字符、数字、连字符(-)和句点(.)。
- 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，因为这是ISE操作所必需的。
- 时区:输入时区，例如EST/UTC。建议将所有思科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。此过程可确保始终同步来自部署中各个节点的报告和日志的时间戳。
- password：为基于GUI的登录思科ISE配置密码。您输入的密码必须符合思科ISE密码策略。密码必须包含6到25个字符，并且至少包含一个数字、一个大写字母和一个小写字母。密码不能与用户名相同，也不能与用户名相反（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”部分，了解您的版本。
- ersapi:输入yes以启用ERS，或输入no以禁止ERS。
- openapi:输入yes以启用OpenAPI，或输入no以禁止OpenAPI。
- pxGrid:输入yes以启用pxGrid，或输入no以禁用pxGrid。
- pxgrid_cloud:输入yes以启用pxGrid云，或输入no以禁用pxGrid云。要启用pxGrid云，必须启用pxGrid。如果禁用pxGrid，但启用pxGrid云，则在启动时不会启用pxGrid云服务。

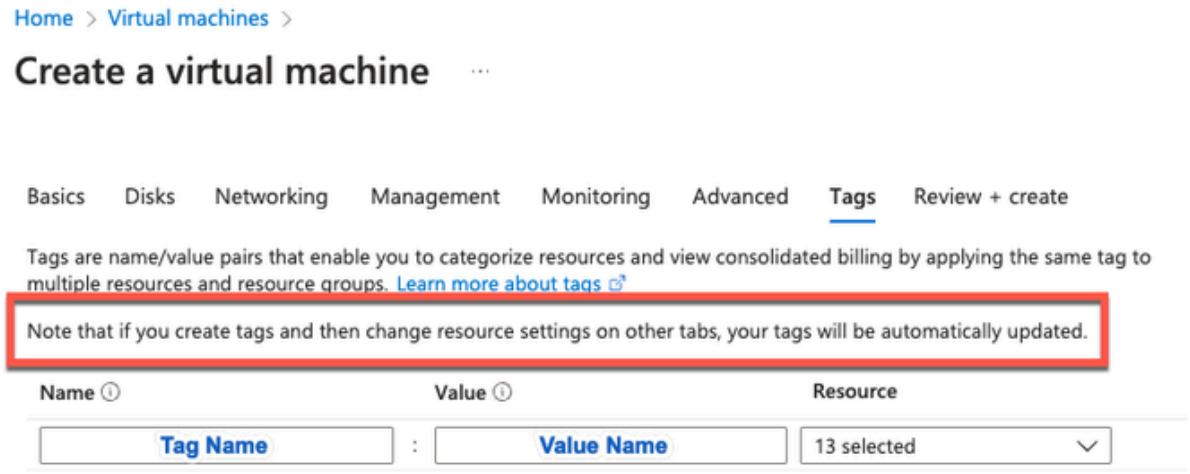


用户数据部分

13.单击下一步：标签.



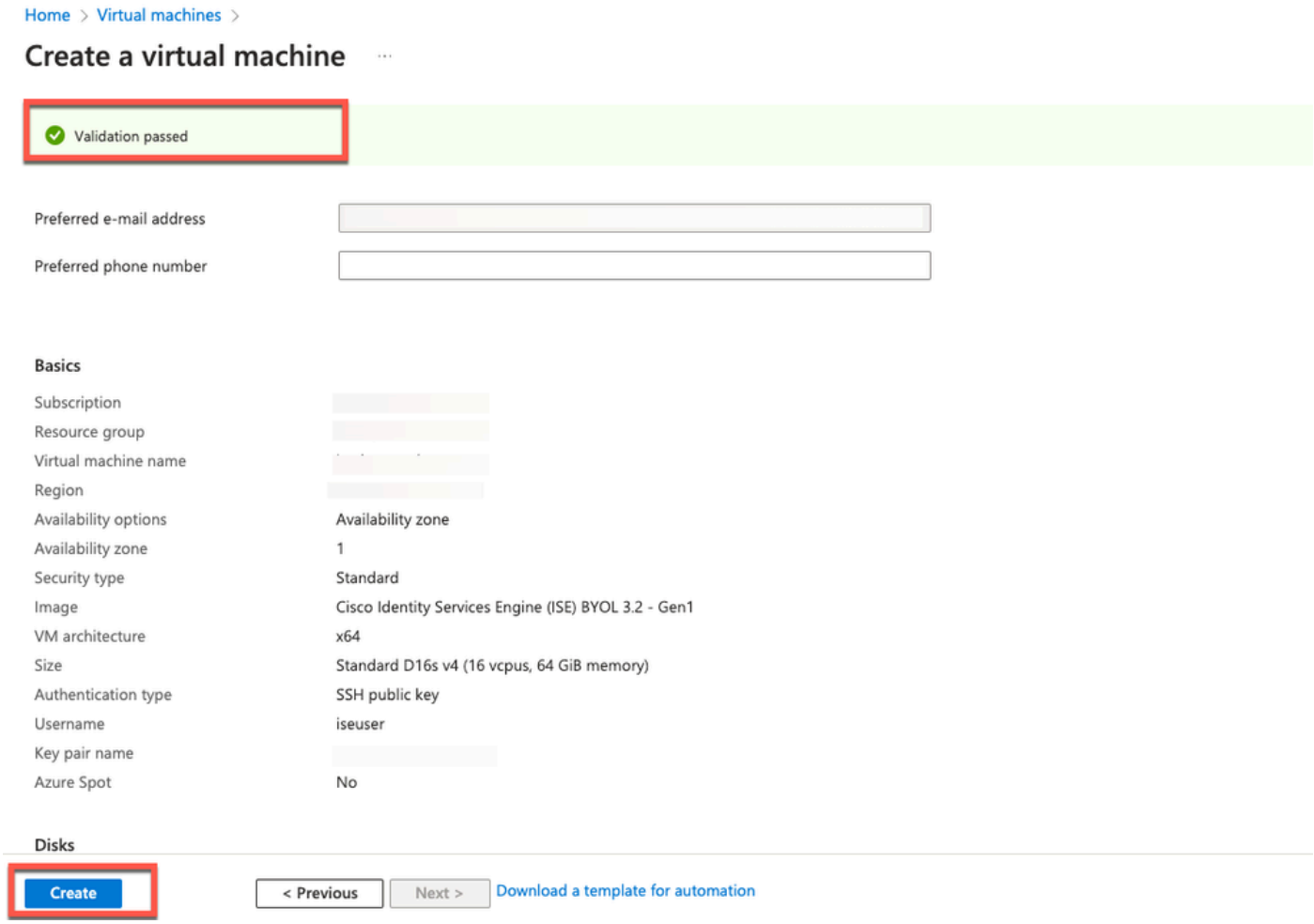
14.创建名称 — 值对，使您可以对资源进行分类，并合并多个资源和资源组；在名称和值字段中输入值。

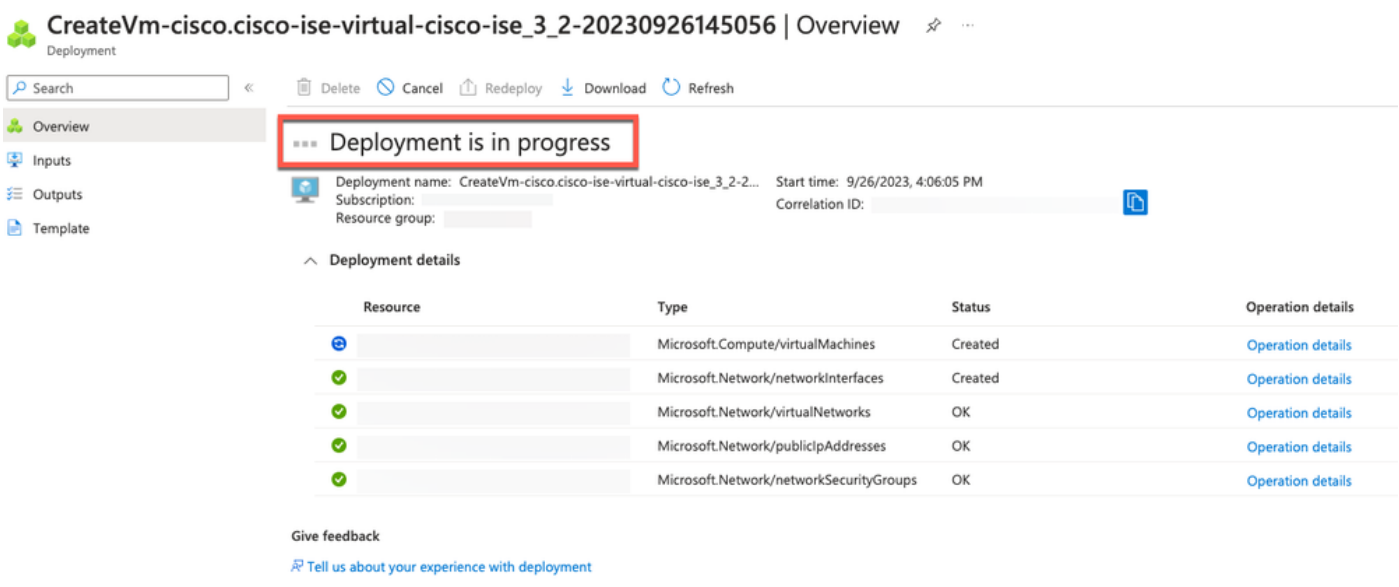


15.单击下一步：审阅+创建。



16.复查到目前为止提供的信息，然后单击创建。此时将显示“部署正在进行”窗口。创建思科ISE实例并可供使用大约需要30分钟。Cisco ISE VM实例显示在Virtual Machines窗口中（使用主搜索字段查找窗口）。



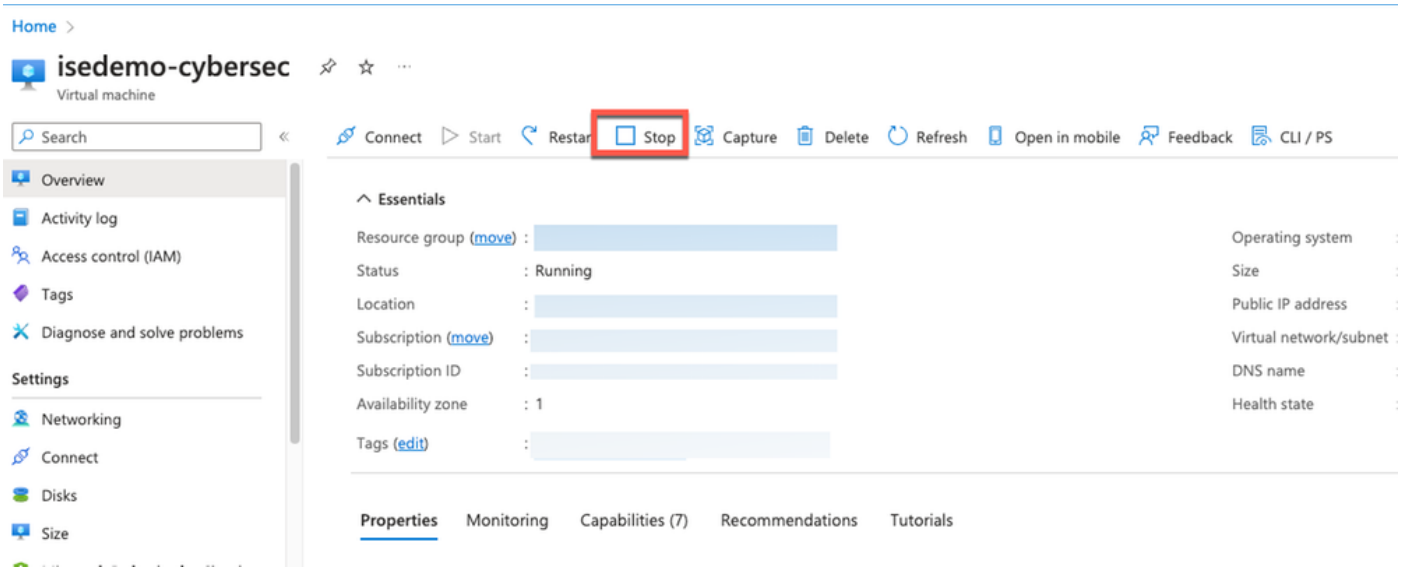


下一步工作

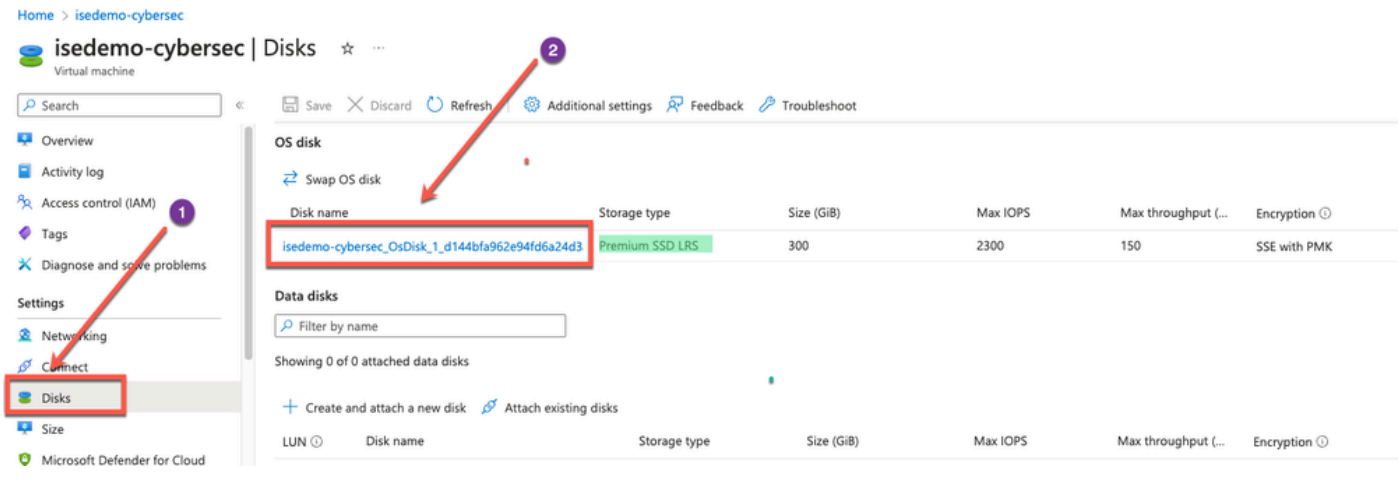
由于Microsoft Azure默认设置，您创建的思科ISE VM仅配置了300 GB磁盘大小。Cisco ISE节点通常需要超过300 GB的磁盘大小。首次从Microsoft Azure启动Cisco ISE时，您可以看到Insufficient Virtual Memory警报。

完成思科ISE VM创建后，登录思科ISE管理门户验证思科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：

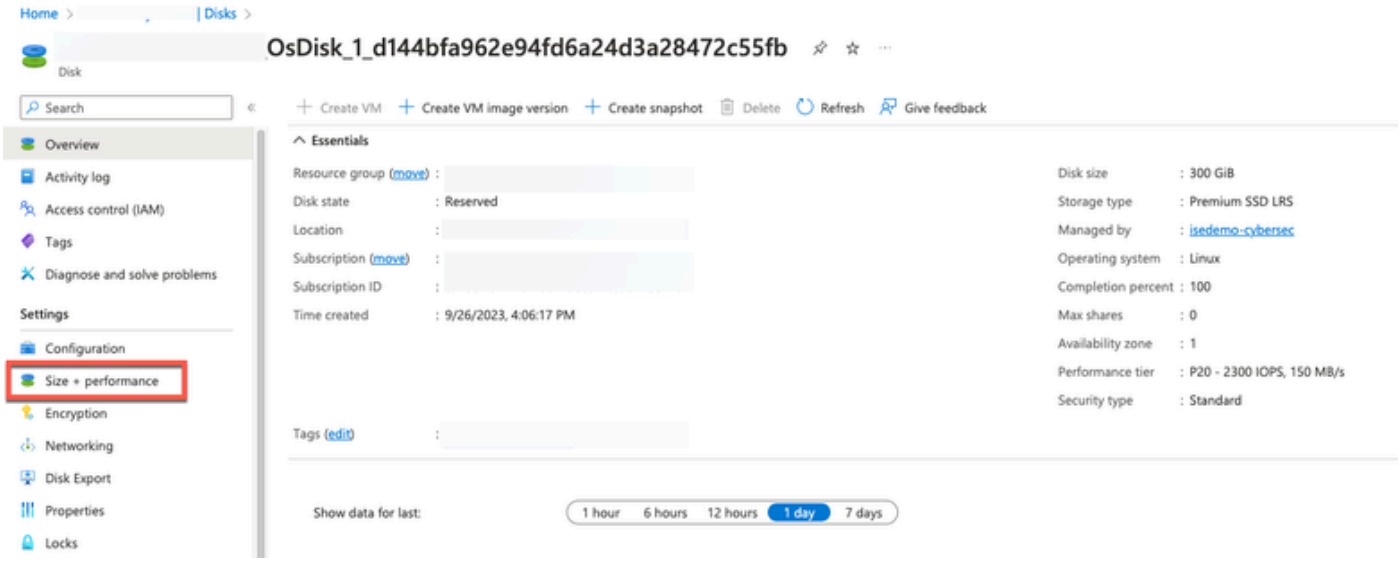
1.停止Cisco ISE实例。



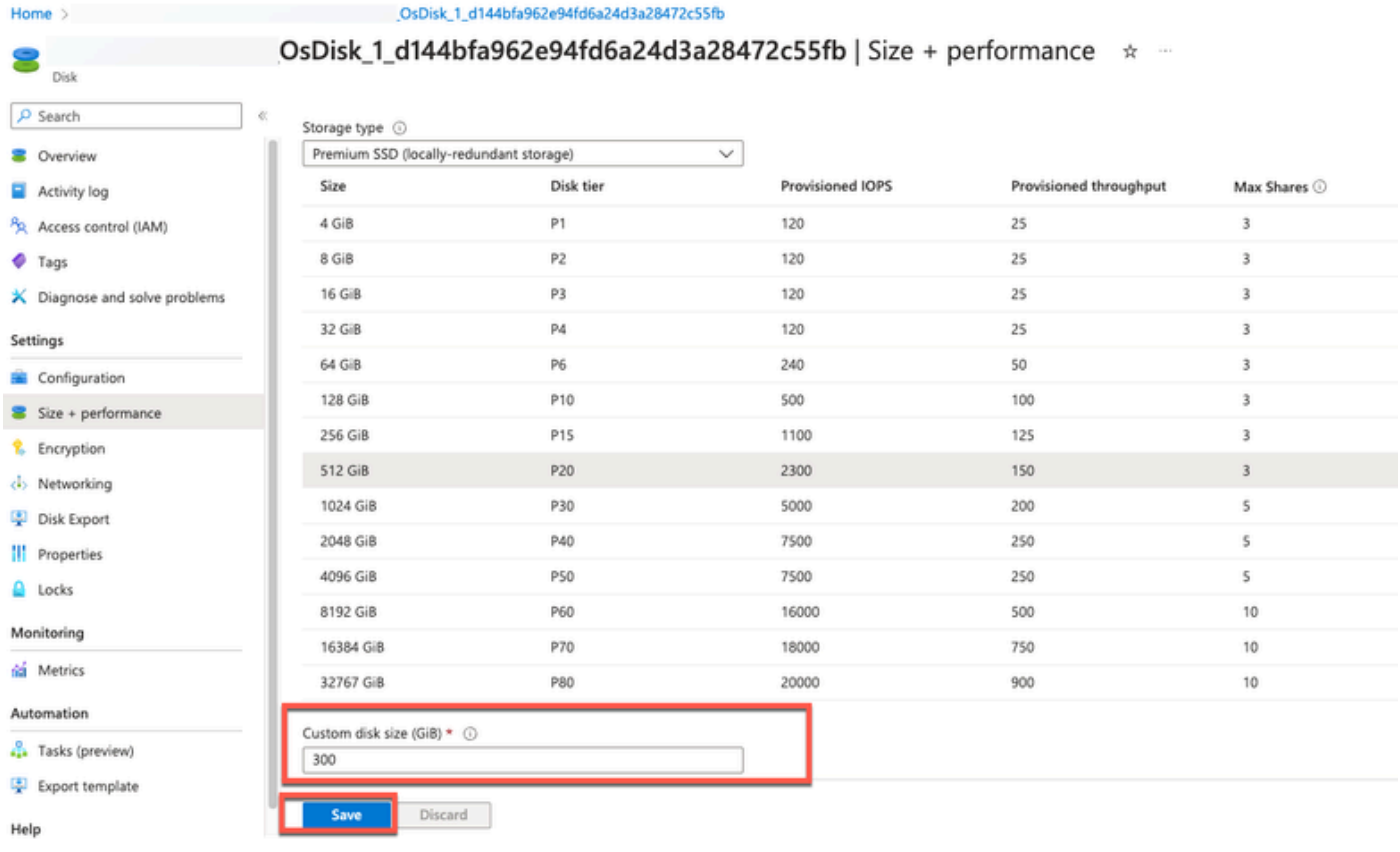
2.点击左侧窗格中的Disk，然后点击您正用于思科ISE的磁盘。



3.单击左侧窗格中的大小+性能。



4.在Custom Disk Size字段中，在GiB中输入所需的磁盘大小。



安装后任务

有关成功创建思科ISE实例后必须执行的安装后任务的信息，请参阅适用于您的思科ISE版本的思科ISE安装指南中的“安装验证和安装后任务”章节。

Azure云上的密码恢复和重置

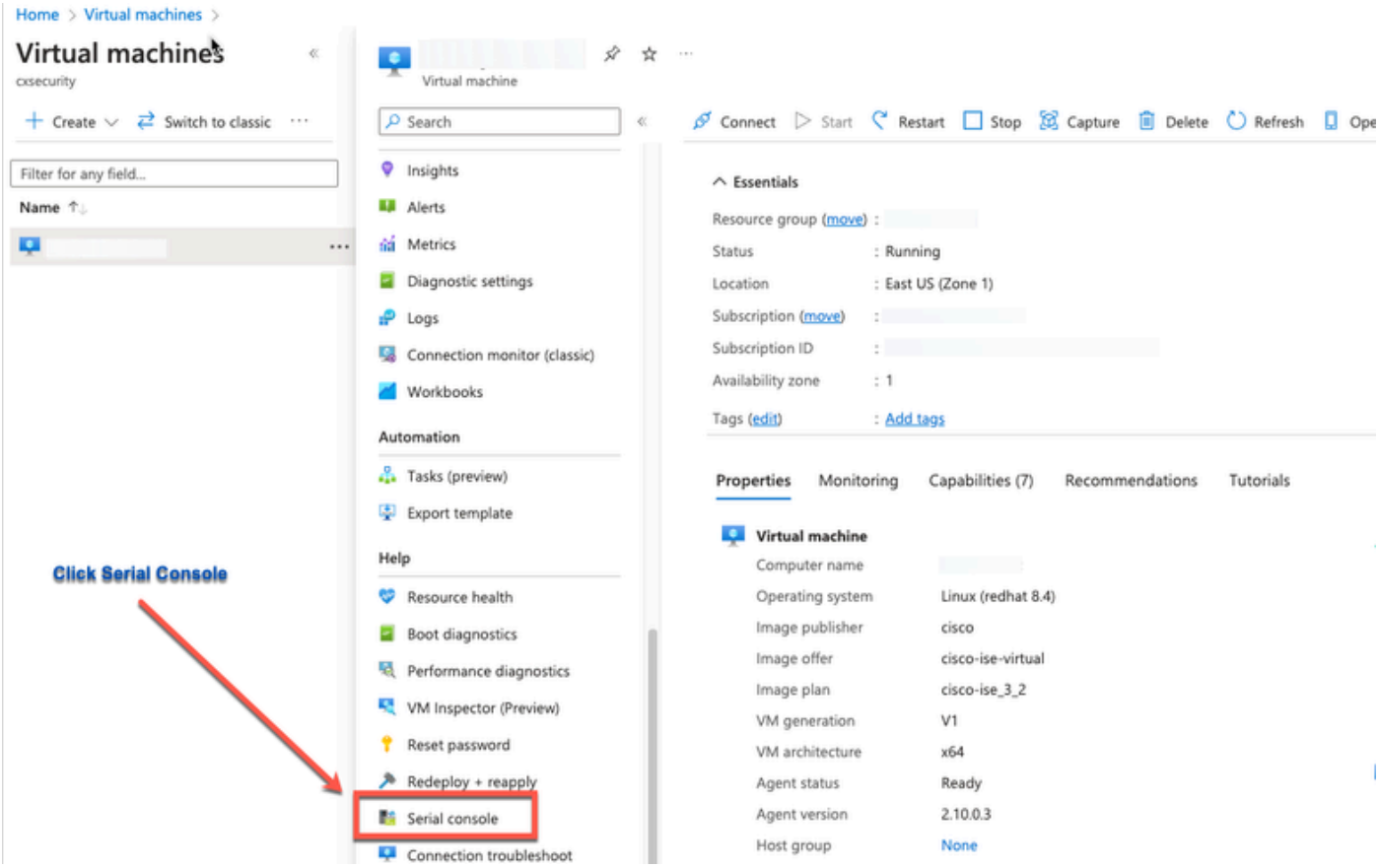
完成帮助您重置或恢复思科ISE虚拟机密码的任务。选择您需要的任务，并执行详细步骤。

通过串行控制台重置思科ISE GUI密码

1.登录到Azure云并选择包含您的思科ISE虚拟机的资源组。

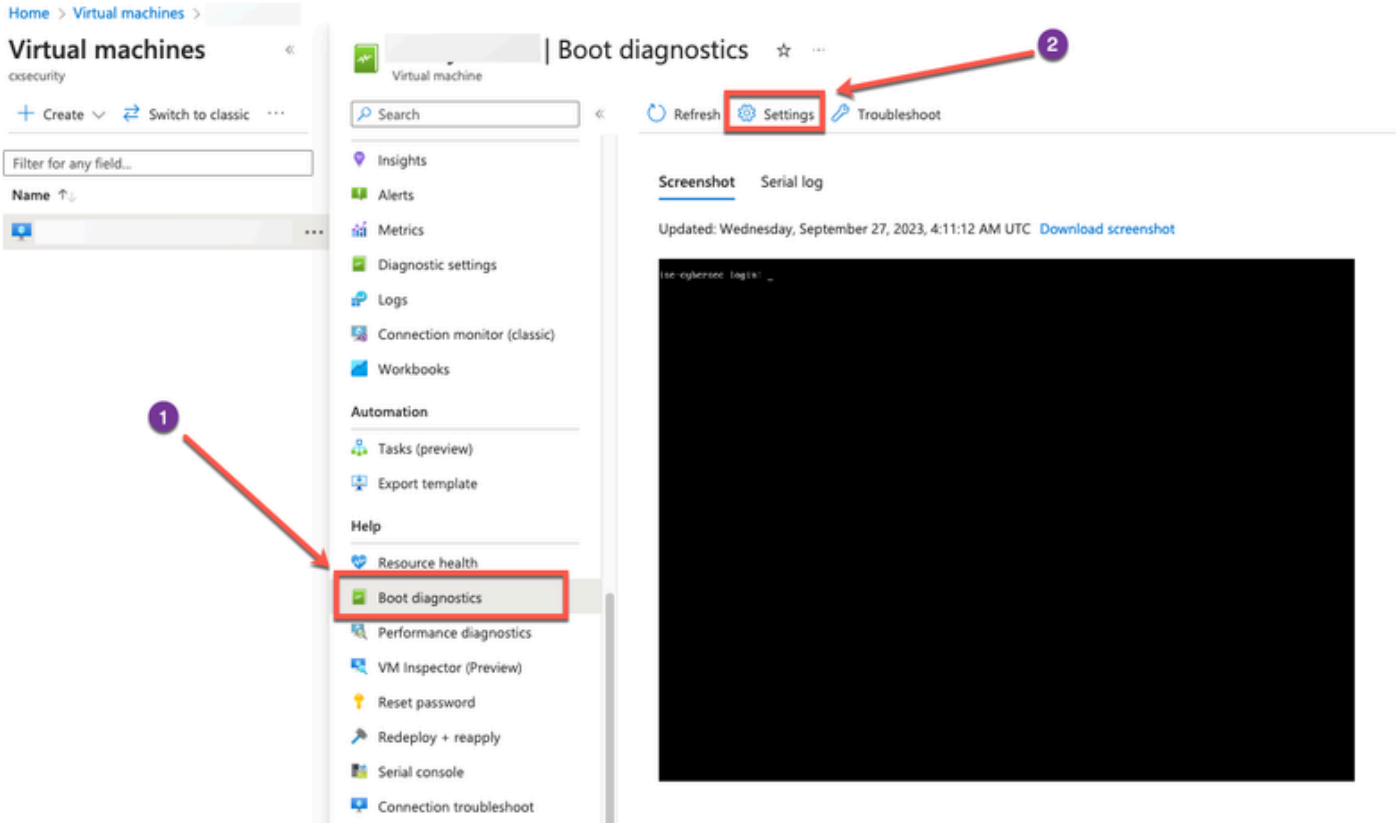
2.从资源列表中，点击要为其重置密码的思科ISE实例。

3.在左侧菜单中，从支持+故障排除部分中，单击串行控制台。

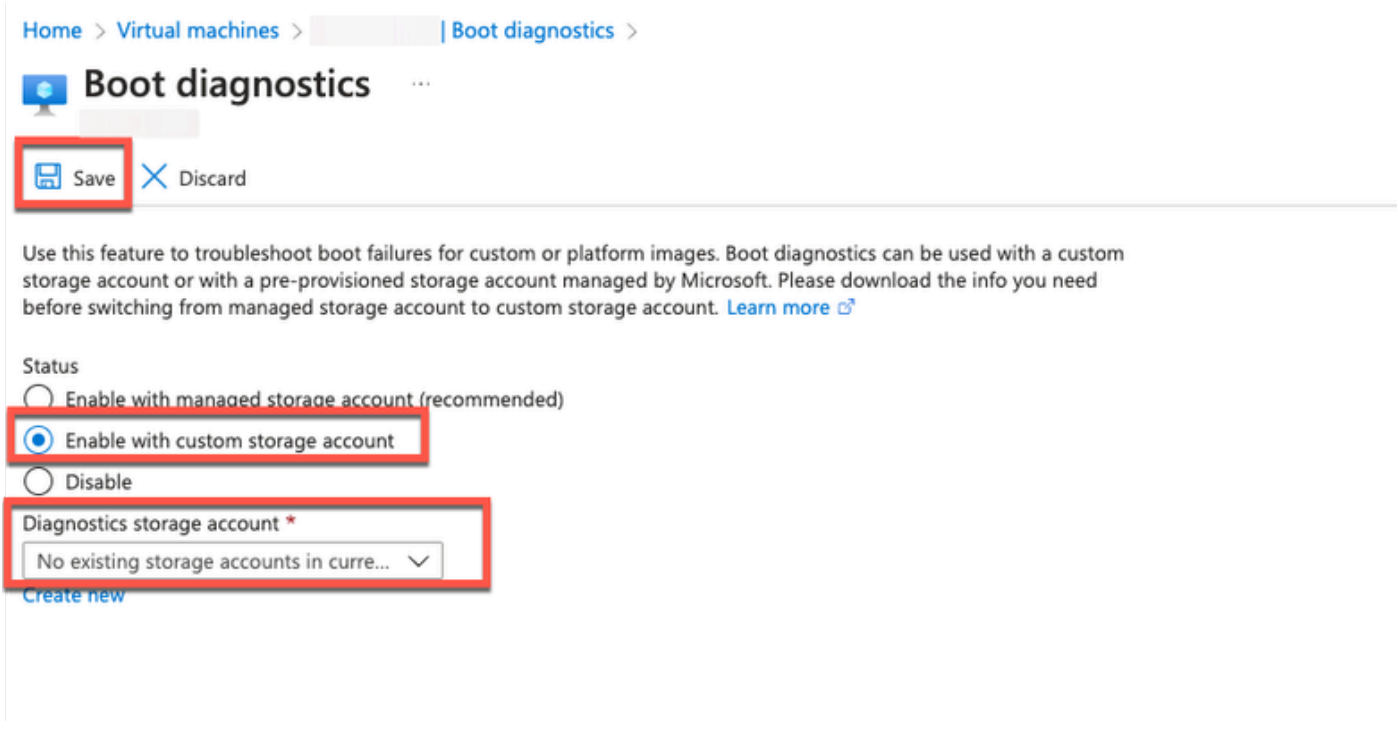


4.如果看到错误消息，您必须执行以下步骤来启用引导诊断：

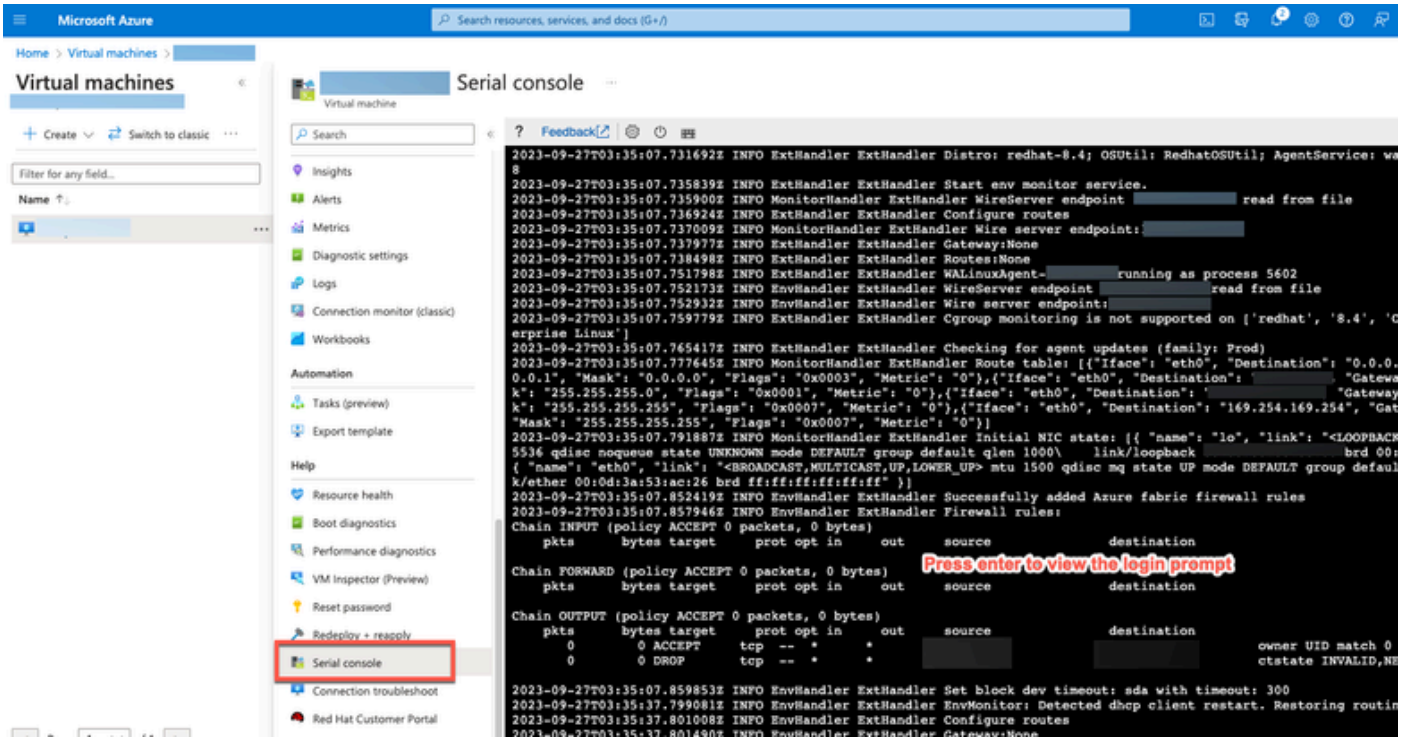
- 从左侧菜单中，单击Boot Diagnostics。



- 点击使用自定义存储帐户启用。Click Save.



5.从左侧菜单的支持+故障排除部分中，单击串行控制台。Azure Cloud Shell在新窗口中显示。如果屏幕为黑色/空白，请按Enter查看登录提示。



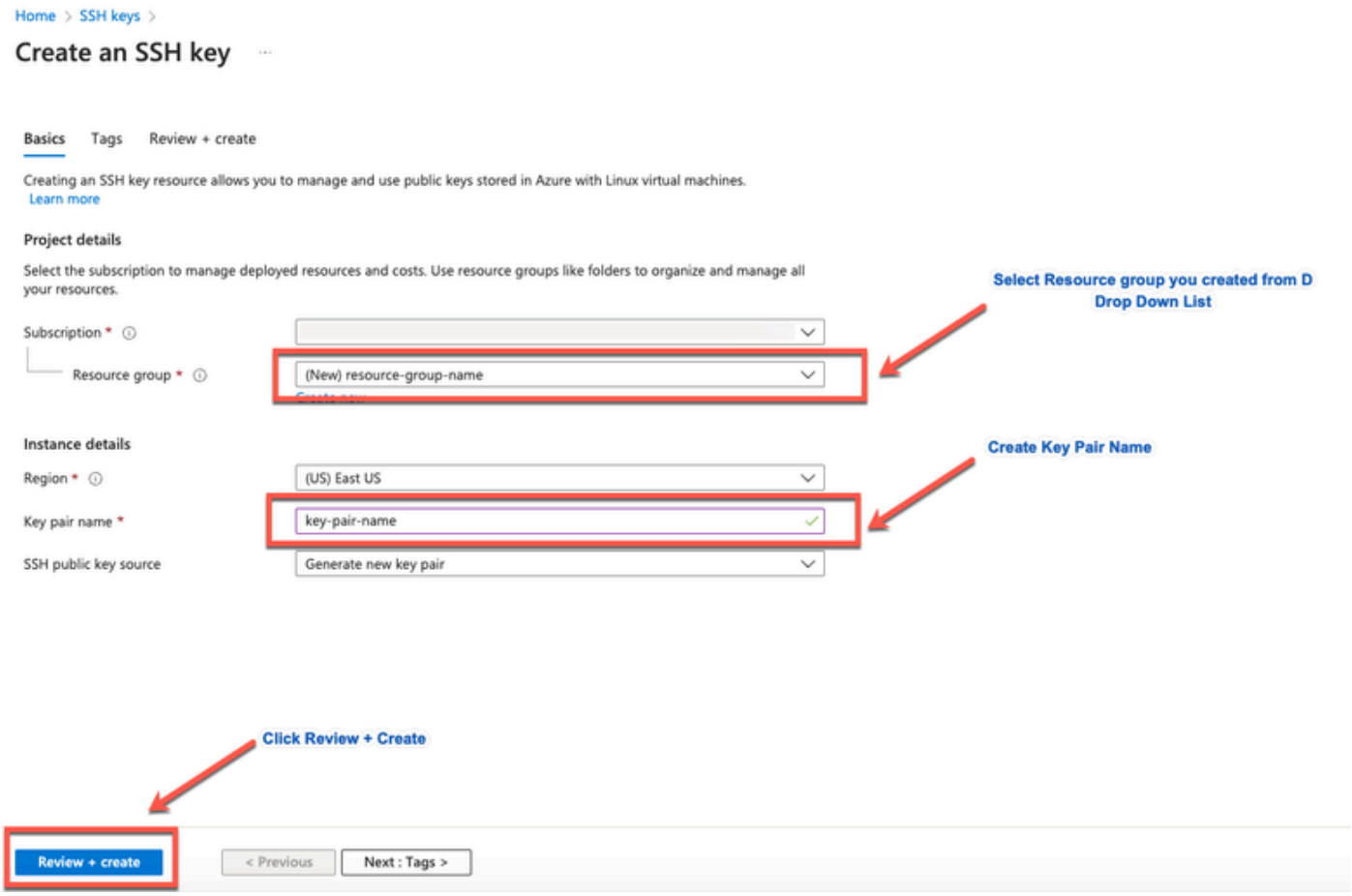
6.登录到串行控制台。要登录串行控制台，必须使用安装实例时配置的原始密码。

7.运行application reset-passwd ise iseadmin命令为iseadmin帐户配置新的GUI密码。

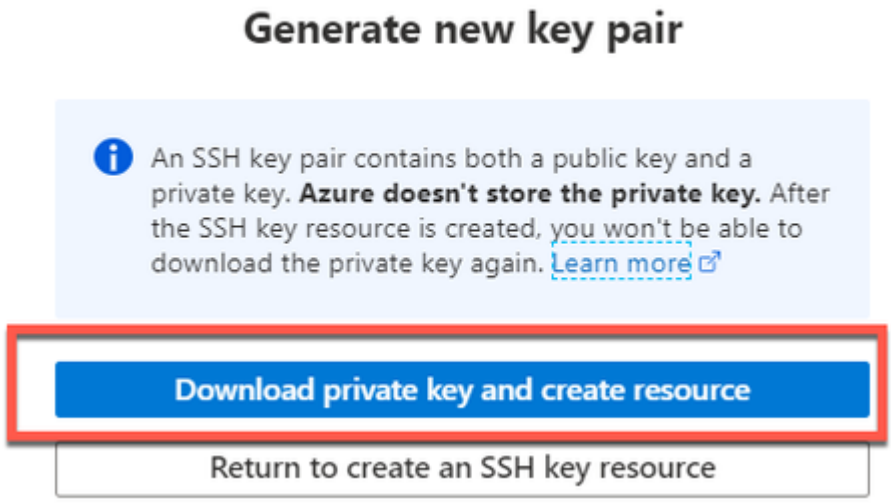
为SSH访问创建新的公钥对

通过此任务，可以向存储库添加其他密钥对。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。

1.在Azure云中创建新公钥。



2.您将收到一个弹出窗口，选择Download Private Key and Create a Resource，以将SSH密钥下载为.pem文件。



3.要创建新的存储库以将公钥保存到，请参阅Azure Repos文档。如果您已经拥有可通过CLI访问的

存储库，请跳到步骤3。

4.要导入新的公钥，请运行crypto key import <public key filename> repository <repository name> 命令。

5.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）。