Install ISE on Azure Cloud Services

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Procedure

- Virtual Network and Security Groups
- Azure VM Sizes Supported by Cisco ISE
- Limitations of Cisco ISE in Microsoft Azure Cloud Services

Configure

- Example of ISE Deployment Connected to Azure Cloud
- Configurations

What to do Next

Post Installation Tasks

Password Recovery and Reset on Azure Cloud

- Create a New Public Key Pairfor SSH Access

Introduction

This document describes how to Install a Cisco ISE IOS® instance using Azure Virtual Machine. Cisco ISE IOS® is available on Azure Cloud Services.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Subscriptions and Resource Groups

Components Used

The information in this document is based on Cisco ISE Version 3.2 and Microsoft Azure Cloud Services.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Procedure

1. Navigate to **All Services > Subscriptions**. Ensure that an Azure account with an active subscription and an enterprise agreement with Microsoft are present.

---

2. Use Microsoft PowerShell Azure module CLI to execute commands to reserve space. You can refer to How to install Azure PowerShell for installing power shell and relevant packages.

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

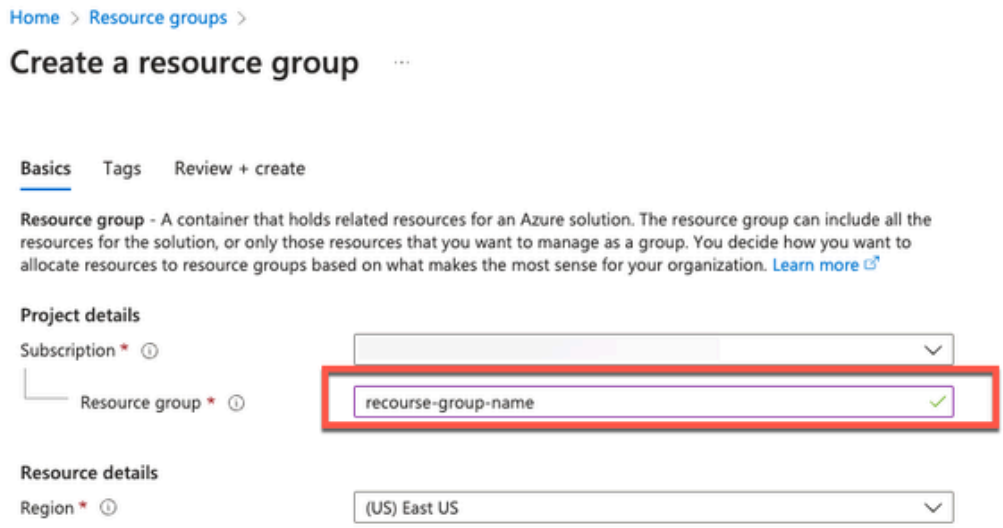
Note: Replace the Tenant ID with your actual Tenant ID.

---

3. Complete the prerequisites at Request host quota for Azure VMware Solution for more details.

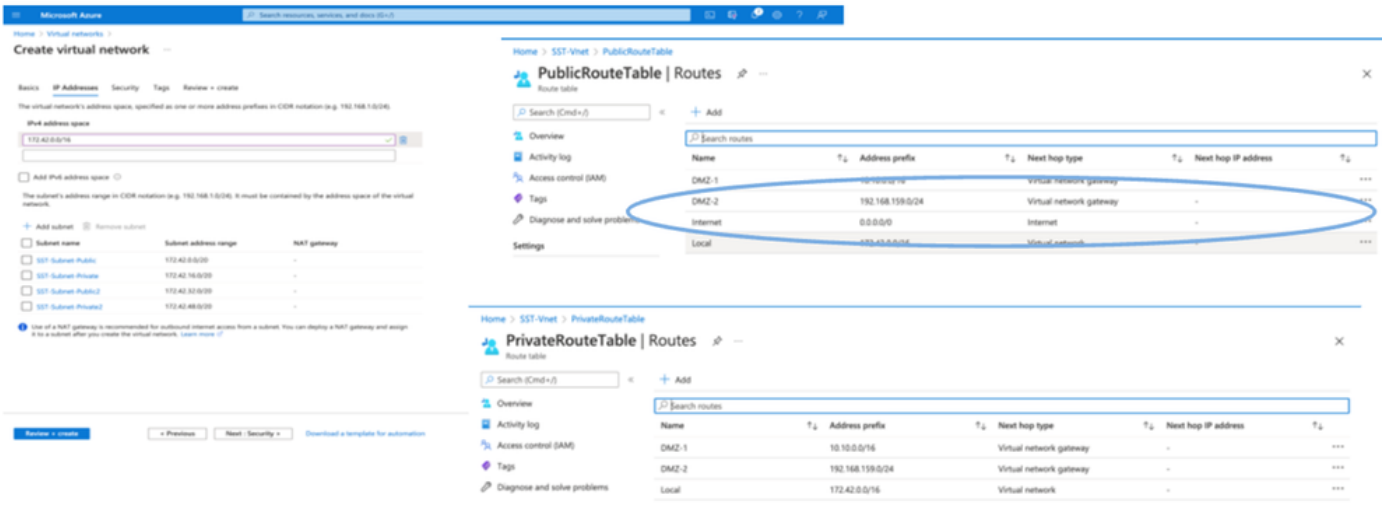
---

4. Create a Resource Group right after subscription. Navigating to **All Services > Resource groups**. Click **Add**. Enter the **Resource group** name.



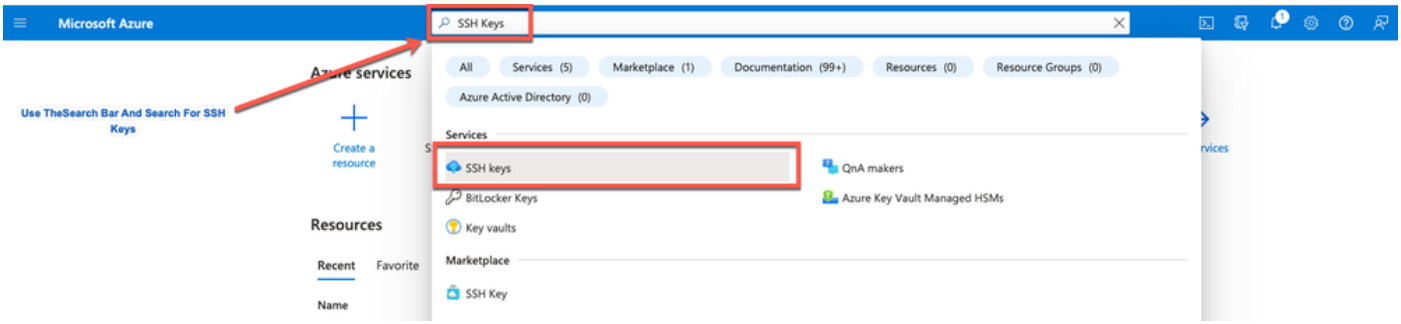
Virtual Network and Security Groups

The Subnet that requires internet reachability must have the route table configured with the next hop as internet. See the examples of public and private subnetwork. PAN with public IP has both offline and online feed update working, while PAN with private IP must rely on offline feed updates.



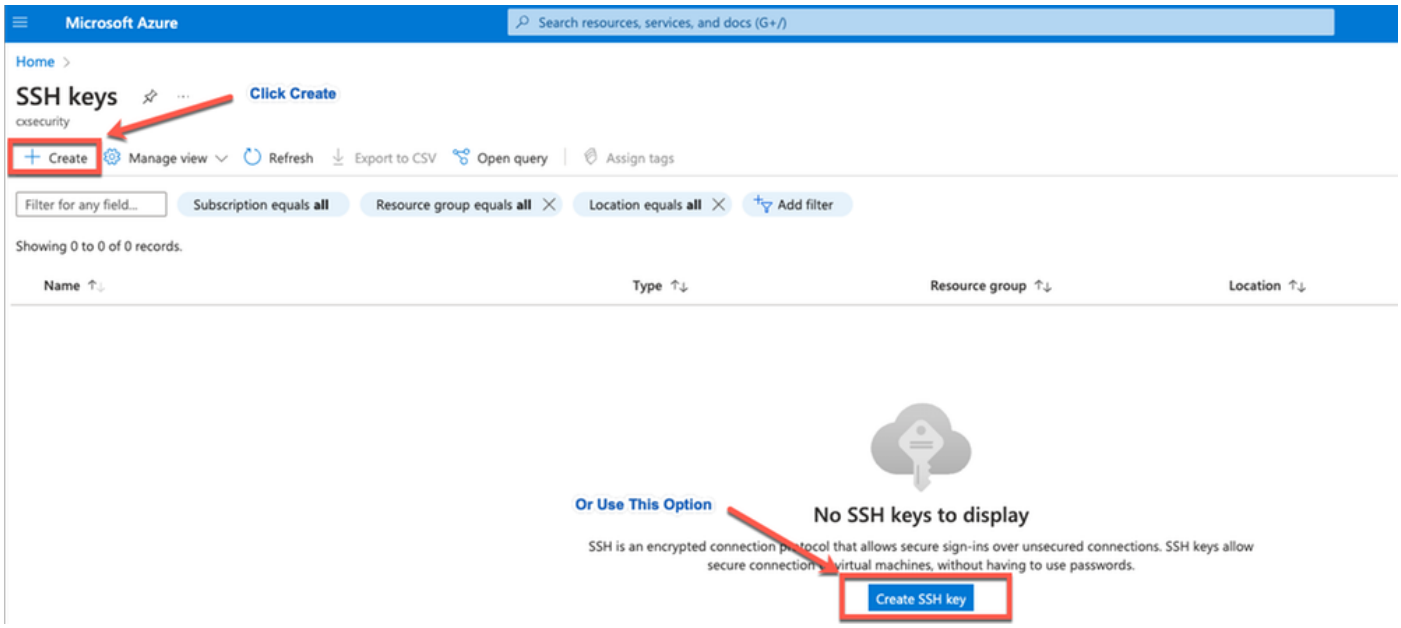
Create an SSH Key Pair

1. Use the search bar from the Azure Web Portal homepage and search for **SSH Keys**.

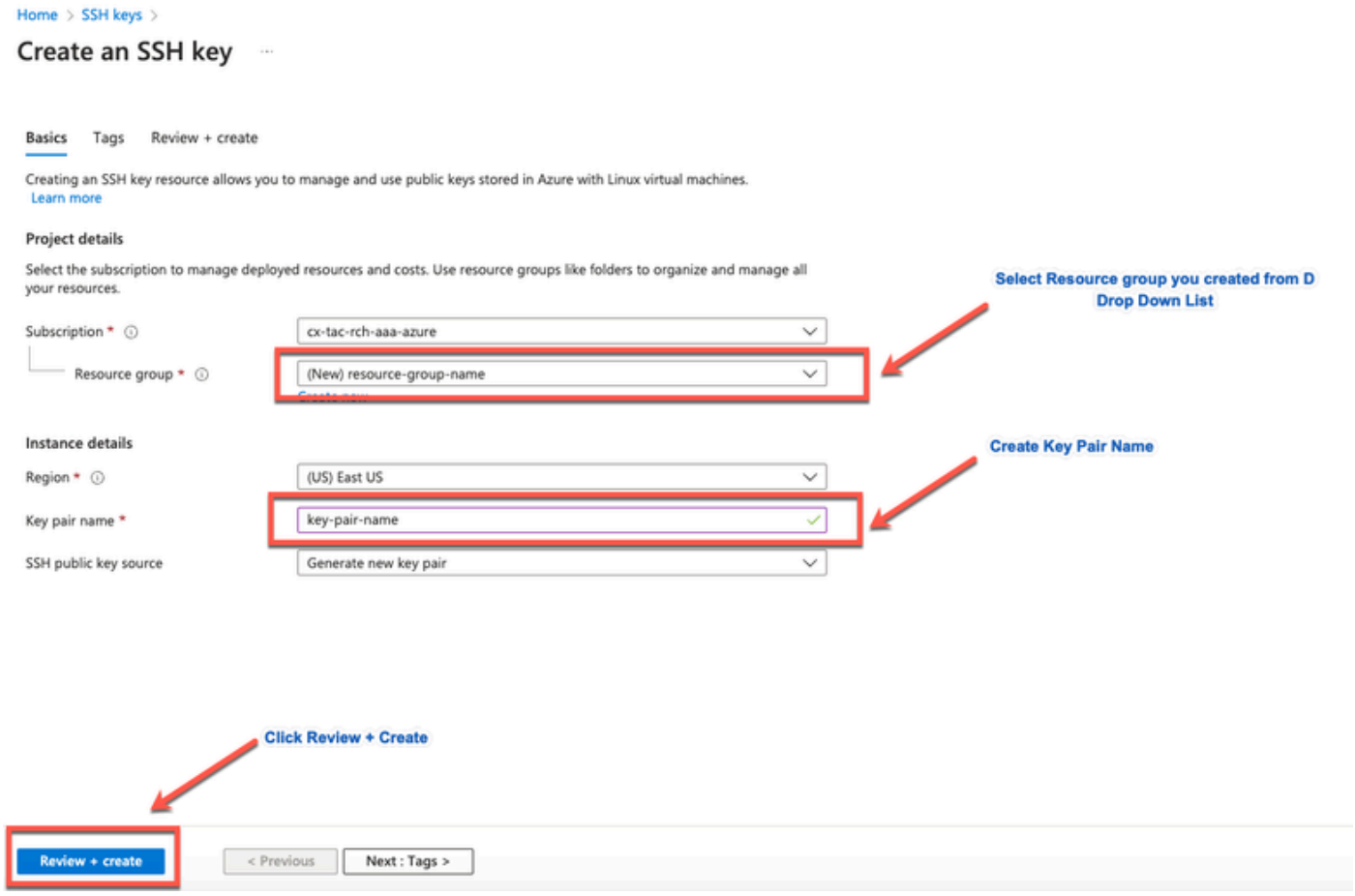


---

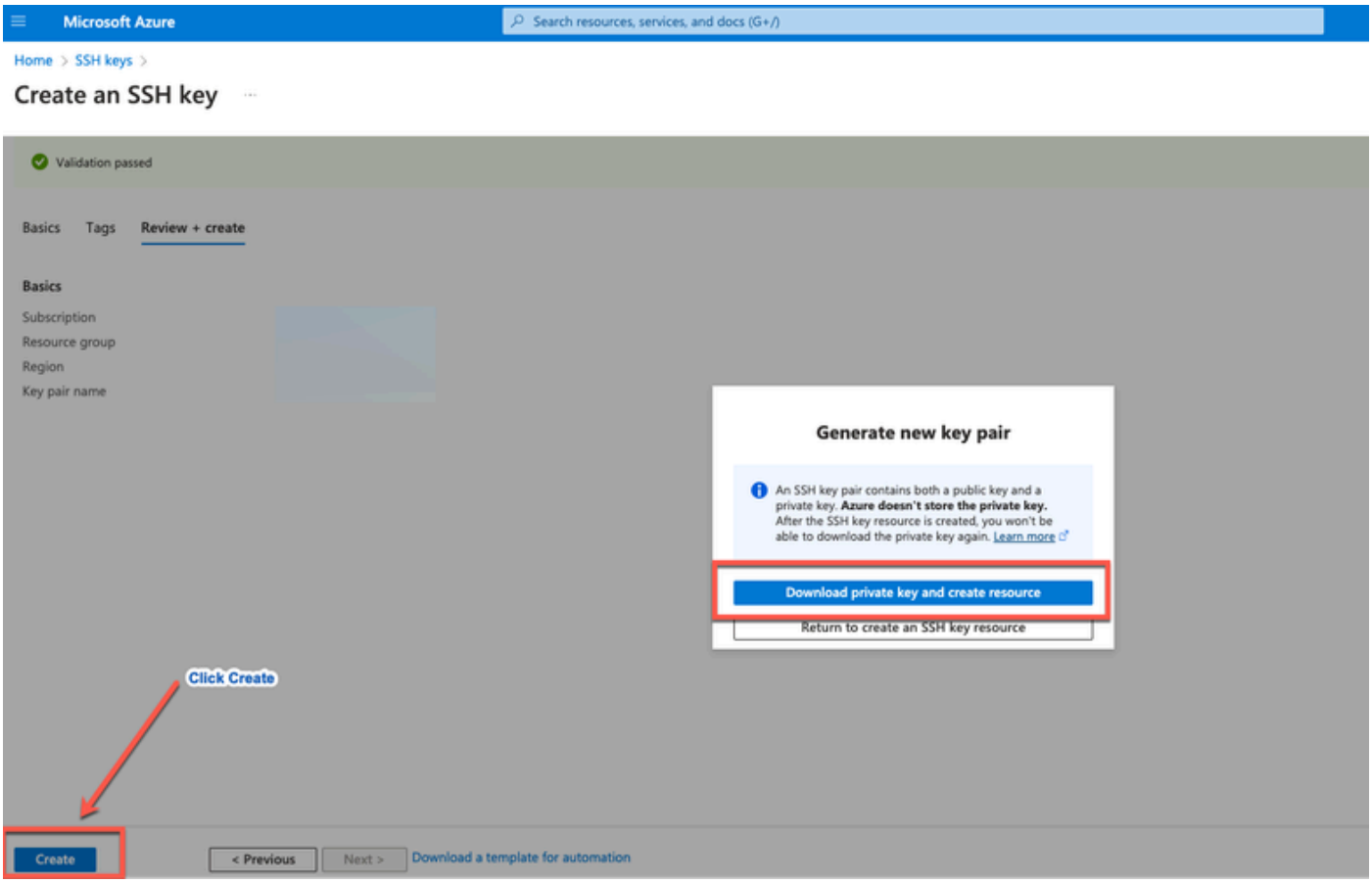
2. Click **Create**.



3. Choose the **Resource Group** and **Key Name**. Then, click **Review + Create**.



4. Then click **Create** and download the **Private Key**.



Azure VM Sizes Supported by Cisco ISE

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

- The Fsv2-series Azure VM sizes are compute-optimized and are best suited for use as PSNs for compute-intensive tasks and applications.
- The Dsv4-series are general purpose Azure VM sizes that are best suited for use as PAN or MnT nodes or both and are intended for data processing tasks and database operations.

If you use a general-purpose instance as a PSN, the performance numbers are lower than the performance of a compute-optimized instance as a PSN. The Standard_D8s_v4 VM size must be used as an extra small PSN

only.

Note: Do not clone an existing Azure Cloud image to create a Cisco ISE instance. Doing so can cause random and unexpected malfunctions in the created ISE machine.

Limitations of Cisco ISE in Microsoft Azure Cloud Services

- If you create Cisco ISE Using the Azure Virtual Machine, by default, Microsoft Azure assigns private IP addresses to VMs through DHCP servers. Before you create a Cisco ISE deployment on Microsoft Azure, you must update the forward and reverse DNS entries with the IP addresses assigned by Microsoft Azure.
- Alternatively, after you install Cisco ISE, assign a static IP address to your VM by updating the Network Interface object in Microsoft Azure:

    1. Stop the VM.
    2. In the Private IP address settings area of the VM, in the Assignment area, click **Static**.
    3. Restart the VM.
    4. In the Cisco ISE serial console, assign the IP address as Gi0.
    5. Restart the Cisco ISE application server.

- Dual NIC is supported with only two NICs—Gigabit Ethernet 0 and Gigabit Ethernet 1. To configure a secondary NIC in your Cisco ISE instance, you must first create a network interface object in Azure, power off your Cisco ISE instance, and then attach this network interface object to Cisco ISE. After you install and launch Cisco ISE on Azure, use the Cisco ISE CLI to manually configure the IP address of the network interface object as the secondary NIC.
- The Cisco ISE upgrade workflow is not available in Cisco ISE on Microsoft Azure. Only fresh installs are supported. However, you can carry out backup and restoration of the configuration data.
- The public cloud supports Layer 3 features only. Cisco ISE nodes on Microsoft Azure do not support Cisco ISE functions that depend on Layer 2 capabilities. For example, working with DHCP SPAN profiler probes and CDP protocol functions through the Cisco ISE CLI are functions that are currently not supported.
- When you carry out the restore and backup function of configuration data, after the backup operation is complete, first restart Cisco ISE through the CLI. Then, initiate the restore operation from the Cisco ISE GUI.
- SSH access to Cisco ISE CLI using password-based authentication is not supported in Azure. You can only access the Cisco ISE CLI through a key pair, and this key pair must be stored securely. If you are using a Private Key (or PEM) file and you lose the file, you cannot access the Cisco ISE CLI. Any integration that uses a password-based authentication method to access Cisco ISE CLI is not supported (Cisco DNA Center Release 2.1.2 and earlier).
- Cisco ISE IOS® deployments on Azure typically leverage VPN solutions like Dynamic Multipoint Virtual Private Networks (DMVPN) and Software-Defined Wide Area Networks (SD-WAN), where the IPSec tunnel overheads can cause MTU and fragmentation issues. In such scenarios, Cisco ISE

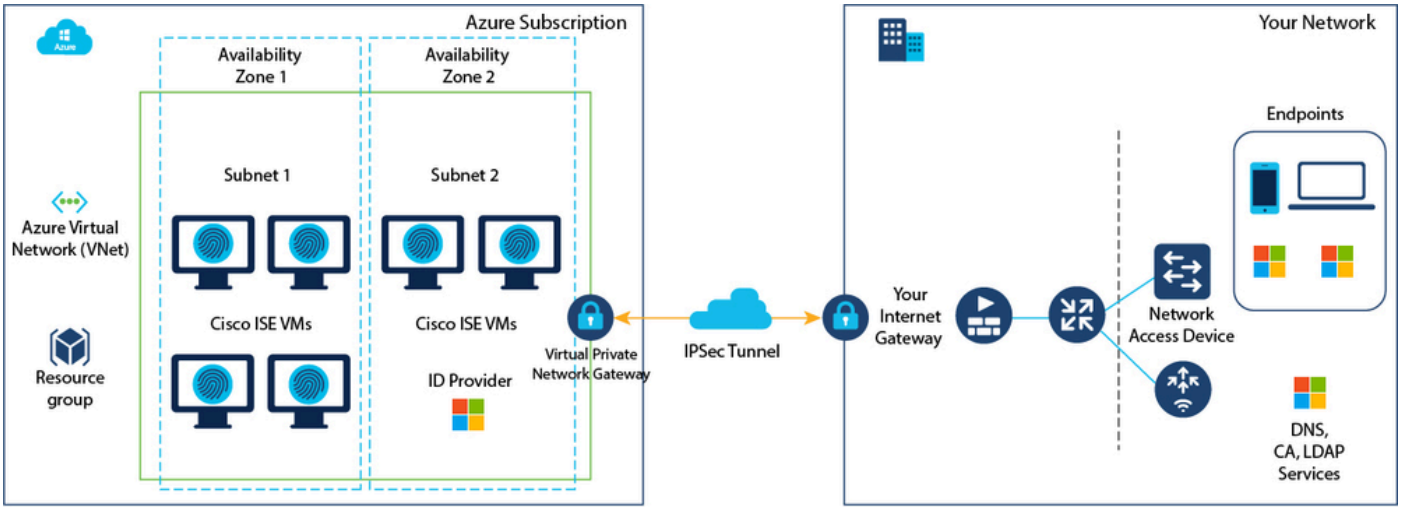
IOS® does not receive complete RADIUS packets and an authentication failure occurs without triggering a failure error log.

  - A possible workaround is to seek Microsoft technical support to explore any solutions in Azure that can allow out-of-order fragments to pass to the destination instead of being dropped.

- A CLI Admin user must be '**iseadmin**'.

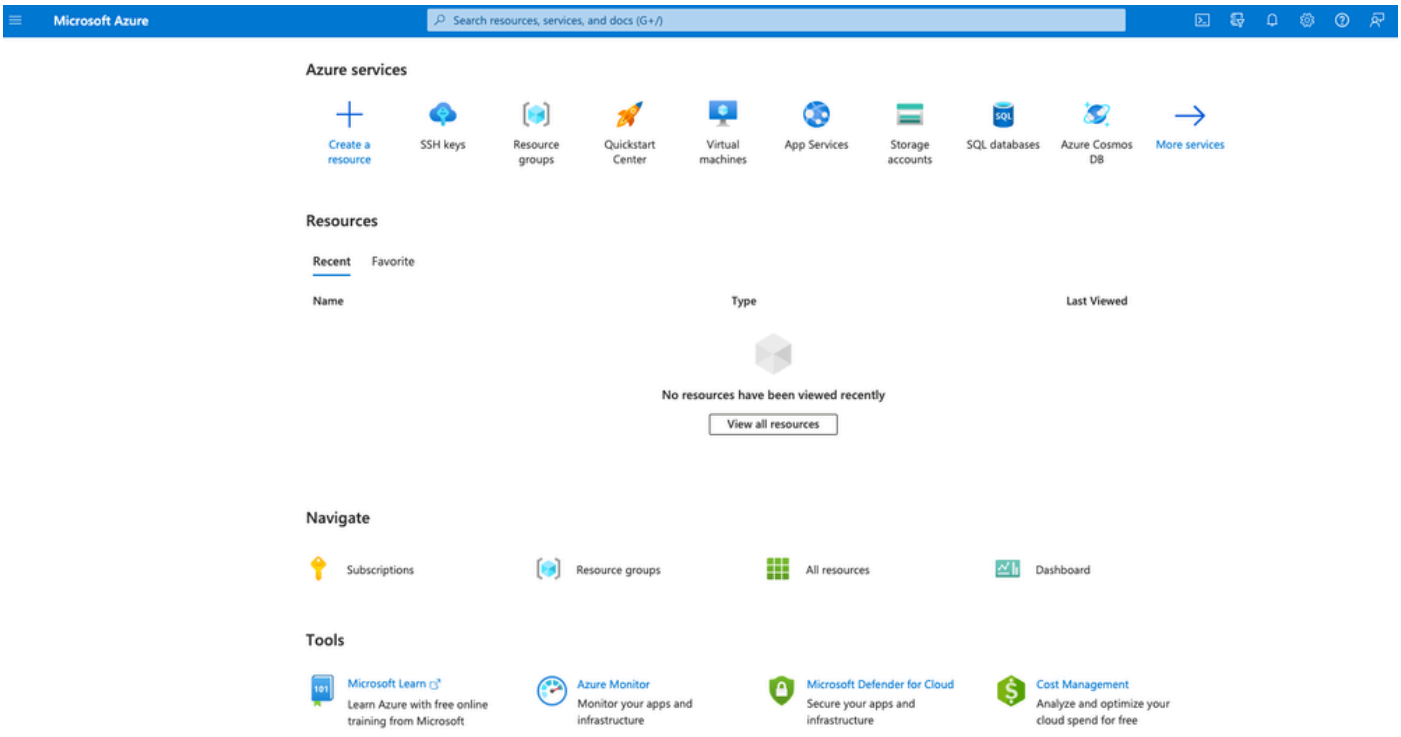
Configure

Example of ISE Deployment Connected to Azure Cloud

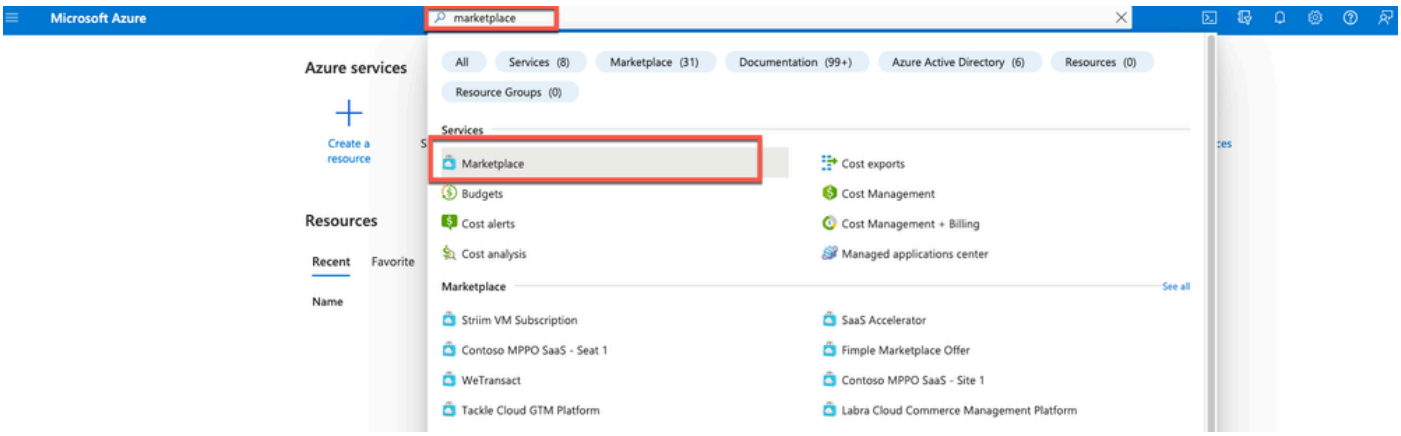


Configurations

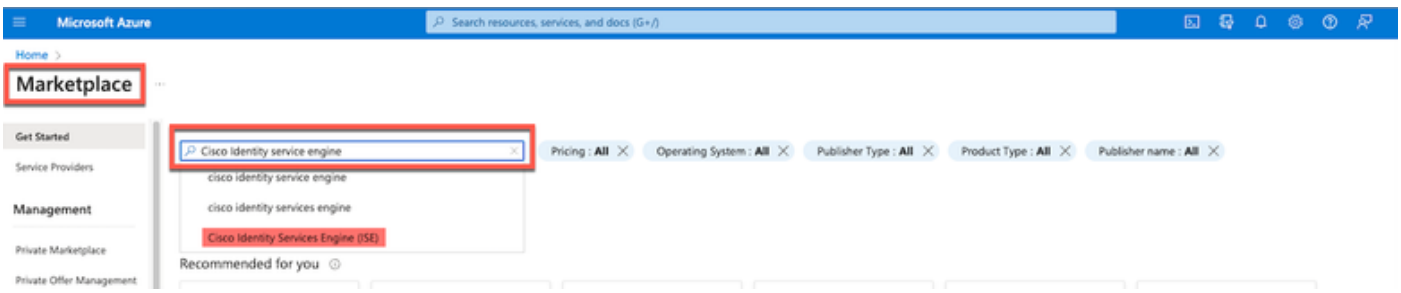
1. Navigate to the Azure Portal and log in to your Microsoft Azure account.



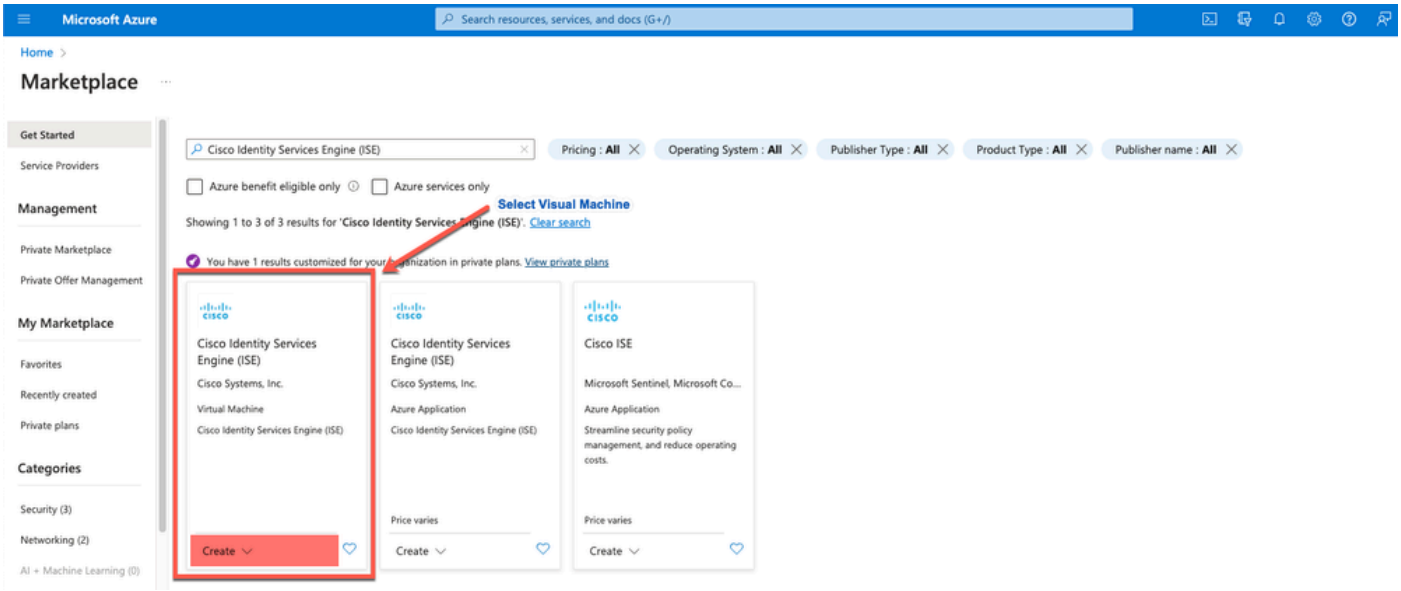
2. Use the search field at the top of the window to search for **Marketplace**.



3. Use the **Search the Marketplace** search field to search for **Cisco Identity Services Engine (ISE)**.

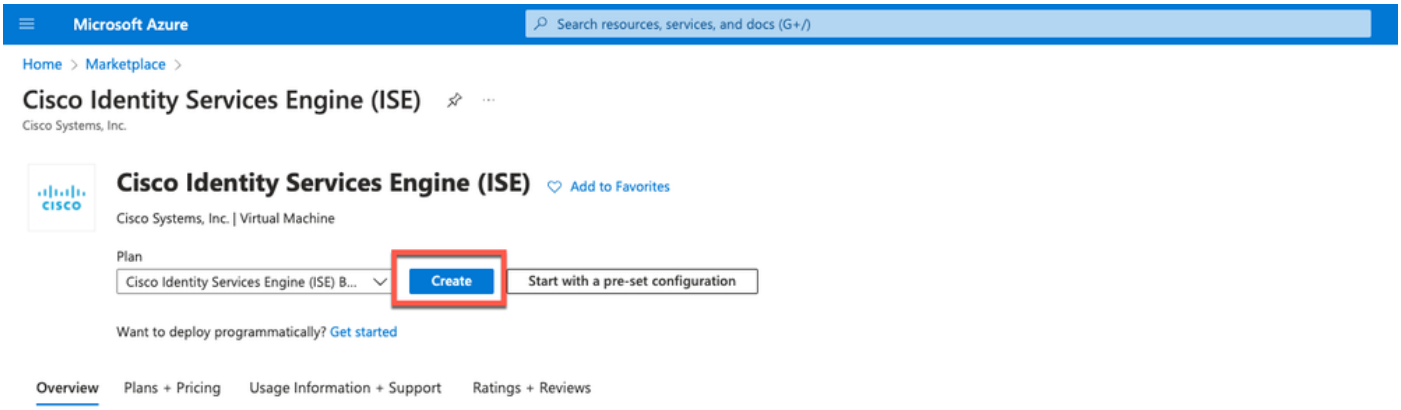


4. Click **Virtual Machine**.



---

5. In the new window, click **Create**.



---

6. In the Basics tab:

- In the **Project details** area, choose the required values from the **Subscription** and **Resource** Group drop-down lists.
- In the **Instance details** area, enter a value in the **Virtual Machine Name** field.
- From the **Image** drop-down list, choose the **Cisco ISE Image**.
- From the **Size** drop-down list, choose the instance size you want to install Cisco ISE with. Choose an instance supported by Cisco ISE, as listed in the table titled **Azure Cloud**.

Instances supported by Cisco ISE are listed in the Cisco ISE on Azure Cloud section.

e. In the **Administrator Account > Authentication type** area, click the **SSH Public Key** radio button.

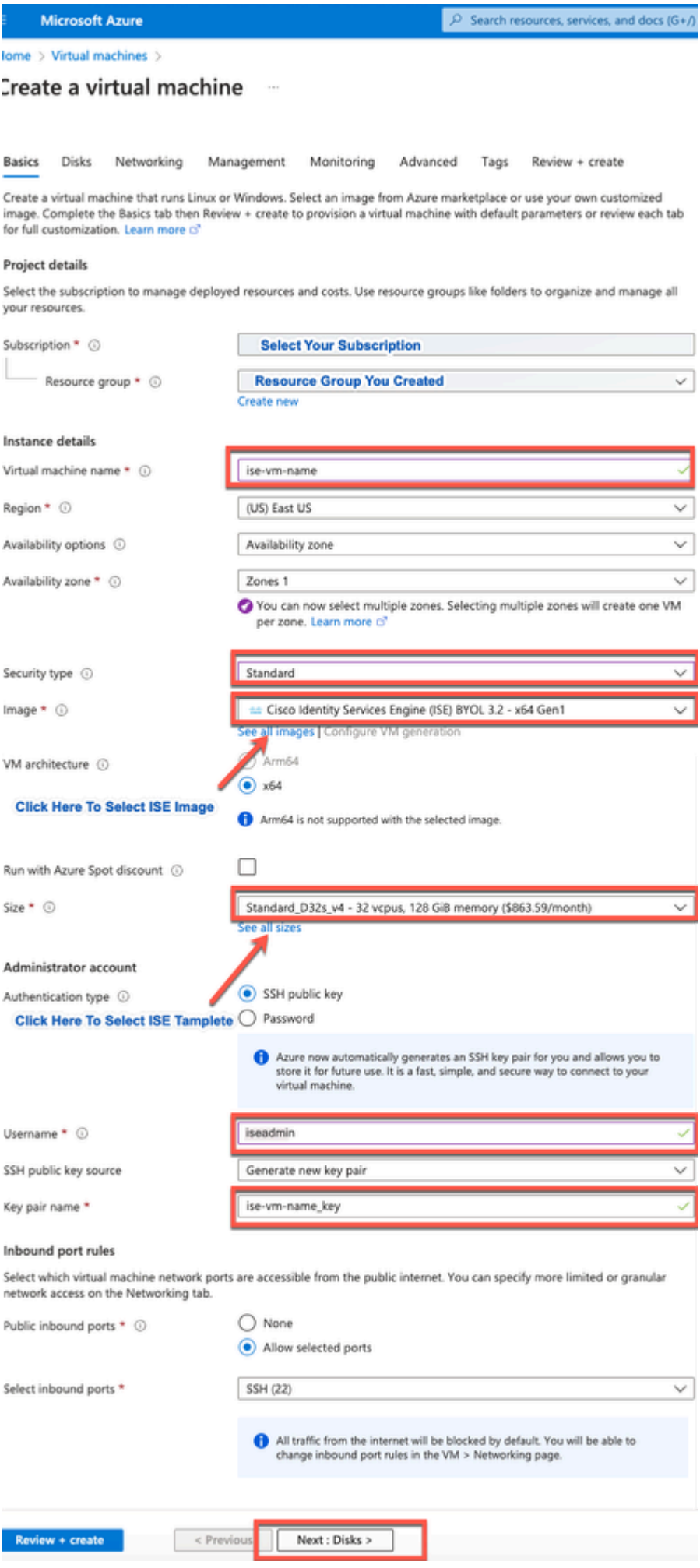
f. In the **Username** field, enter **iseadmin**.

g. From the **SSH public key source** drop-down list, choose **Use existing key stored in Azure.**

h. From the **Stored keys** drop-down list, choose the key pair that you created as a prerequisite for this task.

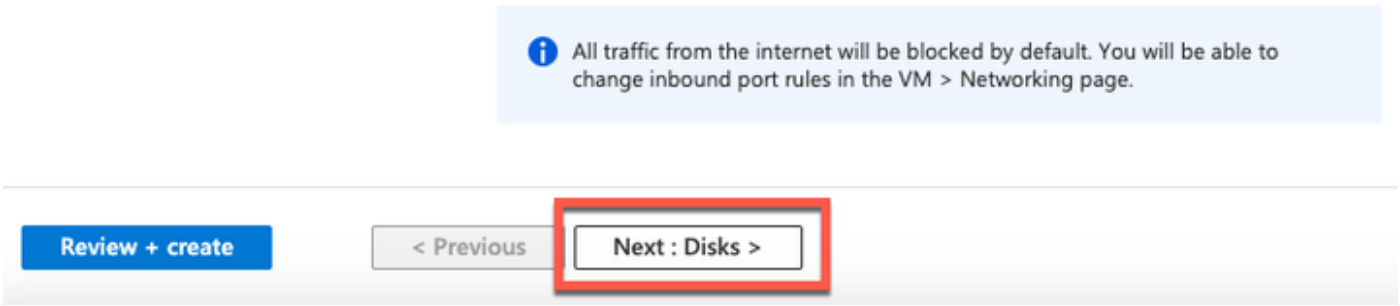
j. In the **Inbound port rules** area, click the **Allow selected ports** radio button.

k. In the **Licensing** area, from the **Licensing type** drop-down list, choose **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 >

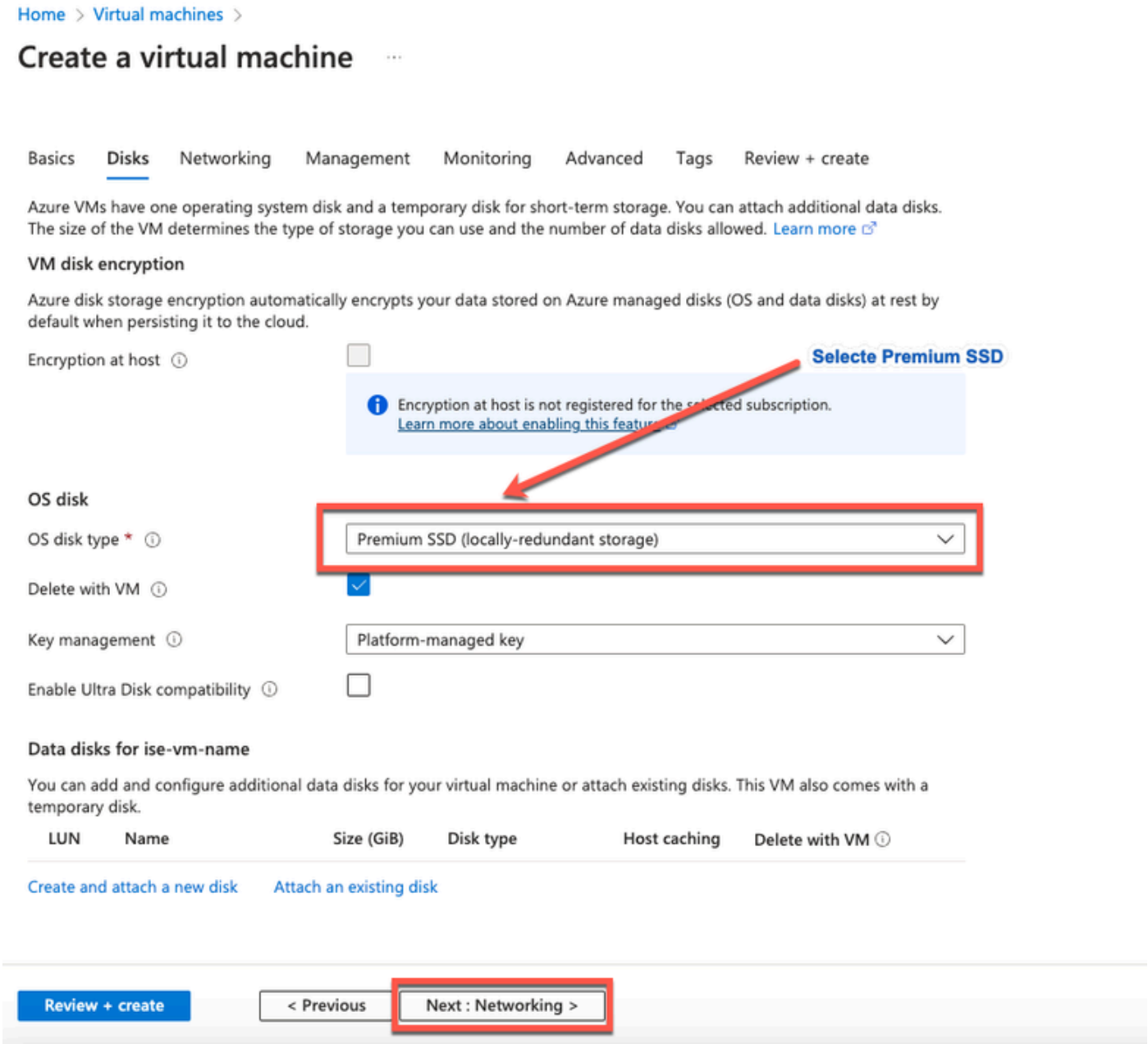
---

7. Click **Next: Disks**.



---

8. In the **Disks** tab, retain the default values for the mandatory fields and click **Next: Networking**.

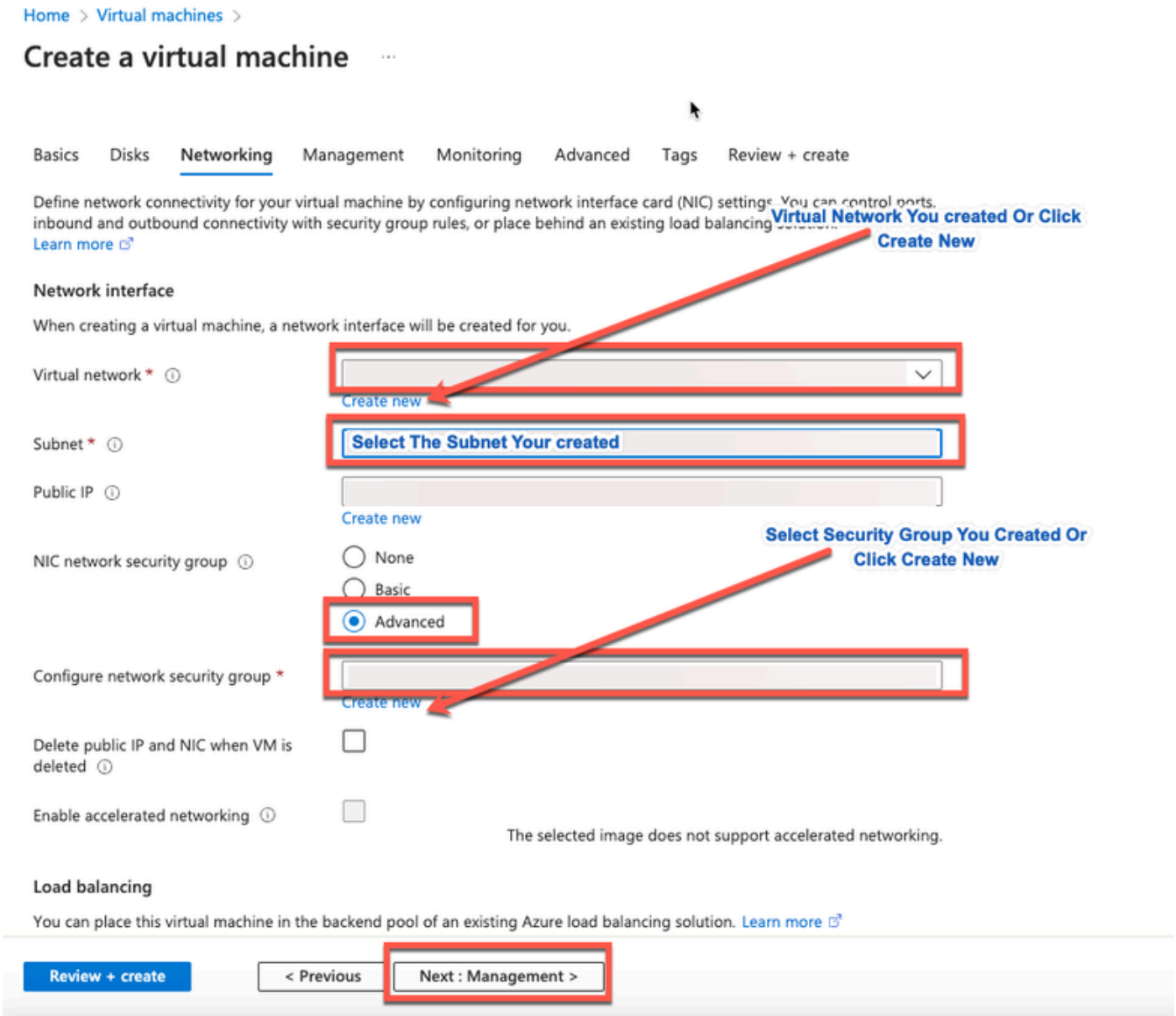


Note: For The Disk Type, there are more options from the drop-down list to choose from. You can choose the one that meets your Needs. Premium SSD is the Recommended Type for Production and Performance Sensitive Workloads.

---

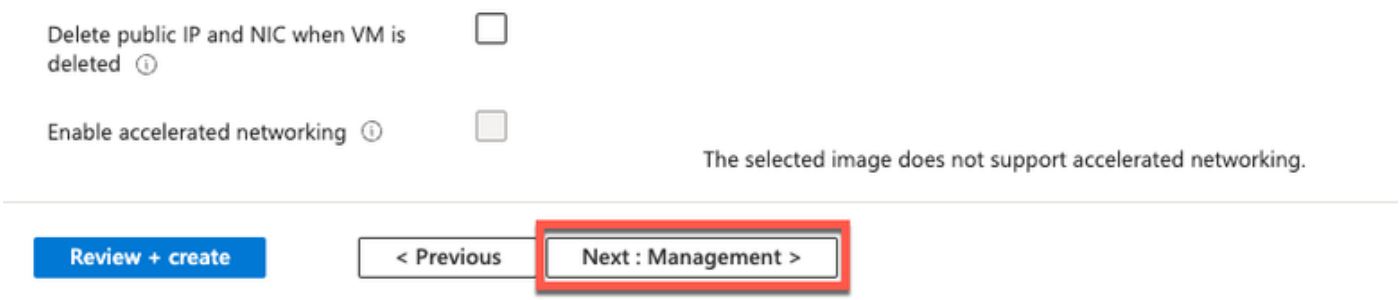
9. In the **Network Interface** area, from the **Virtual Network**, **Subnet**, and **Configure Network Security Group** drop-down lists, choose the virtual network and subnet you created.

Note: The subnet with a public IP address receives online and offline posture feed updates, while a subnet with a private IP address only receives offline posture feed updates.



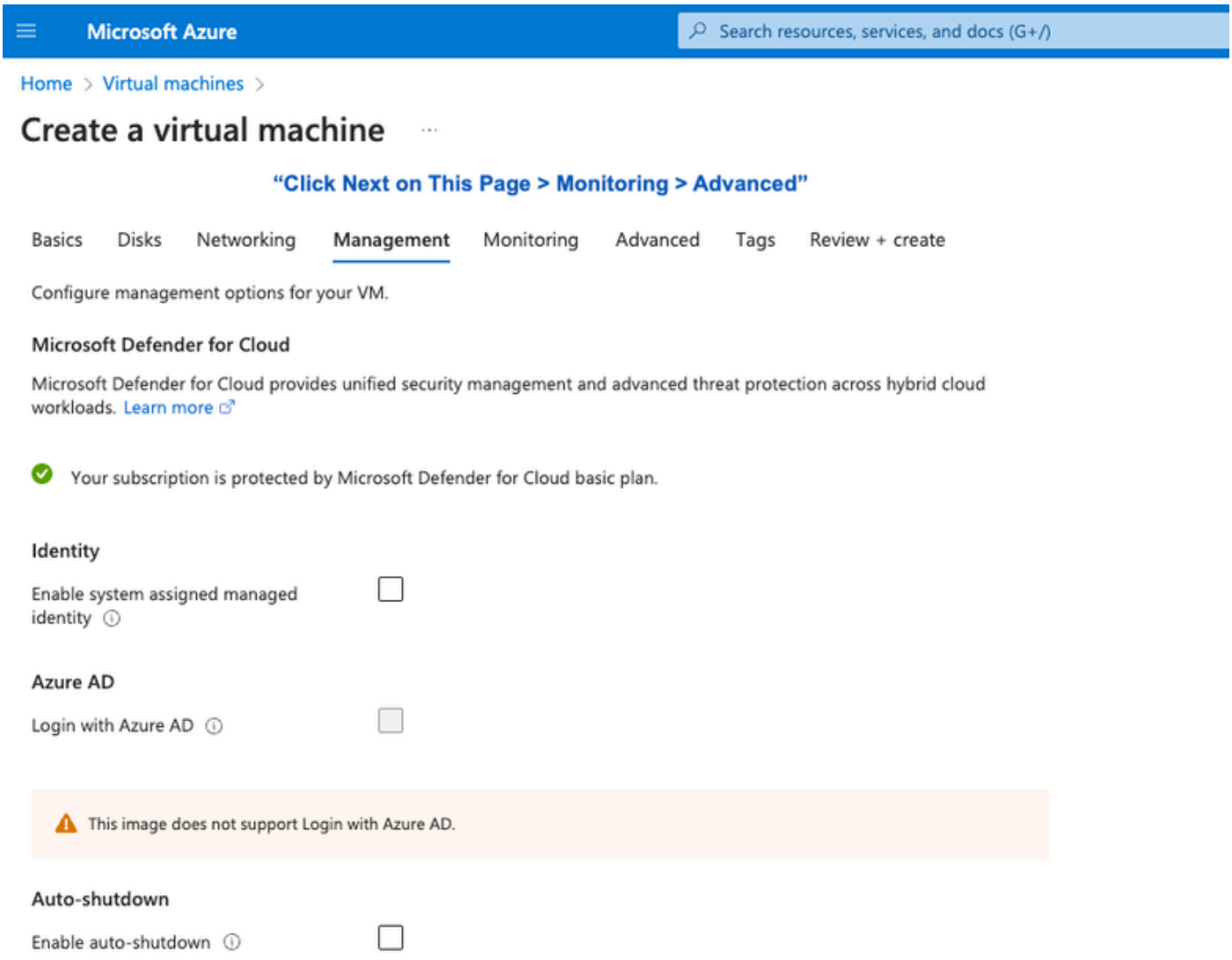
---

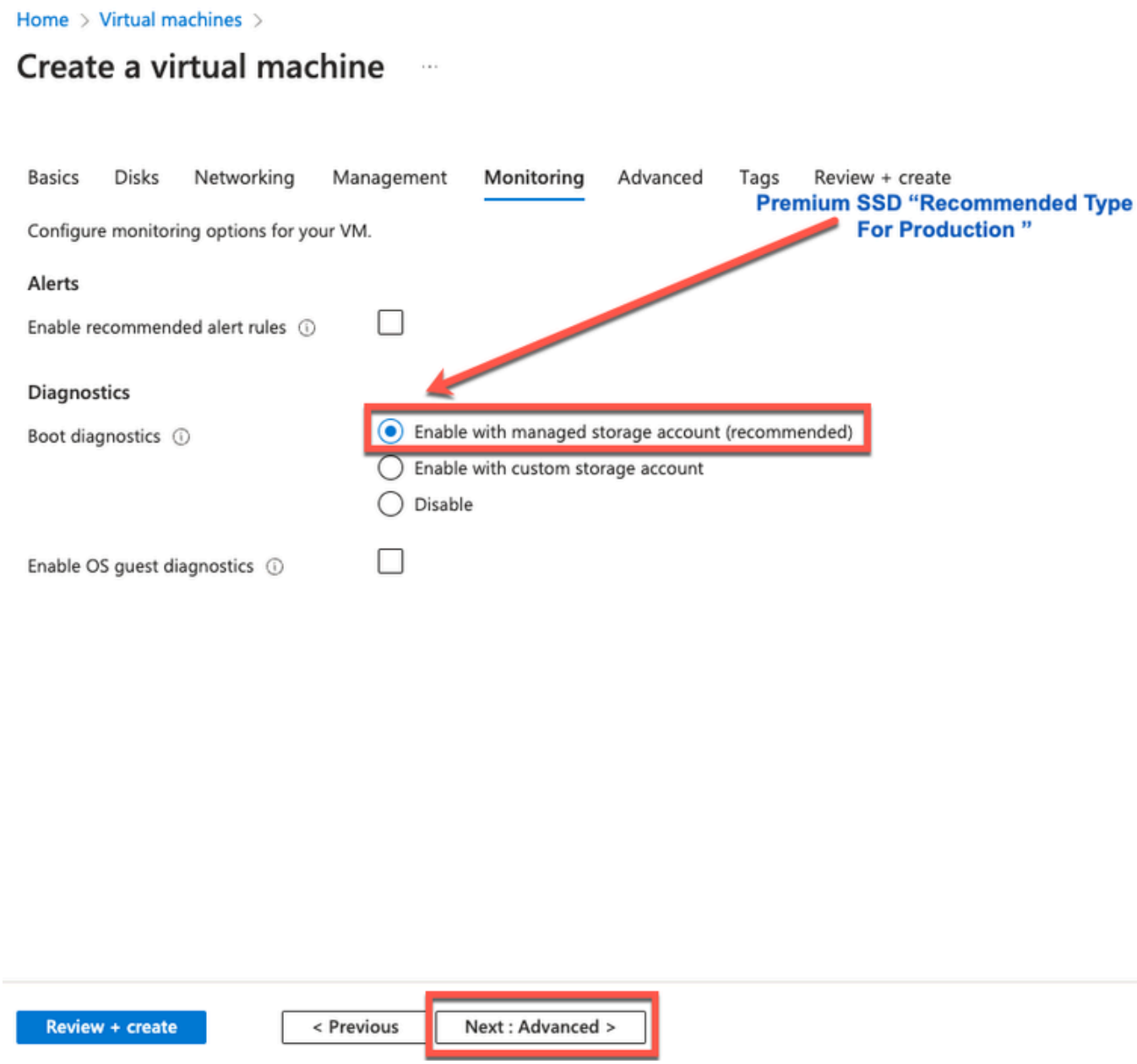
10. Click **Next: Management**.



---

11. In the **Management** tab, retain the default values for the mandatory fields and click **Next: Advanced**.


Microsoft Azure
Search resources, services, and docs (G+/)
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



---

12. In the **User Data** area, check the **Enable User Data** checkbox.

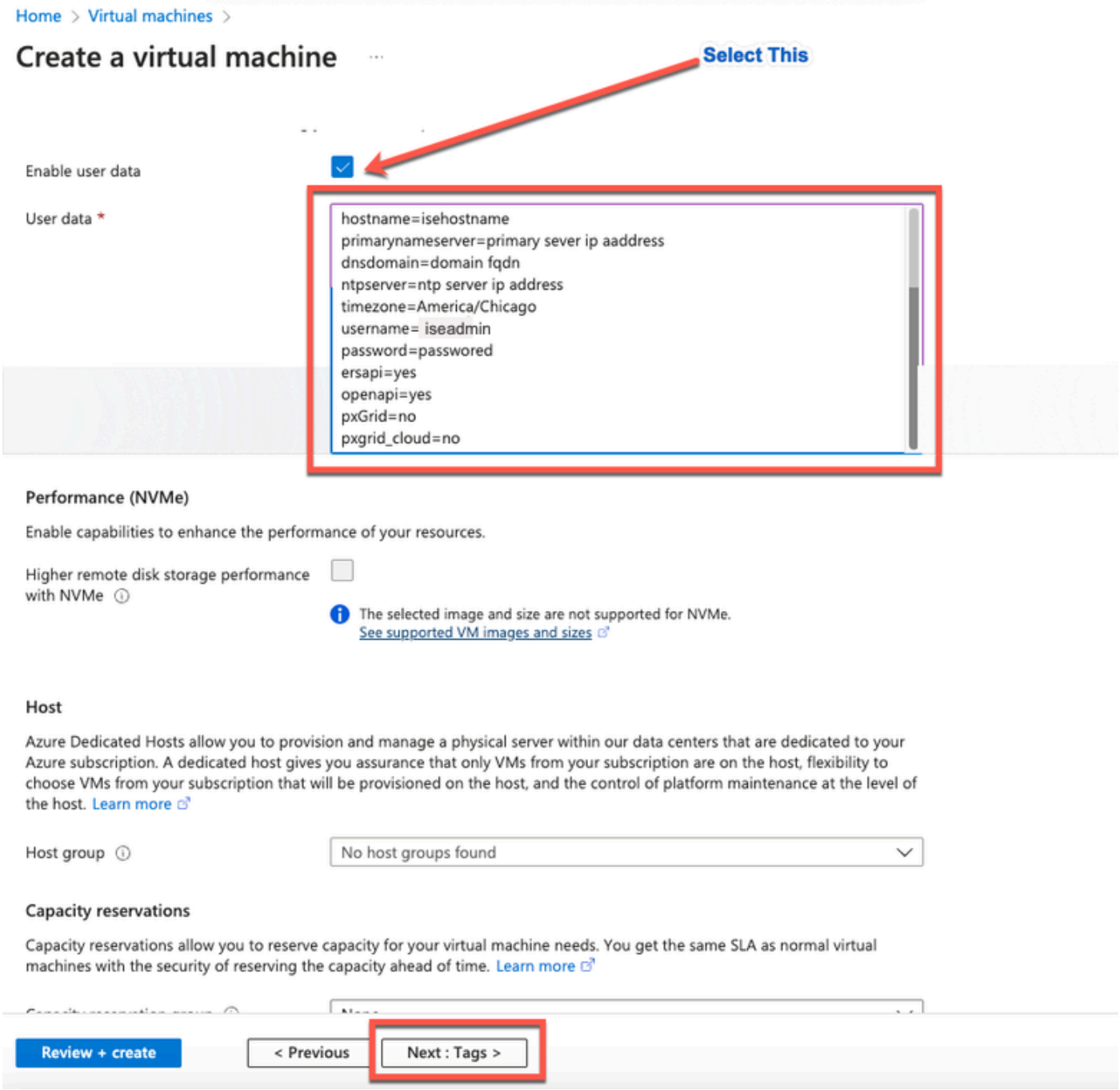
- In the **User Data** field, complete this information:
  - hostname=<*hostname of Cisco ISE*>
  - primarynameserver=<*IPv4 address*>
  - dnsdomain=<*domain name*>
  - ntpserver=<*IPv4 address or FQDN of the NTP server*>
  - timezone=<*timezone*>
  - password=<*password*>
  - ersapi=<*yes/no*>
  - openapi=<*yes/no*>
  - pxGrid=<*yes/no*>
  - pxgrid_cloud=<*yes/no*>

Note: You must use the correct syntax for each of the fields you configure through the user data entry. The information you enter in the User data field is not validated when it is entered. If you use the wrong syntax, Cisco ISE Services does not load when you launch the image.

From Cisco ISE Release 3.4, The ntpserver field name is changed to primaryntpserver. If you use ntpserver, Cisco ISE Services cannot start. OpenAPI is enabled by default, hence, the **openapi=<yes/no>** field is not required. If you leave the **secondarynameserver** field blank and only use the **tertiarynameserver** field, the Cisco ISE Services cannot start. If you leave the **secondaryntpserver** field blank and only use the **tertiaryntpserver** field, the Cisco ISE Services cannot start.

Refer to the **Guidelines** for the configurations you must submit through the user data field:

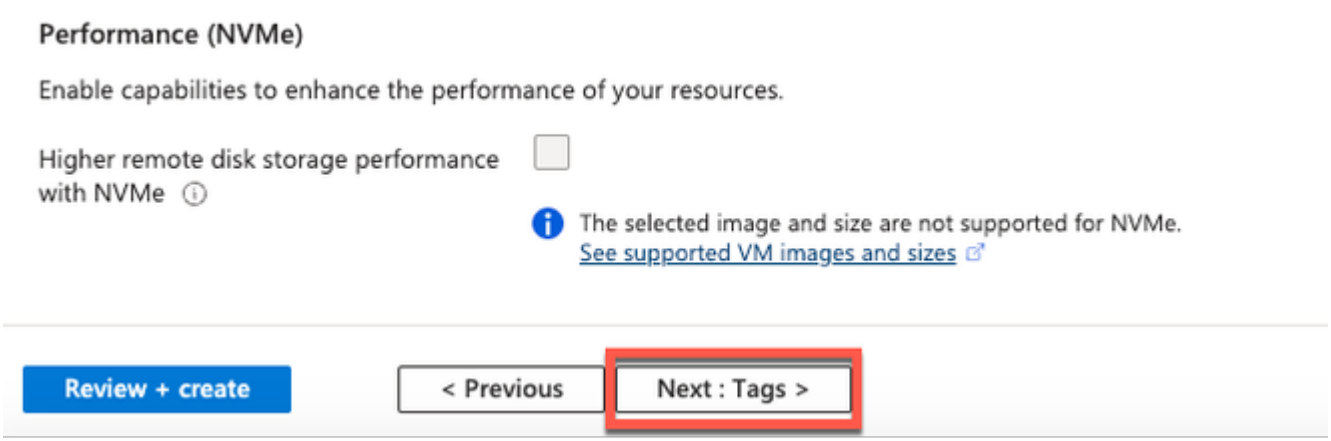
- **hostname**: Enter a hostname that contains only alphanumeric characters and hyphens (-). The length of the hostname must not exceed 19 characters and cannot contain underscores (_).
- **primary nameserver**: Enter the IP address of the primary name server. Only IPv4 addresses are supported. You can add only one DNS server in this step. You can add additional DNS servers through the Cisco ISE CLI after installation.
- **dnsdomain**: Enter the FQDN of the DNS domain. The entry can contain ASCII characters, numerals, hyphens (-), and periods (.).
- **ntpserver**: Enter the IPv4 address or FQDN of the NTP server that must be used for synchronization. You can add only one NTP server in this step. You can add additional NTP servers through Cisco ISE CLI after installation. Use a valid and reachable NTP Server as this is required for ISE Operations.
- **time zone**: Enter a time zone, for example, EST/UTC. It is recommended you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) time zone, especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures the time stamps of reports and logs from various nodes in your deployment are always synchronized.
- **password**: Configure a password for GUI-based login to Cisco ISE. The password you enter must comply with the Cisco ISE password policy. The password must contain 6 to 25 characters and include at least **one numeral**, **one uppercase letter**, and **one lowercase letter**. The password cannot be the same as the username or its reverse (iseadmin or nimdaesi), cisco, or ocsic. The allowed special characters are @~*!,+=_-. Refer to the 'User Password Policy' section in the Chapter 'Basic Setup' of the Cisco ISE Administrator Guide for your release.
- **ersapi**: Enter **yes** to enable ERS, or **no** to disallow ERS.
- **openapi**: Enter **yes** to enable OpenAPI, or **no** to disallow OpenAPI.
- pxGrid: Enter **yes** to enable pxGrid, or **no** to disallow pxGrid.
- **pxgrid_cloud**: Enter **yes** to enable pxGrid Cloud or **no** to disallow pxGrid Cloud. To enable pxGrid Cloud, you must enable pxGrid. If you disallow pxGrid, but enable pxGrid Cloud, pxGrid Cloud services are not enabled on launch.



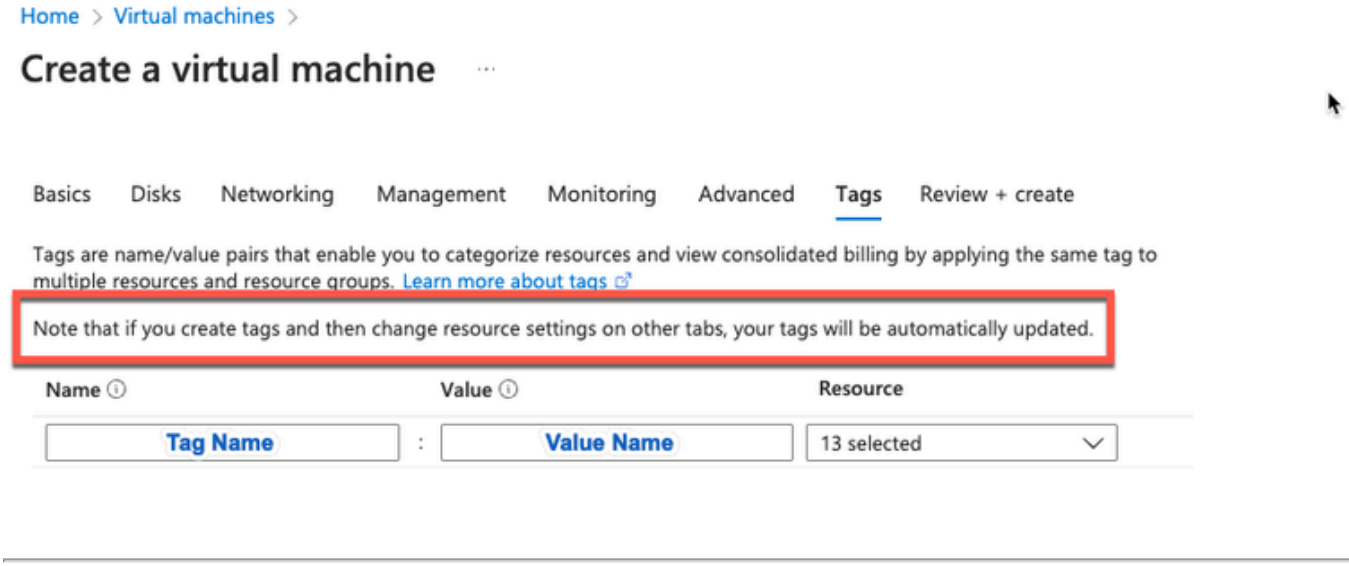
User Data Section

---

13. Click **Next: Tags**.



14. To create name-value pairs that allow you to categorize resources, and consolidate multiple resources and resource groups; enter values in the **Name** and **Value** fields.

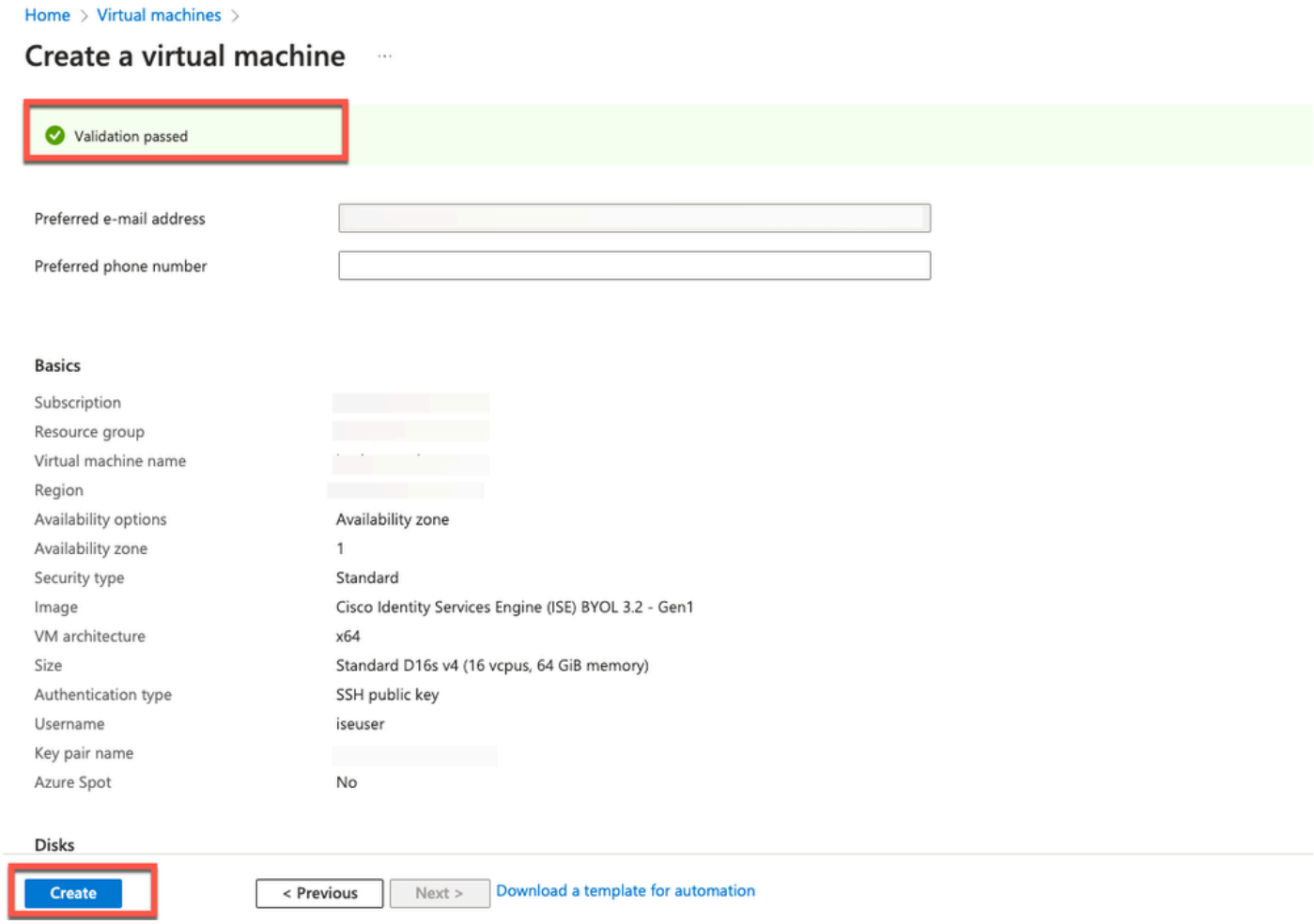


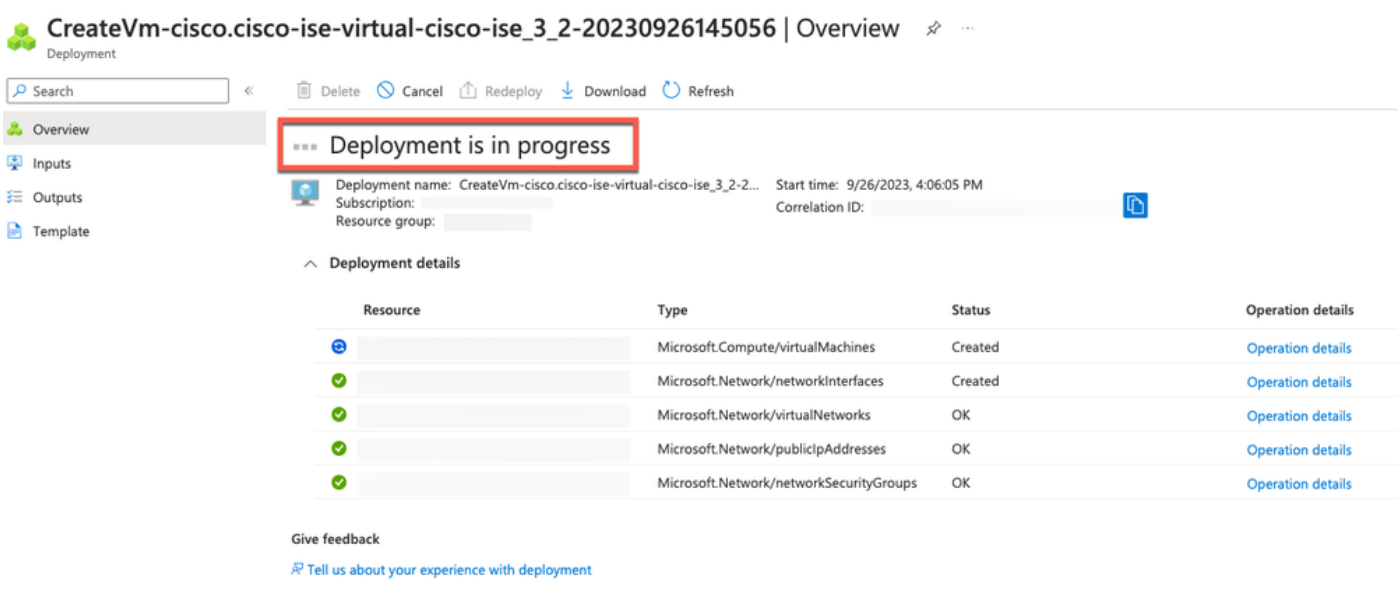
15. Click **Next: Review + Create**.



16. Review the information you have provided so far and click **Create**. The **Deployment is in Progress**

window is displayed. It takes approximately 30 minutes for the Cisco ISE instance to be created and available for use. The Cisco ISE VM instance is displayed in the **Virtual Machines** window (use the main search field to find the window).





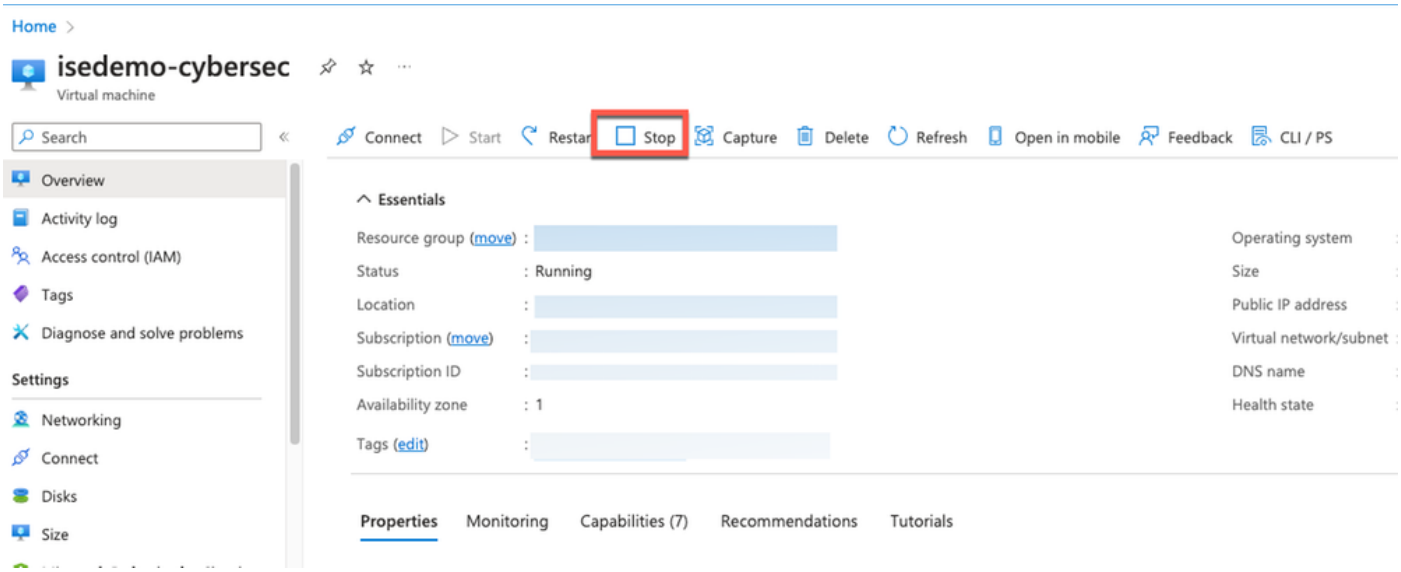
What to do Next

Due to a Microsoft Azure default setting, the Cisco ISE VM you have created is configured with only a 300 GB disk size. Cisco ISE nodes typically require more than 300 GB disk size. You can see the **Insufficient Virtual Memory** alarm when you first launch Cisco ISE from Microsoft Azure.

After the Cisco ISE VM creation is complete, log in to the Cisco ISE Administration Portal to verify that Cisco ISE is set up. Then, in the Microsoft Azure Portal, carry out and complete steps in the **Virtual Machines** window to edit the disk size:

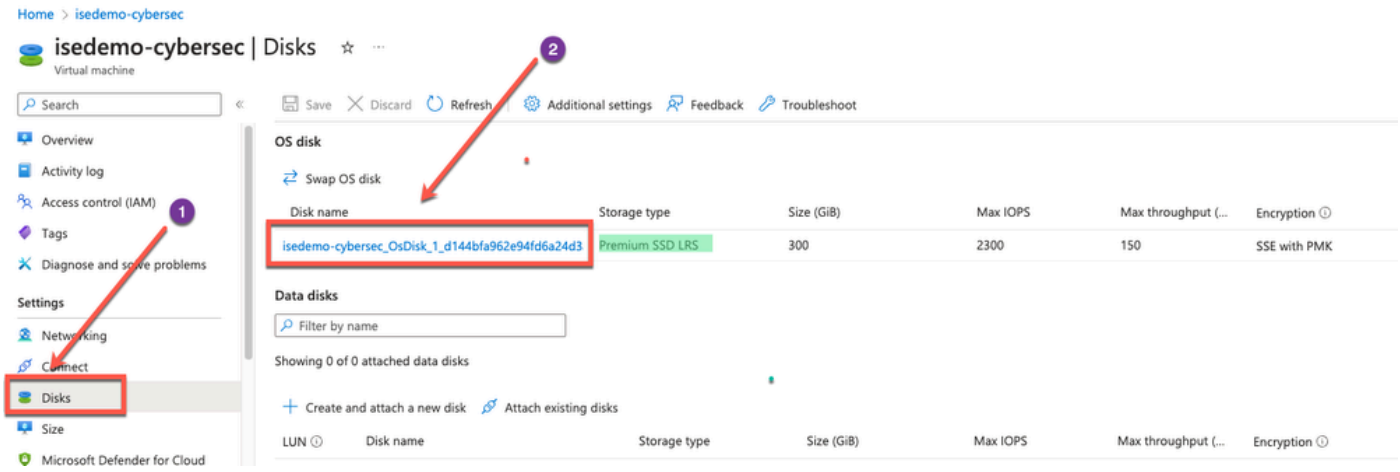
---

1. Stop the Cisco ISE instance.



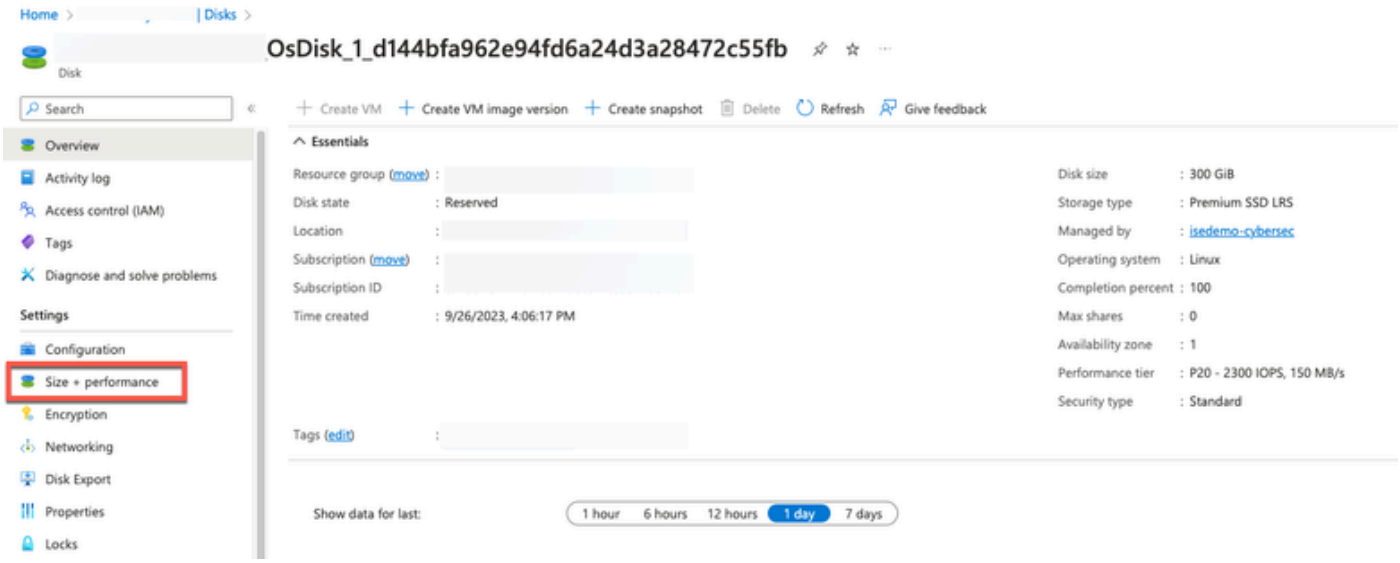
---

2. Click **Disk** in the left pane and click the disk you are using with Cisco ISE.



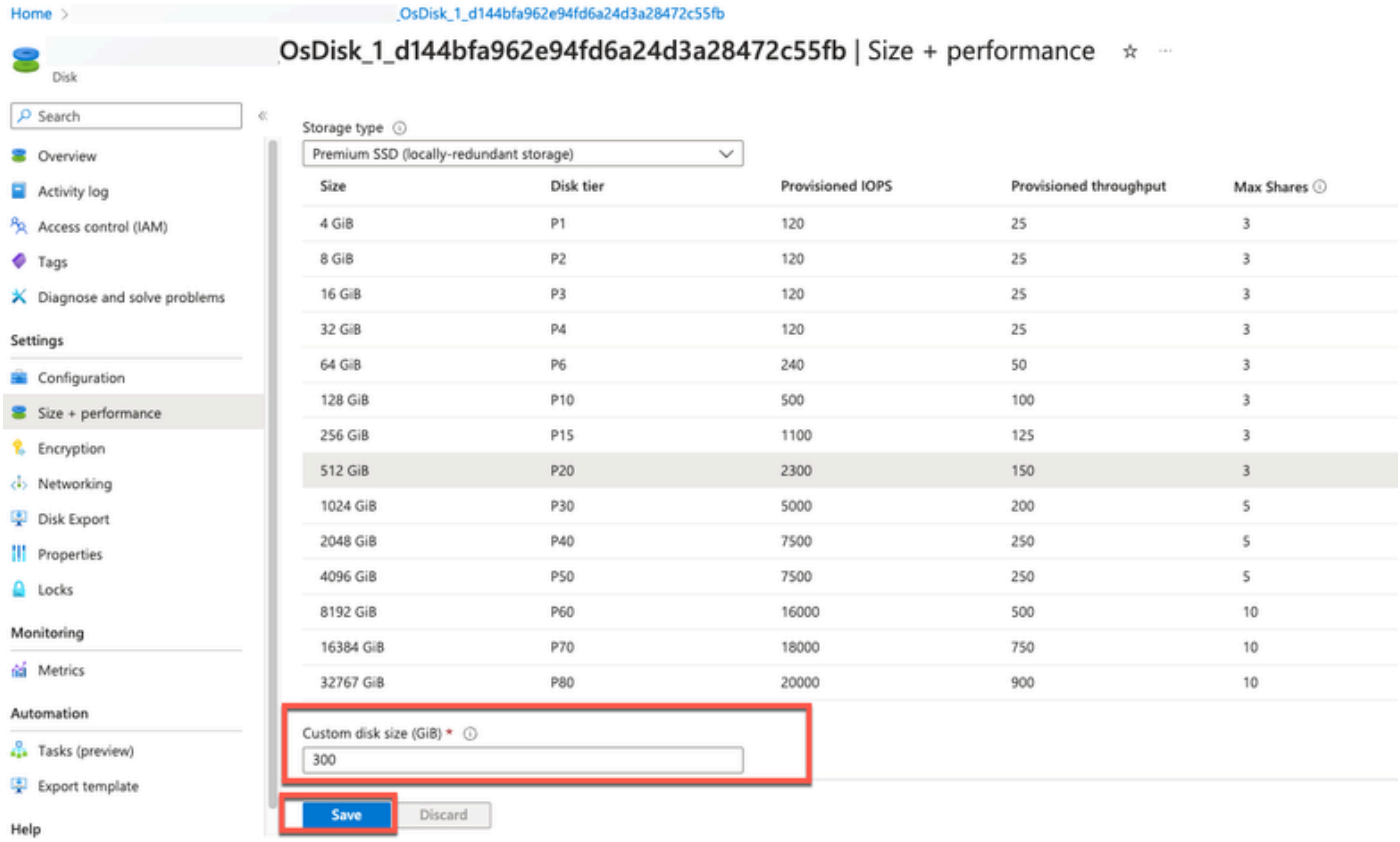
---

3. Click **Size + Performance** in the left pane.



---

4. In the **Custom Disk Size** field, enter the disk size you want in GiB.



Post Installation Tasks

For information on post-installation tasks that you must carry out after successfully creating a Cisco ISE instance, refer to the 'Installation Verification and Post Installation Tasks' Chapters in the Cisco ISE Installation Guide for your Cisco ISE release.

Password Recovery and Reset on Azure Cloud

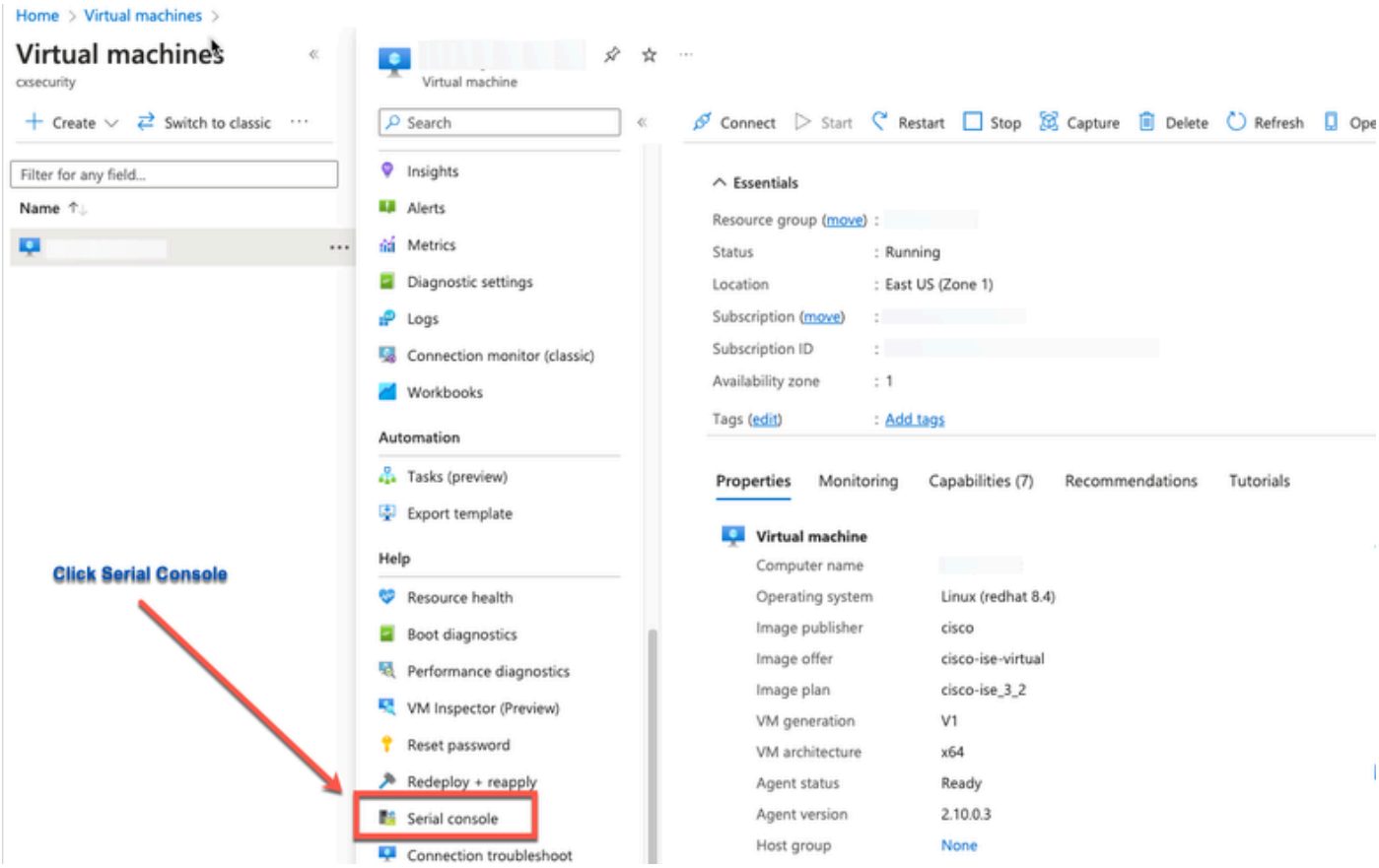
Complete the tasks that help you reset or recover your Cisco ISE Virtual Machine password. Choose the tasks that you need and carry out the steps detailed.

Reset Cisco ISE GUI Password Through Serial Console

1. Log in to Azure Cloud and choose the resource group that contains your Cisco ISE Virtual Machine.

2. From the list of resources, click the Cisco ISE instance you want to reset the password for.

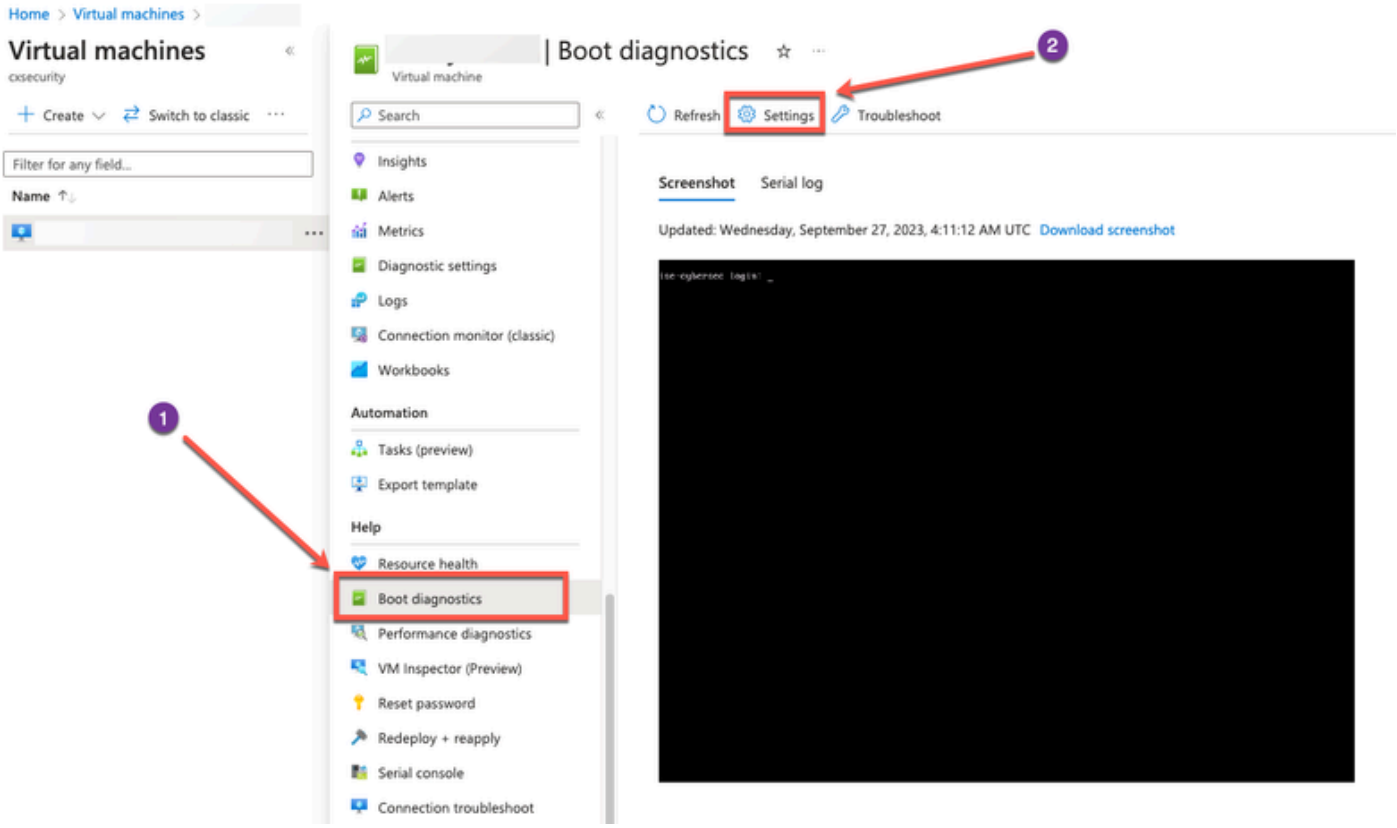
3. From the left-side menu, from the **Support + Troubleshooting** section, click **Serial Console**.



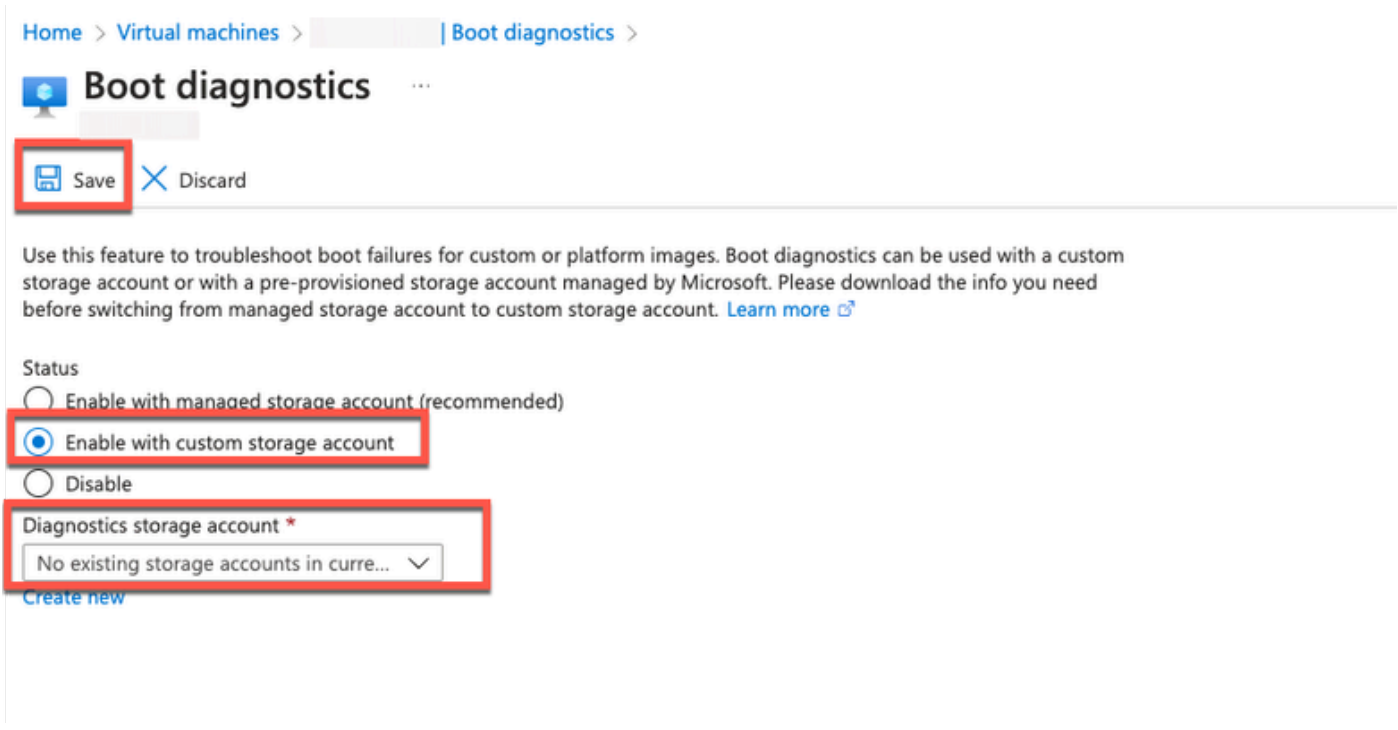
---

4. If you see an error message, you must enable boot diagnostics by carrying out these steps:

- From the left-side menu, click **Boot Diagnostics**.

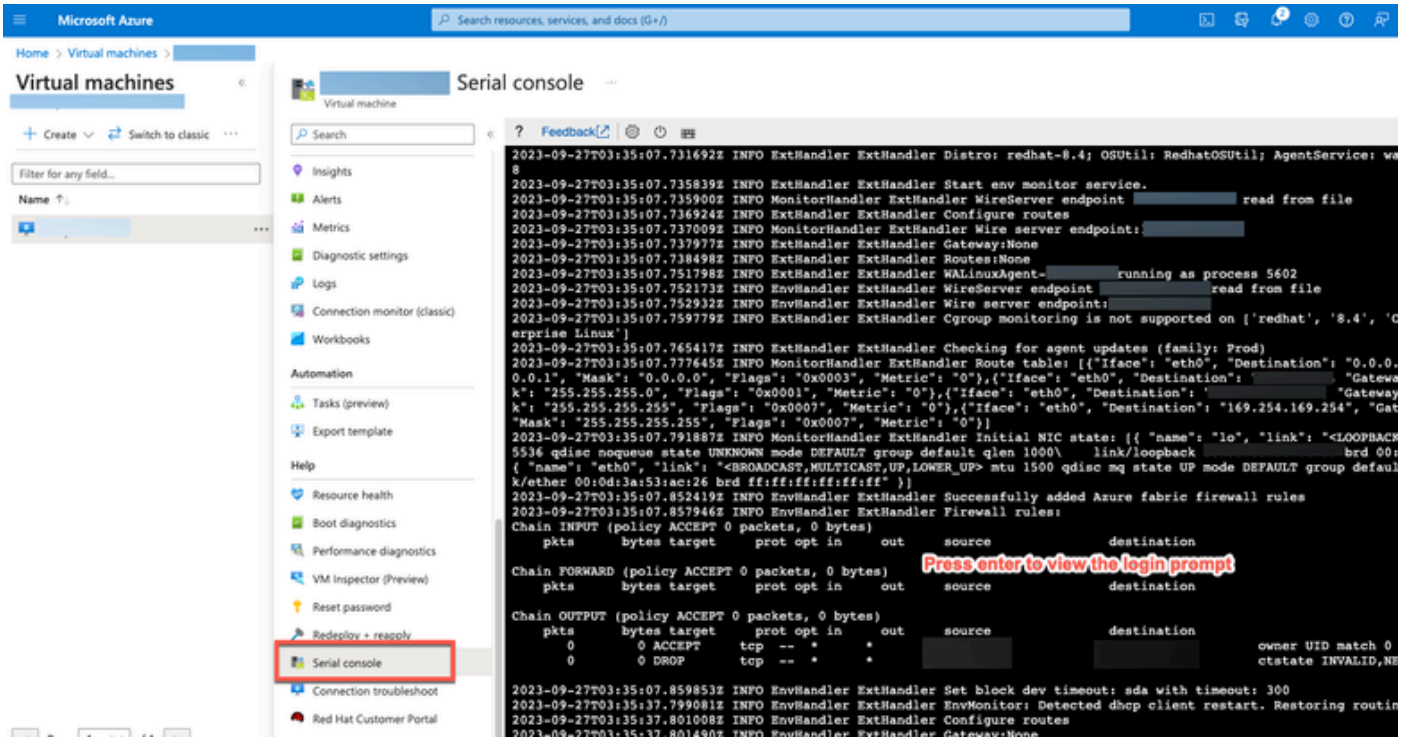


- Click **Enable with a Custom Storage Account**. Click **Save.**



---

5. From the left-side menu, from the **Support + Troubleshooting** section, click **Serial Console**. The Azure Cloud Shell is displayed in a new window. If the screen is black/blank, press **Enter** to view the login prompt.



---

6. Log in to the serial console. To log into the serial console, you must use the original password that was configured at the installation of the instance.

---

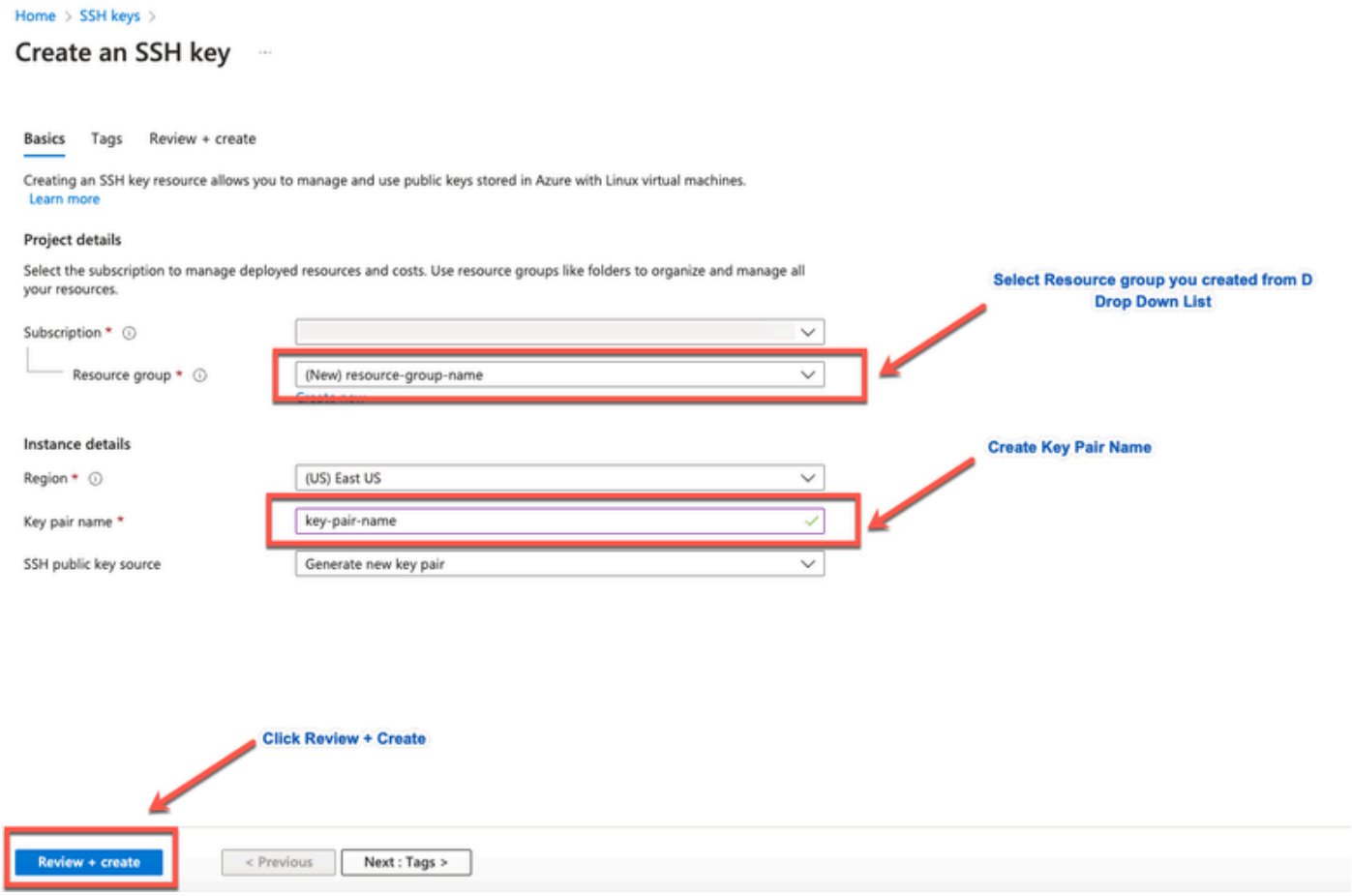
7. Run the **application reset-passwd ise iseadmin** command to configure a new GUI password for the iseadmin account.

Create a New Public Key Pair for SSH Access

Through this task, you can add additional key pairs to a repository. The existing key pair that was created at the time of the Cisco ISE instance configuration is not replaced by the new public key that you created.

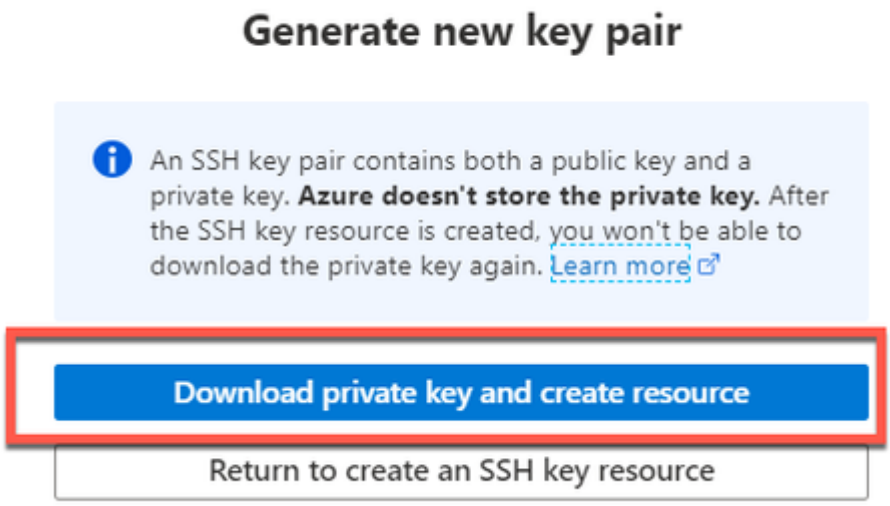
---

1. Create a new public key in Azure Cloud.



---

2. You receive a pop-up window to choose **Download Private Key and Create a Resource** that downloads the SSH key as a **.pem** file.



---

3. To create a new repository to save the public key to, refer to the Azure Repos documentation. If you already have a repository that is accessible through the CLI, skip to Step 3.

---

4. To import the new Public Key, run the **crypto key import <public key filename> repository <repository name>** command.

---

5. When the import is complete, you can log in to Cisco ISE via SSH using the new public key.