

在Azure雲服務上安裝ISE

目錄

[簡介](#)

[必要條件](#)

[採用元件](#)

[思科ISE支援的Azure VM大小](#)

[Microsoft Azure雲服務中Cisco ISE的限制](#)

[設定](#)

[連線到Azure雲的ISE部署示例](#)

[組態](#)

[下一步要做什麼](#)

[安裝後任務](#)

[在Azure Cloud上恢復並重置密碼](#)

1. [透過串列控制權重置思科ISE GUI密碼](#)

2. [為SSH訪問建立新的公鑰對](#)

簡介

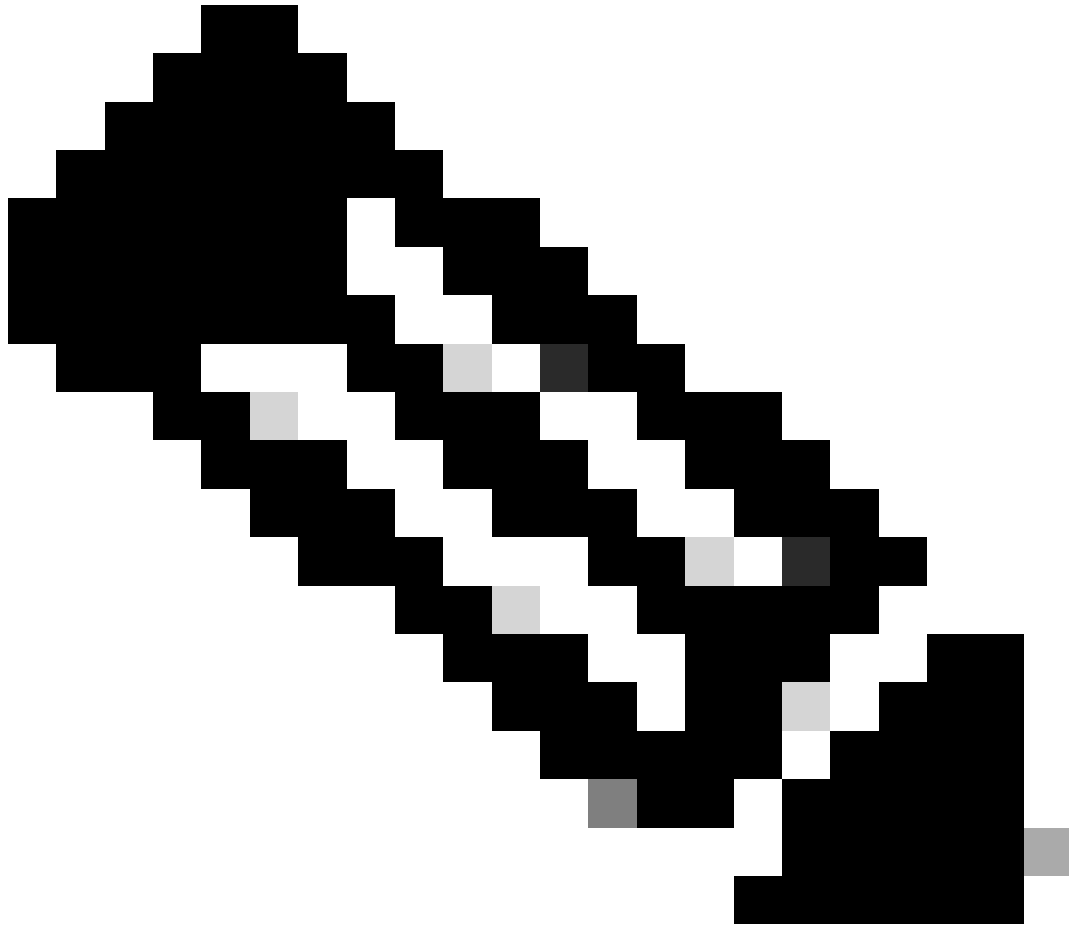
本文檔介紹如何使用Azure虛擬機器安裝Cisco ISE IOS例項。Cisco ISE IOS在Azure雲服務上可用。

必要條件

- 訂閱和資源群組。

導航到所有服務>訂用。確保具有與Microsoft達成企業協定的活動訂閱的Azure帳戶存在。使用Microsoft PowerShell Azure模組CLI執行命令以保留空間：(請參閱[<如何安裝Azure PowerShell>](#)以瞭解如何安裝Power Shell和相關包)。

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



注意：用您的實際租戶ID替換租戶ID

完成[Azure VMware解決方案](#)的[atRequest主機配額](#)預要求，瞭解更多詳細資訊。

在右側的訂閱後建立資源組，導航到所有服務>資源組。按一下Add。輸入資源組名稱。

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 * ⓘ

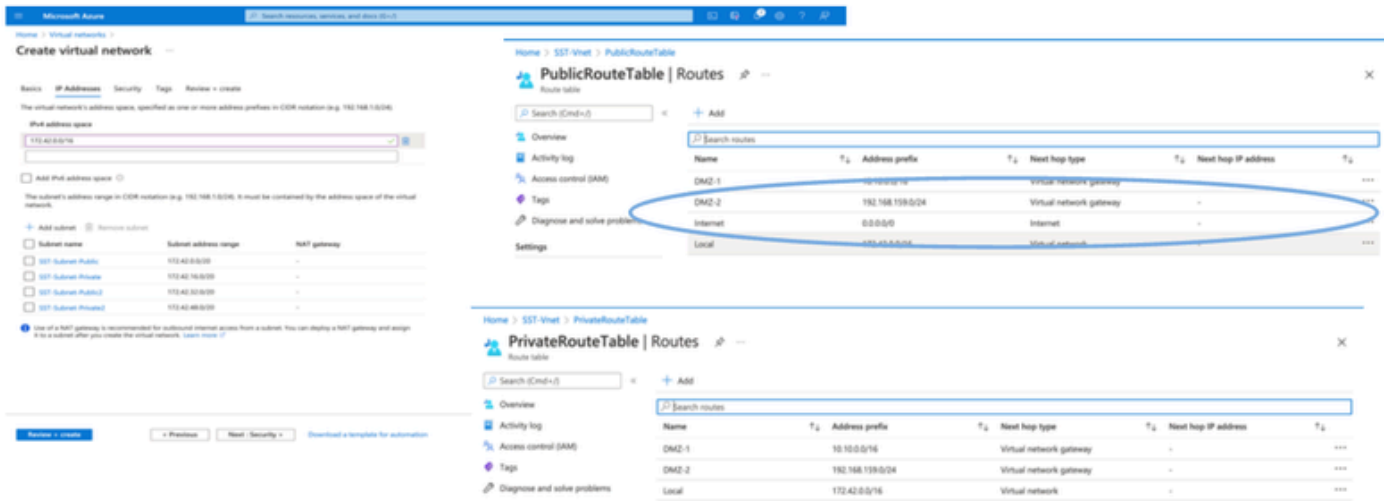
Resource group * ⓘ

Resource details

Region * ⓘ

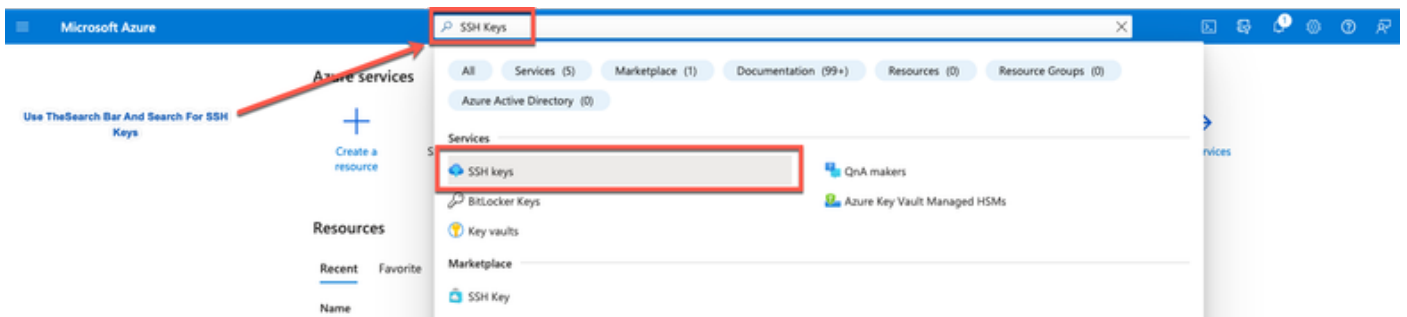
- 虛擬網路和安全組。

需要網際網路可達性的子網必須配置路由表，將下一跳作為internet。請參閱公用子網和專用子網示例。具有公共IP的PAN使離線饋送和線上饋送更新工作，具有專用IP的PAN需要依賴離線饋送更新。

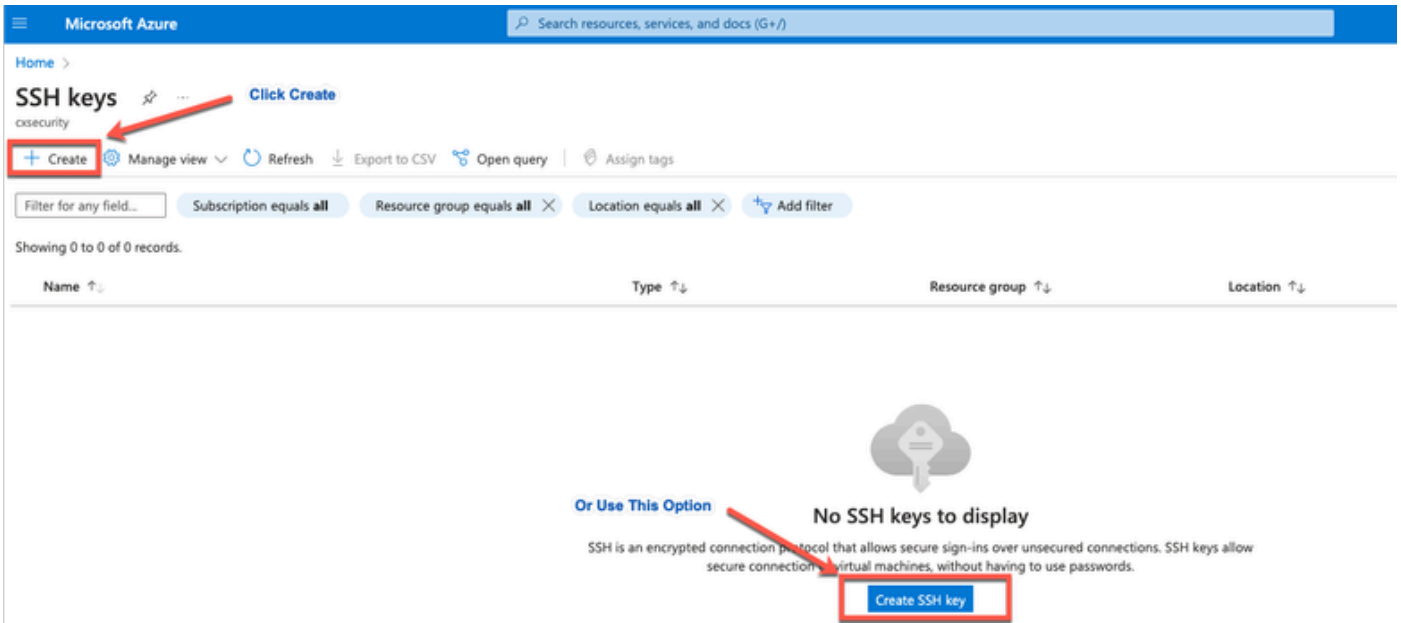


- 建立SSH金鑰對。

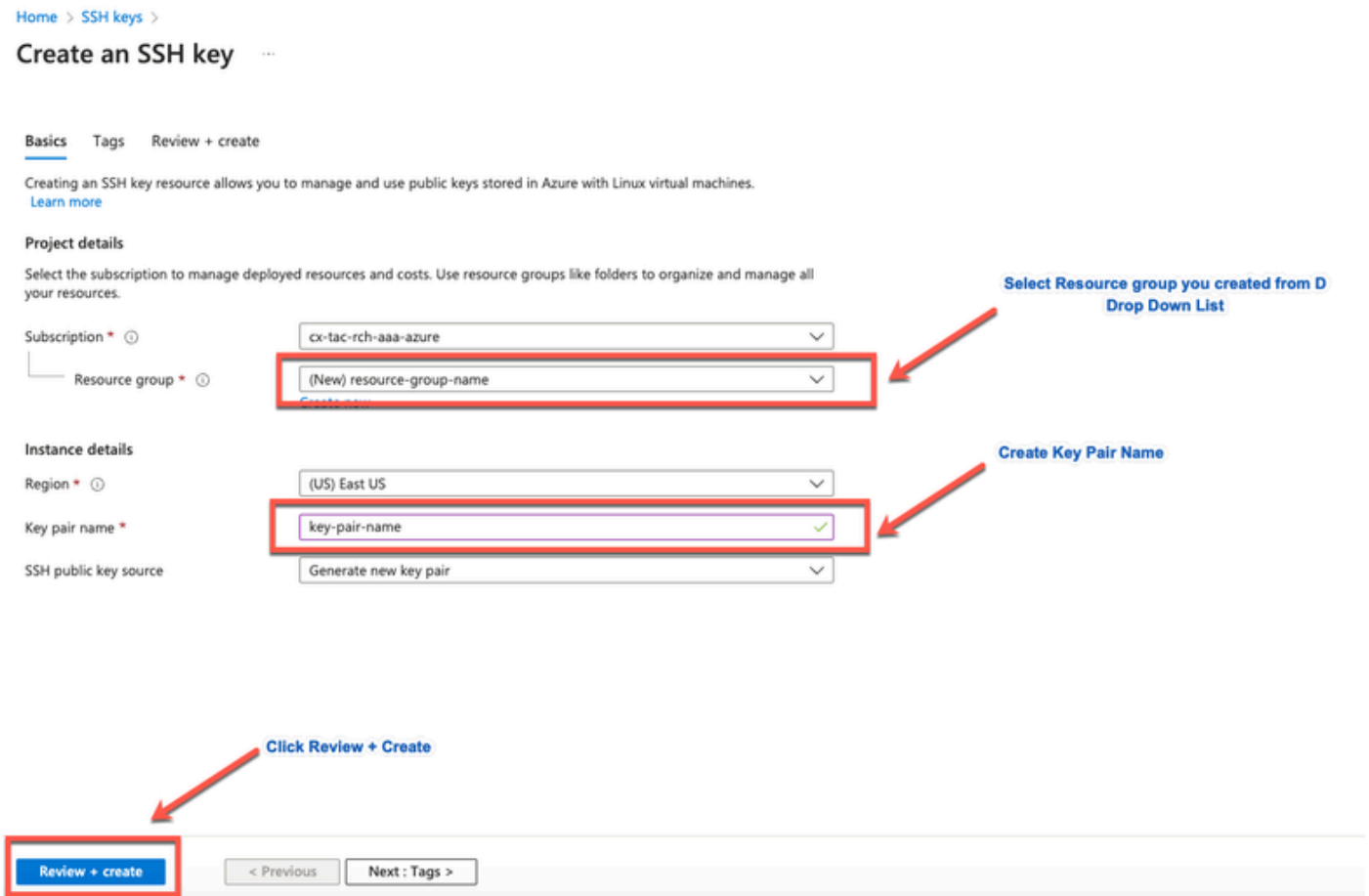
a.使用Azure Web Portal首頁上的搜尋欄搜尋SSH金鑰。



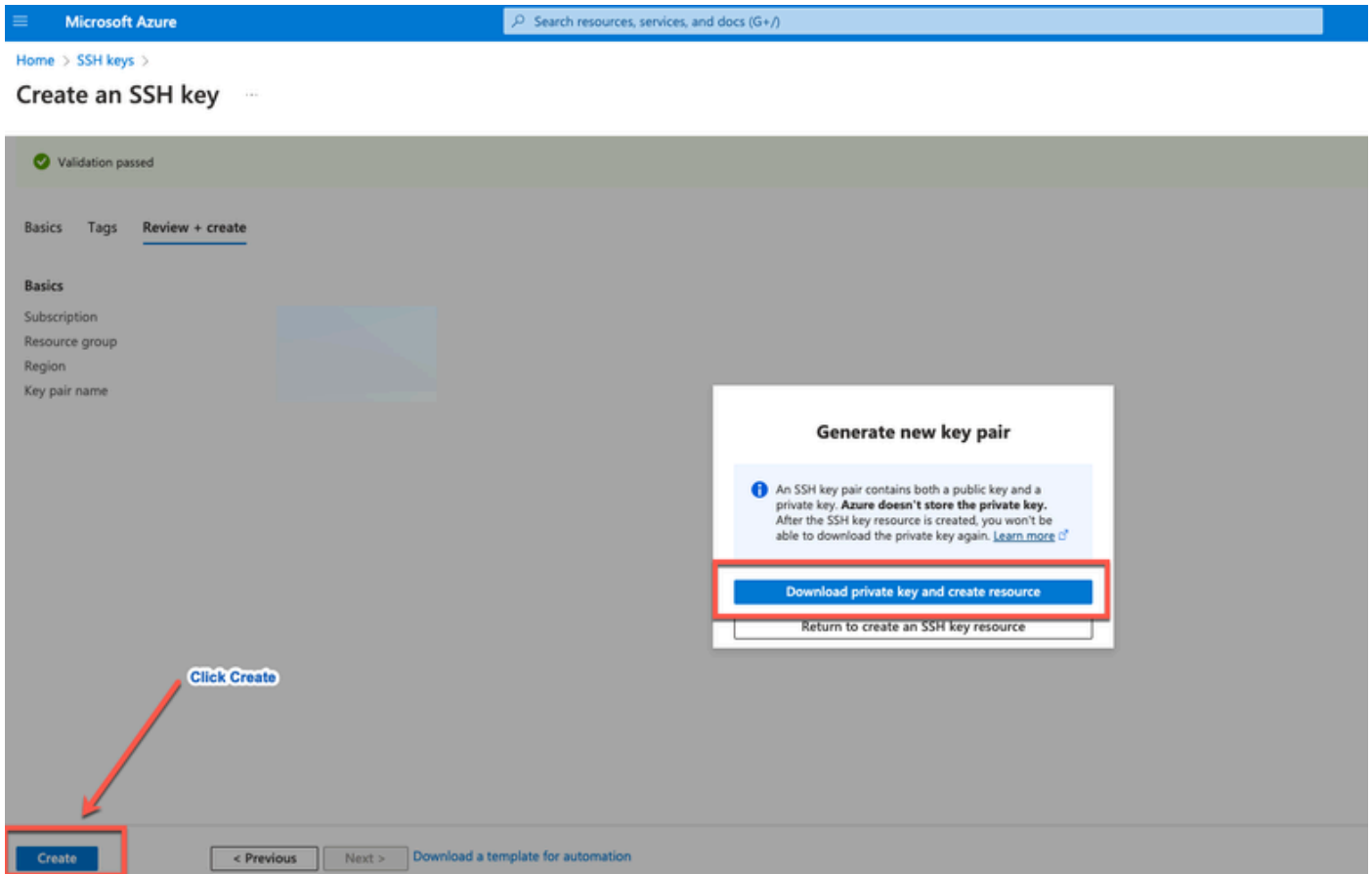
b. 從下一個視窗按一下建立。



c. 從下一個窗口中選擇資源組和金鑰名稱。然後按一下Review + Create。



d. 在下一個窗口中，按一下Create和Download Private Key。



採用元件

本文檔的內容基於這些軟體和雲服務。

- Cisco ISE版本3.2。
- Microsoft Azure雲服務

本文檔中的資訊是在特定實驗室環境中的裝置上建立的。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

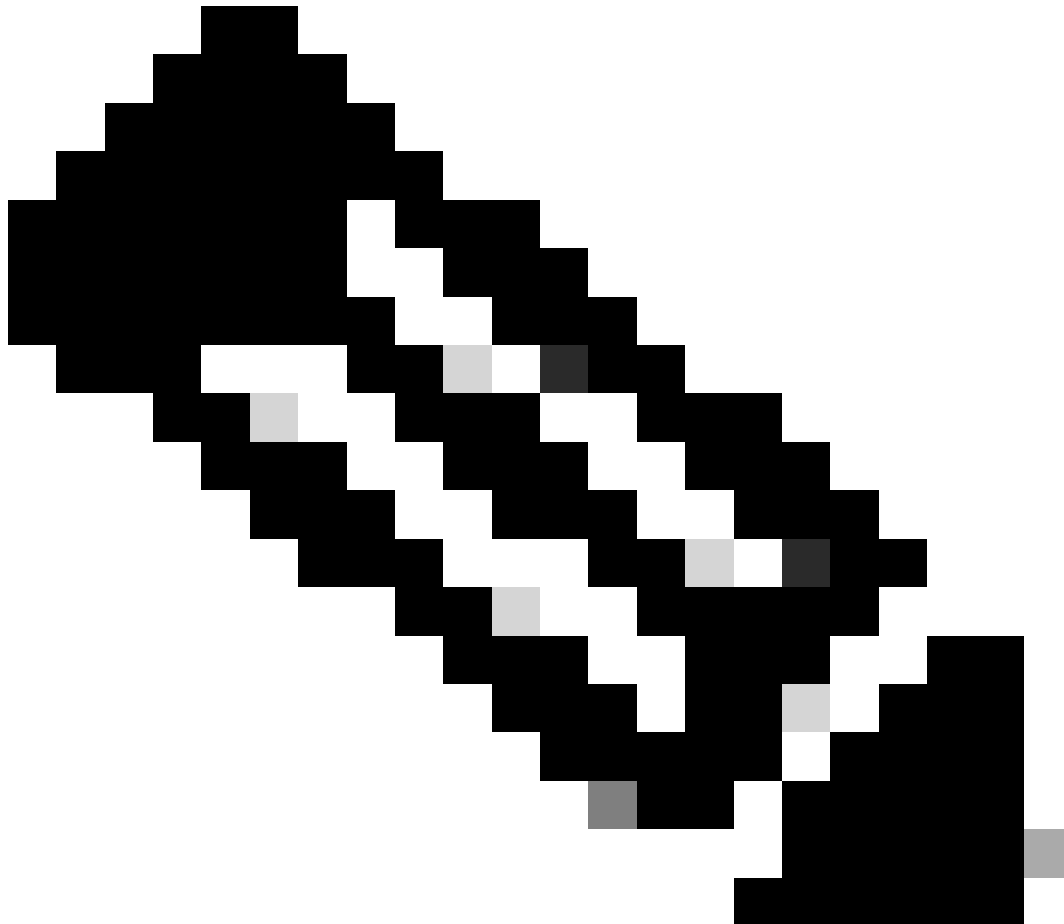
思科ISE支援的Azure VM大小

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大小經過計算最佳化，最適合用作計算密集型任務和應用程式的PSN。

- Dsv4系列是一般用途的Azure VM大小，最適合用作PAN或MnT節點或兩者，用於資料處理任務和資料庫操作。

如果您使用一般用途執行處理作為PSN，則效能數值會低於作為PSN之計算最佳化執行處理的效能。Standard_D8s_v4 VM大小只能用作額外的小型PSN。



注意：請勿克隆現有Azure雲映像以建立思科ISE例項。執行此操作可能導致所建立的ISE機器出現隨機和意外故障。

Microsoft Azure雲服務中Cisco ISE的限制

- 如果您[使用Azure虛擬機器](#)建立[Cisco ISE](#)，預設情況下，Microsoft Azure透過DHCP伺服器向VM分配專用IP地址。在Microsoft Azure上建立思科ISE部署之前，您必須使用Microsoft Azure分配的IP地址更新轉發和逆向DNS條目。

或者，在安裝思科ISE後，透過更新Microsoft Azure中的網路介面對象為虛擬機器分配靜態IP地址：

1. 停止虛擬機器。
 2. 在VM的「專用IP地址設定」區域中的「分配」區域中，按一下「靜態」。
 3. 重新啟動虛擬機器。
 4. 在思科ISE串列控制檯中，將IP地址分配為Gi0。
 5. 重新啟動Cisco ISE應用伺服器。
- 只有兩個NIC (千兆乙太網0和千兆乙太網1) 支援雙NIC。要在思科ISE例項中配置輔助NIC，您必須首先在Azure中建立網路介面對象，關閉思科ISE例項的電源，然後將此網路介面對象附加到思科ISE。在Azure上安裝並啟動Cisco ISE後，使用Cisco ISE CLI手動將網路介面對象的IP地址配置為輔助NIC。
 - Cisco ISE升級工作流程在Microsoft Azure上的Cisco ISE中不可用。僅支援全新安裝。但是，您可以執行配置資料的備份和恢復。
 - 公共雲僅支援第3層功能。Microsoft Azure上的思科ISE節點不支援依賴第2層功能的思科ISE功能。例如，透過Cisco ISE CLI使用DHCP SPAN分析器探測功能和CDP協定功能是當前不支援的功能。
 - 當您執行配置資料的恢復和備份功能時，在備份操作完成後，首先透過CLI重新啟動思科ISE。然後，從Cisco ISE GUI啟動恢復操作。
 - Azure不支援使用基於密碼的身份驗證對思科ISE CLI進行SSH訪問。您只能透過金鑰對訪問思科ISE CLI，並且必須安全地儲存此金鑰對。如果使用私鑰 (或PEM) 檔案並且丟失了檔案，您將無法訪問Cisco ISE CLI。

不支援使用基於密碼的身份驗證方法訪問Cisco ISE CLI的任何整合，例如，Cisco DNA Center 2.1.2版及更早版本。

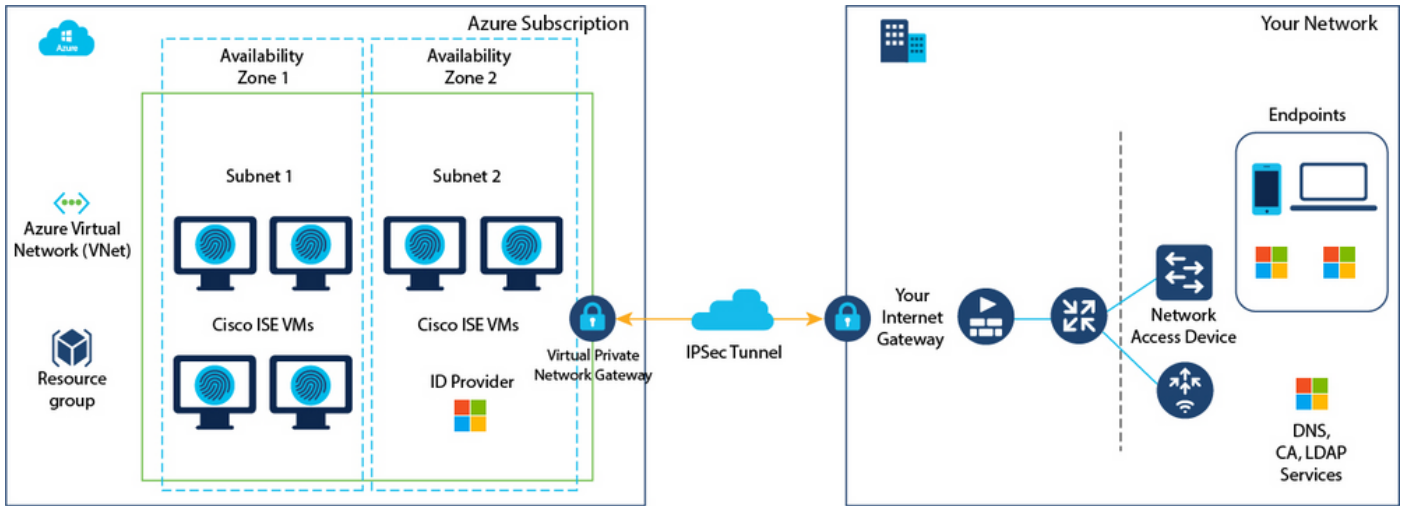
- Azure上的Cisco ISE IOS部署通常利用動態多點虛擬專用網路(DMVPN)和軟體定義廣域網(SD-WAN)等VPN解決方案，其中IPSec隧道開銷可能導致MTU和分段問題。在這種情況下，Cisco ISE IOS不會收到完整的RADIUS資料包，並且身份驗證失敗不會觸發故障錯誤日誌。

一種可能的解決方法是尋找Microsoft技術支援，以探索Azure中允許無序片段傳遞至目標而不会被丟棄的任何解決方案。

- CLI管理員使用者必須為「iseadmin」。

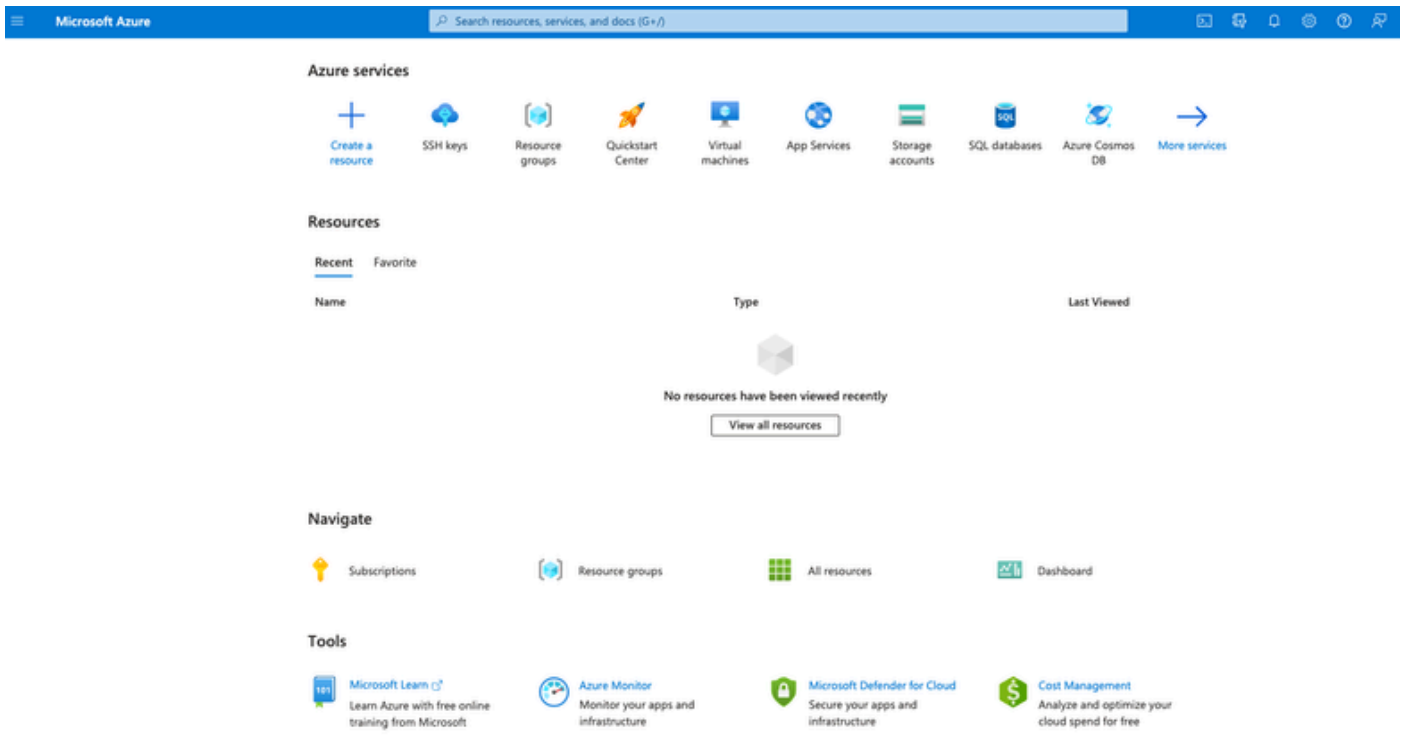
設定

連線到Azure雲的ISE部署示例

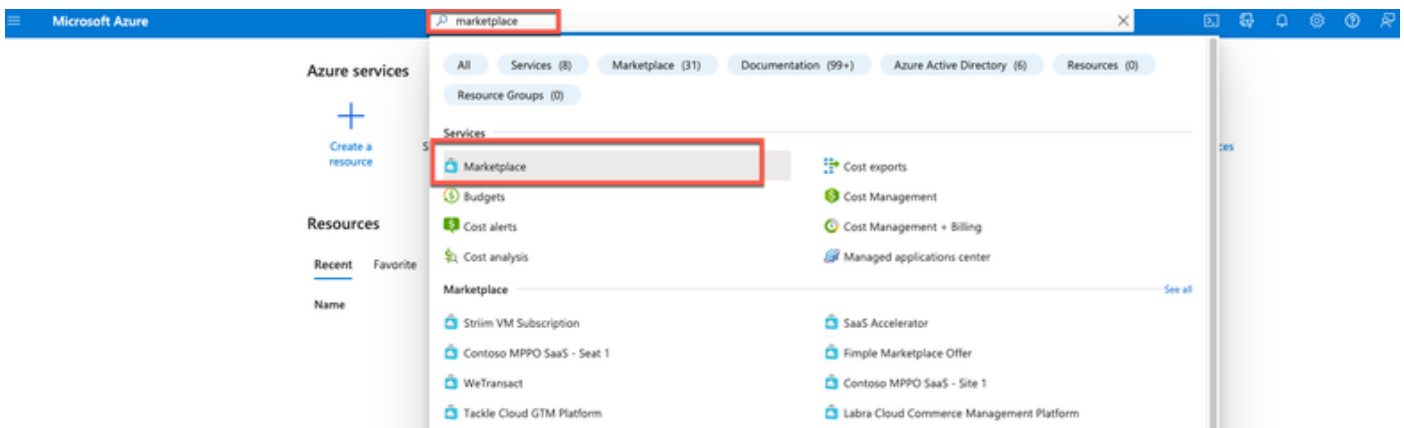


組態

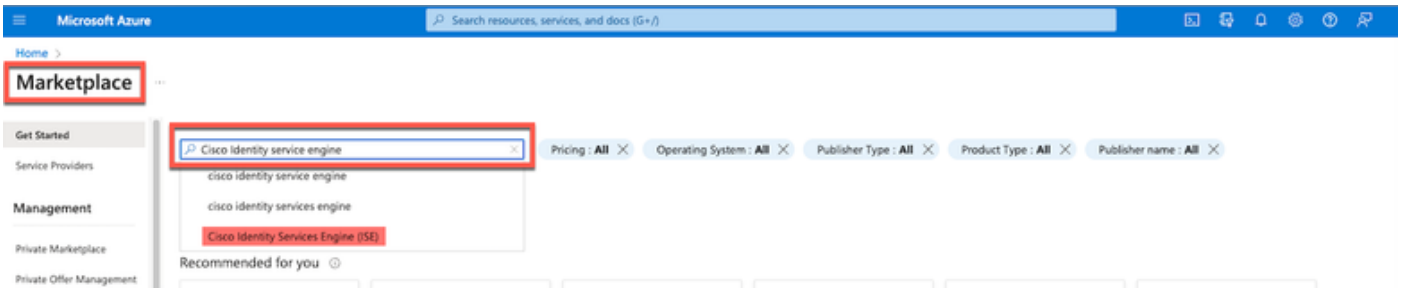
- 第(1)步：轉到[Azure門戶](#)並登入你的Microsoft Azure帳戶。



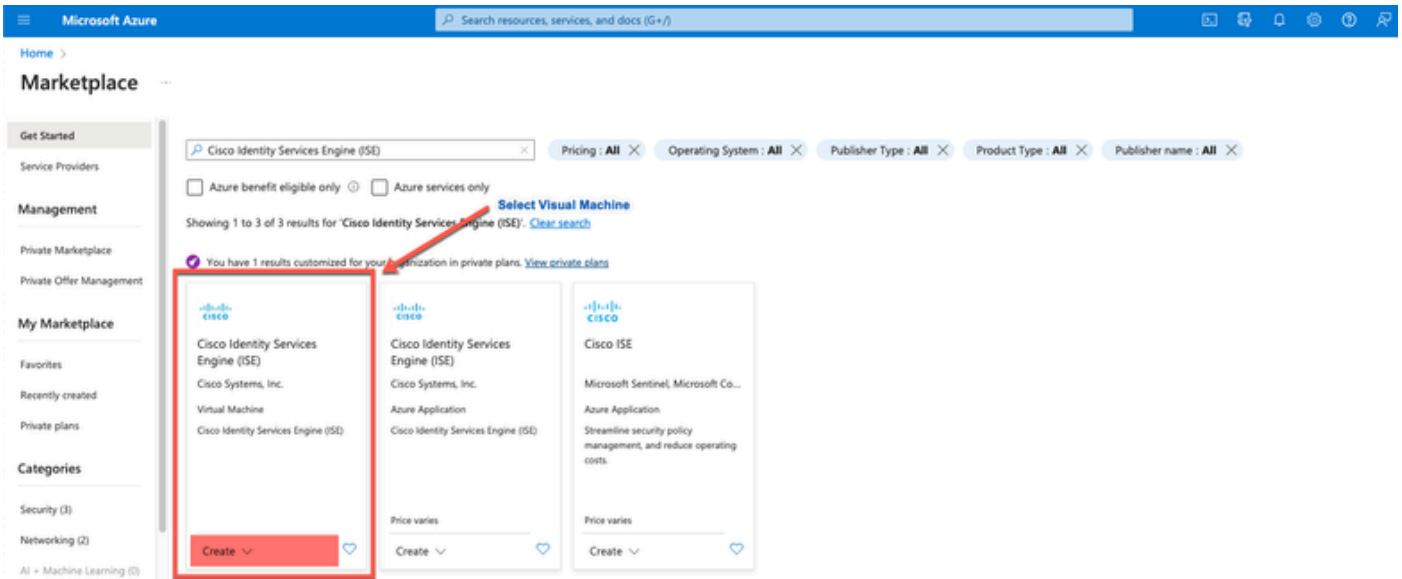
- 步驟(2)：使用窗口頂部的搜尋欄位搜尋Marketplace。



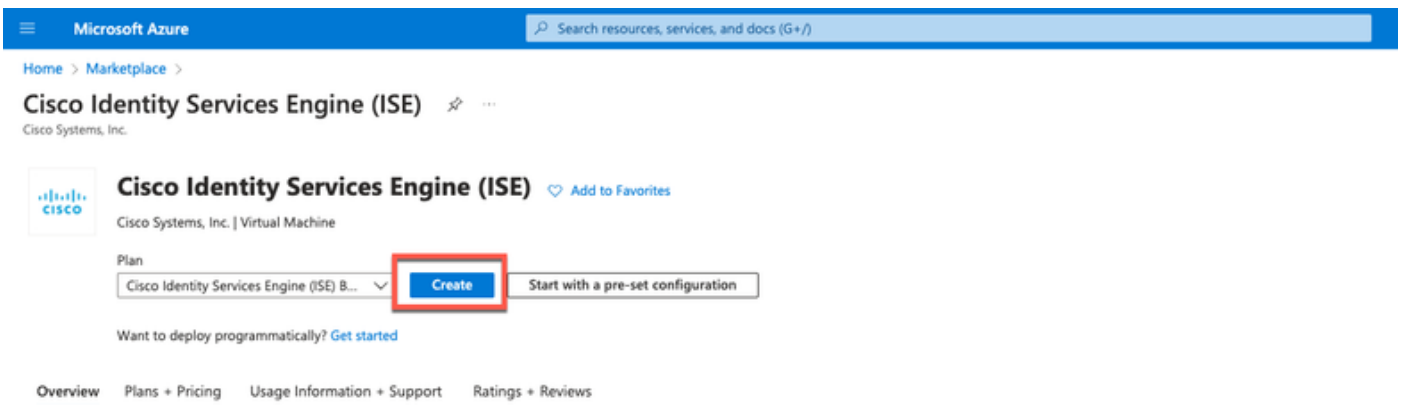
- 第(3)步：使用搜尋Marketplace搜尋欄位搜尋思科身份服務引擎(ISE)。



- 第(4)步：點選虛擬機器。



- 第(5)步：在顯示的新窗口中，按一下建立。



- 步驟(6)：在基礎頁籤中：

- a.在專案詳細資訊區域，從預訂和資源組下拉選單中選擇所需的值。
- b.在例項詳細資訊區域中，在虛擬機器名稱欄位中輸入值。
- c.從Image下拉選單中選擇Cisco ISE映像。
- d.從Size下拉選單中選擇要用來安裝Cisco ISE的例項大小。選擇思科ISE支援的例項，如標題為

Azure Cloud的表中所列

Cisco ISE支援的例項，在[Azure雲上的Cisco ISE](#)部分。

- e. 在Administrator account > Authentication type區域中，按一下SSH Public Key單選按鈕。
- f. 在「Username」欄位中，輸入iseadmin。
- g. 從SSH public key source下拉選單中選擇Use existing key stored in Azure。
- h. 從儲存的金鑰下拉選單中，選擇作為此任務的先決條件而建立的金鑰對。
- j. 在Inbound port rules區域中，點選Allow selected ports單選按鈕。
- k. 在許可區域中，從許可型別下拉選單中選擇「其他」。

[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)

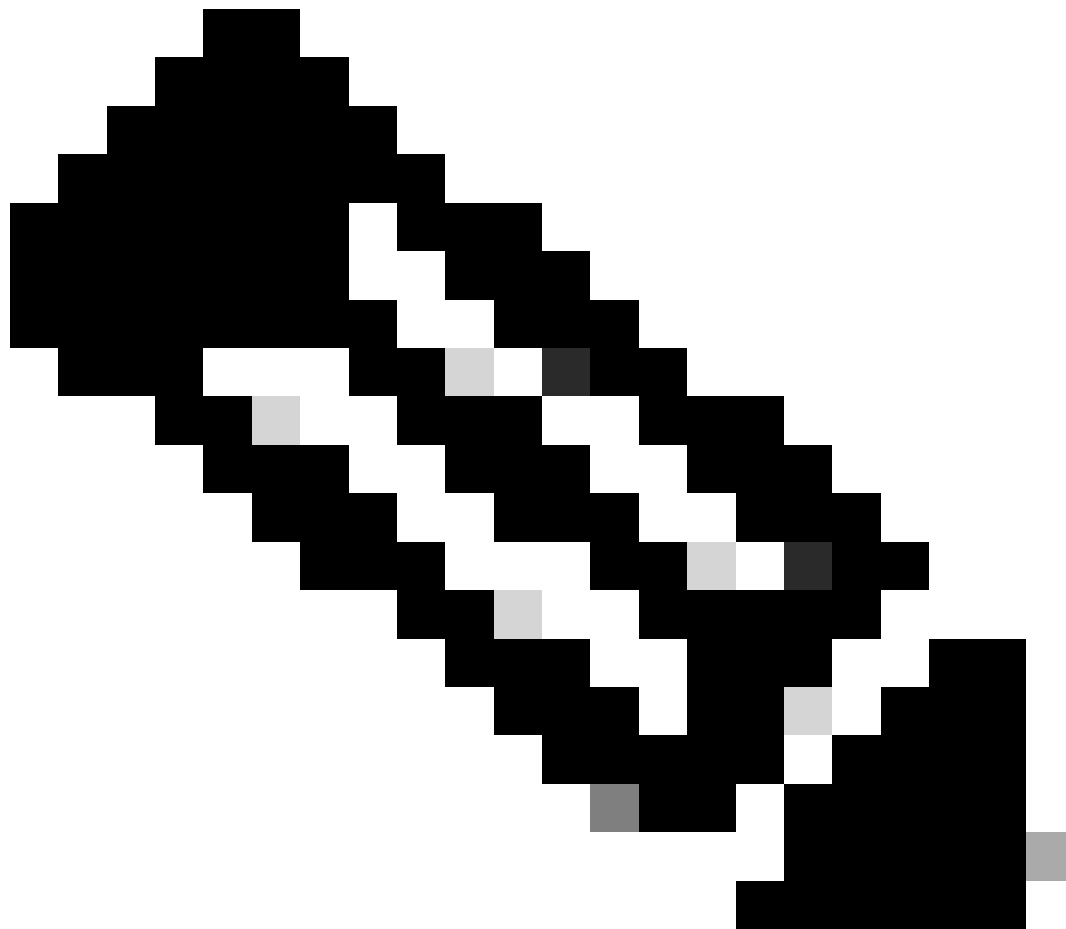
[See all sizes](#)

Administrator account

Authentication type

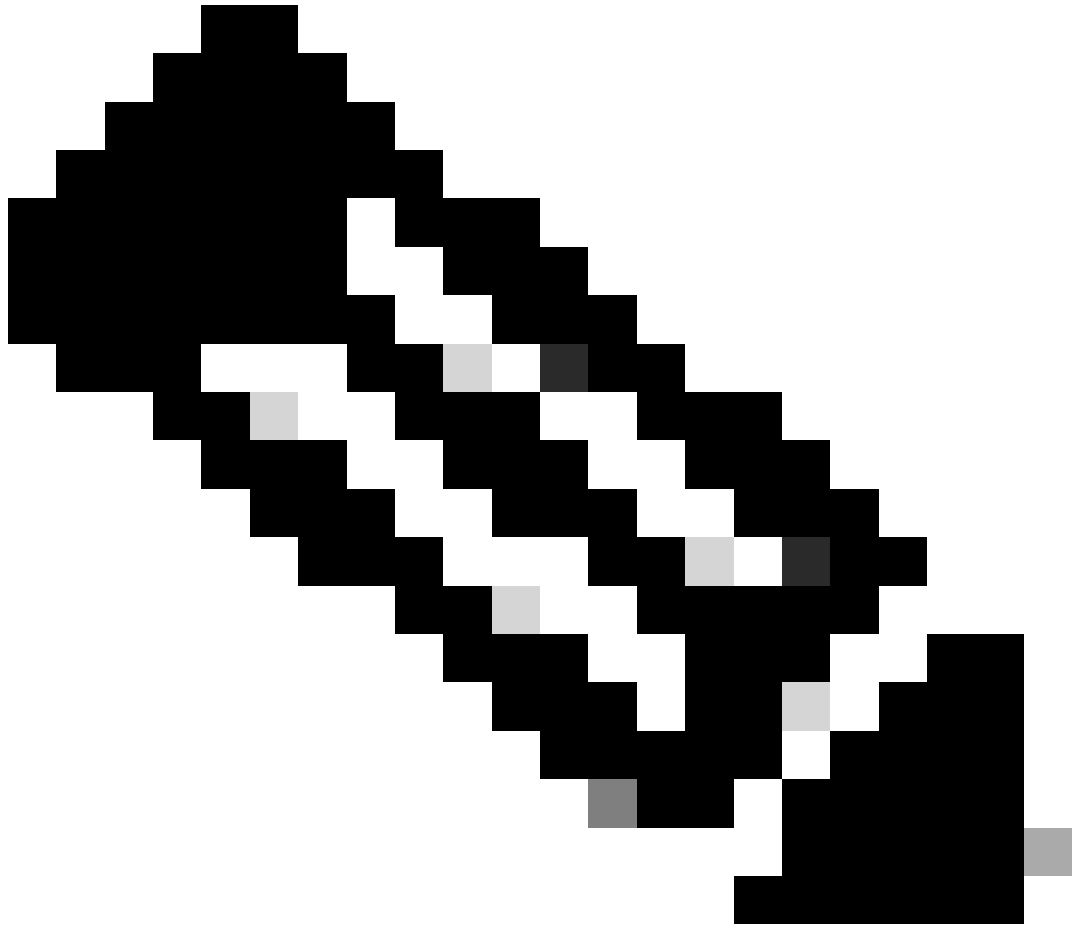
 SSH public key Password[Click Here To Select ISE Template](#)

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



注意：對於「磁碟型別」，可從下拉式清單中選取更多選項。您可以選擇符合您需求的產品。對於對生產和效能敏感的工作負載，推薦使用高級SSD。

-
- 第(9)步：在網路介面區域中，從虛擬網路、子網和配置網路安全組下拉選單中，選擇您建立的虛擬網路和子網。



注意：具有公共IP地址的子網接收線上和離線狀態饋送更新，而具有專用IP地址的子網僅接收離線狀態饋送更新。

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

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：點選下一步：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 >](#)

- 步驟(11)：在管理標籤中，保留必要欄位的預設值，然後按一下下一步：進階。



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"

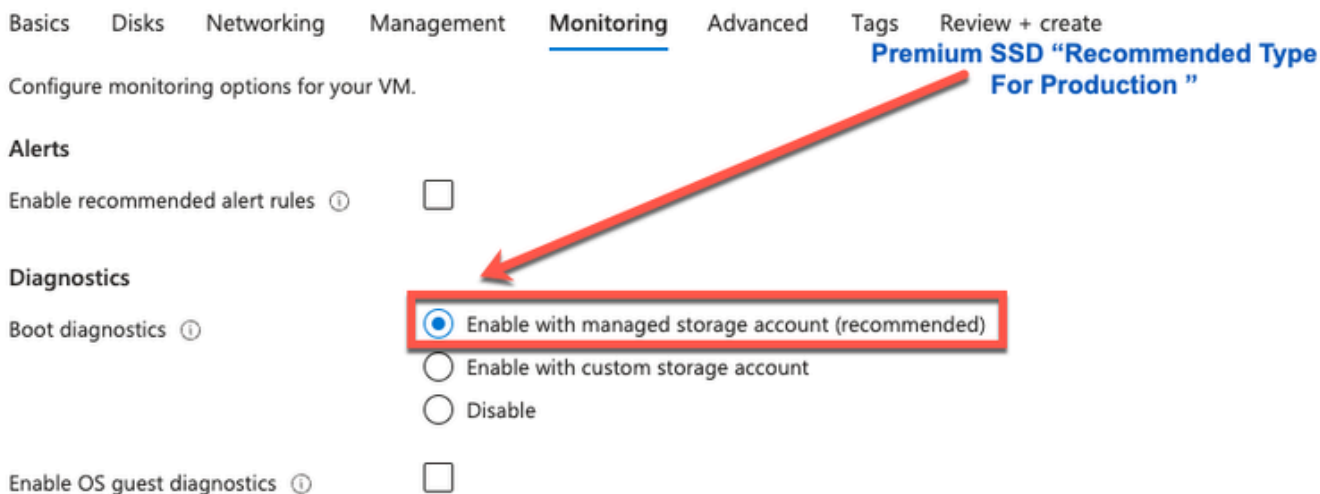
Alerts

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：在使用者資料區域中，選中啟用使用者資料覈取方塊。

在「使用者資料」欄位中，填寫資訊：

hostname=<Cisco ISE的主機名>

primarynameserver=<IPv4地址>

dnsdomain=<域名>

ntpserver=<IPv4地址或NTP伺服器的FQDN>

timezone=<timezone>

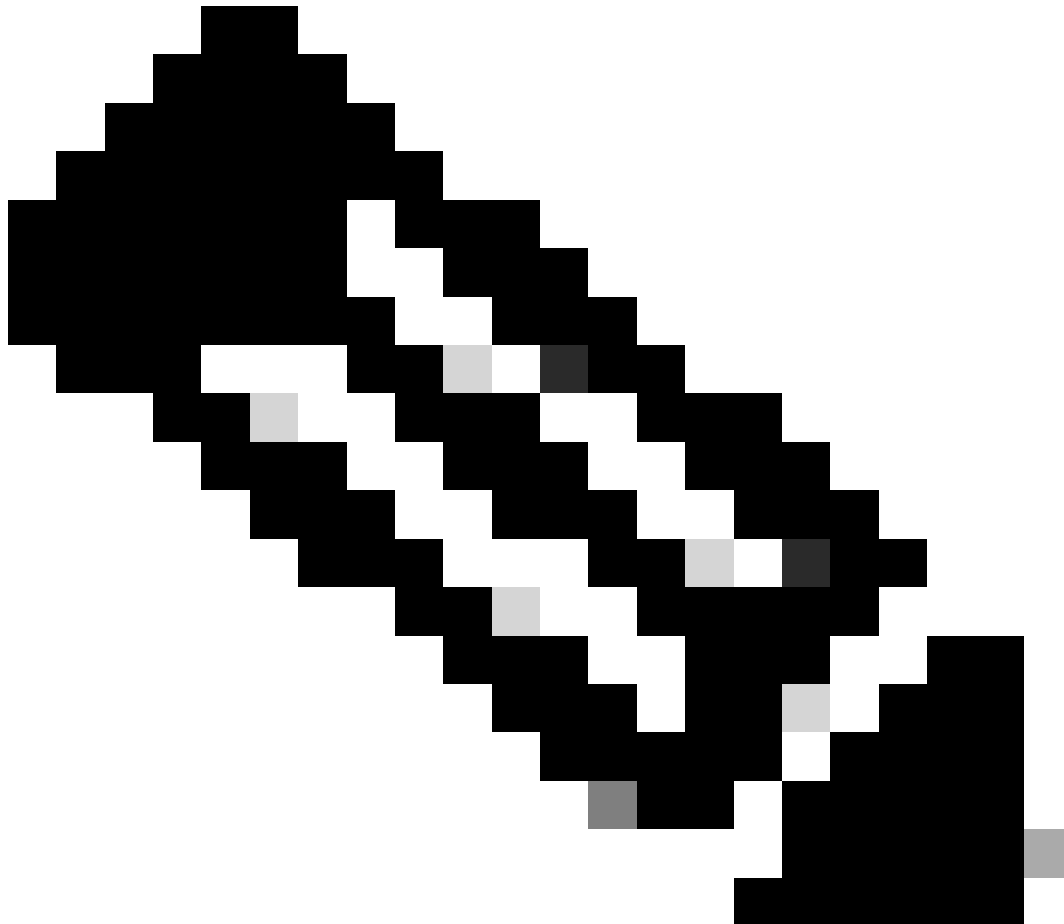
password=<password>

ersapi=<是/否>

openapi=<是/否>

pxGrid=<是/否>

pxgrid_cloud=<是/否>



注意：對於透過使用者資料條目配置的每個欄位，必須使用正確的語法。您在「使用者資料」欄位中輸入的資訊在輸入時不會經過驗證。如果使用錯誤的語法，當您啟動映像時，思科ISE服務不會出現。

有關必須透過User Data欄位提交的配置，請參閱準則：

- a.主機名：輸入僅包含字母數字字元和連字元(-)的主機名。主機名的長度不能超過19個字元，並且不能包含下劃線(_)。
- b.主名稱伺服器：輸入主名稱伺服器的IP地址。僅支援IPv4地址。

在此步驟中，您只能增加一個DNS伺服器。您可以在安裝後透過Cisco ISE CLI增加其他DNS伺服器

o.

c. dnsdomain : 輸入DNS域的FQDN。條目可以包含ASCII字元、數字、連字元(-)和句點(.)。

d. ntpserver : 輸入必須用於同步的NTP伺服器的IPv4地址或FQDN。

在此步驟中只能增加一個NTP伺服器。您可以在安裝後透過Cisco ISE CLI增加其他NTP伺服器。使用有效且可訪問的NTP伺服器，因為ISE操作需要該伺服器。

e.時區 : 輸入時區，例如Etc/UTC。我們建議您將所有思科ISE節點設定為協調世界時(UTC)時區，特別是如果您的思科ISE節點安裝在分散式部署中。此程式可確保來自部署中各個節點的報告和記錄的時間戳始終同步。

f.密碼 : 配置基於GUI的登入思科ISE的密碼。您輸入的密碼必須符合Cisco ISE密碼策略。密碼必須包含6到25個字元，且至少包含一個數字、一個大寫字母和一個小寫字母。密碼不能與使用者名稱相同，也不能與使用者名稱相反 (iseadmin或nimdaesi)、cisco或ocsic。允許的特殊字元為@~*!，+=_-。請參閱[Cisco ISE管理員指南](#)的「基本設定」一章中的「使用者密碼策略」一節瞭解您的版本。

g. ersapi : 輸入yes以啟用ERS，或輸入no以禁止ERS。

h. openapi : 輸入yes以啟用OpenAPI，或輸入no以禁止OpenAPI。

i. pxGrid : 輸入yes以啟用pxGrid，或輸入no以停用pxGrid。

j. pxgrid_cloud : 輸入yes以啟用pxGrid雲，或輸入no以停用pxGrid雲。要啟用pxGrid雲，必須啟用pxGrid。如果停用pxGrid，但啟用pxGrid雲，則在啟動時不會啟用pxGrid雲服務。

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

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 >

使用者資料段落

- 第(13)步：點選下一步：標籤。

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 >

- 步驟(14)：若要建立可讓您分類資源的名稱-值配對，並合併多個資源與資源群組，請在名稱與值欄位中輸入值。

[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：點選下一步：複查+建立。

Review + create

< Previous

Next : Review + create >

- 第(16)步：檢視您目前提供的資訊，然後點選建立。

會顯示Deployment is in progress視窗。建立思科ISE例項並可供使用大約需要30分鐘。Cisco ISE VM例項顯示在

Virtual Machines窗口（使用主搜尋欄位查詢該窗口）。

Create a virtual machine

Validation passed

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

Create < Previous Next > [Download a template for automation](#)

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

Search Delete Cancel Redeploy Download Refresh

- 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](#)

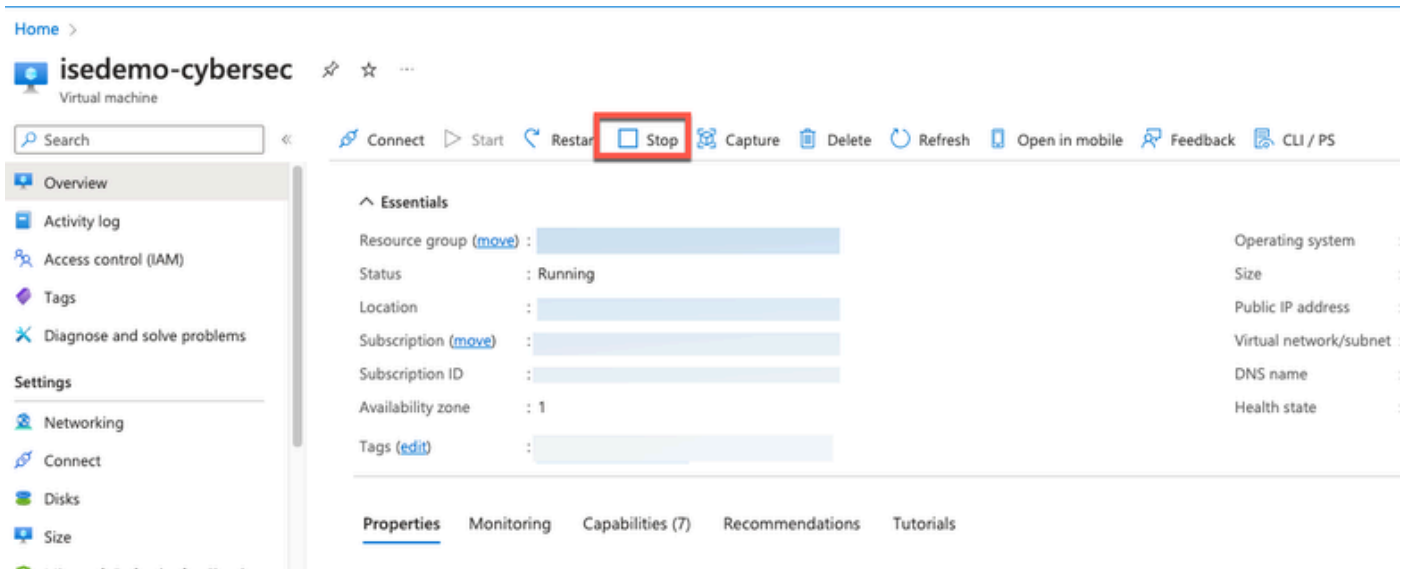
下一步要做什麼

由於Microsoft Azure預設設定，您建立的思科ISE VM僅配置為300 GB磁碟大小。Cisco ISE節點通常需要300 GB以上的磁碟大小。首次從Microsoft Azure啟動Cisco ISE時，您可以看到Insufficient Virtual Memory警報。

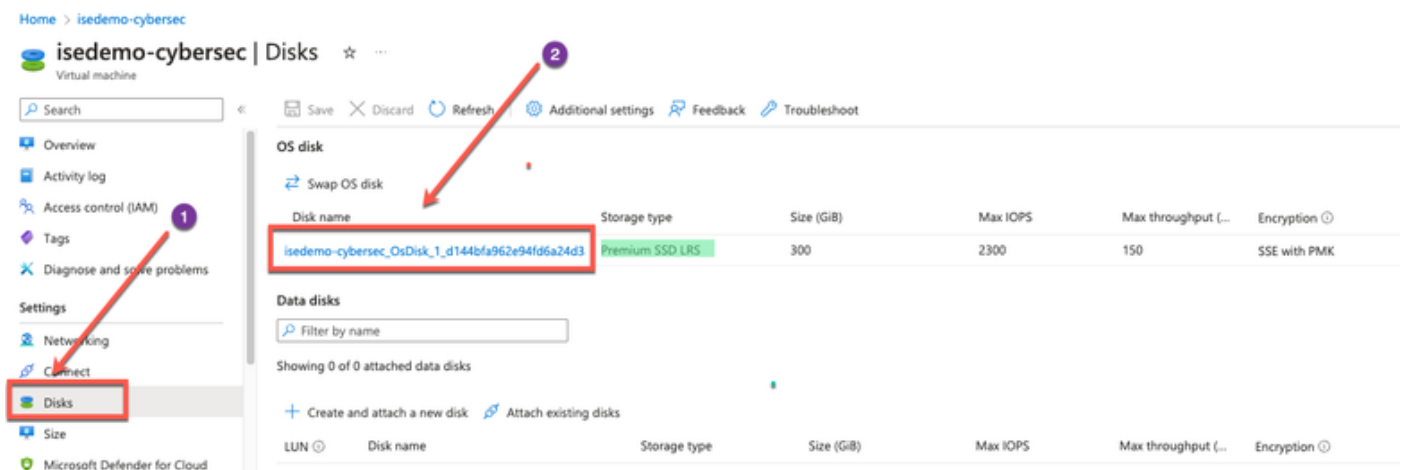
在思科ISE VM建立完成後，登入思科ISE管理門戶驗證思科ISE已設定。然後，在Microsoft Azure門

戶中，執行並完成虛擬機器窗口中的步驟以編輯磁碟大小：

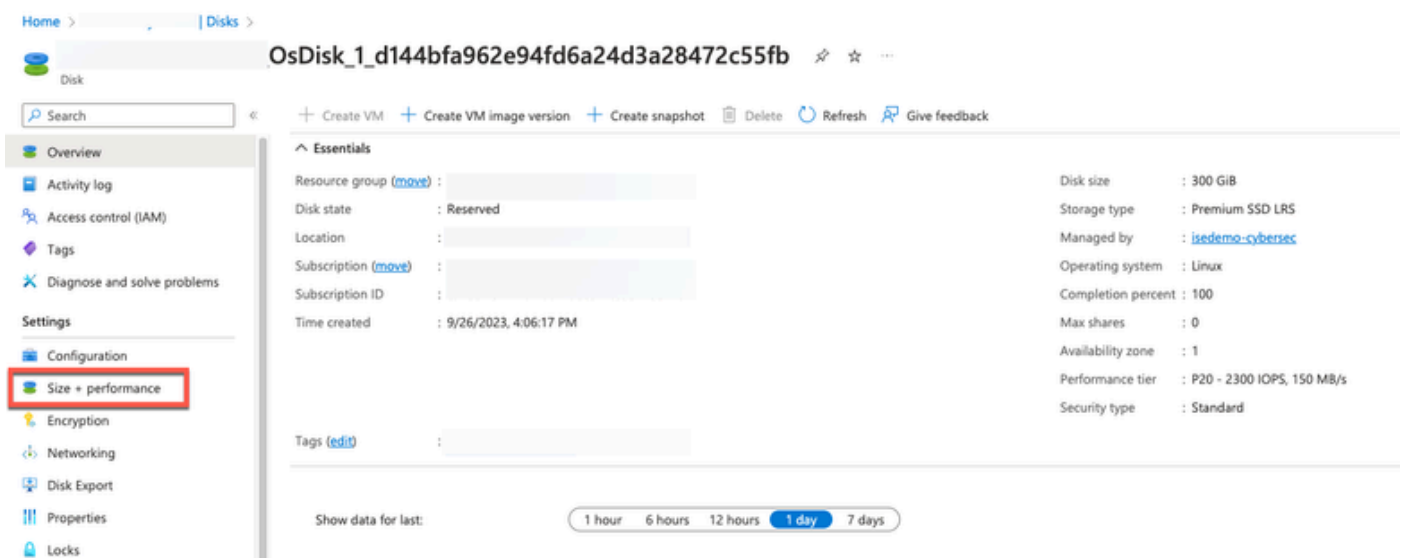
1. 停止Cisco ISE例項。



2. 在左側窗格中按一下Disk，然後按一下要與Cisco ISE一起使用的磁碟。



3. 按一下左側窗格中的大小+效能。



4. 在自定義磁碟大小欄位中，輸入所需的磁碟大小（以GiB表示）。

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

安裝後任務

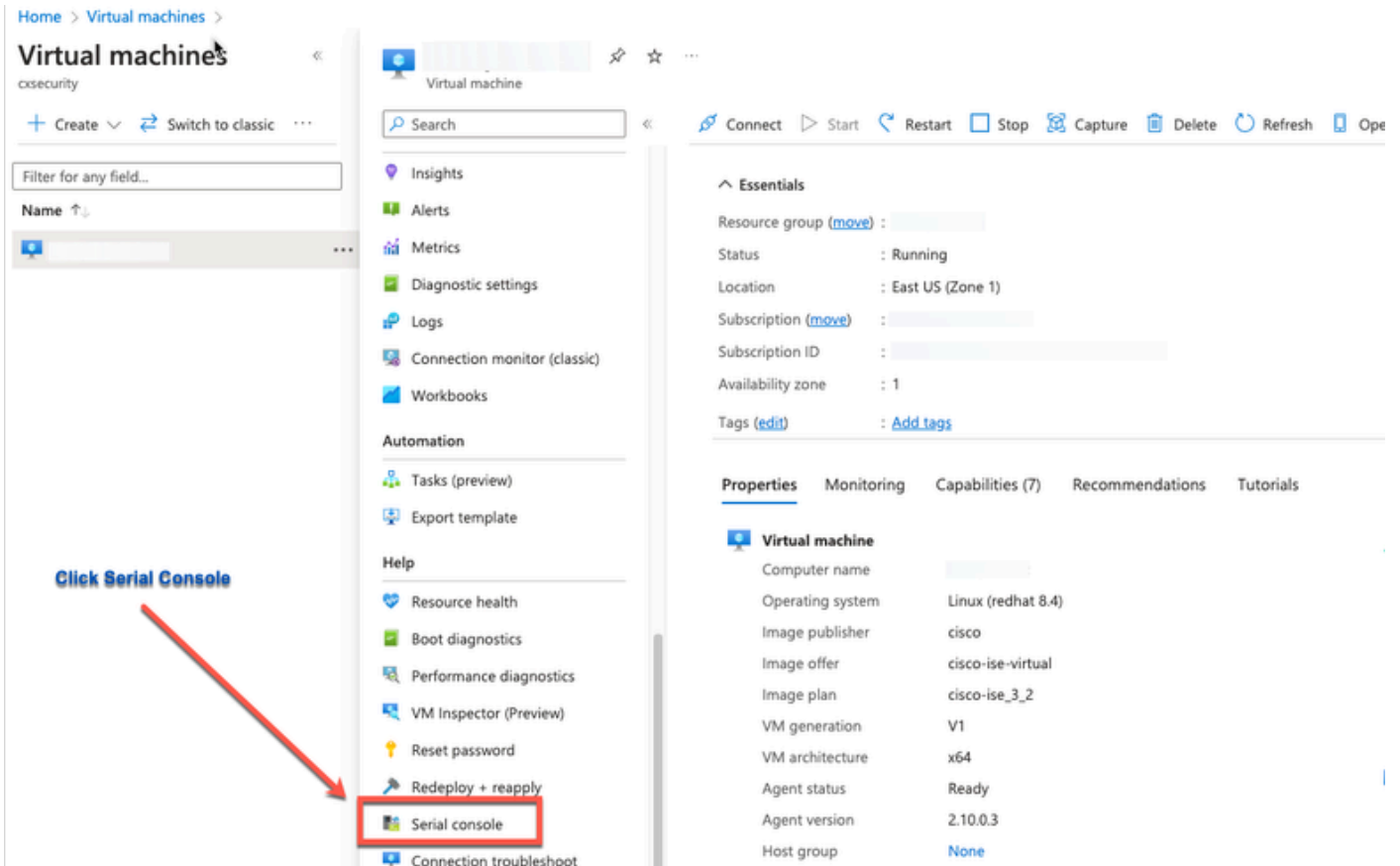
有關成功建立Cisco ISE例項後必須執行的安裝後任務的資訊，請參閱您的Cisco ISE版本的[Cisco ISE安裝指南](#)中的「安裝驗證和安裝後任務」一章。

在Azure Cloud上恢復並重置密碼

完成幫助重置或恢復思科ISE虛擬機器密碼的任務。選擇您需要的任務，並執行詳細步驟。

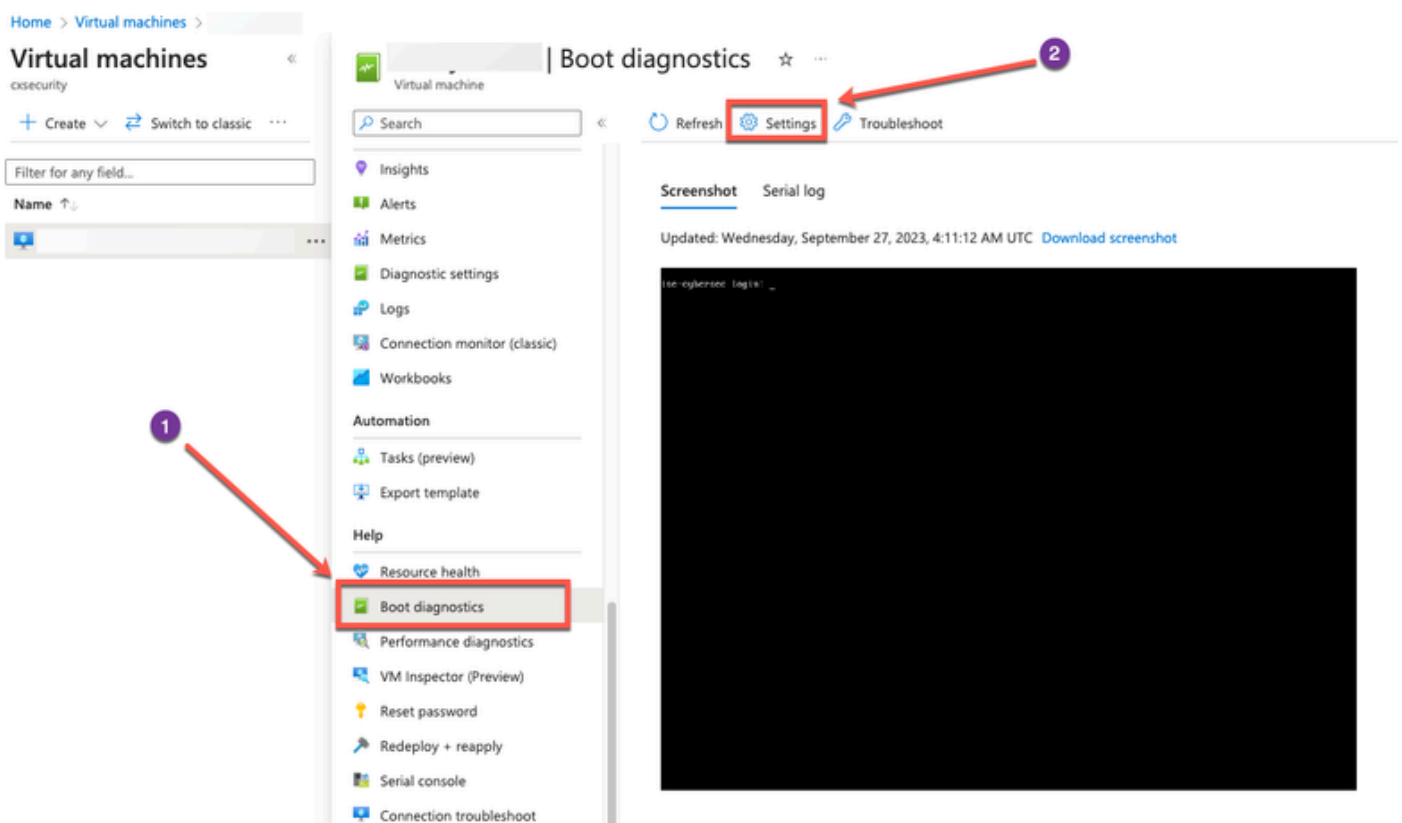
1. 透過串列控制檯重置思科ISE GUI密碼

- 第(1)步：登入到Azure雲並選擇包含您的Cisco ISE虛擬機器的資源組。
- 第(2)步：從資源清單中，點選要重置其密碼的思科ISE例項。
- 第(3)步：從左側選單中從支援+故障排除部分按一下串列控制檯。

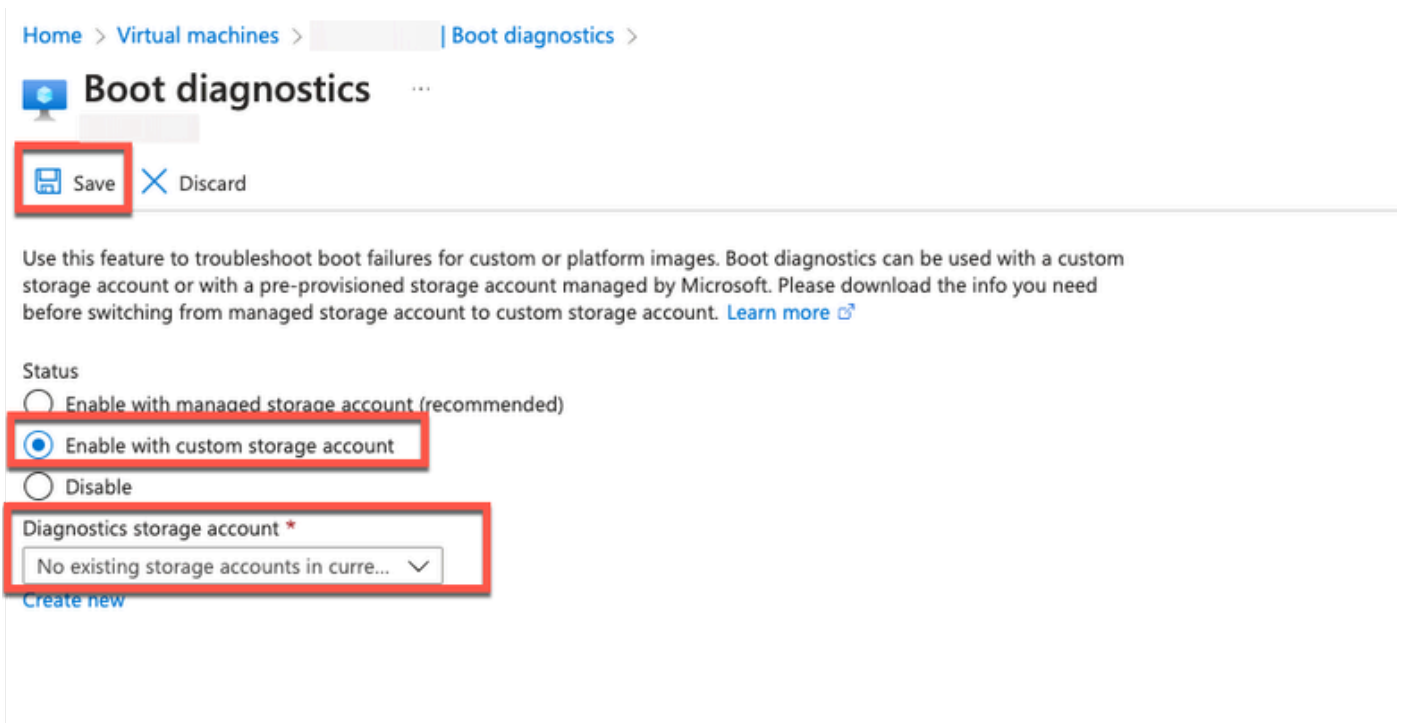


- 步驟(4)：如果您在此檢視錯誤訊息，您必須執行並完成以下步驟來啟用開機診斷：

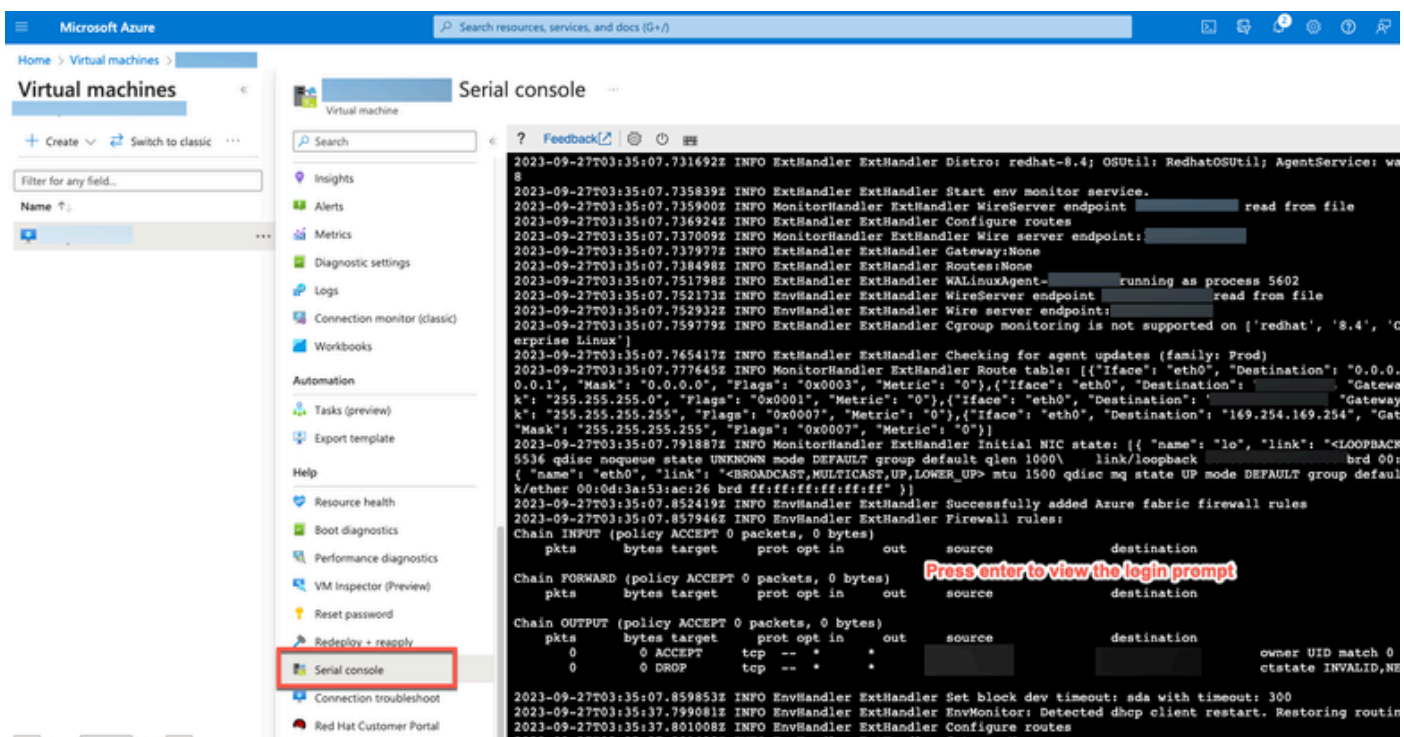
a. 從左側選單中按一下 Boot diagnostics。



b. 按一下 Enable with custom storage account。然後按一下 Save。



- 第(5)步：從左側選單中從支援+故障排除部分按一下串列控制檯。 Azure Cloud Shell將顯示在新窗口中。如果螢幕為黑色，請按Enter檢視登入提示。



- 步驟(8)：登入序列主控台。若要登入序列主控台，您必須使用安裝執行處理時設定的原始密碼。
- 第(9)步：使用application reset-password iseadmin命令為iseadmin帳戶配置新的GUI密碼。

2. 為SSH訪問建立新的公鑰對

透過此任務，您可以向儲存庫中增加其他金鑰對。在Cisco ISE例項配置時建立的現有金鑰對不會被

您建立的新公鑰替換。

- 第(1)步：在Azure雲中建立新的公鑰。

[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 >

您將看到一個彈出窗口，提示您選擇Download private key and create resource，以便將SSH金鑰作為.pem檔案下載。

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 an SSH key resource](#)

- 第(2)步：要建立新儲存庫以儲存公共金鑰，請參閱[Azure Repos文檔](#)。

如果已經有一個可透過CLI訪問的儲存庫，請跳到步驟3。

- 第(3)步：要導入新的公鑰，請使用命令`crypto key import <public key filename> repository <repository name>`。
- 第(4)步：導入完成後，您可以使用新公鑰透過SSH登入思科ISE。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。