Installieren von ISE auf Azure Cloud Services

Inhalt

Einleitung

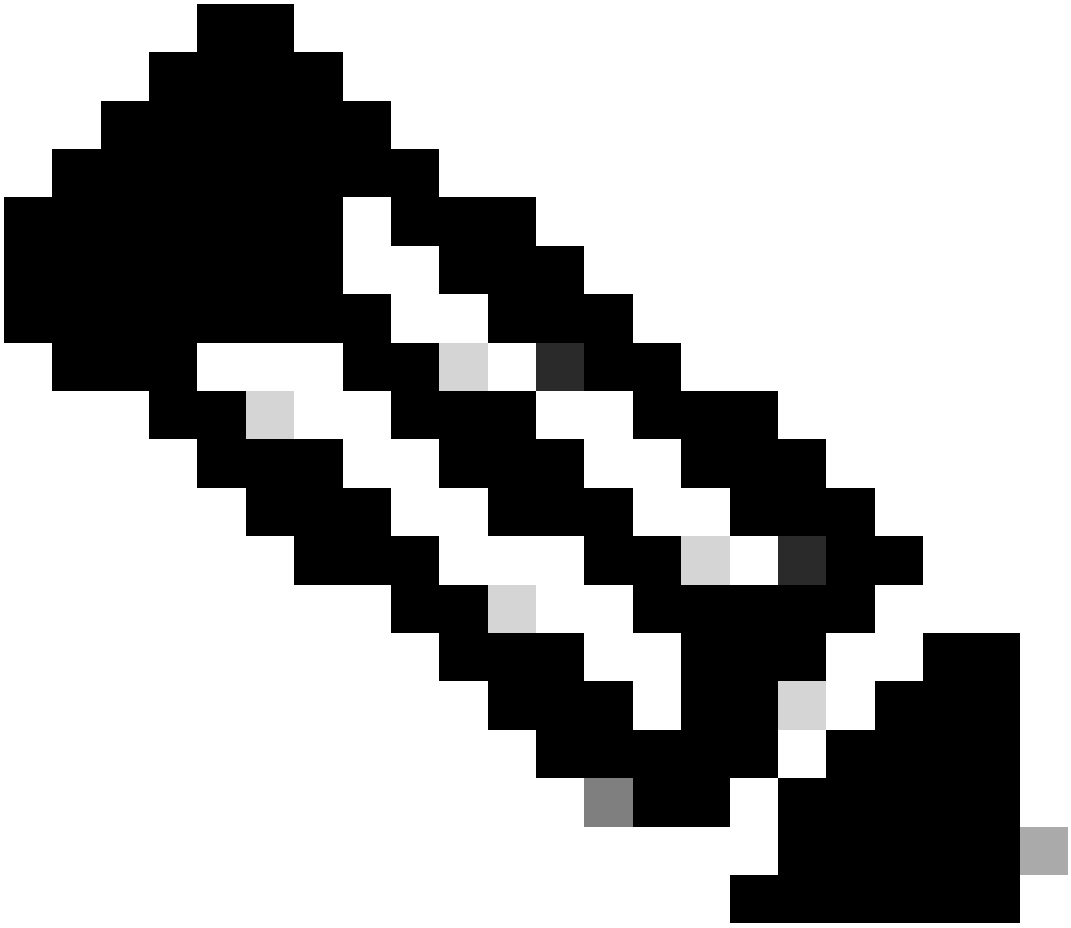
In diesem Dokument wird beschrieben, wie Sie die Cisco ISE IOS-Instanz mithilfe von Azure Virtual Machine installieren. Cisco ISE IOS ist für Azure Cloud Services verfügbar.

Voraussetzungen

- Abonnements und Ressourcengruppen.

Navigieren Sie zu Alle Services > Abonnements. Stellen Sie sicher, dass ein Azure-Konto mit aktivem Abonnement vorhanden ist, für das eine Enterprise-Vereinbarung mit Microsoft besteht. Verwenden der CLI des Microsoft PowerShell Azure-Moduls zum Reservieren von Speicherplatz: (Informationen zum Installieren der Power Shell und relevanter Pakete finden Sie unter <How to install Azure PowerShell > (Informationen zum Installieren von Power Shell und relevanten Paketen).

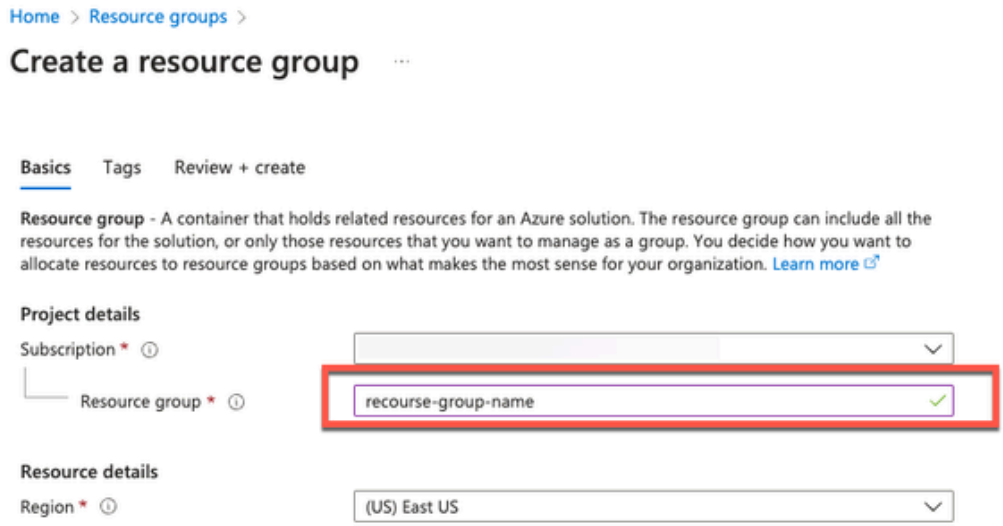
```
Connect-AzAccount -TenantID <Tenant-ID>
Register-AzResourceProvider -ProviderNamespace Microsoft.AVS
Register-AzResourceProvider -ProviderNamespace Microsoft.Batch
```



Hinweis: Ersetzen Sie die Tenant-ID durch Ihre tatsächliche Tenant-ID.

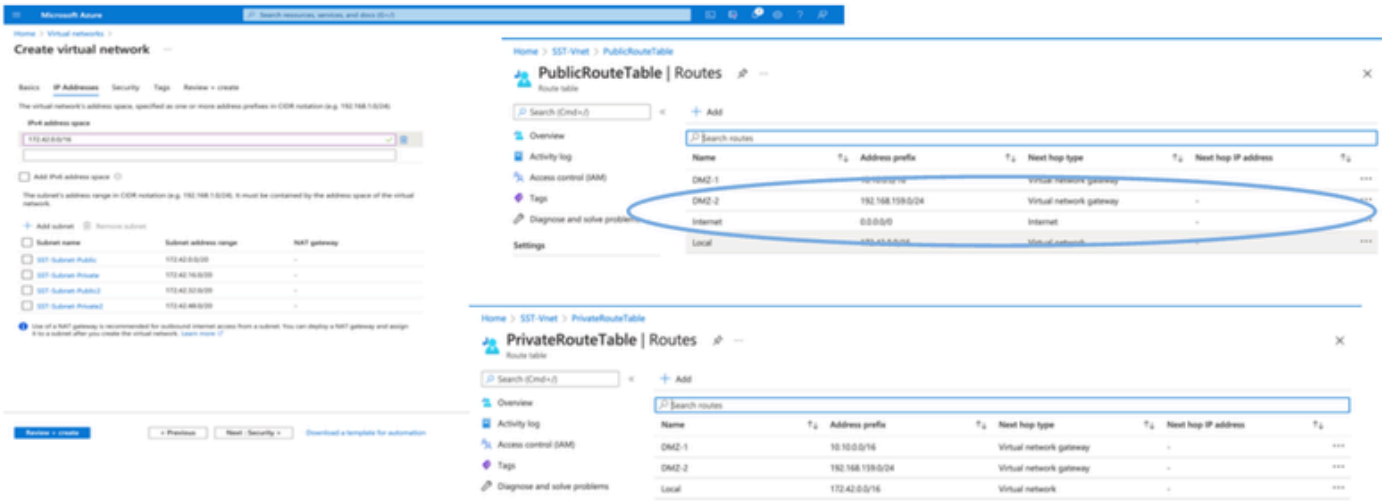
Für weitere Details müssen Sie beiRequest-Hostkontingent für Azure VMware-Lösung ausfüllen.

Erstellen Sie eine Ressourcengruppe nach dem richtigen Abonnement, und navigieren Sie zu Alle Dienste > Ressourcengruppen. Klicken Sie auf Hinzufügen. Geben Sie den Namen der Ressourcengruppe ein.



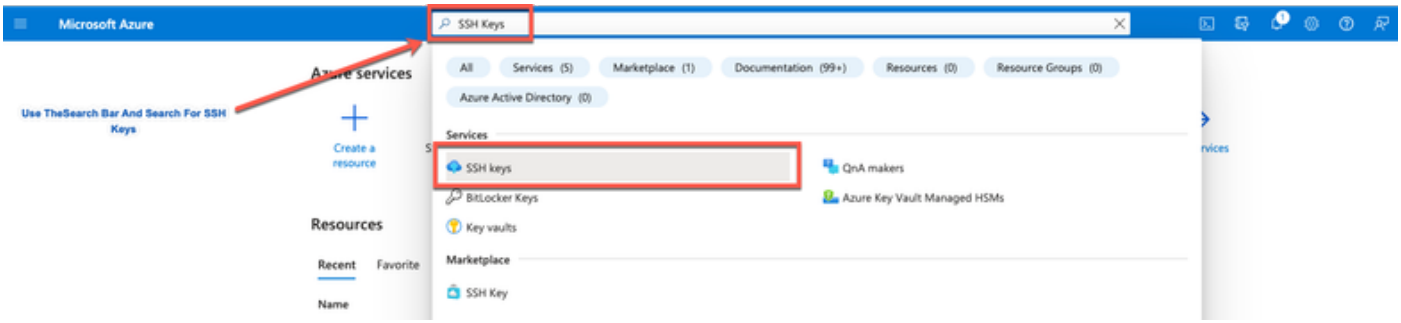
- Virtuelles Netzwerk und Sicherheitsgruppen

Für das Subnetz, das eine Interneterreichbarkeit erfordert, muss die Routing-Tabelle mit dem nächsten Hop als Internet konfiguriert sein. Siehe Beispiele für öffentliche und private Subnetze. PAN mit öffentlicher IP-Adresse Offline- und Online-Feed-Updates sind verfügbar, PAN mit privater IP muss auf Offline-Feed-Updates angewiesen sein.

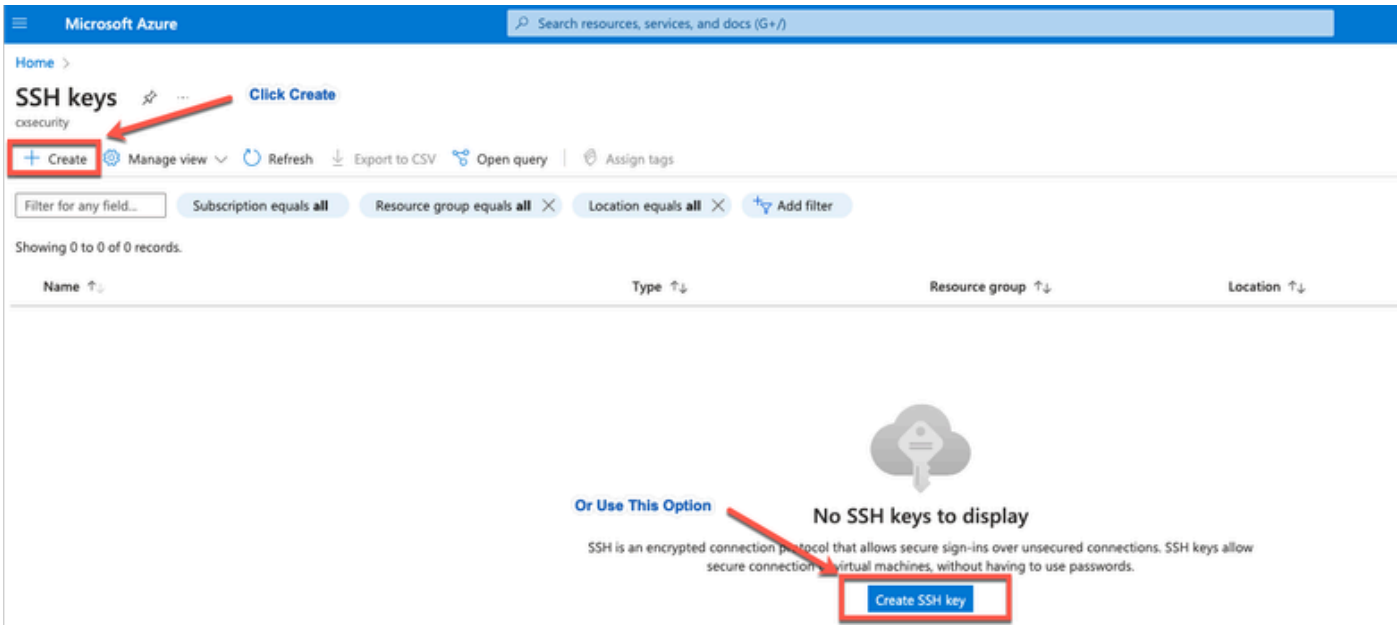


- Erstellen Sie ein SSH-Schlüsselpaar.

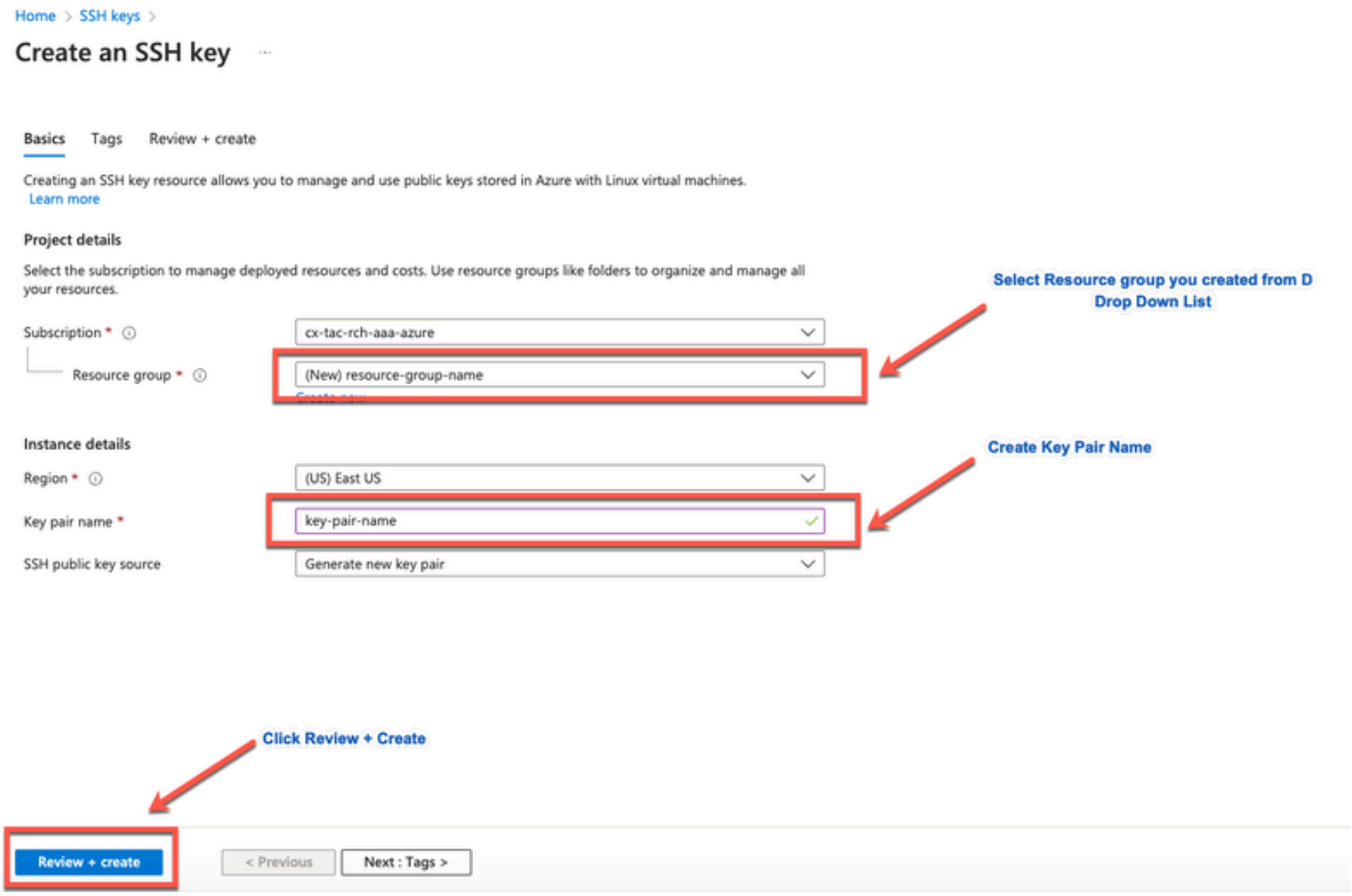
a. Verwenden Sie die Suchleiste auf der Startseite des Azure-Webportals, und suchen Sie nach SSH-Schlüsseln.



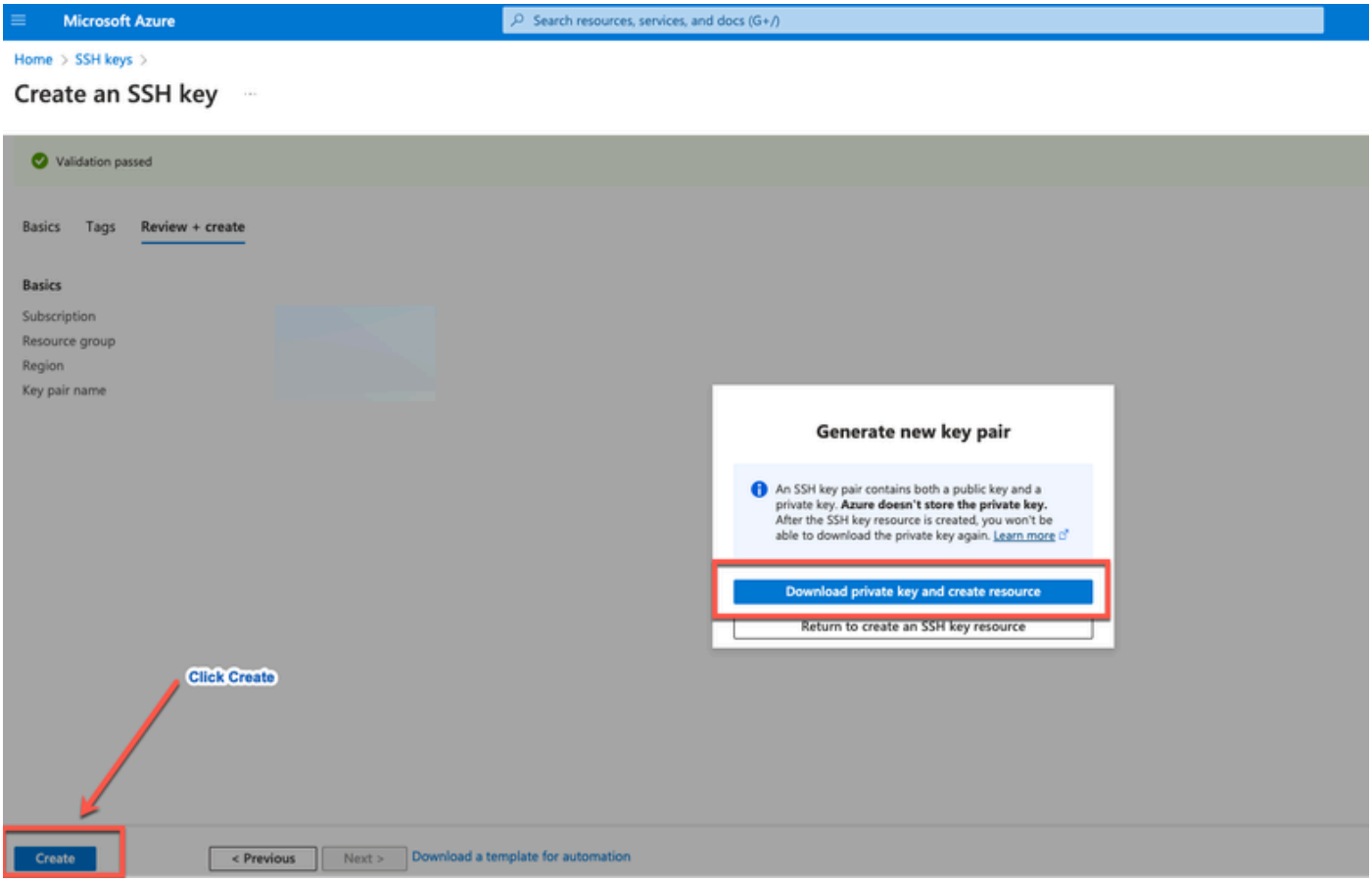
b. Klicken Sie im nächsten Fenster auf Erstellen.



c. Wählen Sie im nächsten Fenster die Ressourcengruppe und den Schlüsselnamen aus. Klicken Sie dann auf Prüfen + Erstellen.



d. Klicken Sie im nächsten Fenster auf Privaten Schlüssel erstellen und herunterladen.



Verwendete Komponente

Der Inhalt dieses Dokuments basiert auf dieser Software und den Cloud-Services.

- Cisco ISE Version 3.2
- Microsoft Azure Cloud-Services

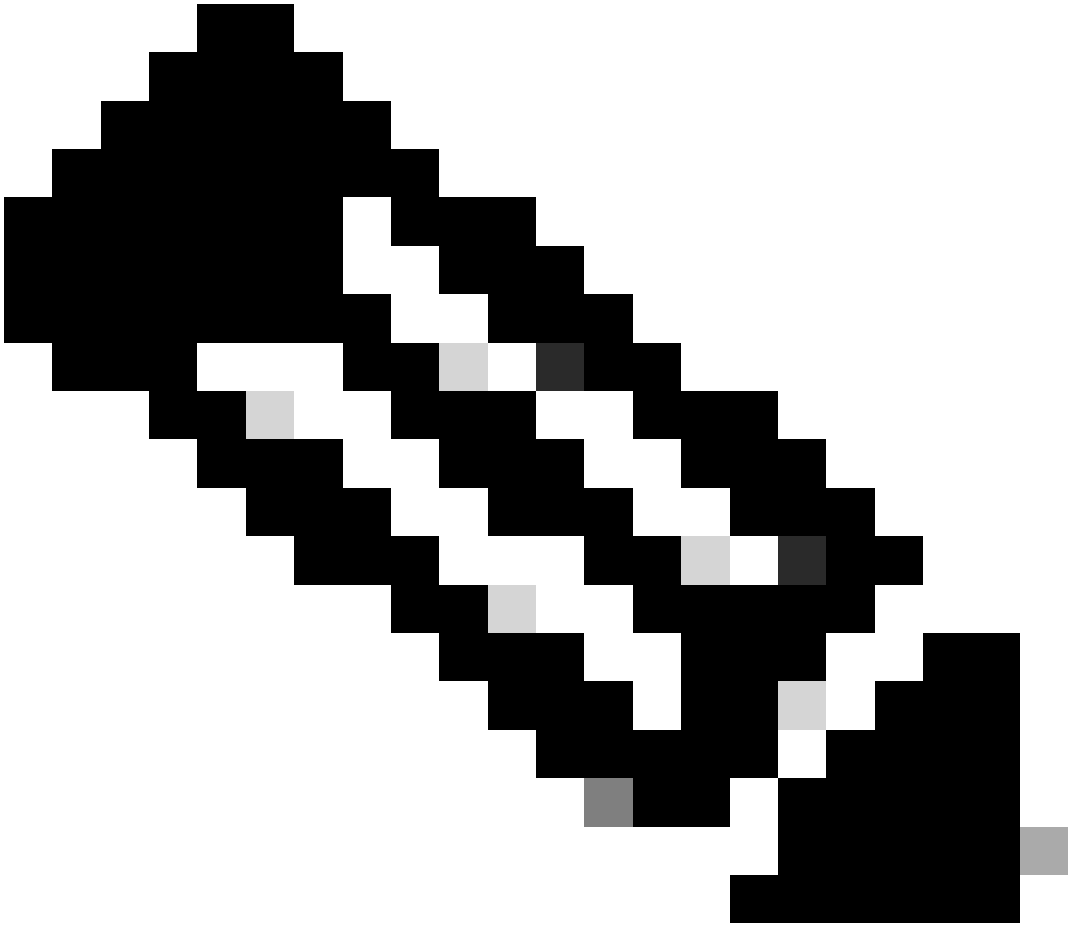
Die Informationen in diesem Dokument wurden auf dem Gerät aus einer spezifischen Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte begannen mit einer gelöschten (Standard-)Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Von der Cisco ISE unterstützte Azure VM-Größen

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

- Die Azure VM-Größen der Fsv2-Serie sind für die Verarbeitung optimiert und eignen sich am besten als PSNs für rechenintensive Aufgaben und Anwendungen.
- Die Dsv4-Serie sind allgemeine Azure VM-Größen, die sich am besten als PAN- oder MnT-Knoten oder für beide eignen und für Datenverarbeitungsaufgaben und Datenbankoperationen vorgesehen sind.

Wenn Sie eine Allzweck-Instanz als PSN verwenden, sind die Leistungszahlen niedriger als die Leistung einer für Computing optimierten Instanz als PSN. Die VM-Größe Standard_D8s_v4 darf nur als extra kleines PSN verwendet werden.



Hinweis: Klonen Sie kein vorhandenes Azure Cloud-Image, um eine Cisco ISE-Instanz zu erstellen. Dies kann zufällige und unerwartete Fehlfunktionen im erstellten ISE-System verursachen.

Einschränkungen der Cisco ISE bei Microsoft Azure Cloud Services

- Wenn Sie die Cisco ISE mit dem virtuellen Azure-Computer erstellen, weist Microsoft Azure den virtuellen Systemen standardmäßig private IP-Adressen über DHCP-Server zu. Bevor Sie eine Cisco ISE-Bereitstellung auf Microsoft Azure erstellen, müssen Sie die DNS-Vorwärts- und -Rückwärtseinträge mit den von Microsoft Azure zugewiesenen IP-Adressen aktualisieren.

  Alternativ können Sie nach der Installation der Cisco ISE dem virtuellen System eine statische IP-Adresse zuweisen, indem Sie das Network Interface-Objekt in Microsoft Azure aktualisieren:

  1. Stoppen Sie das virtuelle System.

2. Klicken Sie im Bereich Private IP address settings der VM im Bereich Assignment (Zuweisung) auf Static (Statisch).

3. Starten Sie das virtuelle System neu.

4. Weisen Sie in der seriellen Cisco ISE-Konsole die IP-Adresse als Gi0 zu.

5. Starten Sie den Cisco ISE-Anwendungsserver neu.

- Eine duale Netzwerkkarte wird nur mit zwei Netzwerkkarten unterstützt: Gigabit Ethernet 0 und Gigabit Ethernet 1. Um eine sekundäre NIC in der Cisco ISE-Instanz zu konfigurieren, müssen Sie zunächst ein Netzwerkschnittstellenobjekt in Azure erstellen, die Cisco ISE-Instanz ausschalten und dieses Netzwerkschnittstellenobjekt dann an die Cisco ISE anschließen. Nachdem Sie Cisco ISE auf Azure installiert und gestartet haben, konfigurieren Sie die IP-Adresse des Netzwerkschnittstellenobjekts mithilfe der Cisco ISE-CLI manuell als sekundäre NIC.

- Der Cisco ISE-Upgrade-Workflow ist in Cisco ISE auf Microsoft Azure nicht verfügbar. Nur Neuinstallationen werden unterstützt. Sie können jedoch Backups und Wiederherstellungen von Konfigurationsdaten durchführen.
- Die Public Cloud unterstützt nur Layer-3-Funktionen. Cisco ISE-Knoten auf Microsoft Azure unterstützen keine Cisco ISE-Funktionen, die von Layer-2-Funktionen abhängen. Die Verwendung von DHCP-SPAN-Profilerproben und CDP-Protokollfunktionen über die Cisco ISE-CLI stellt beispielsweise Funktionen dar, die derzeit nicht unterstützt werden.
- Wenn Sie die Wiederherstellungs- und Sicherungsfunktion für Konfigurationsdaten ausführen, starten Sie nach Abschluss der Sicherung zuerst die Cisco ISE über die CLI neu. Starten Sie dann den Wiederherstellungsvorgang über die Cisco ISE-GUI.
- Der SSH-Zugriff auf die Cisco ISE CLI mithilfe der kennwortbasierten Authentifizierung wird in Azure nicht unterstützt. Sie können nur über ein Schlüsselpaar auf die Cisco ISE-CLI zugreifen, und dieses Schlüsselpaar muss sicher gespeichert werden. Wenn Sie einen privaten Schlüssel (oder eine PEM-Datei) verwenden und die Datei verlieren, können Sie nicht auf die Cisco ISE CLI zugreifen.

Eine Integration, die eine kennwortbasierte Authentifizierungsmethode für den Zugriff auf die Cisco ISE CLI verwendet, wird nicht unterstützt, z. B. Cisco DNA Center Version 2.1.2 und frühere Versionen.

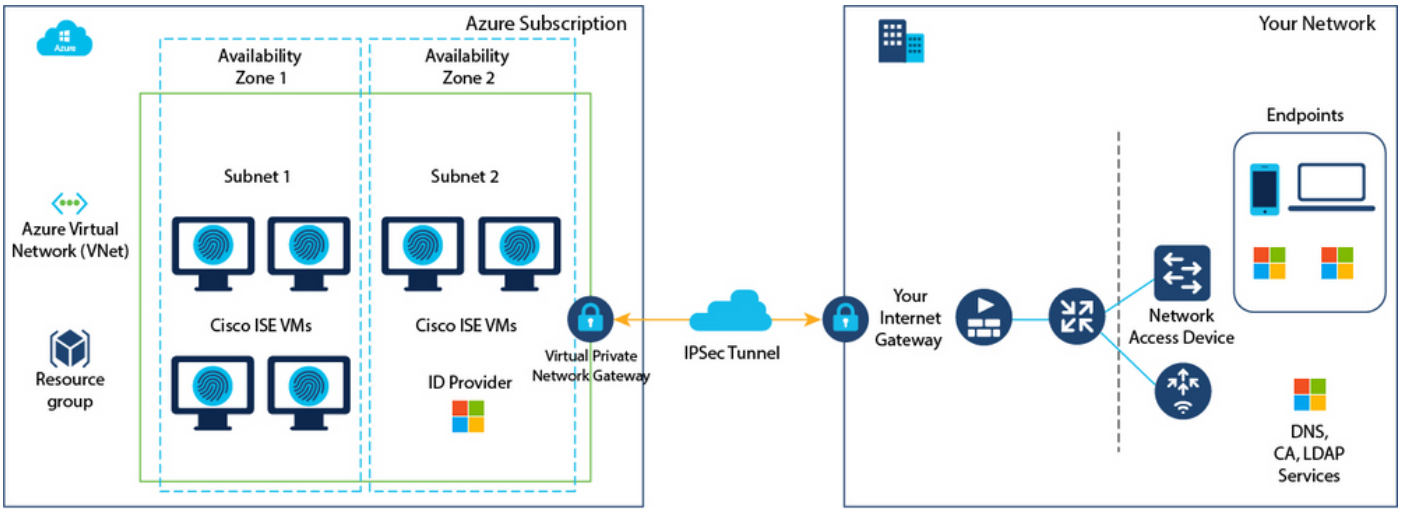
- Cisco ISE IOS-Bereitstellungen auf Azure nutzen in der Regel VPN-Lösungen wie Dynamic Multipoint Virtual Private Networks (DMVPN) und Software-Defined Wide Area Networks (SD-WAN), wobei die IPSec-Tunnelgemeinkosten MTU- und Fragmentierungsprobleme verursachen können. In solchen Szenarien würde Cisco ISE IOS keine vollständigen RADIUS-Pakete empfangen, und ein Authentifizierungsfehler tritt auf, ohne ein Fehlerprotokoll auszulösen.

  Eine mögliche Problemumgehung besteht darin, den technischen Support von Microsoft in Anspruch zu nehmen, um Lösungen in Azure zu erkunden, bei denen außer Betrieb befindliche Fragmente an das Ziel weitergeleitet werden können, anstatt verworfen zu werden.

- CLI-Admin-Benutzer muss "iseadmin" sein.

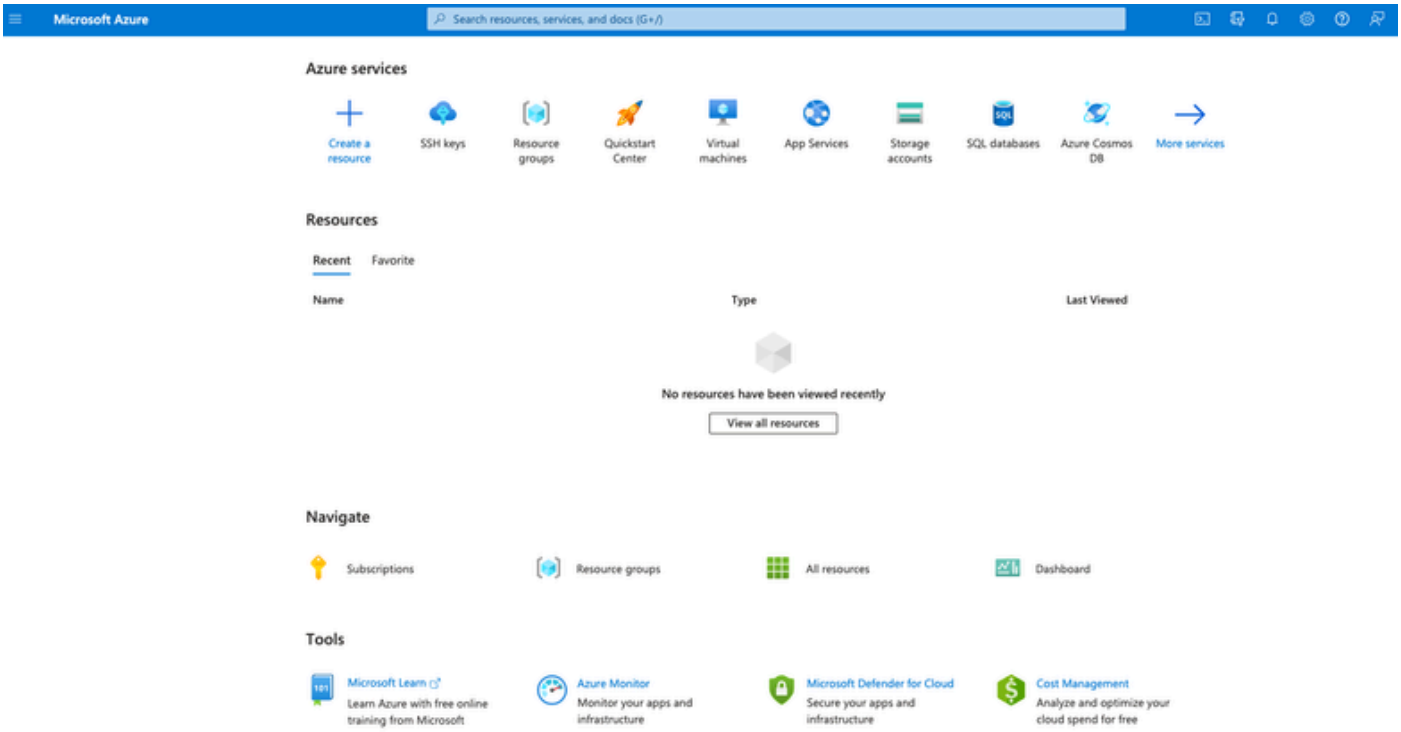
Konfigurieren

Beispiel einer mit Azure Cloud verbundenen ISE-Bereitstellung

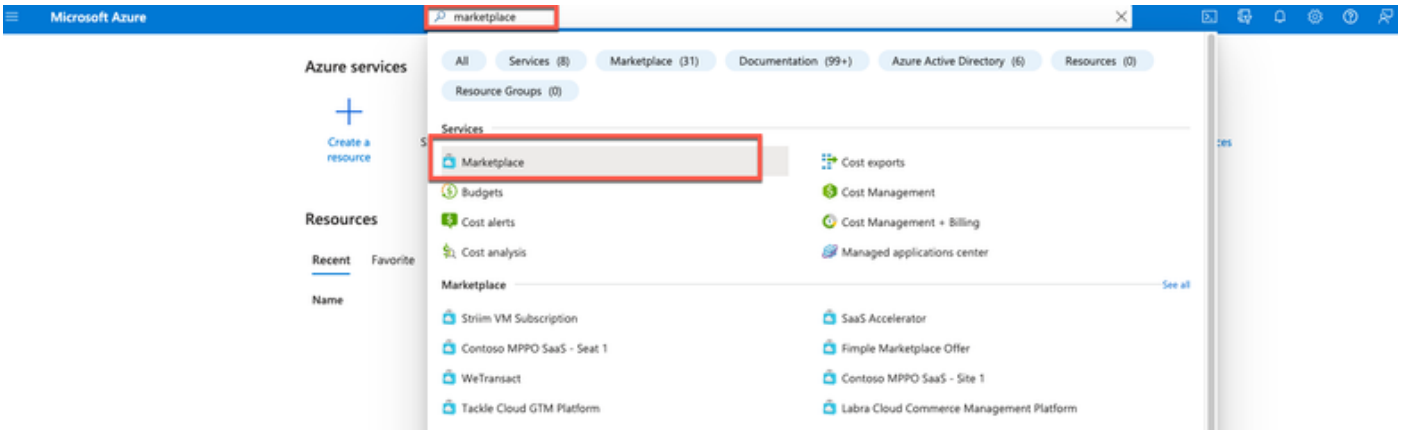


Konfigurationen

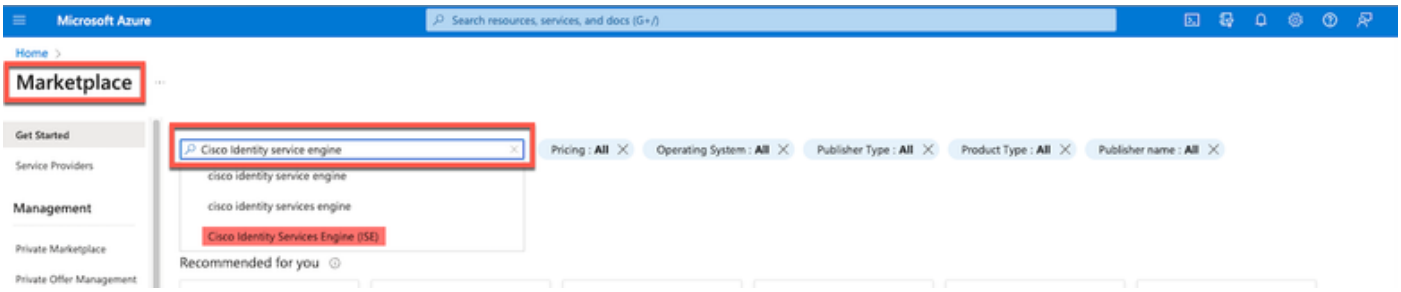
- Schritt (1): Gehen Sie zum Azure-Portal, und melden Sie sich bei Ihrem Microsoft Azure-Konto an.



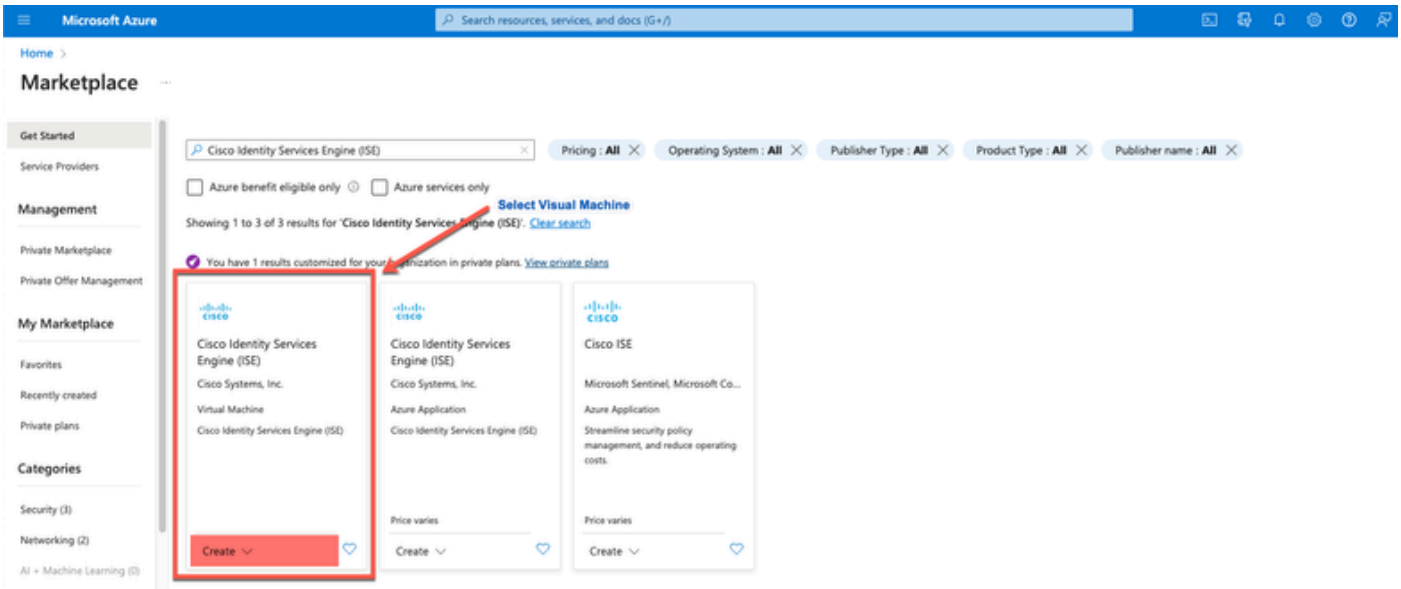
- Schritt (2): Verwenden Sie das Suchfeld oben im Fenster, um nach Marketplace zu suchen.



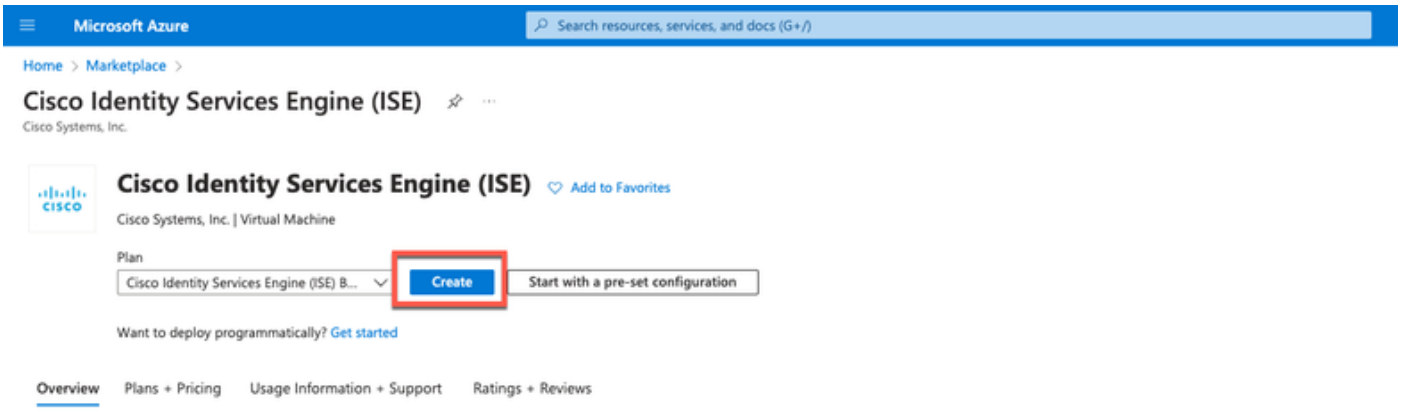
- Schritt 3: Verwenden Sie das Suchfeld Search the Marketplace (Marktplatz durchsuchen), um nach der Cisco Identity Services Engine (ISE) zu suchen.



- Schritt (4): Klicken Sie auf Virtuelles System.



- Schritt (5): Klicken Sie in dem neuen Fenster, das angezeigt wird, auf Erstellen.



- Schritt (6): Auf der Registerkarte Basics (Grundlagen):

antwort: Wählen Sie im Bereich Projektdetails die erforderlichen Werte aus den Dropdown-Listen für Abonnements und Ressourcen aus.

b. Geben Sie im Bereich Instanzdetails einen Wert in das Feld Name des virtuellen Computers ein.

c. Wählen Sie aus der Dropdown-Liste Image (Image) das Cisco ISE-Image aus.

d. Wählen Sie aus der Dropdown-Liste Size (Größe) die Instanzgröße aus, mit der die Cisco ISE installiert werden soll. Wählen Sie eine von der Cisco ISE unterstützte Instanz aus, wie in der Tabelle Azure Cloud aufgeführt.

Instanzen, die von der Cisco ISE unterstützt werden, im Abschnitt Cisco ISE auf Azure Cloud.

e. Klicken Sie im Bereich Administratorkonto > Authentifizierungstyp auf das Optionsfeld Öffentlicher SSH-Schlüssel.

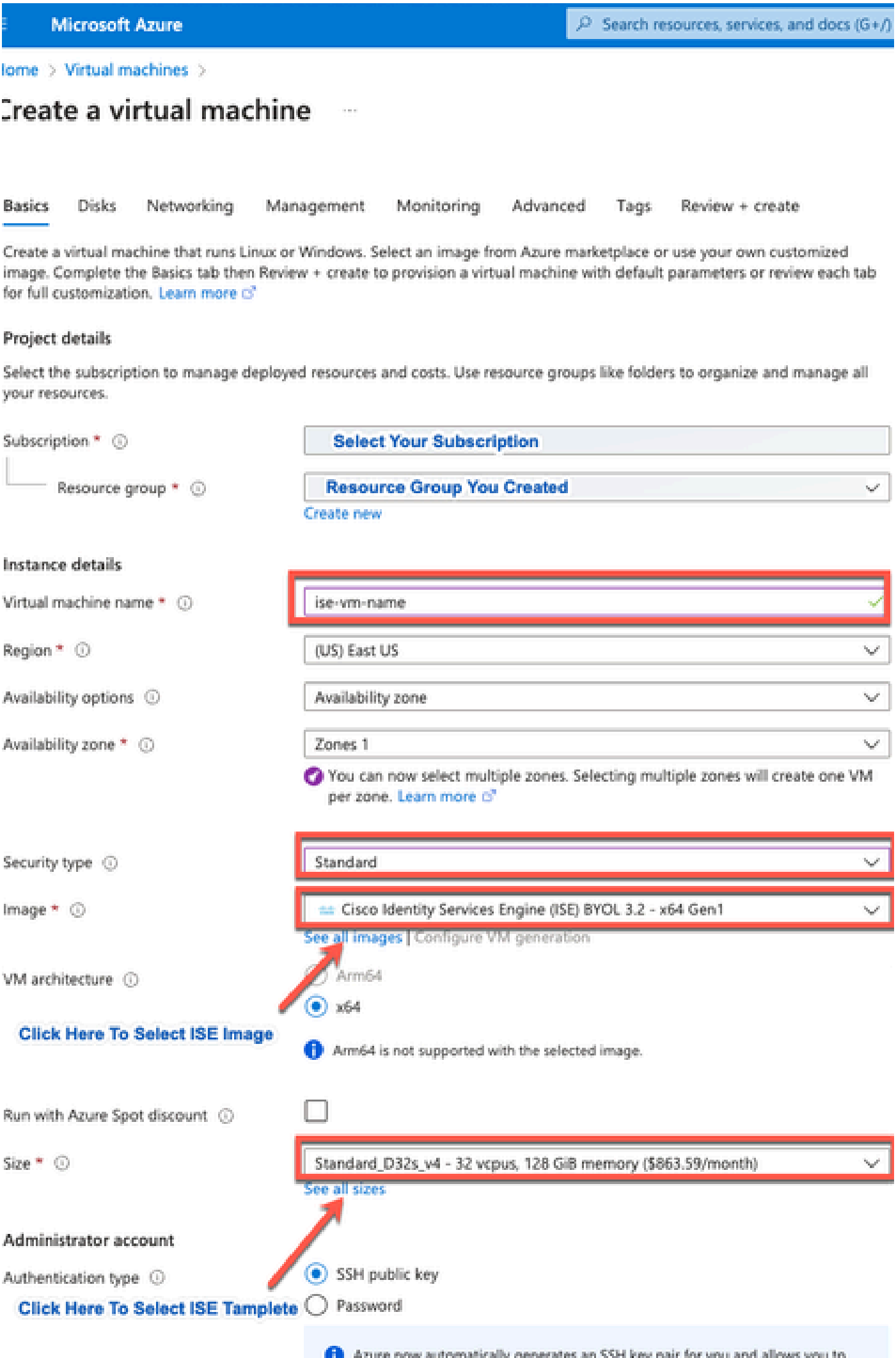
f. Geben Sie im Feld Username (Benutzername) iseadmin ein.

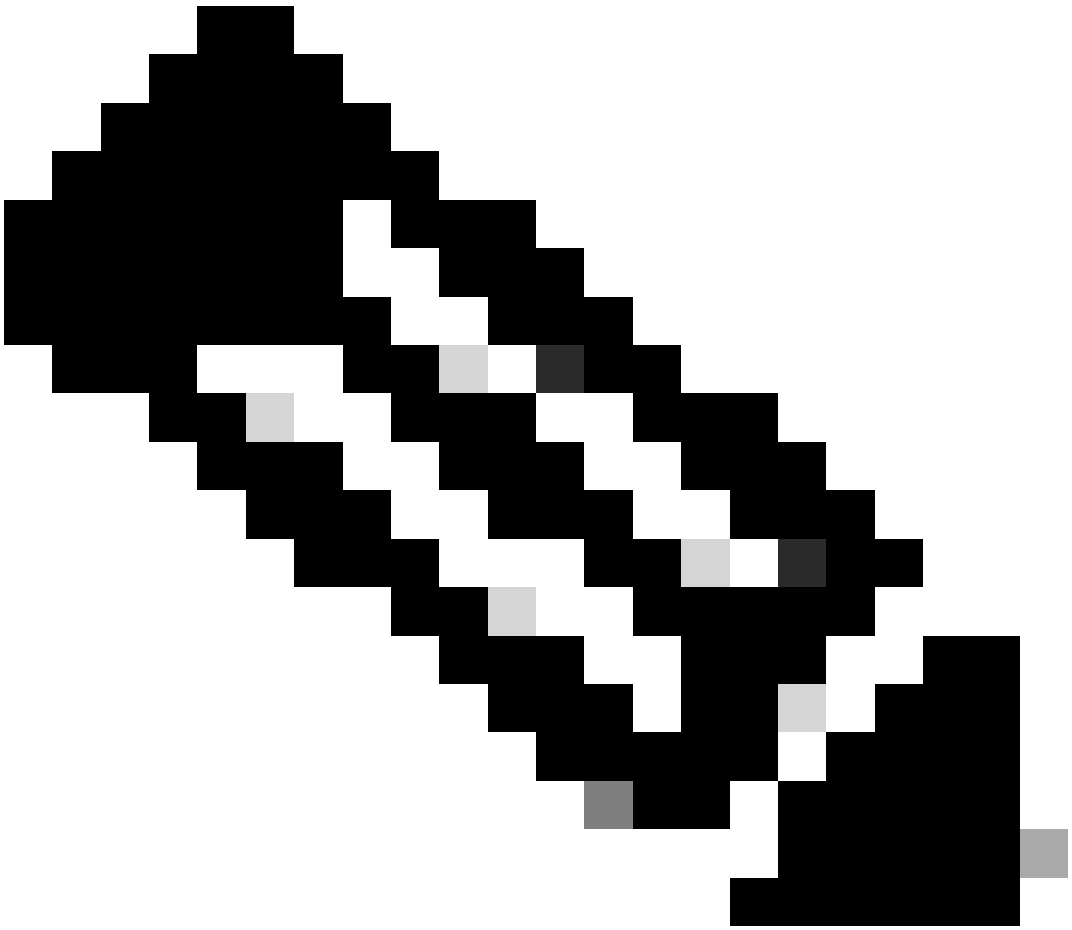
g. Wählen Sie in der Dropdown-Liste SSH-Quelle für öffentlichen Schlüssel die Option Vorhandenen Schlüssel verwenden, der in Azure gespeichert ist.

h. Wählen Sie aus der Dropdown-Liste Gespeicherte Schlüssel das Schlüsselpaar aus, das Sie als Voraussetzung für diese Aufgabe erstellt haben.

j) Klicken Sie im Bereich Inbound port rules (Regeln für eingehenden Port) auf das Optionsfeld Allow selected ports (Ausgewählte Ports zulassen).

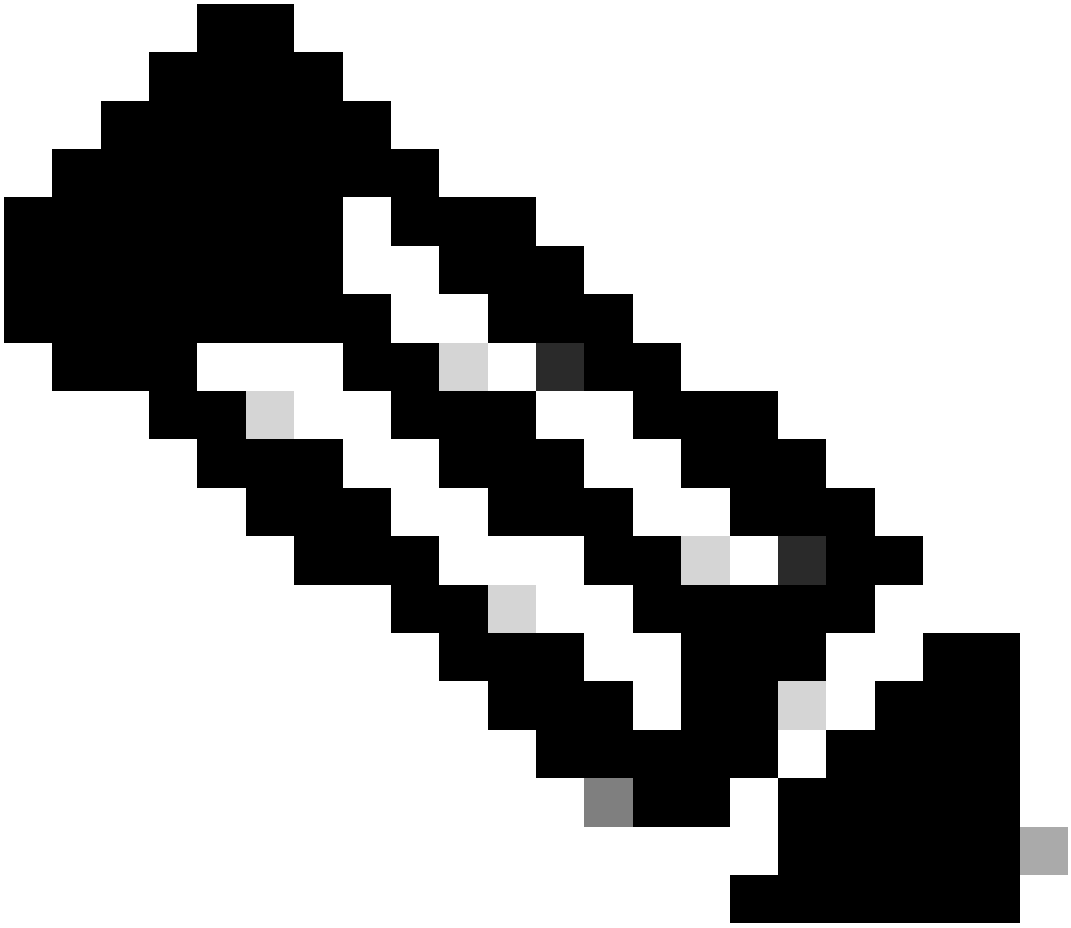
K. Wählen Sie im Bereich Licensing (Lizenzierung) in der Dropdown-Liste Licensing Type (Lizenztyp) die Option Other (Andere) aus.


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

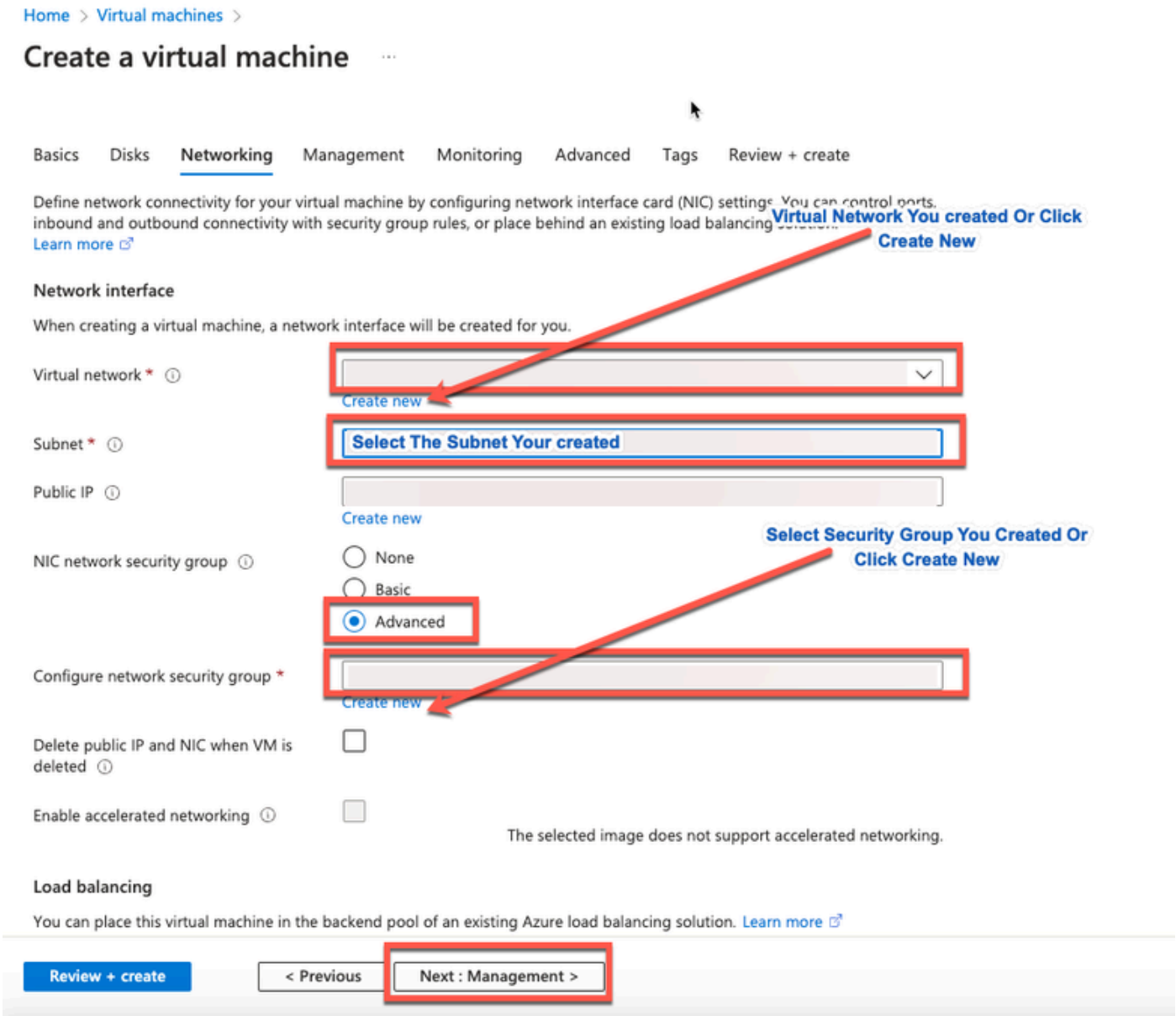


Hinweis: Für den Datenträgertyp stehen in der Dropdown-Liste weitere Optionen zur Auswahl. Sie können den auswählen, der Ihre Bedürfnisse erfüllt. Premium SSD ist der empfohlene Typ für produktions- und leistungsempfindliche Workloads.

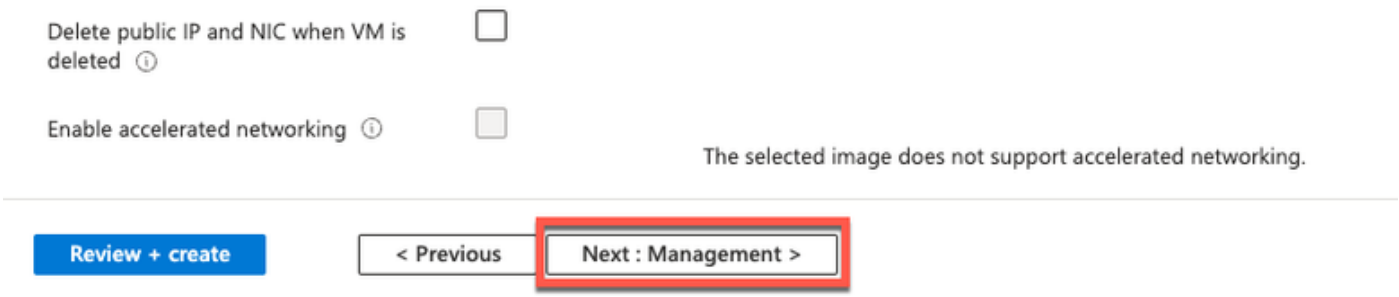
- Schritt (9): Wählen Sie im Bereich Netzwerkschnittstelle aus den Dropdown-Listen Virtuelles Netzwerk, Subnetz und Netzwerksicherheitsgruppe konfigurieren das von Ihnen erstellte virtuelle Netzwerk und Subnetz aus.



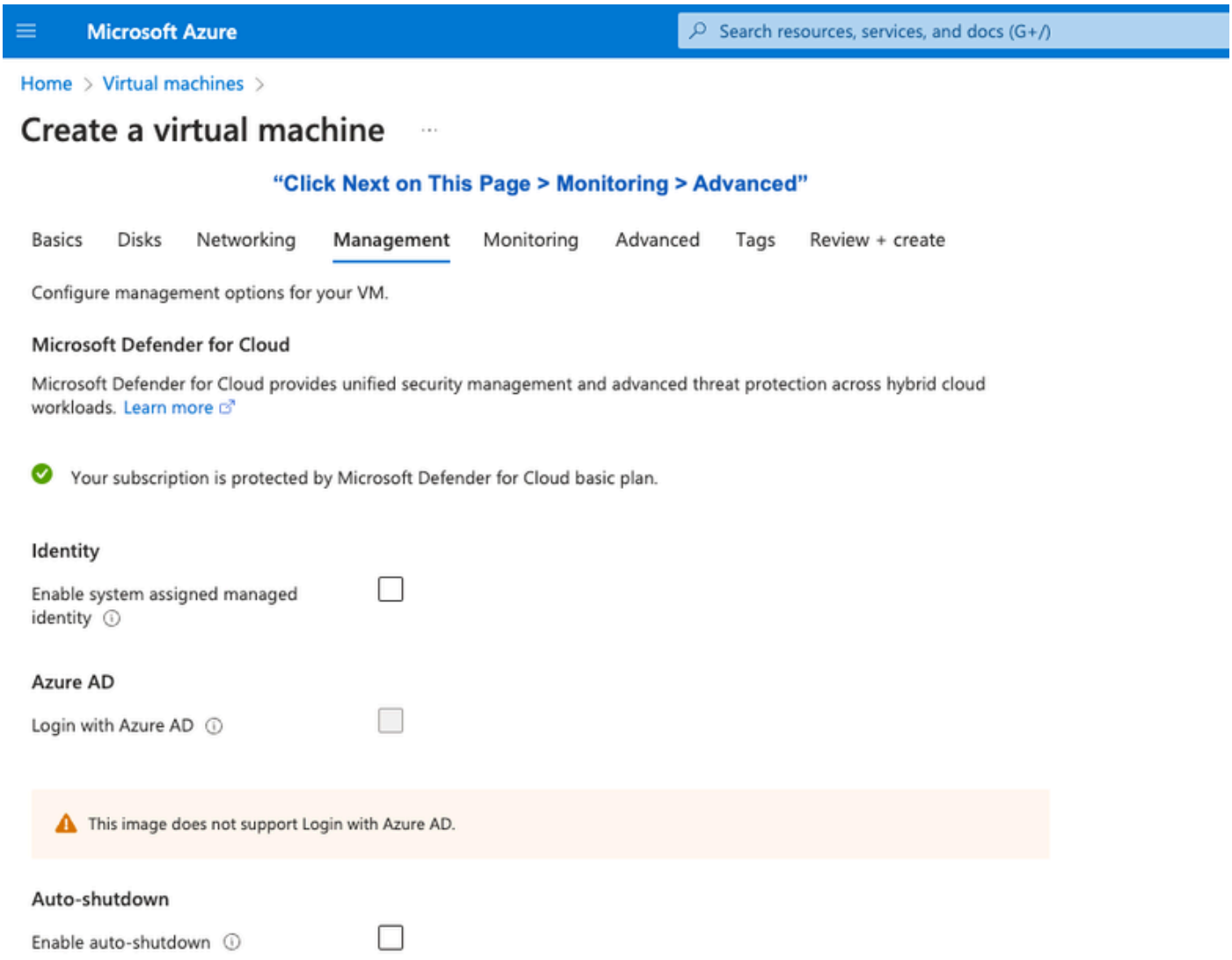
Hinweis: Das Subnetz mit einer öffentlichen IP-Adresse erhält Online- und Offline-Statusfeed-Updates, während ein Subnetz mit einer privaten IP-Adresse nur Offline-Statusfeed-Updates empfängt.

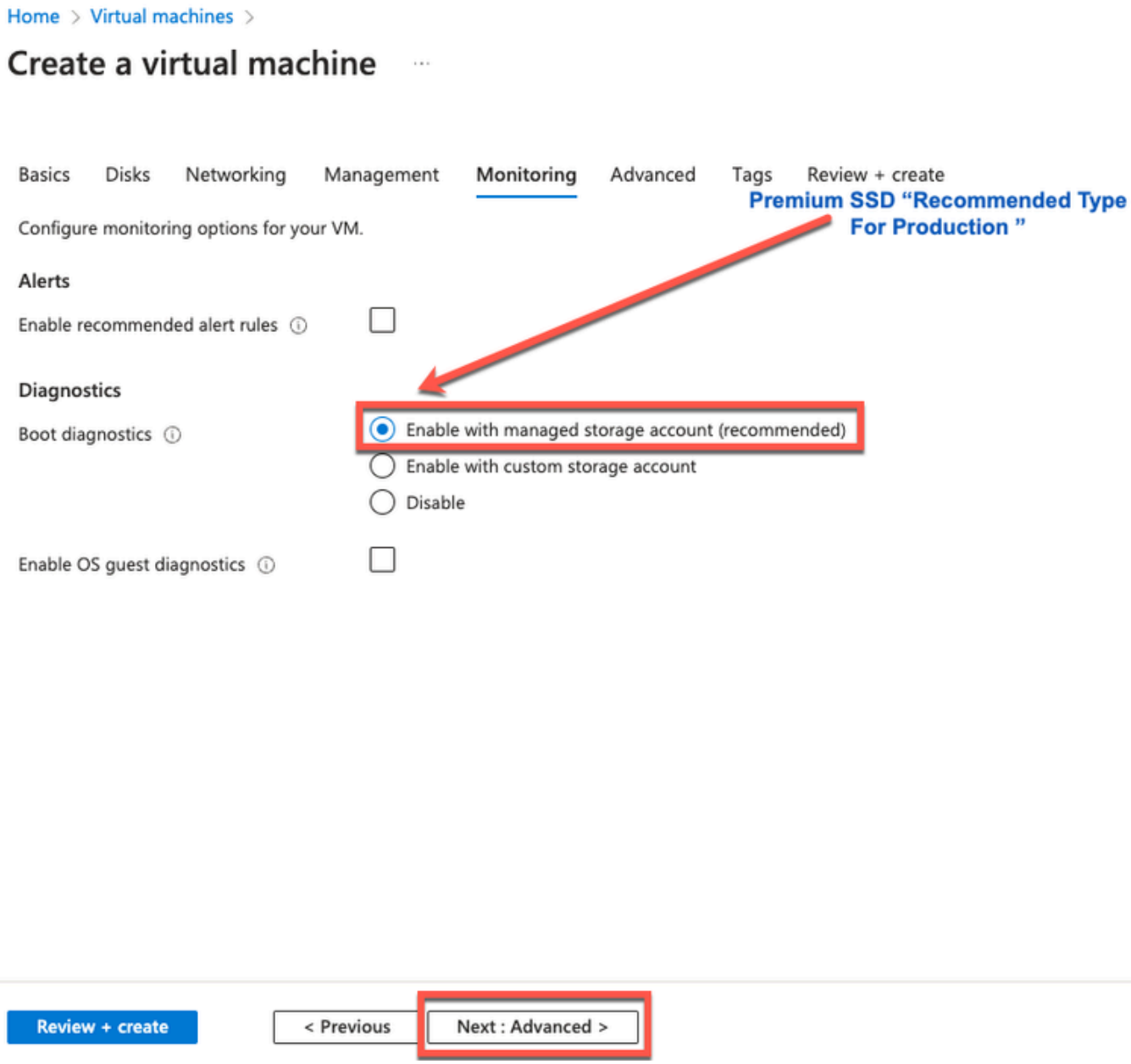


- Schritt (10): Klicken Sie auf Weiter: Verwaltung.



- Schritt (11): Behalten Sie auf der Registerkarte Verwaltung die Standardwerte für die Pflichtfelder bei, und klicken Sie auf Weiter: Erweitert.


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



- Schritt (12): Aktivieren Sie im Bereich Benutzerdaten das Kontrollkästchen Benutzerdaten aktivieren.

Geben Sie im Feld Benutzerdaten die vollständigen Informationen ein:

hostname=<Hostname der Cisco ISE>

primarynameserver=<IPv4-Adresse>

dnsdomain=<Domänenname>

ntpserver=<IPv4-Adresse oder FQDN des NTP-Servers>

timezone=<Zeitzone>

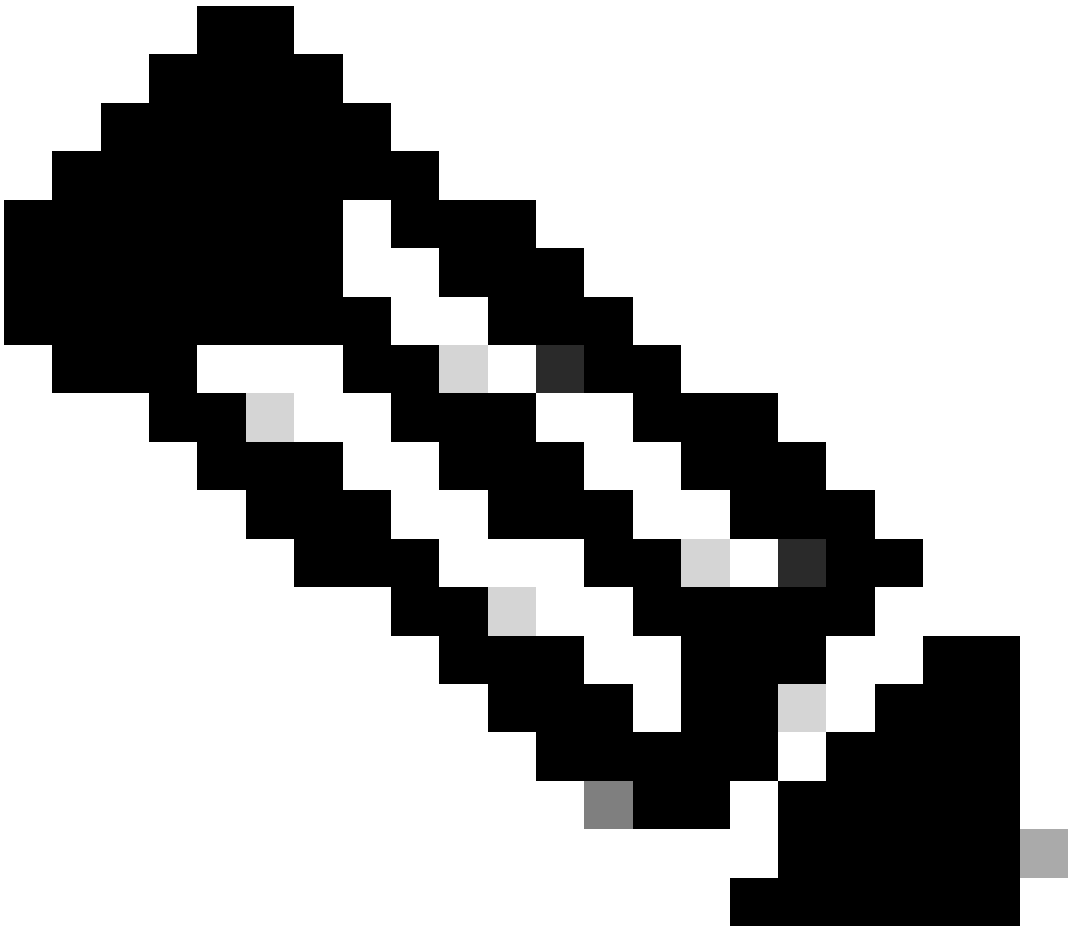
password=<Kennwort>

ersapi=<ja/nein>

openapi=<ja/nein>

pxGrid=<ja/nein>

pxgrid_cloud=<ja/nein>



Hinweis: Sie müssen für jedes der Felder, die Sie über die Benutzerdateneingabe konfigurieren, die richtige Syntax verwenden. Die Informationen, die Sie in das Feld Benutzerdaten eingeben, werden bei der Eingabe nicht validiert. Wenn Sie die falsche Syntax verwenden, werden die Cisco ISE-Services beim Start des Images nicht angezeigt.

Siehe Richtlinien für Konfigurationen, die Sie über das Feld "Benutzerdaten" einsenden müssen:

a. hostname: Geben Sie einen Hostnamen ein, der nur alphanumerische Zeichen und Bindestriche (-) enthält. Der Hostname darf maximal 19 Zeichen lang sein und keine Unterstriche (_) enthalten.

b. Primärer Namenserver: Geben Sie die IP-Adresse des primären Namenservers ein. Nur IPv4-Adressen werden unterstützt.

In diesem Schritt können Sie nur einen DNS-Server hinzufügen. Sie können nach der Installation über die Cisco ISE-CLI weitere DNS-Server hinzufügen.

c. dnsdomain: Geben Sie den FQDN der DNS-Domäne ein. Der Eintrag kann ASCII-Zeichen, Ziffern, Bindestriche (-) und Punkte (.) enthalten.

d. ntpserver: Geben Sie die IPv4-Adresse oder den FQDN des NTP-Servers ein, der für die Synchronisierung verwendet werden soll.

In diesem Schritt können Sie nur einen NTP-Server hinzufügen. Sie können nach der Installation über die Cisco ISE-CLI weitere NTP-Server hinzufügen. Verwenden Sie einen gültigen und erreichbaren NTP-Server, da dieser für den ISE-Betrieb benötigt wird.

e. Zeitzone: Geben Sie eine Zeitzone ein, z. B. Etc/UTC. Es wird empfohlen, alle Cisco ISE-Knoten auf die UTC-Zeitzone (Coordinated Universal Time) zu setzen, insbesondere wenn die Cisco ISE-Knoten in einer verteilten Bereitstellung installiert sind. Mit diesem Verfahren wird sichergestellt, dass die Zeitstempel der Berichte und Protokolle der verschiedenen Knoten in der Bereitstellung immer synchronisiert werden.

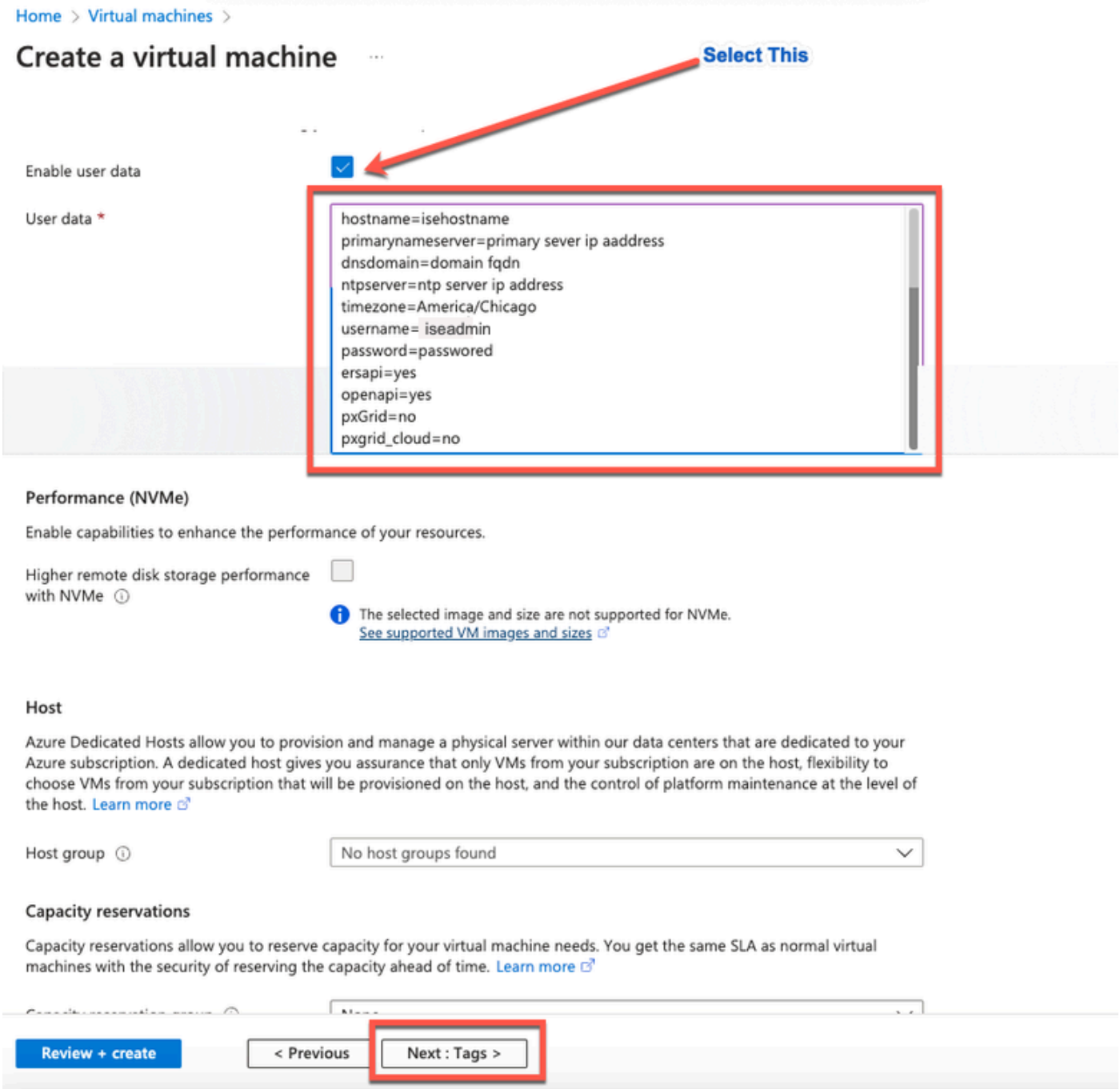
f. password: Konfigurieren Sie ein Kennwort für die GUI-basierte Anmeldung bei der Cisco ISE. Das eingegebene Kennwort muss mit der Cisco ISE-Kennwortrichtlinie übereinstimmen. Das Passwort muss zwischen 6 und 25 Zeichen lang sein und mindestens eine Ziffer, einen Großbuchstaben und einen Kleinbuchstaben enthalten. Das Passwort darf nicht mit dem Benutzernamen oder dessen Umkehrung (iseadmin oder nimdaesi), cisco oder ocsic identisch sein. Die zulässigen Sonderzeichen lauten @~*!,+=_-. Weitere Informationen finden Sie im Abschnitt "Richtlinie für Benutzerkennwörter" im Kapitel "Grundlegende Einrichtung" des Cisco ISE Administratorhandbuchs für Ihre Version.

g. ersapi: Geben Sie yes (Ja) ein, um ERS zu aktivieren, oder no (Nein), um ERS zu deaktivieren.

h. openapi: Geben Sie yes ein, um OpenAPI zu aktivieren, oder no, um OpenAPI zu deaktivieren.

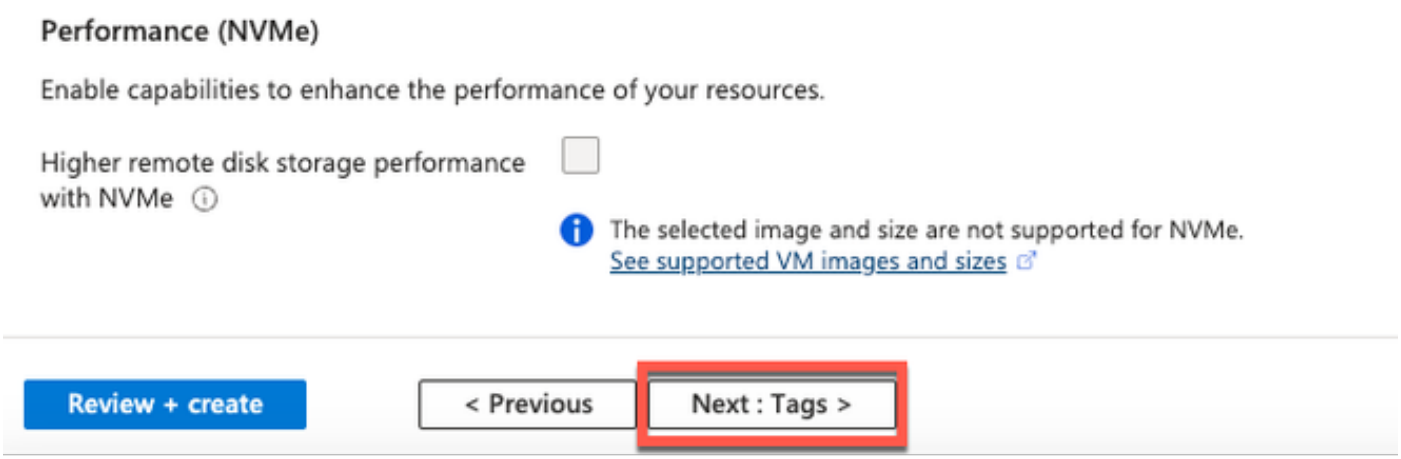
i. pxGrid: Geben Sie yes ein, um pxGrid zu aktivieren, oder no, um pxGrid zu deaktivieren.

j. pxgrid_cloud: Geben Sie yes ein, um pxGrid Cloud zu aktivieren, oder no, um pxGrid Cloud zu deaktivieren. Um pxGrid Cloud zu aktivieren, müssen Sie pxGrid aktivieren. Wenn Sie pxGrid nicht zulassen, aber pxGrid Cloud aktivieren, werden pxGrid Cloud-Services beim Start nicht aktiviert.

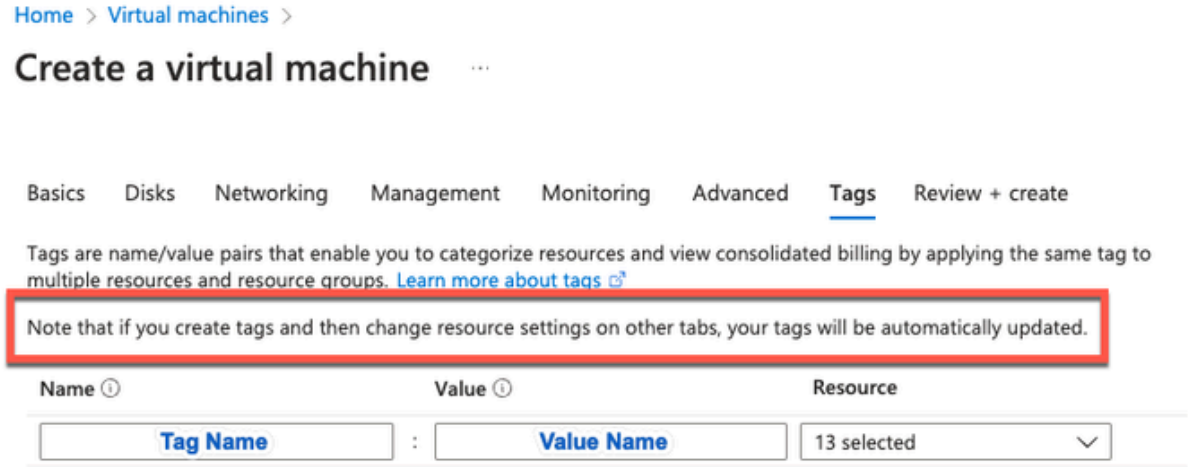


Abschnitt "Benutzerdaten"

- Schritt (13): Klicken Sie auf Weiter: Tags.



- Schritt (14): Um Name-Wert-Paare zu erstellen, mit denen Sie Ressourcen kategorisieren und mehrere Ressourcen und Ressourcengruppen konsolidieren können, geben Sie Werte in die Felder Name und Wert ein.

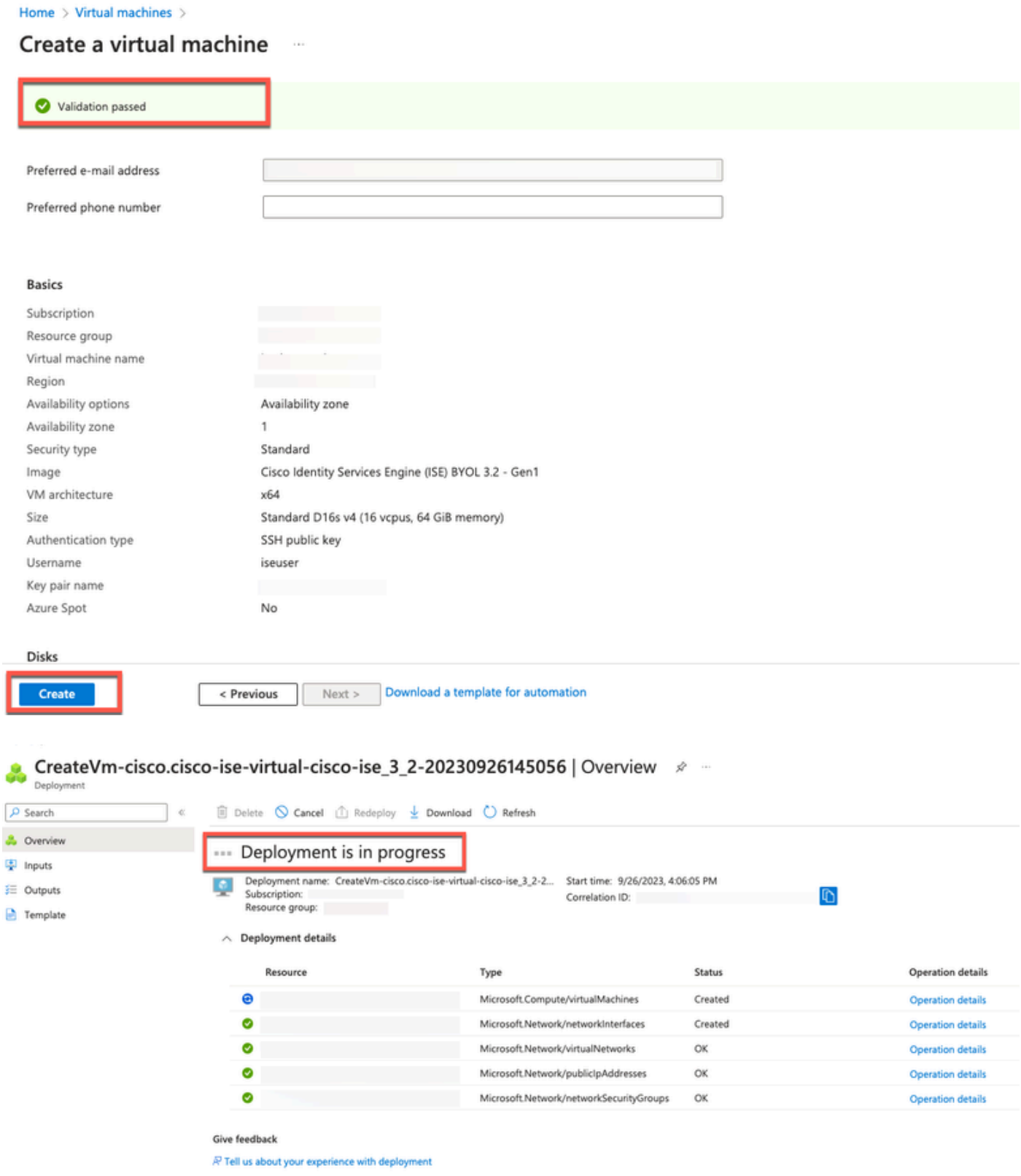


- Schritt (15): Klicken Sie auf Weiter: Prüfen + Erstellen.

- Schritt (16): Überprüfen Sie die bisher von Ihnen bereitgestellten Informationen, und klicken Sie auf Erstellen.

Das Fenster Deployment is in progress wird angezeigt. Es dauert ca. 30 Minuten, bis die Cisco ISE-Instanz erstellt wurde und einsatzbereit ist. Die Cisco ISE VM-Instanz wird im

Fenster "Virtuelle Maschinen" (verwenden Sie das Hauptsuchfeld, um das Fenster zu finden).

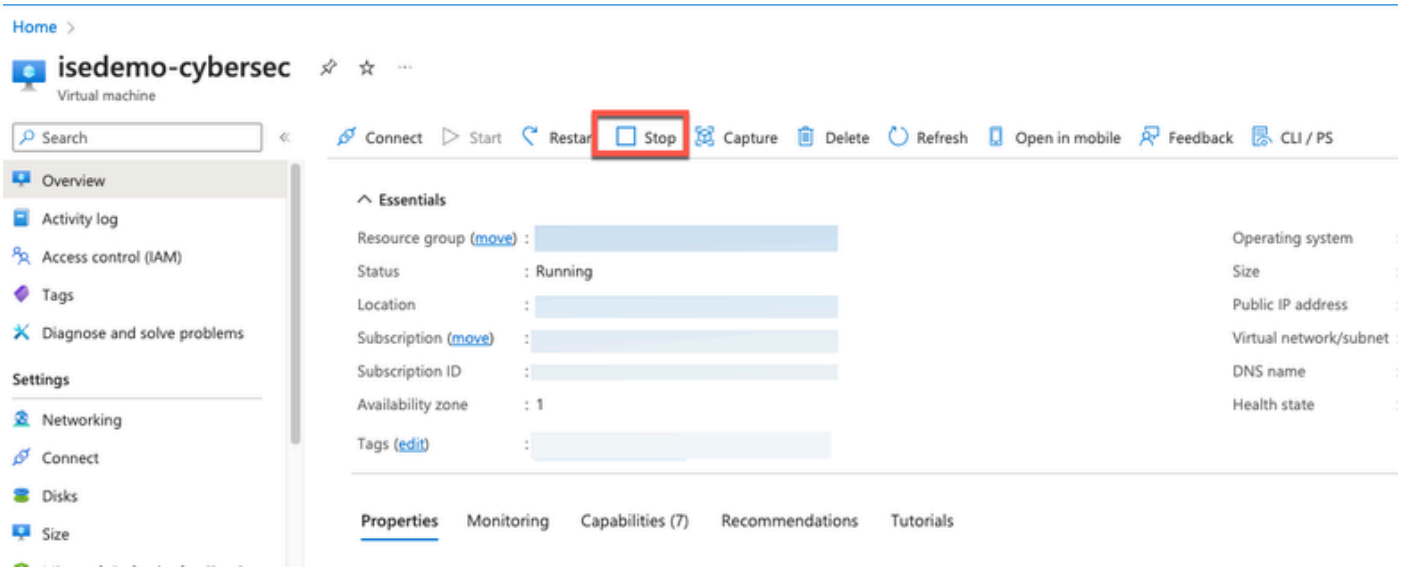


Nächste Schritte

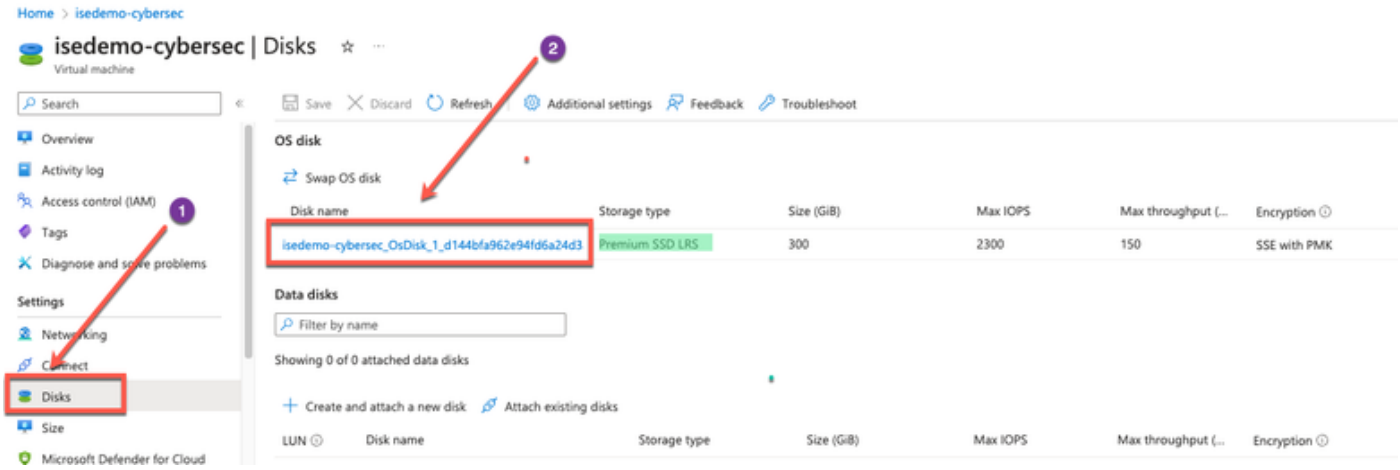
Aufgrund einer Microsoft Azure-Standardeinstellung ist die von Ihnen erstellte Cisco ISE VM mit nur 300 GB Festplattengröße konfiguriert. Cisco ISE-Knoten benötigen in der Regel mehr als 300 GB Festplattenkapazität. Der Alarm "Unzureichender virtueller Arbeitsspeicher" wird angezeigt, wenn Sie die Cisco ISE zum ersten Mal von Microsoft Azure aus starten.

Melden Sie sich nach Abschluss der Erstellung der Cisco ISE VM beim Cisco ISE-Administrationsportal an, um sicherzustellen, dass die Cisco ISE eingerichtet ist. Führen Sie dann im Microsoft Azure-Portal die Schritte im Fenster Virtuelle Maschinen aus, um die Datenträgergröße zu bearbeiten, und schließen Sie diese ab:

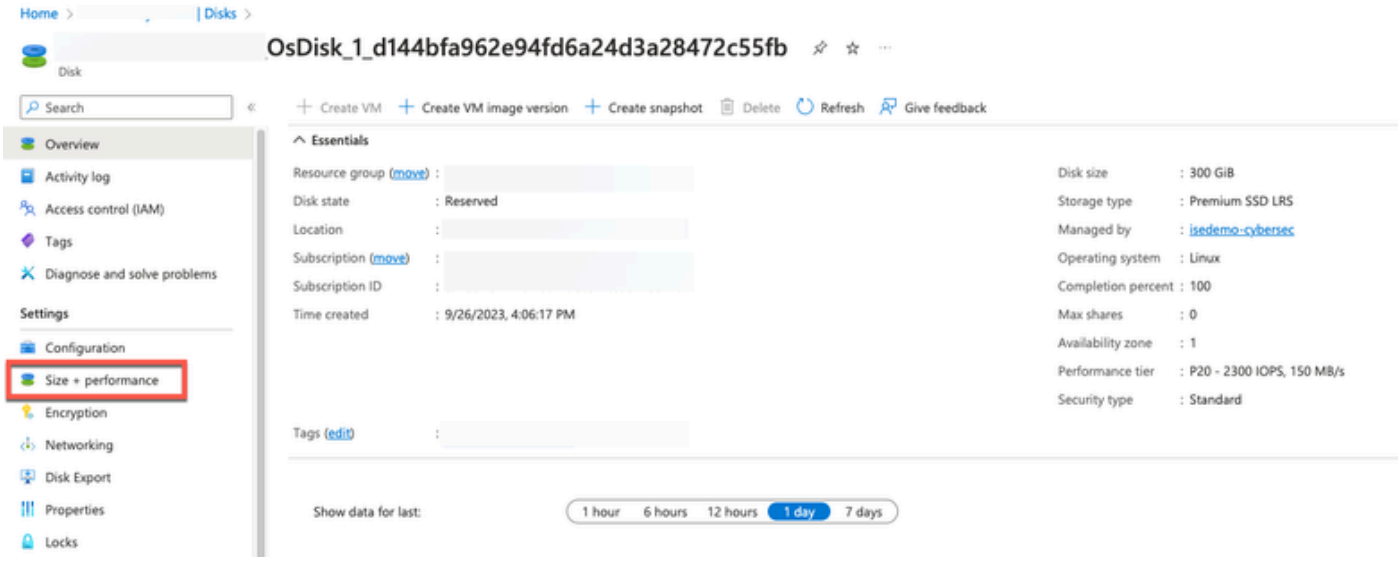
1. Beenden Sie die Cisco ISE-Instanz.



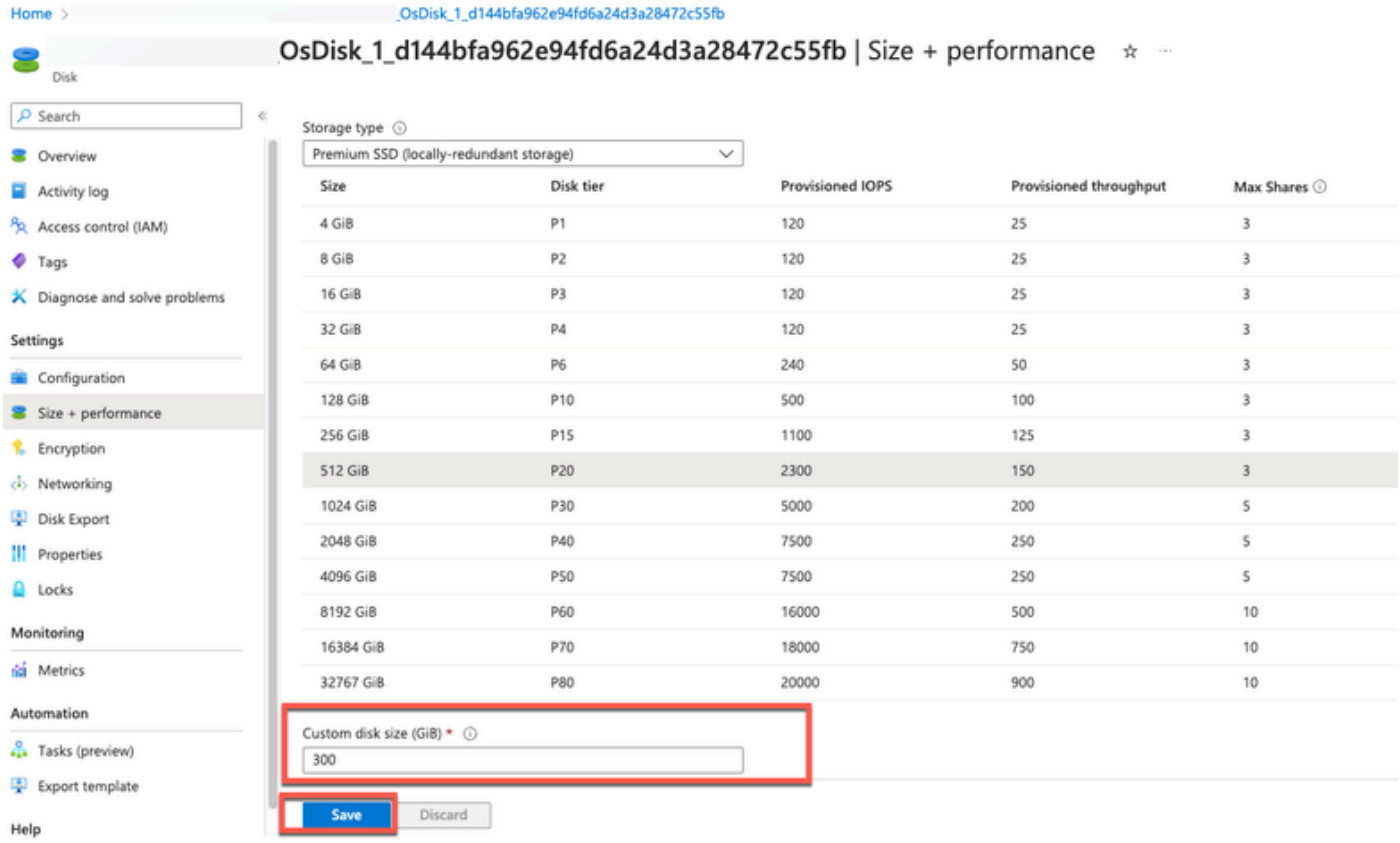
2. Klicken Sie im linken Bereich auf Datenträger, und klicken Sie auf den Datenträger, den Sie mit Cisco ISE verwenden.



3. Klicken Sie im linken Bereich auf Größe + Leistung.



4. Geben Sie im Feld Benutzerdefinierte Festplattengröße die gewünschte Festplattengröße in GiB ein.



Aufgaben nach der Installation

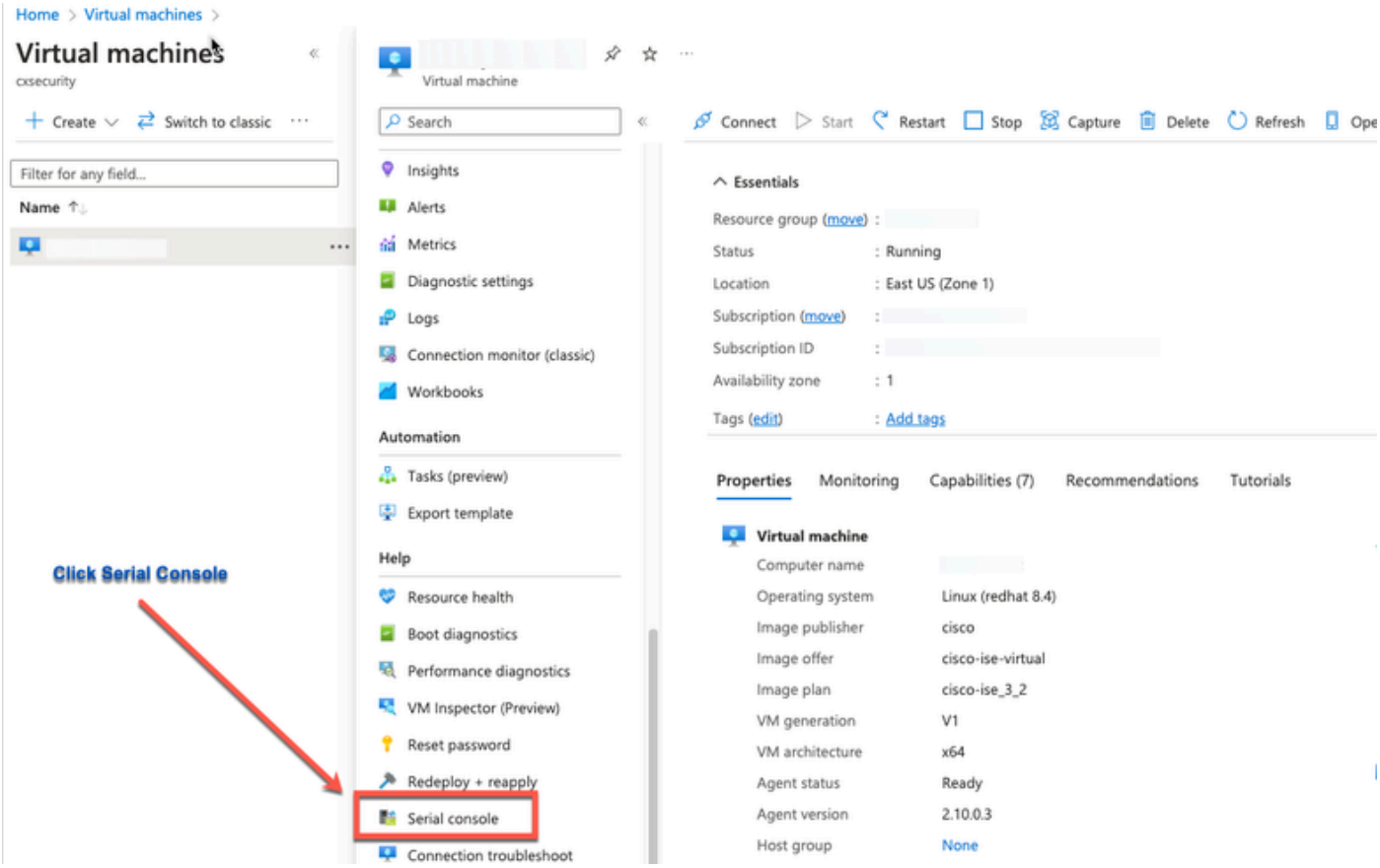
Informationen zu den Aufgaben, die Sie nach der Installation durchführen müssen, nachdem Sie eine Cisco ISE-Instanz erfolgreich erstellt haben, finden Sie im Kapitel "Verification and Post Installation Tasks" im Cisco ISE-Installationshandbuch für Ihre Cisco ISE-Version.

Kennwortwiederherstellung und -zurücksetzung in Azure Cloud

Führen Sie die Aufgaben aus, die Ihnen beim Zurücksetzen oder Wiederherstellen des Kennworts für das virtuelle Cisco ISE-System helfen. Wählen Sie die Aufgaben aus, die Sie benötigen, und führen Sie die detaillierten Schritte aus.

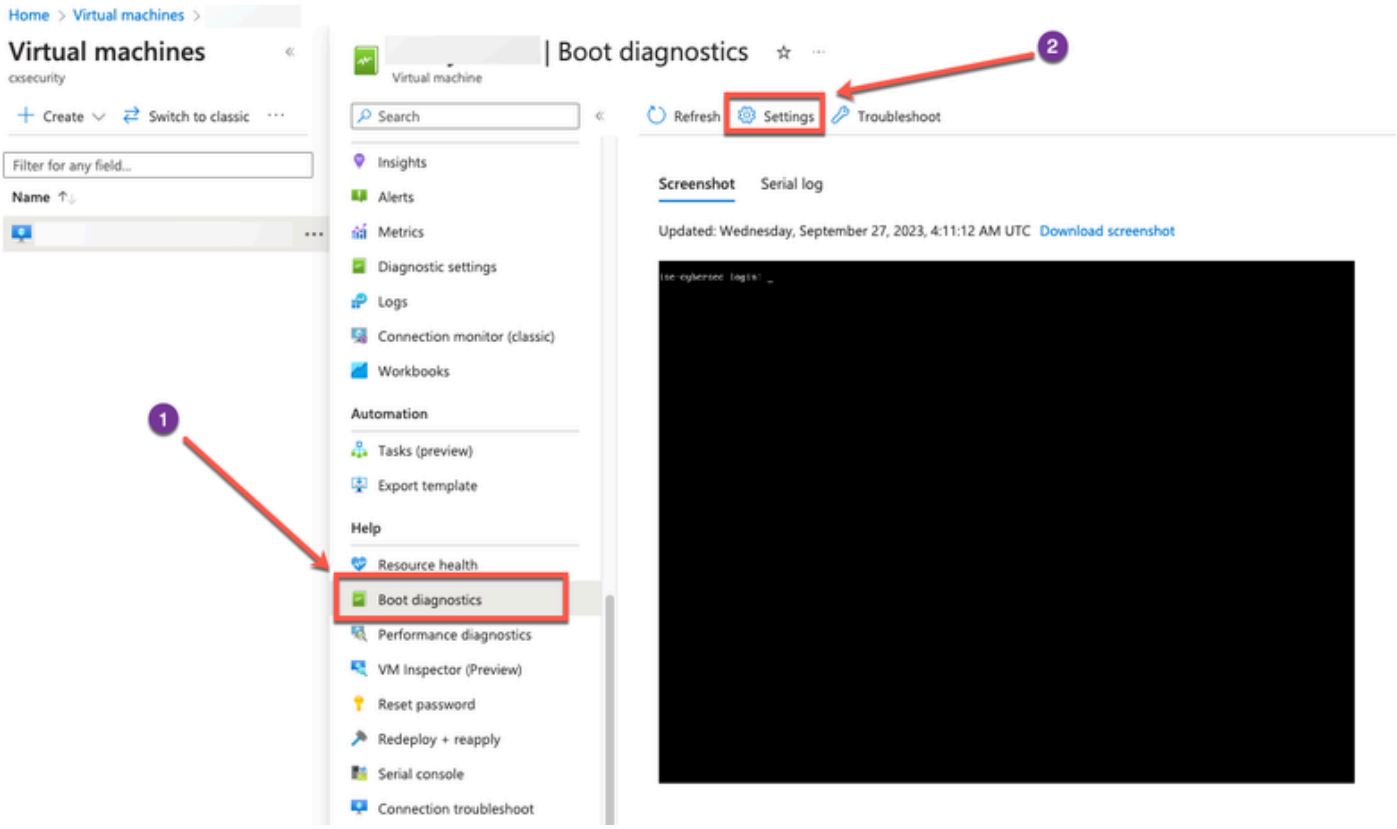
1. Zurücksetzen des Cisco ISE-GUI-Kennworts über die serielle Konsole

- Schritt (1): Melden Sie sich bei Azure Cloud an, und wählen Sie die Ressourcengruppe aus, die das virtuelle Cisco ISE-System enthält.
- Schritt 2: Klicken Sie in der Ressourcenliste auf die Cisco ISE-Instanz, für die Sie das Kennwort zurücksetzen möchten.
- Schritt (3): Klicken Sie im Menü auf der linken Seite im Abschnitt Support + Fehlerbehebung auf Serielle Konsole.

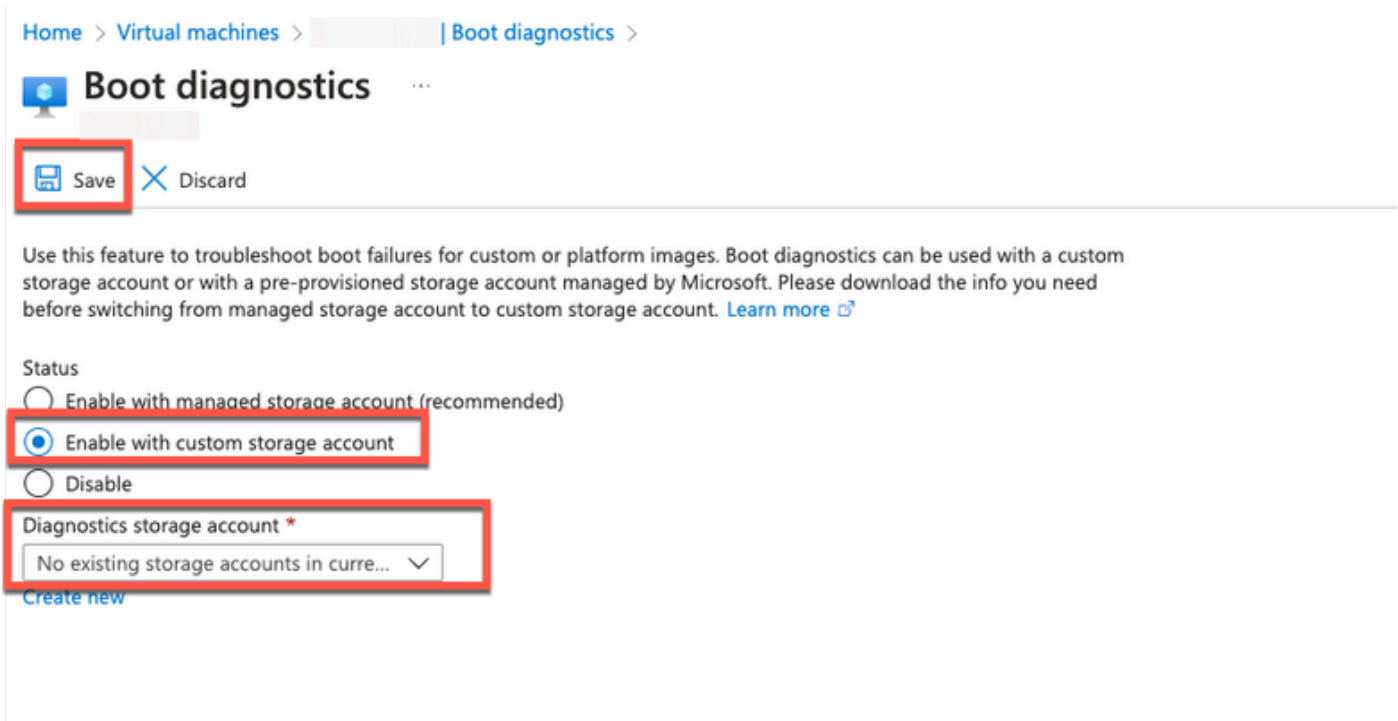


- Schritt 4: Wenn Sie hier eine Fehlermeldung anzeigen, müssen Sie die Bootdiagnose aktivieren, indem Sie die folgenden Schritte ausführen und ausführen:

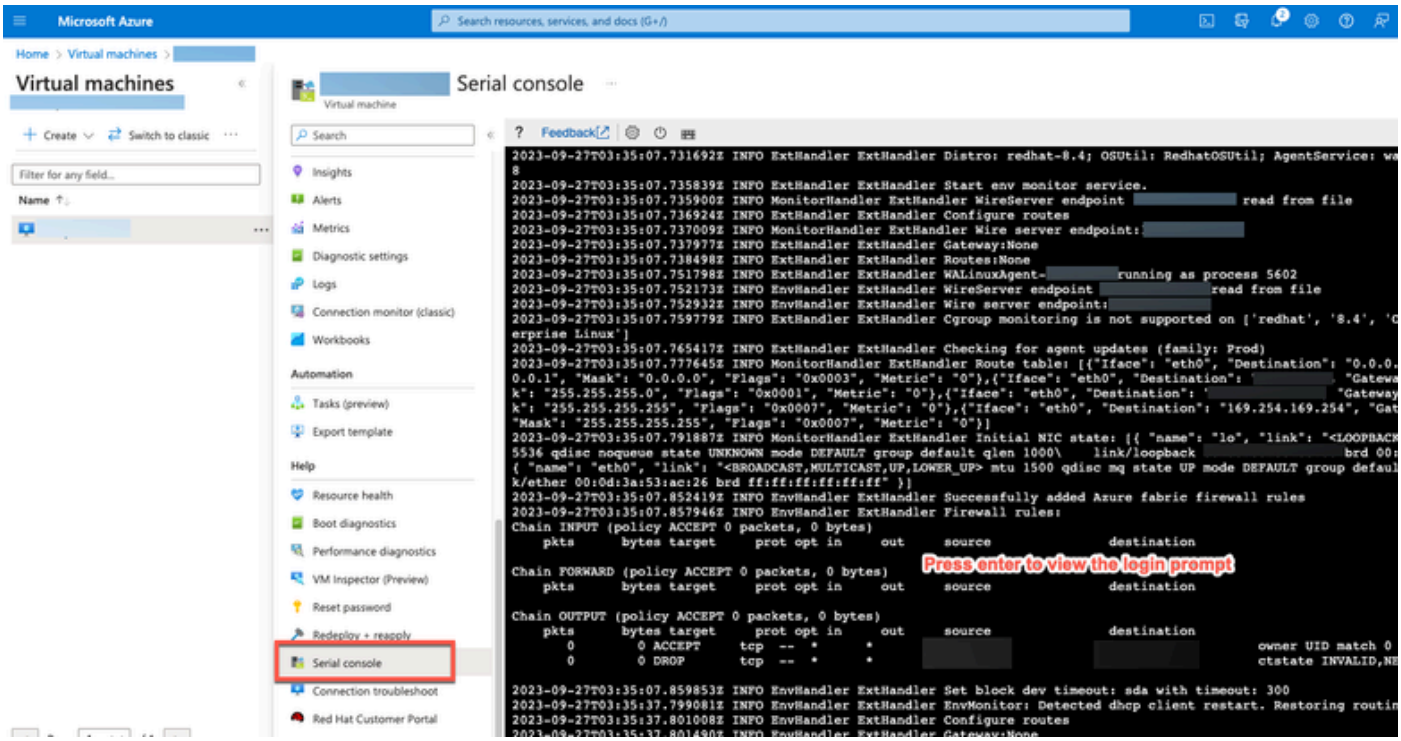
antwort: Klicken Sie im Menü auf der linken Seite auf Diagnose starten.



b. Klicken Sie auf Mit benutzerdefiniertem Speicherkonto aktivieren. Klicken Sie dann auf Speichern.



- Schritt (5): Klicken Sie im Menü auf der linken Seite im Abschnitt Support + Fehlerbehebung auf Serielle Konsole. Die Azure Cloud Shell wird in einem neuen Fenster angezeigt. Wenn der Bildschirm schwarz ist, drücken Sie die Eingabetaste, um die Anmeldeaufforderung anzuzeigen.

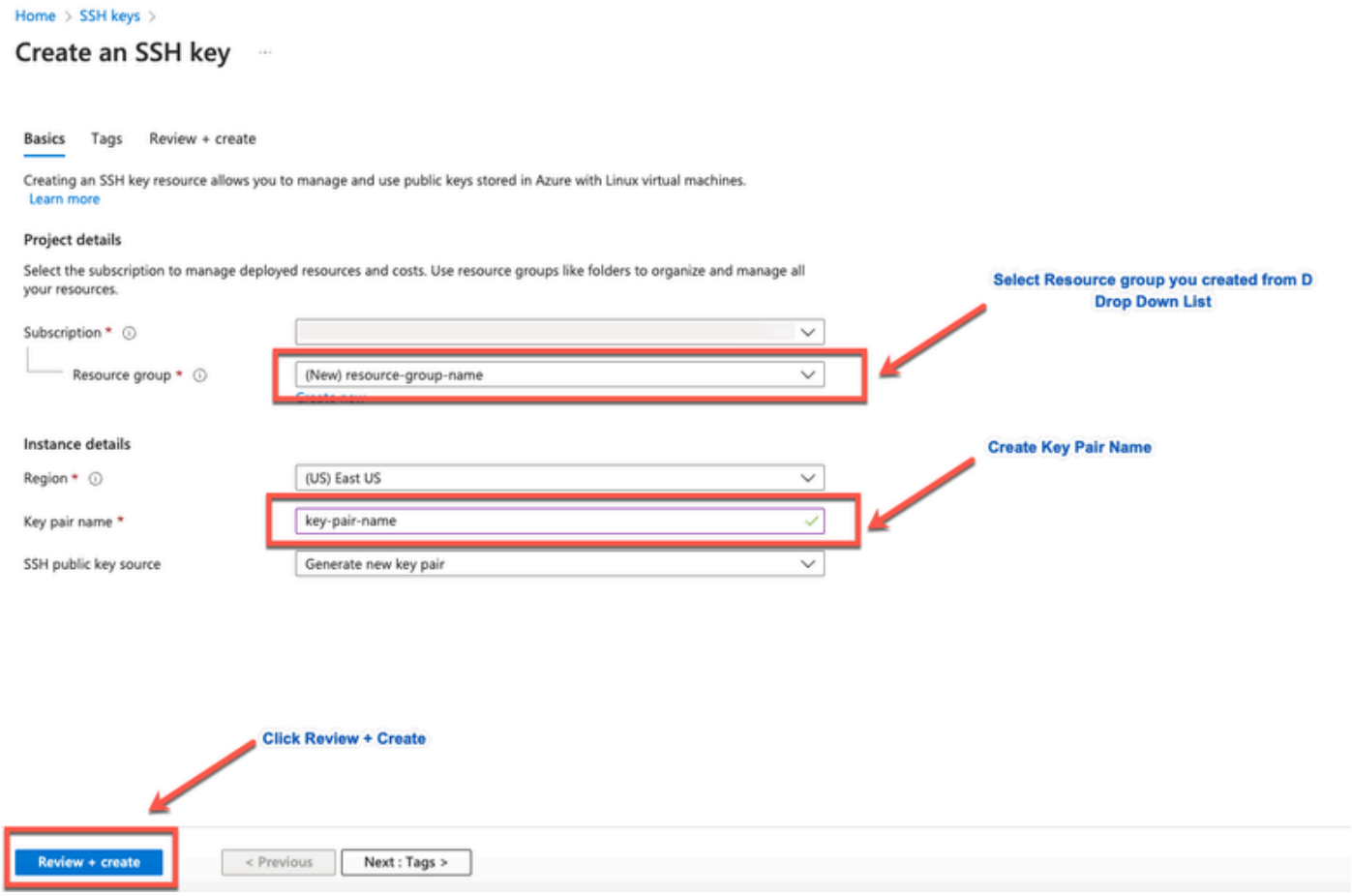


- Schritt (8): Melden Sie sich bei der seriellen Konsole an. Um sich bei der seriellen Konsole anzumelden, müssen Sie das ursprüngliche Kennwort verwenden, das bei der Installation der Instanz konfiguriert wurde.
- Schritt (9): Verwenden Sie den Befehl reset-passwd ise iseadmin der Anwendung, um ein neues GUI-Kennwort für das iseadmin-Konto zu konfigurieren.

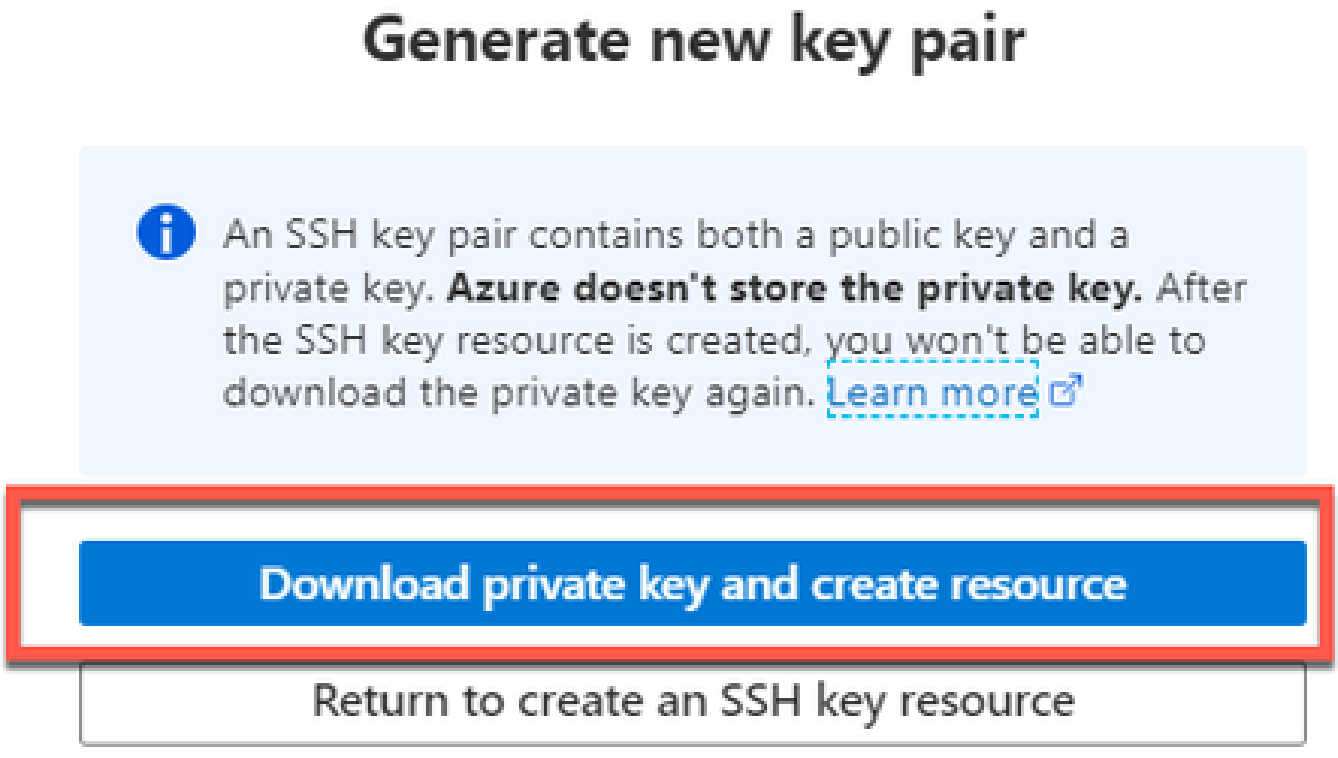
2. Erstellen Sie ein neues Public Key-Paar für den SSH-Zugriff.

Durch diese Aufgabe fügen Sie einem Repository zusätzliche Schlüsselpaare hinzu. Das vorhandene Schlüsselpaar, das zum Zeitpunkt der Cisco ISE-Instanzkonfiguration erstellt wurde, wird nicht durch den neuen öffentlichen Schlüssel ersetzt, den Sie erstellen.

- Schritt (1): Erstellen eines neuen öffentlichen Schlüssels in Azure Cloud



Sie erhalten ein Popup-Fenster, in dem Sie privaten Schlüssel herunterladen auswählen und eine Ressource erstellen können, die den SSH-Schlüssel als PEM-Datei herunterlädt.



- Schritt (2): Informationen zum Erstellen eines neuen Repositorys zum Speichern des öffentlichen Schlüssels finden Sie in der Azure Repos-Dokumentation.

Wenn Sie bereits über ein Repository verfügen, auf das über die CLI zugegriffen werden kann, fahren Sie mit Schritt 3 fort.

- Schritt (3): Um den neuen öffentlichen Schlüssel zu importieren, verwenden Sie den Befehl crypto key import <Dateiname des öffentlichen Schlüssels> repository <Projektarchivname>.
- Schritt 4: Nach Abschluss des Imports können Sie sich mit dem neuen öffentlichen Schlüssel über SSH bei der Cisco ISE anmelden.

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.