Installer ISE sur Azure Cloud Services

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Procédure

- Réseau virtuel et groupes de sécurité
- Tailles de VM Azure prises en charge par Cisco ISE
- Limites de Cisco ISE dans les services cloud Microsoft Azure

Configurer

- Exemple de déploiement ISE connecté au cloud Azure
- Configurations

Que faire ensuite ?

Tâches post-installation

Récupération et réinitialisation de mot de passe sur le cloud Azure

- Créer une nouvelle paire de clés publiques pour l'accès SSH

Introduction

Ce document décrit comment installer une instance Cisco ISE IOS® à l'aide d'une machine virtuelle Azure. Cisco ISE IOS® est disponible sur les services cloud Azure.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Abonnements et groupes de ressources

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco ISE version 3.2 et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Procédure

1. Accédez à Tous les services > Abonnements. Assurez-vous qu'un compte Azure avec un abonnement actif et un contrat d'entreprise avec Microsoft sont présents.

---

2. Utilisez l'interface de ligne de commande du module Microsoft PowerShell Azure pour exécuter des commandes afin de réserver de l'espace. Vous pouvez vous référer à Comment installer Azure PowerShell pour installer Power Shell et les packages appropriés.

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



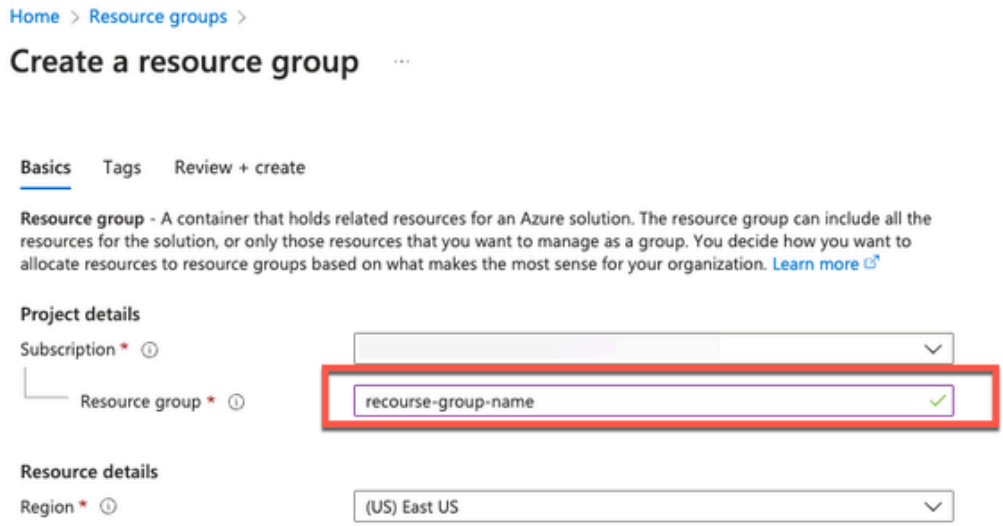
Remarque : Remplacez l'ID de locataire par votre ID de locataire réel.

---

3. Remplissez les conditions préalables à la demande de quota d'hôte pour la solution Azure VMware pour plus de détails.

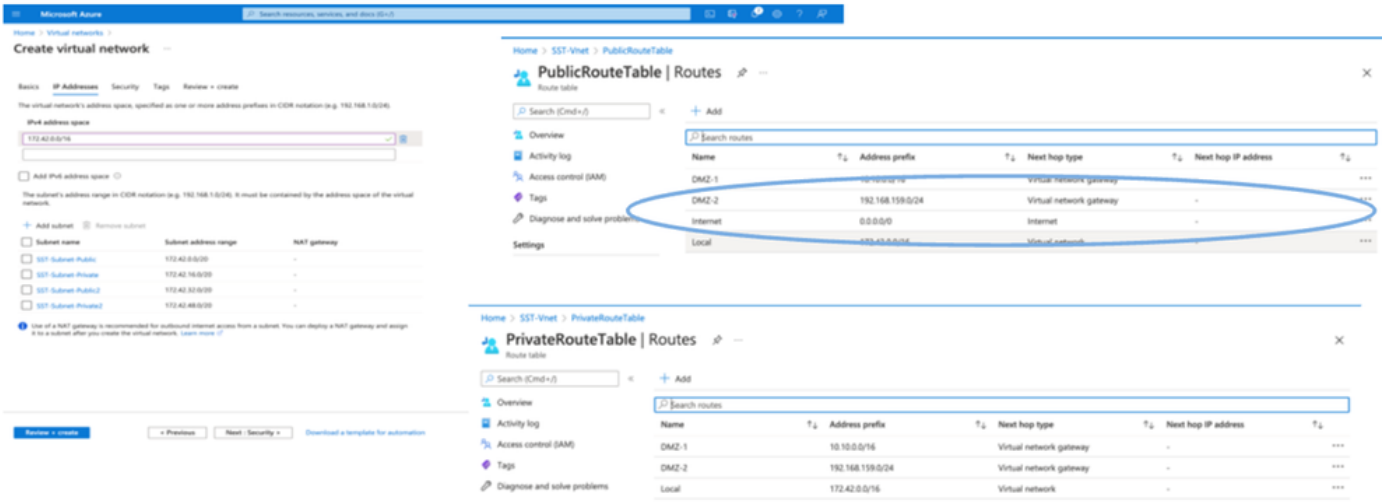
---

4. Créez un groupe de ressources juste après l'abonnement. Accédez à Tous les services > Groupes de ressources. Cliquez sur Ajouter. Entrez le nom du groupe de ressources.



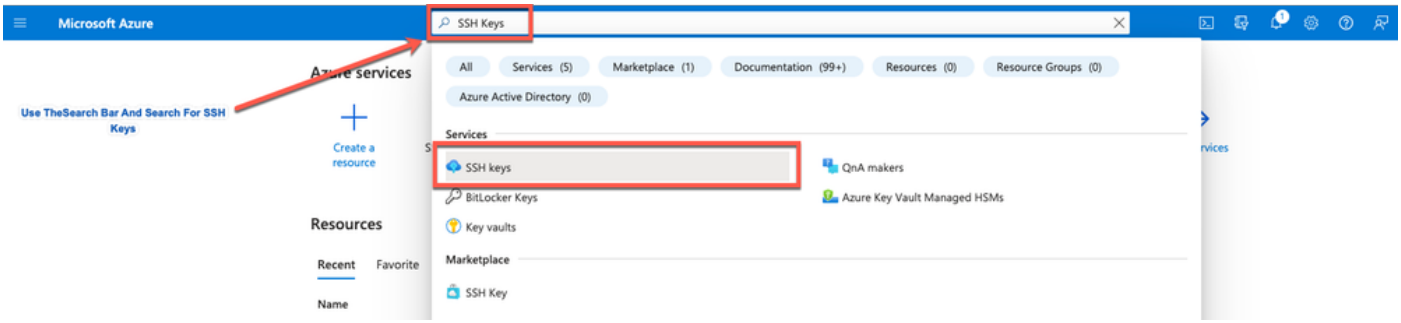
Réseau virtuel et groupes de sécurité

La table de routage du sous-réseau qui nécessite l'accessibilité à Internet doit être configurée avec le tronçon suivant en tant qu'Internet. Reportez-vous aux exemples de sous-réseaux publics et privés. Le PAN avec IP publique a des mises à jour de flux en ligne et hors connexion, tandis que le PAN avec IP privée doit s'appuyer sur des mises à jour de flux hors connexion.

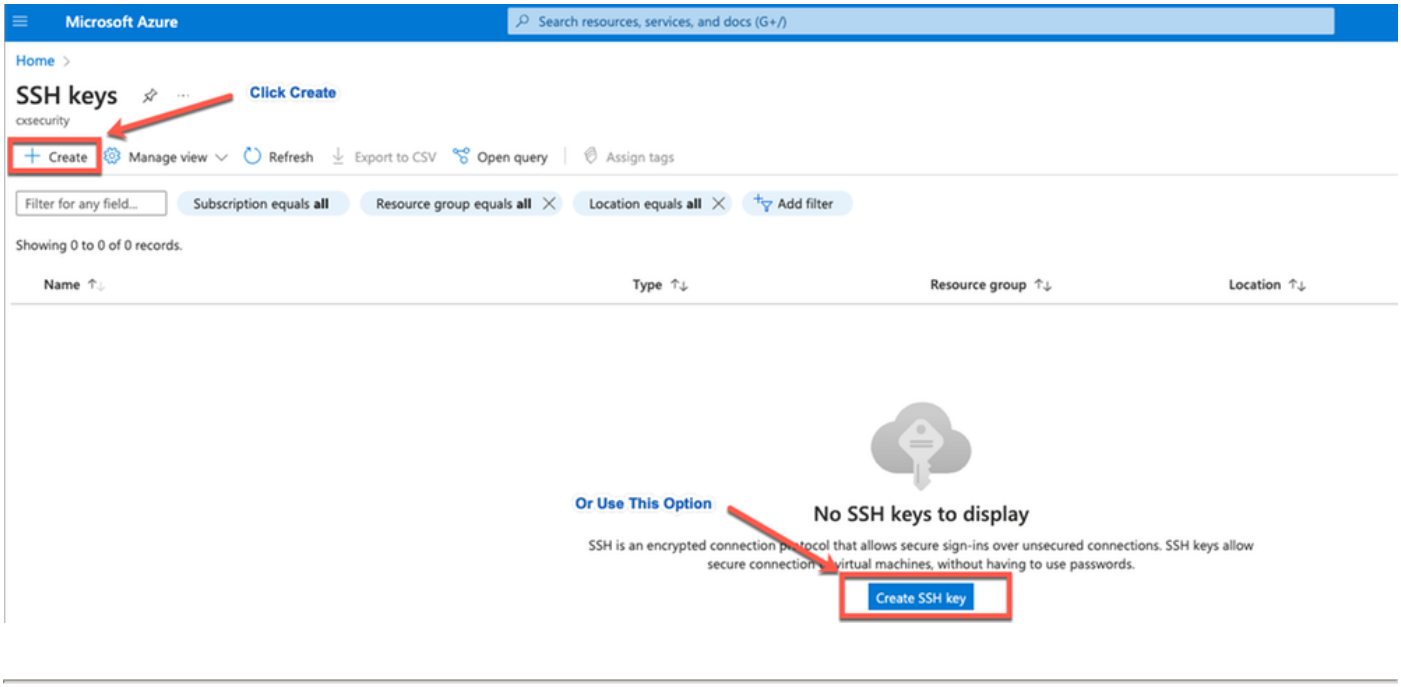


Créer une paire de clés SSH

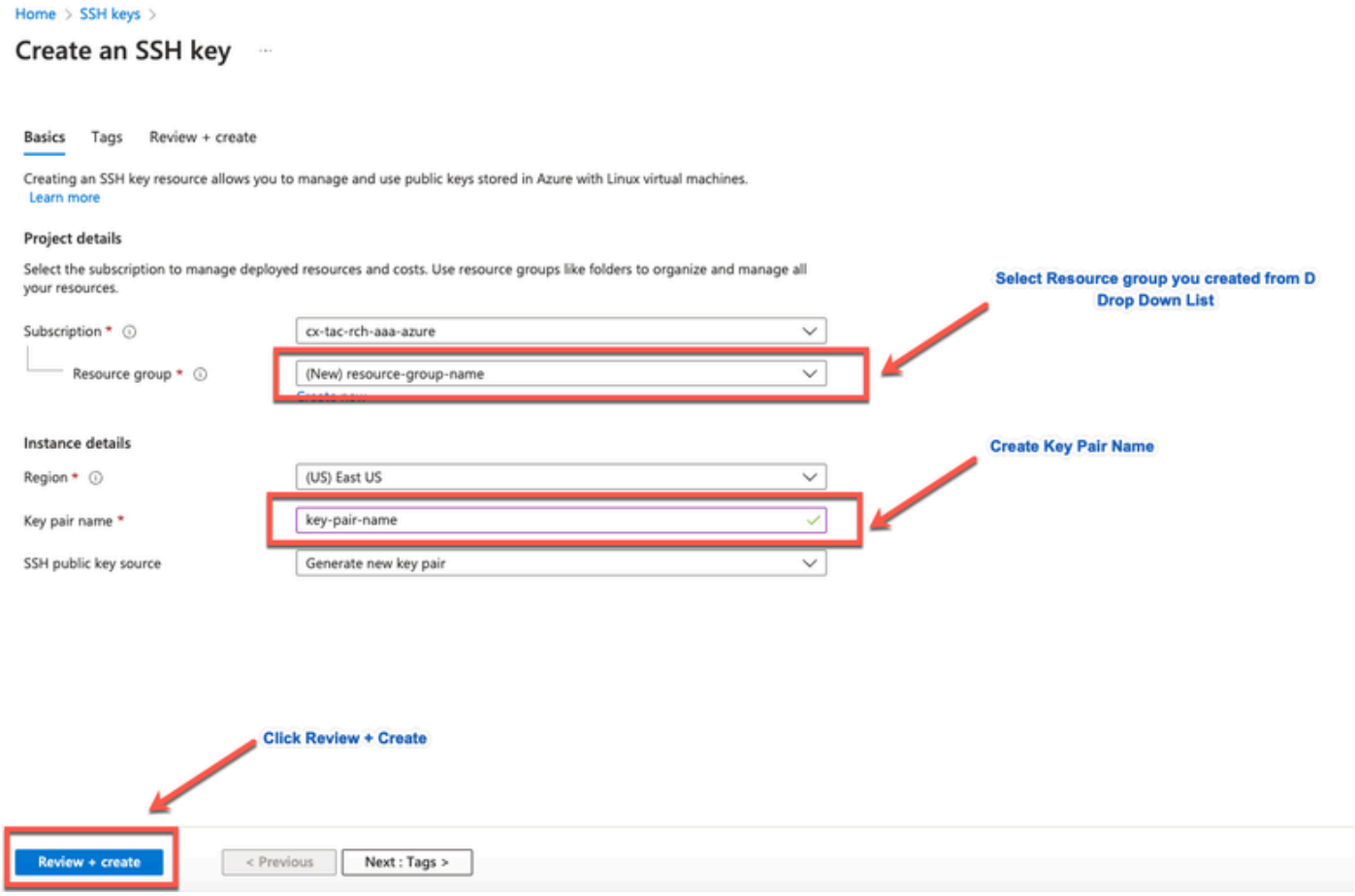
1. Utilisez la barre de recherche de la page d'accueil du portail Web Azure et recherchez des clés SSH.



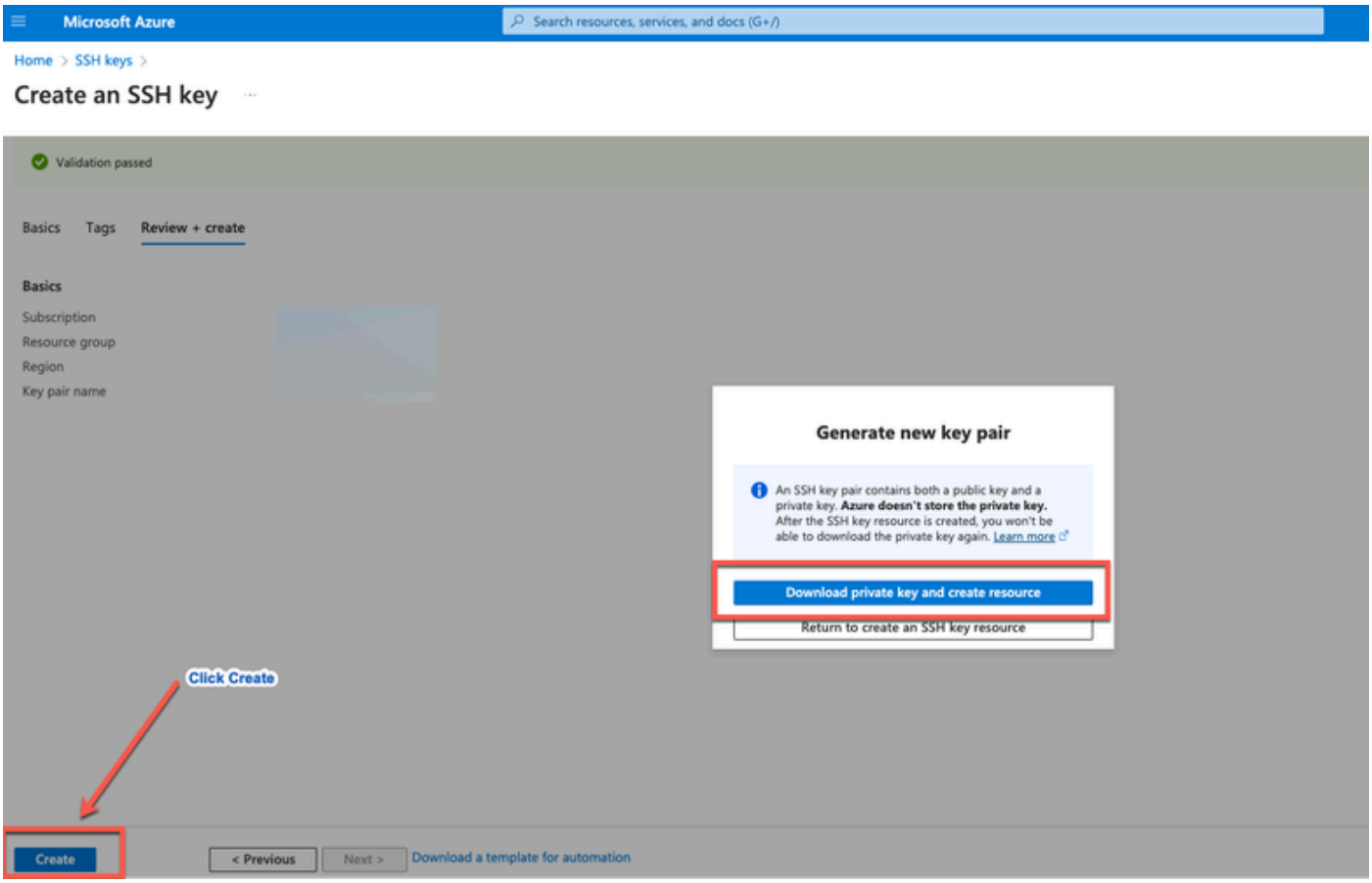
2. Cliquez sur Créer.



3. Choisissez le groupe de ressources et le nom de clé. Cliquez ensuite sur Vérifier + Créer.



4. Cliquez ensuite sur Create et téléchargez la clé privée.



Tailles de VM Azure prises en charge par 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

- Les tailles de VM Azure de la gamme Fsv2 sont optimisées pour le calcul et sont les mieux adaptées pour une utilisation en tant que PSN pour des tâches et des applications gourmandes en calcul.
- Les machines virtuelles Dsv4 sont des tailles de machines virtuelles Azure à usage général, qui conviennent le mieux comme noeuds PAN ou MnT, ou les deux, et sont destinées aux tâches de traitement des données et aux opérations de base de données.

Si vous utilisez une instance à usage général en tant que PSN, les performances sont inférieures à celles d'une instance optimisée pour le traitement informatique en tant que PSN. La taille de la machine virtuelle Standard_D8s_v4 doit être utilisée comme un PSN extra-petit uniquement.

Remarque : Ne clonez pas une image de cloud Azure existante pour créer une instance Cisco ISE. Cela peut provoquer des dysfonctionnements aléatoires et inattendus dans la machine ISE créée.

Limites de Cisco ISE dans les services cloud Microsoft Azure

- Si vous créez Cisco ISE à l'aide de la machine virtuelle Azure, Microsoft Azure attribue par défaut des adresses IP privées aux machines virtuelles via des serveurs DHCP. Avant de créer un déploiement Cisco ISE sur Microsoft Azure, vous devez mettre à jour les entrées DNS avant et arrière avec les adresses IP attribuées par Microsoft Azure.
- Après avoir installé Cisco ISE, vous pouvez également attribuer une adresse IP statique à votre machine virtuelle en mettant à jour l'objet Interface réseau dans Microsoft Azure :

    1. Arrêtez la machine virtuelle.
    2. Dans la zone Private IP address settings de la VM, dans la zone Assignment, cliquez sur Static.
    3. Redémarrez la machine virtuelle.
    4. Dans la console série Cisco ISE, attribuez l'adresse IP Gi0.
    5. Redémarrez le serveur d'applications Cisco ISE.

- La double carte réseau est prise en charge avec seulement deux cartes réseau : Gigabit Ethernet 0 et Gigabit Ethernet 1. Pour configurer une carte réseau secondaire dans votre instance Cisco ISE, vous devez d'abord créer un objet d'interface réseau dans Azure, mettre hors tension votre instance Cisco ISE, puis attacher cet objet d'interface réseau à Cisco ISE. Après avoir installé et lancé Cisco ISE sur Azure, utilisez l'interface de ligne de commande Cisco ISE pour configurer manuellement l'adresse IP de l'objet d'interface réseau en tant que carte réseau secondaire.
- Le workflow de mise à niveau Cisco ISE n'est pas disponible dans Cisco ISE sur Microsoft Azure. Seules les nouvelles installations sont prises en charge. Cependant, vous pouvez effectuer une sauvegarde et une restauration des données de configuration.
- Le cloud public prend uniquement en charge les fonctionnalités de couche 3. Les noeuds Cisco ISE sur Microsoft Azure ne prennent pas en charge les fonctions Cisco ISE qui dépendent des fonctionnalités de couche 2. Par exemple, l'utilisation de sondes de profileur SPAN DHCP et les fonctions de protocole CDP via l'interface de ligne de commande Cisco

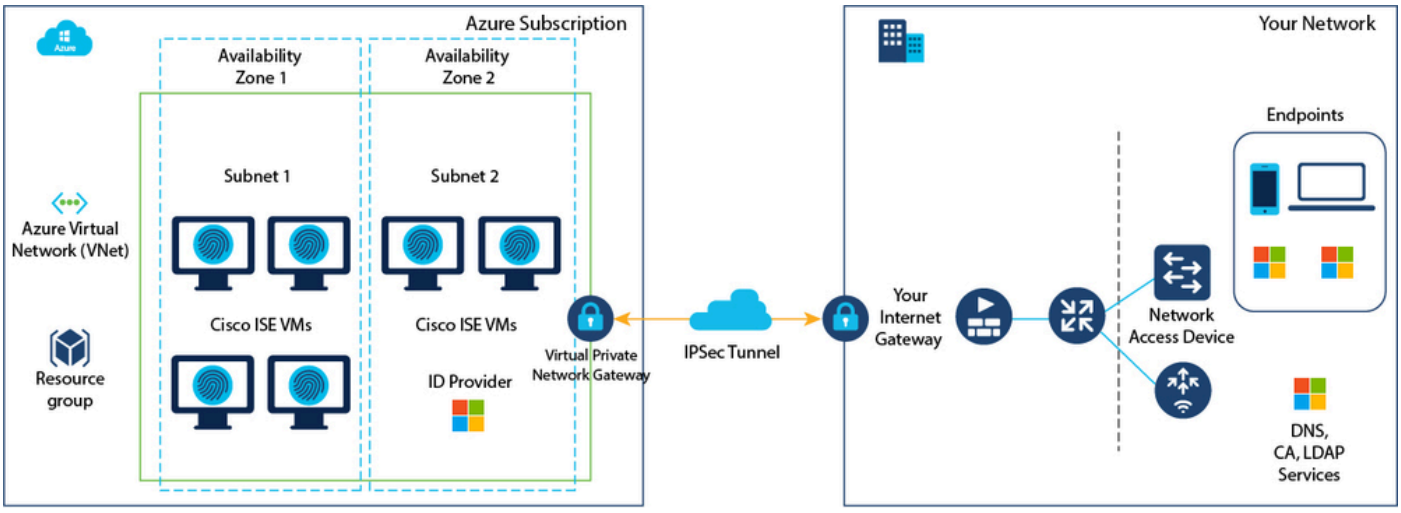
ISE sont des fonctions qui ne sont pas actuellement prises en charge.

- Lorsque vous exécutez la fonction de restauration et de sauvegarde des données de configuration, une fois l'opération de sauvegarde terminée, redémarrez d'abord Cisco ISE via l'interface de ligne de commande. Lancez ensuite l'opération de restauration à partir de l'interface utilisateur graphique Cisco ISE.
- L'accès SSH à l'interface de ligne de commande Cisco ISE avec authentification par mot de passe n'est pas pris en charge dans Azure. Vous ne pouvez accéder à l'interface de ligne de commande Cisco ISE que par l'intermédiaire d'une paire de clés, qui doit être stockée en toute sécurité. Si vous utilisez un fichier de clé privée (ou PEM) et que vous le perdez, vous ne pouvez pas accéder à l'interface de ligne de commande Cisco ISE. Toute intégration qui utilise une méthode d'authentification basée sur un mot de passe pour accéder à l'interface de ligne de commande Cisco ISE n'est pas prise en charge (Cisco DNA Center version 2.1.2 et antérieure).

- Les déploiements Cisco ISE IOS® sur Azure utilisent généralement des solutions VPN telles que DMVPN (Dynamic Multipoint Virtual Private Networks) et SD-WAN (Software-Defined Wide Area Networks), où les surcharges du tunnel IPSec peuvent entraîner des problèmes de MTU et de fragmentation. Dans de tels scénarios, Cisco ISE IOS® ne reçoit pas les paquets RADIUS complets et un échec d'authentification se produit sans déclencher un journal des erreurs d'échec.
    - Une solution de contournement possible consiste à demander au support technique de Microsoft d'explorer toutes les solutions dans Azure qui peuvent permettre aux fragments dans le désordre de passer à la destination au lieu d'être abandonnés.
- Un utilisateur d'administration CLI doit être 'iseadmin'.

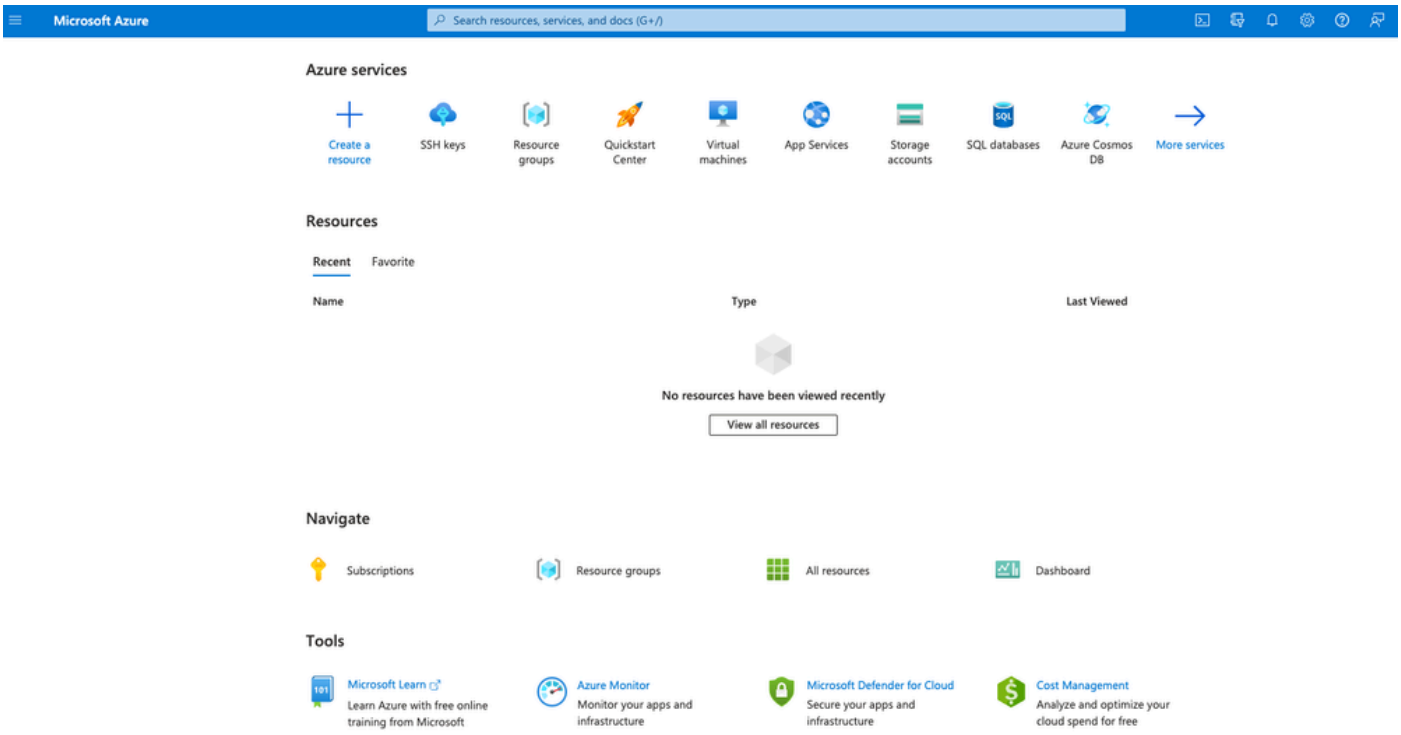
Configurer

Exemple de déploiement ISE connecté au cloud Azure



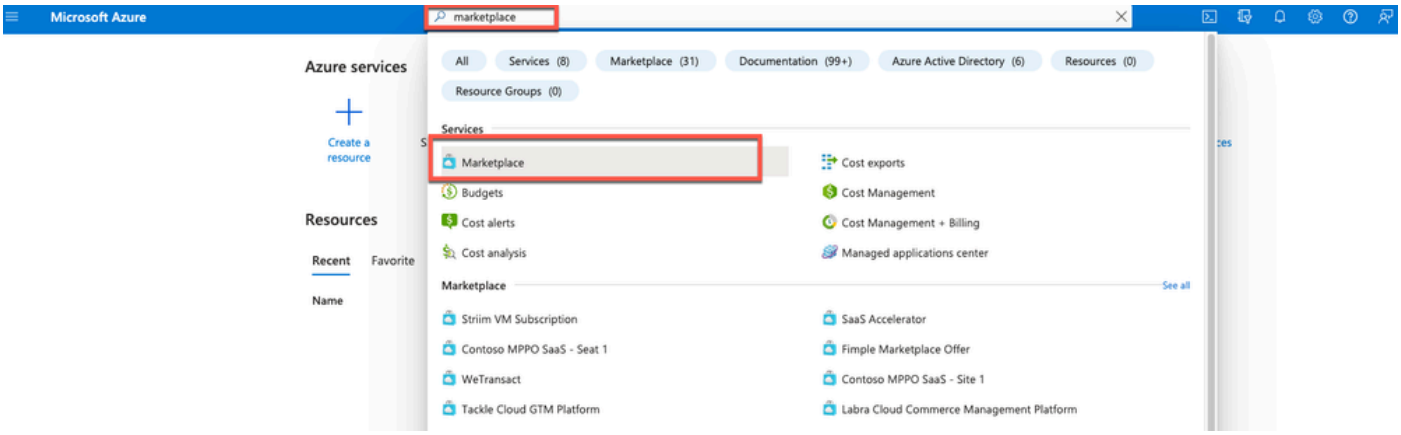
Configurations

1. Accédez au portail Azure et connectez-vous à votre compte Microsoft Azure.



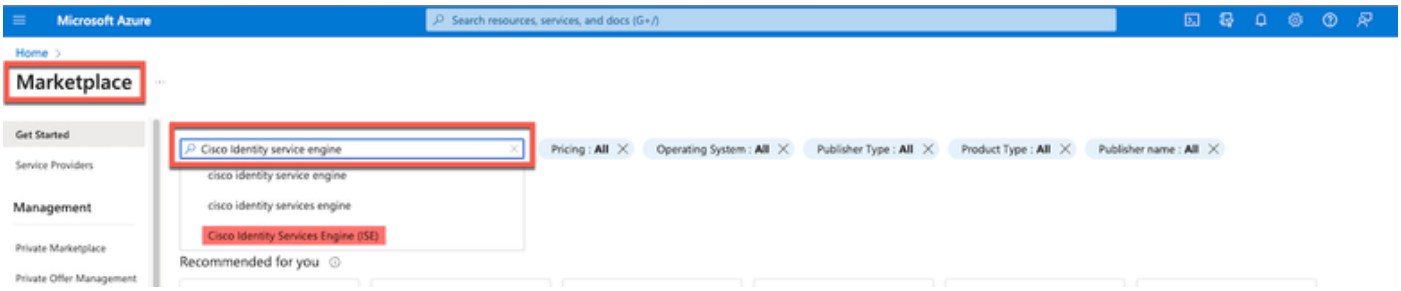
---

2. Utilisez le champ de recherche en haut de la fenêtre pour rechercher Marketplace.

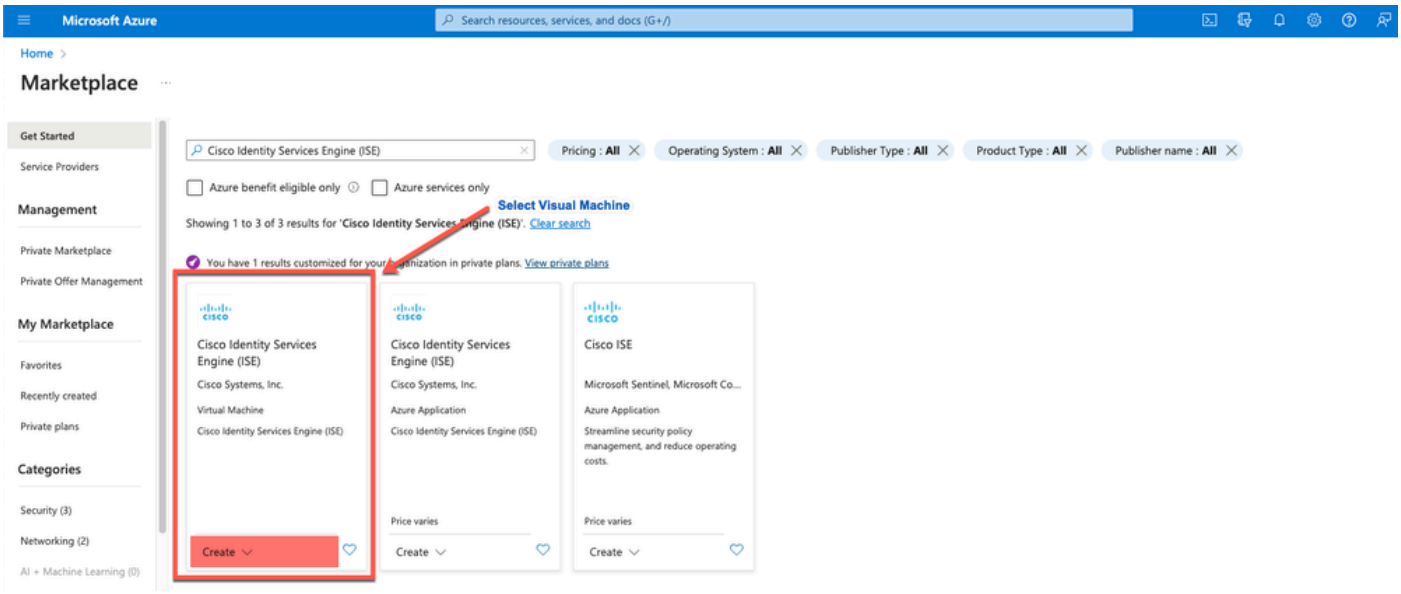


---

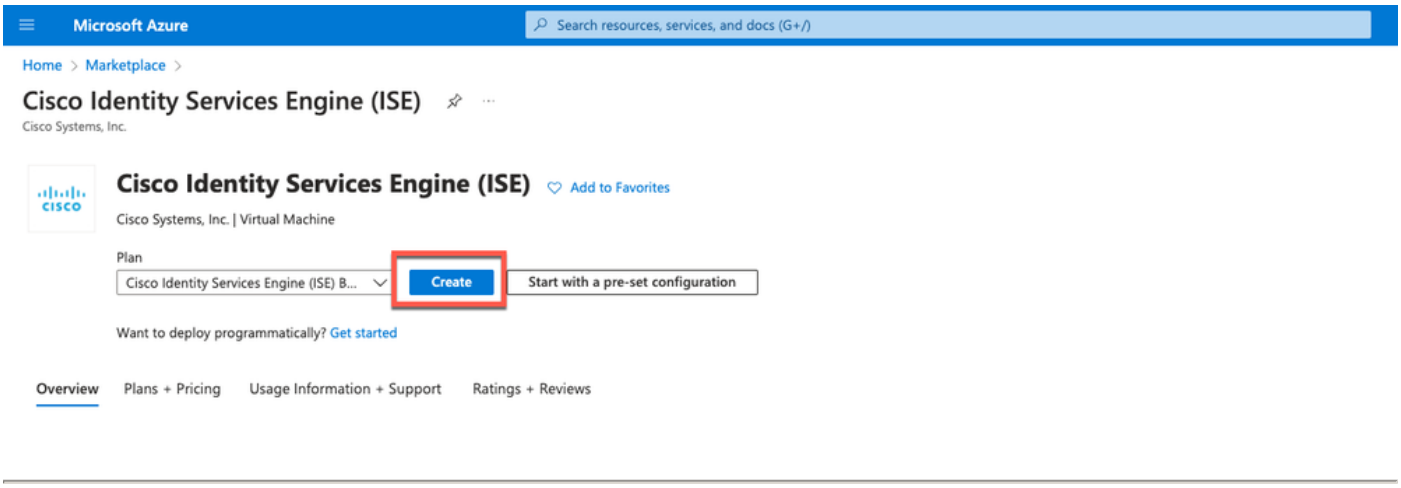
3. Utilisez le champ de recherche Rechercher sur le marché pour rechercher Cisco Identity Services Engine (ISE).



4. Cliquez sur Machine virtuelle.



5. Dans la nouvelle fenêtre, cliquez sur Créer.



6. Dans l'onglet Notions de base :

- Dans la zone Détails du projet, sélectionnez les valeurs requises dans les listes déroulantes Abonnement et Groupe de ressources.
- Dans la zone Détails de l'instance, entrez une valeur dans le champ Nom de la machine virtuelle.
- Dans la liste déroulante Image, sélectionnez l'image Cisco ISE.
- Dans la liste déroulante Size, sélectionnez la taille de l'instance avec laquelle vous souhaitez installer Cisco ISE. Choisissez une instance prise en charge par Cisco ISE, comme indiqué dans le tableau intitulé Azure Cloud.

Les instances prises en charge par Cisco ISE sont répertoriées dans la section Cisco ISE sur le cloud Azure.

e. Dans la zone Administrator Account > Authentication type, cliquez sur la case d'option SSH Public Key.

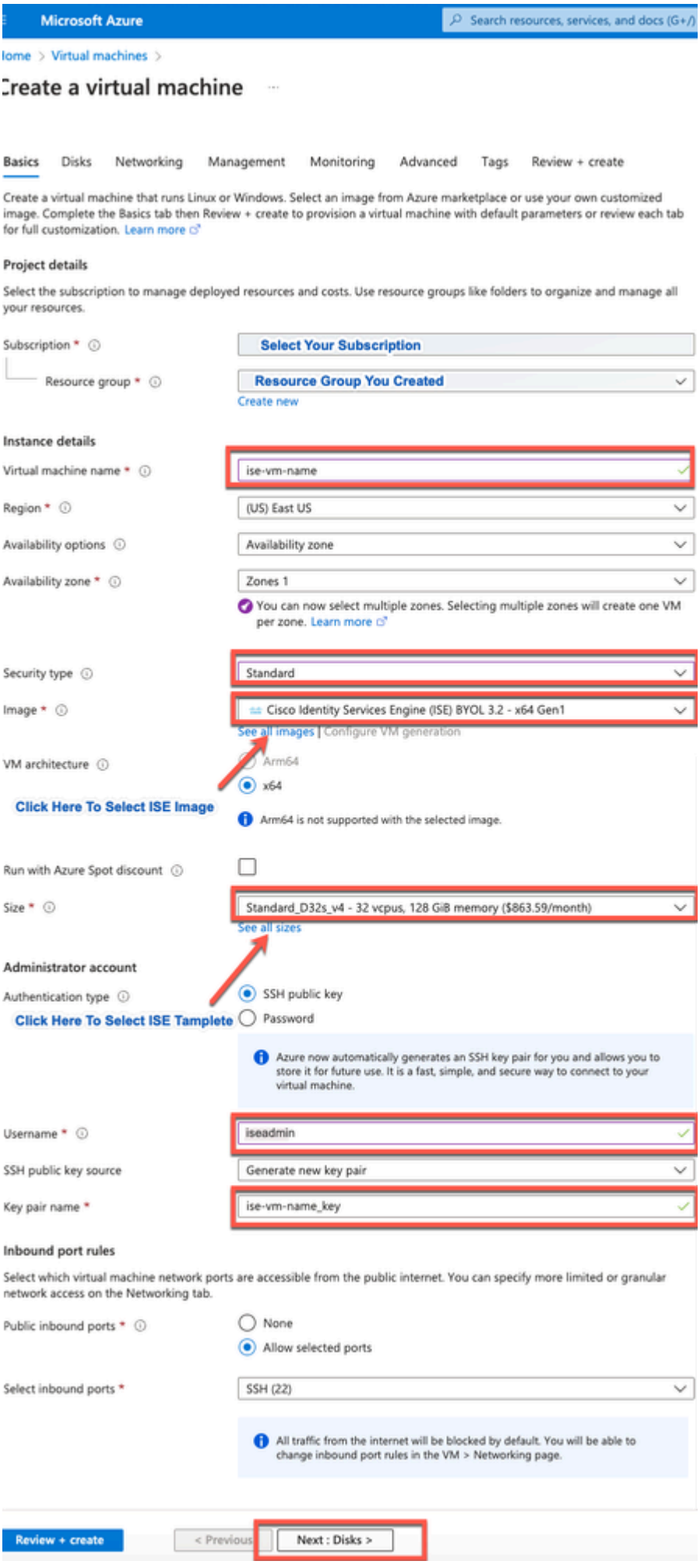
f. Dans le champ Username, saisissez iseadmin.

g. Dans la liste déroulante SSH public key source, sélectionnez Use existing key storage in Azure.

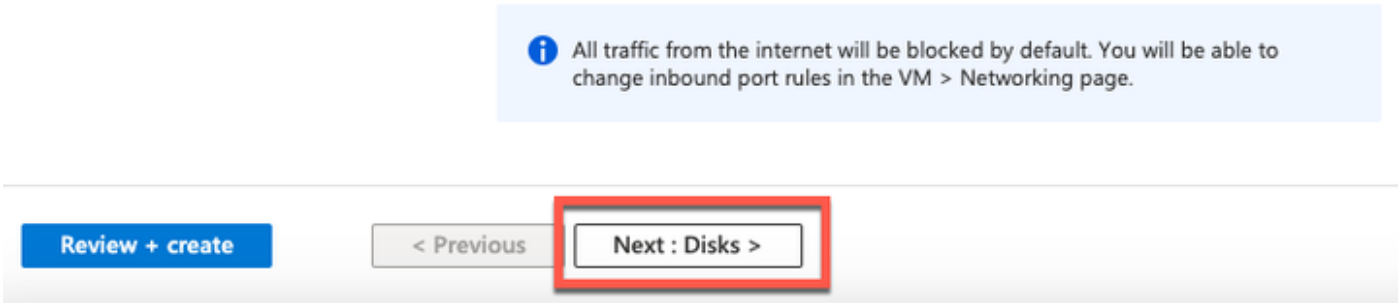
h. Dans la liste déroulante Clés stockées, sélectionnez la paire de clés que vous avez créée comme condition préalable à cette tâche.

j. Dans la zone Inbound port rules, cliquez sur la case d'option Allow selected ports.

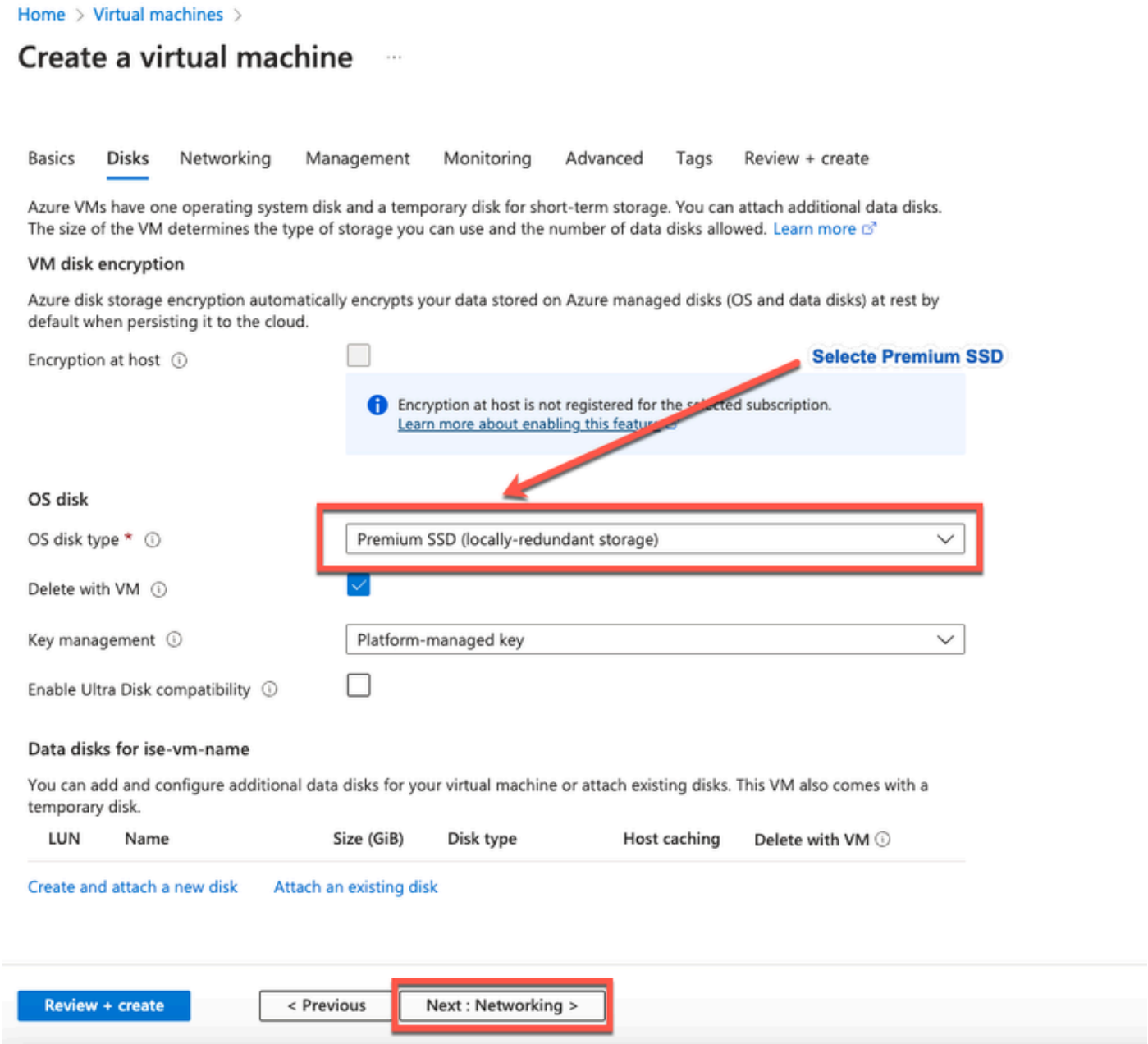
k. Dans la zone Licensing, dans la liste déroulante Licensing type, sélectionnez Other.


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. Cliquez sur Suivant : Disques.



8. Dans l'onglet Disks, conservez les valeurs par défaut pour les champs obligatoires et cliquez sur Next : Réseautage.

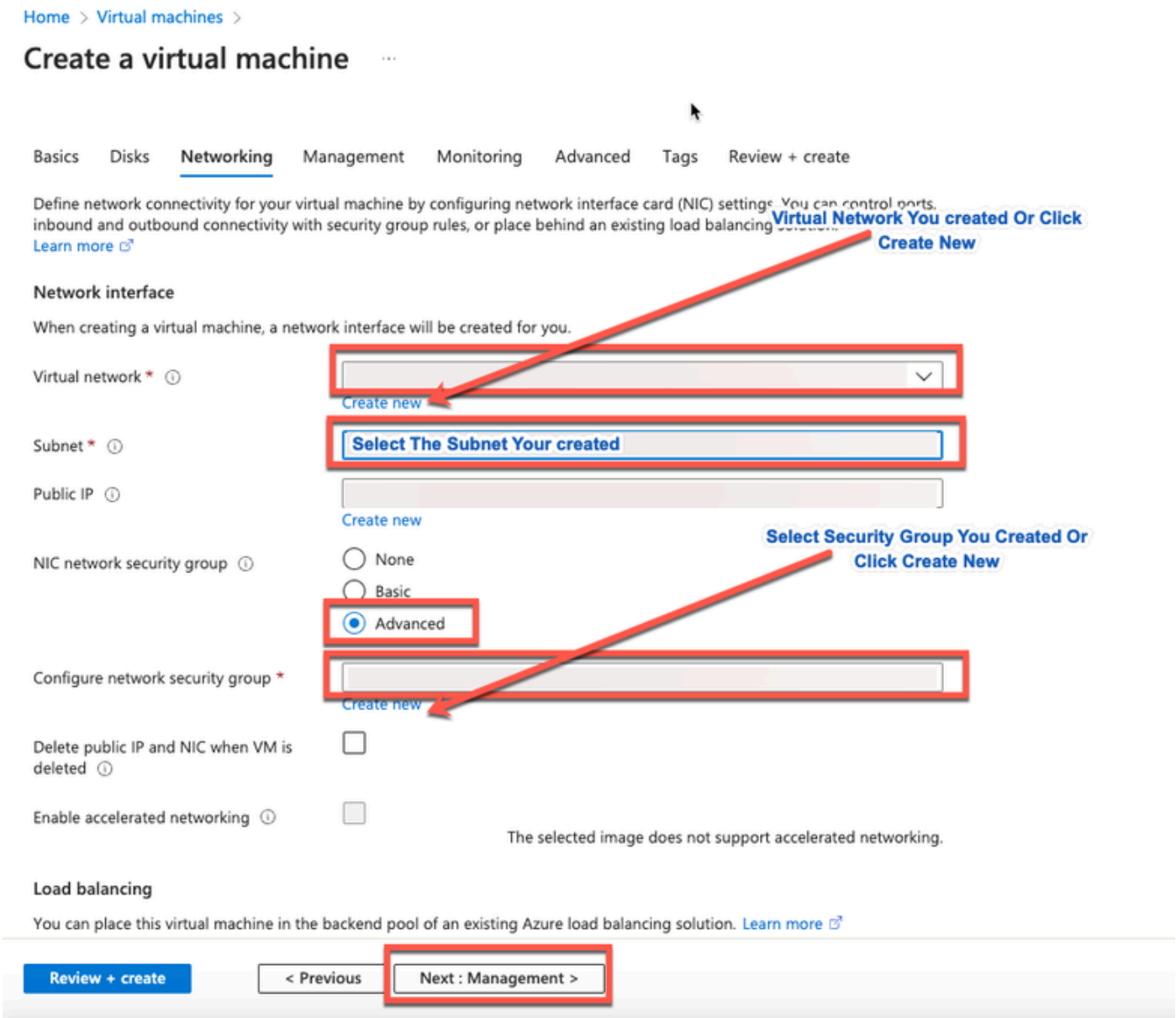


Remarque : Pour le type de disque, vous avez le choix entre plusieurs options dans la liste déroulante. Vous pouvez choisir celui qui répond à vos besoins. Le disque SSD Premium est le type recommandé pour les charges de travail sensibles à la production et aux performances.

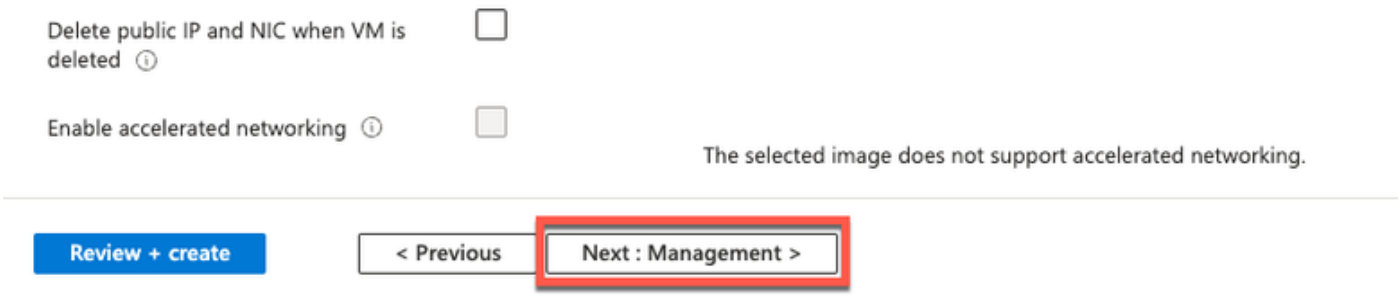
---

9. Dans la zone Network Interface, dans les listes déroulantes Virtual Network, Subnet, et Configure Network Security Group, sélectionnez le réseau virtuel et le sous-réseau que vous avez créés.

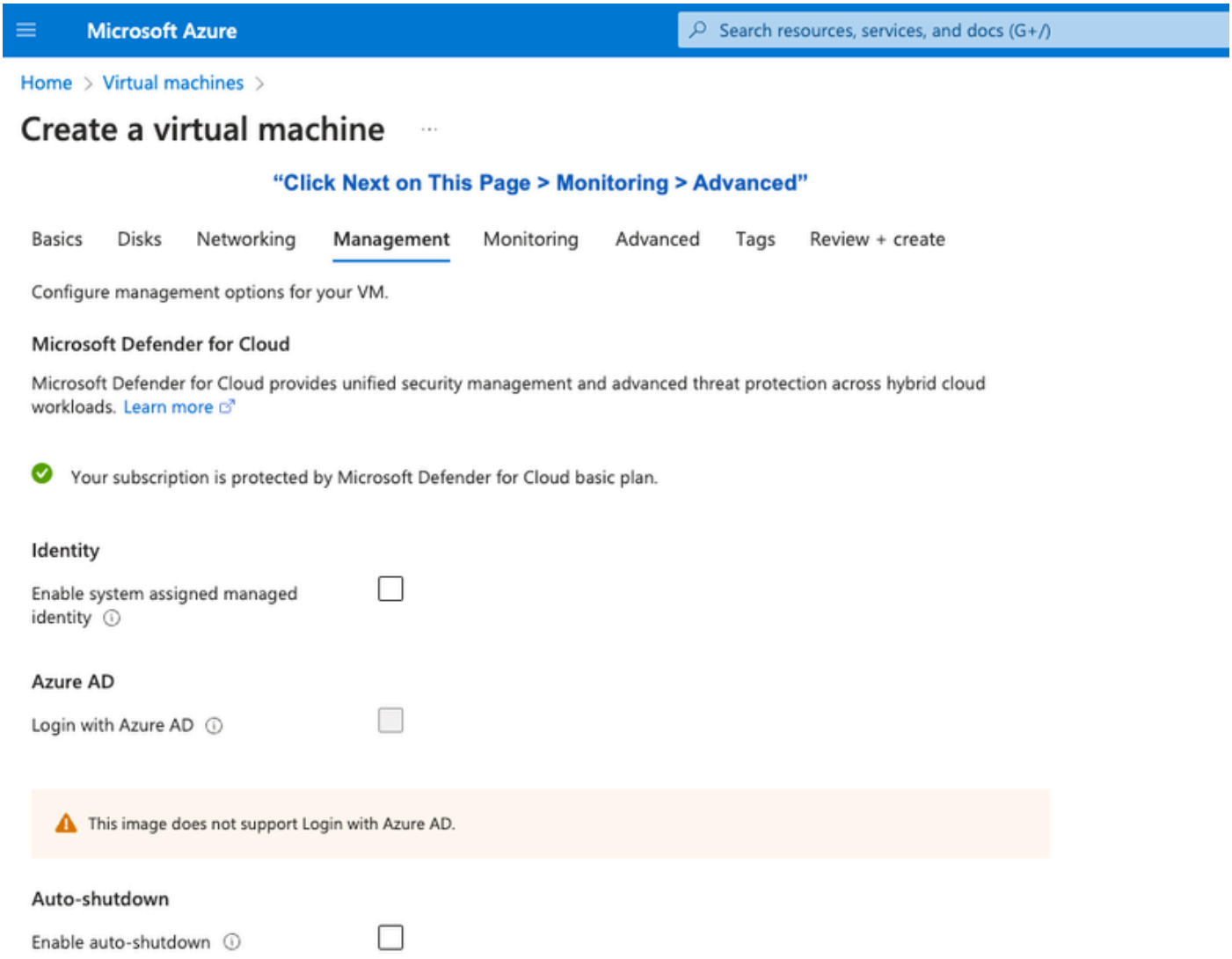
Remarque : Le sous-réseau avec une adresse IP publique reçoit des mises à jour de flux de positionnement en ligne et hors connexion, tandis qu'un sous-réseau avec une adresse IP privée reçoit uniquement des mises à jour de flux de positionnement hors connexion.

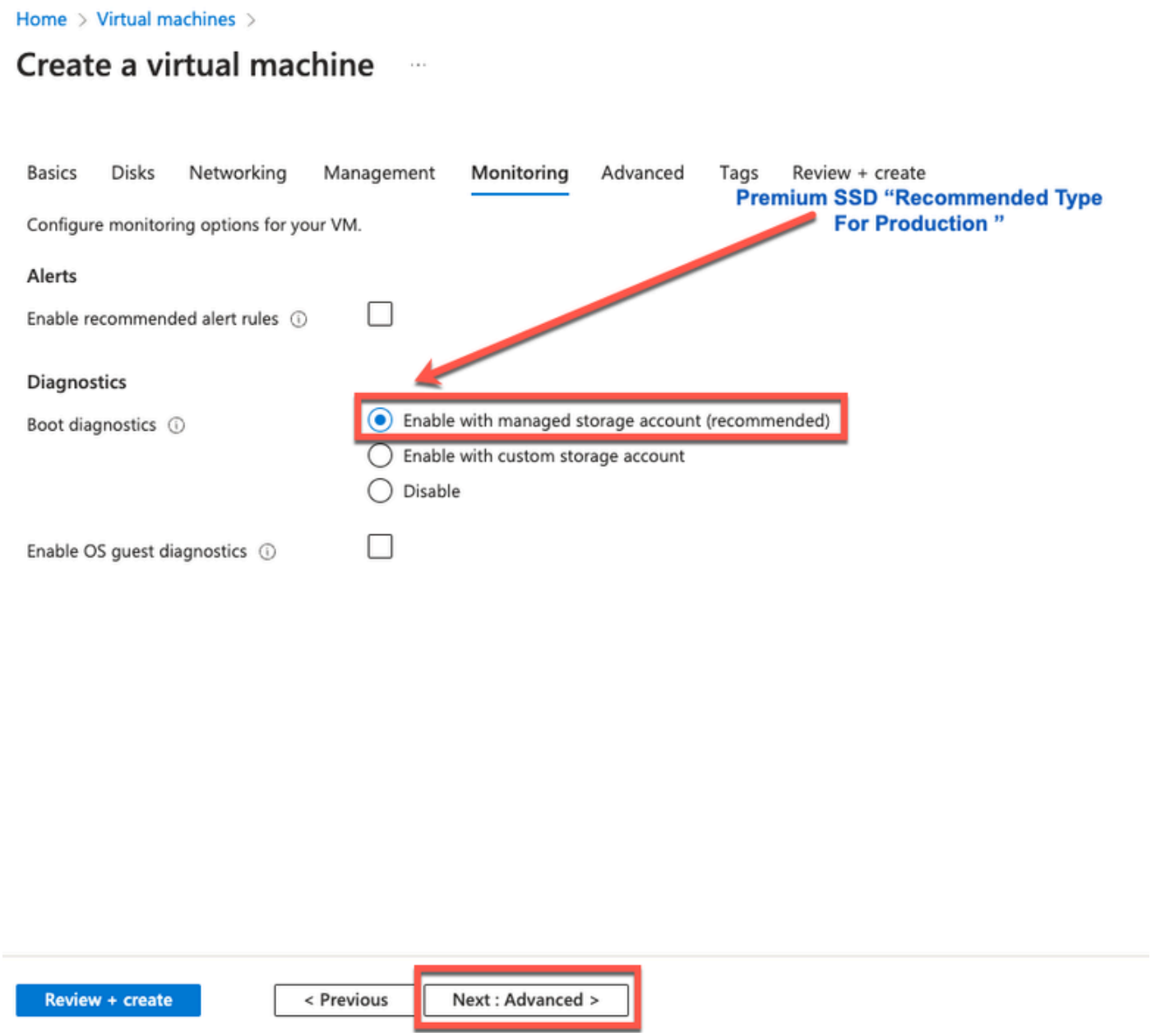


10. Cliquez sur Next : Gestion.



11. Dans l'onglet Gestion, conservez les valeurs par défaut des champs obligatoires et cliquez sur Suivant : Avancé.





---

12. Dans la zone Données utilisateur, cochez la case Activer les données utilisateur.

- Dans le champ Données utilisateur, renseignez les informations suivantes :
  - hostname=<nom d'hôte de Cisco ISE>
  - primarynameserver=<adresse IPv4>
  - dnsdomain=<nom de domaine>
  - ntpserver=<adresse IPv4 ou nom de domaine complet du serveur NTP>
  - timezone=<fuseau horaire>
  - password=<mot de passe>
  - ersapi=<oui/non>
  - openapi=<oui/non>
  - pxGrid=<oui/non>
  - pxgrid_cloud=<oui/non>

Remarque : Vous devez utiliser la syntaxe correcte pour chacun des champs que vous configurez via l'entrée de données utilisateur. Les informations que vous saisissez dans le champ Données utilisateur ne sont pas validées lorsqu'elles sont saisies. Si vous utilisez une syntaxe incorrecte, les services Cisco ISE ne se chargent pas lorsque vous lancez l'image.

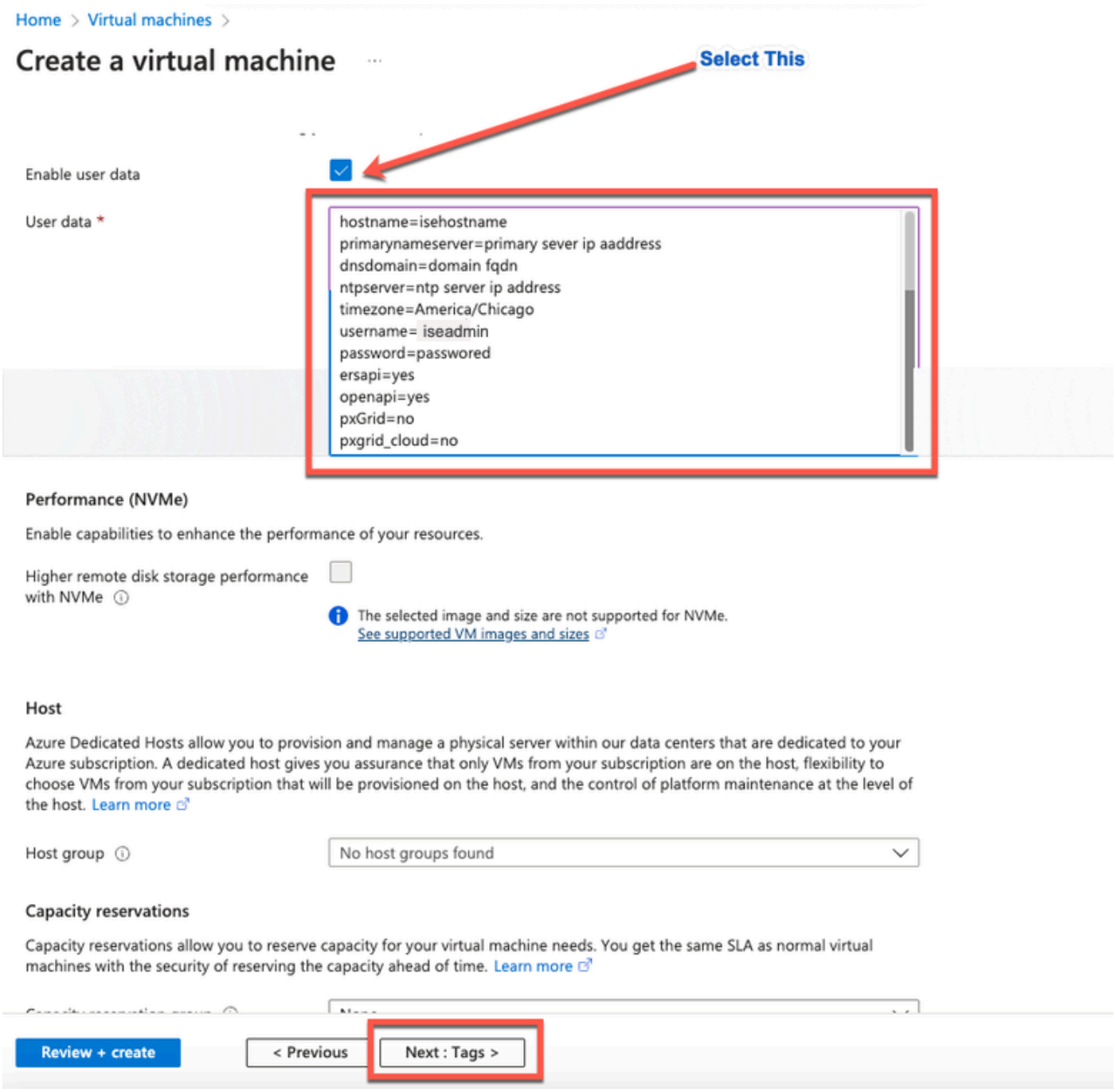
À partir de Cisco ISE version 3.4, le nom du champ ntpserver est remplacé par primaryntpserver. Si vous utilisez ntpserver, les services Cisco ISE ne peuvent pas démarrer. OpenAPI est activé par défaut, par conséquent, le champ openapi=<yes/no> n'est pas requis. Si vous laissez le champ secondarynameserver vide et n'utilisez que le champ tertiarynameserver, les services Cisco ISE ne peuvent pas démarrer. Si vous laissez le champ secondaryntpserver vide et n'utilisez que le champ tertiaryntpserver, les services Cisco ISE ne peuvent pas démarrer.

Reportez-vous aux Directives pour les configurations que vous devez soumettre via le champ de données utilisateur :

- nom de l'hôte: Saisissez un nom d'hôte contenant uniquement des caractères alphanumériques et des tirets (-). La longueur du nom d'hôte ne doit pas dépasser 19 caractères et ne peut pas contenir de traits de soulignement (_).
- serveur de noms principal : Saisissez l'adresse IP du serveur de noms principal. Seules les adresses IPv4 sont prises en charge. Vous ne pouvez ajouter qu'un seul serveur DNS à cette étape. Vous pouvez ajouter des serveurs DNS supplémentaires via l'interface de ligne de commande Cisco ISE après l'installation.
- dnsdomain : Entrez le nom de domaine complet du domaine DNS. L'entrée peut contenir des caractères ASCII, des chiffres, des tirets (-) et des points (.).
- ntpserver : Entrez l'adresse IPv4 ou le nom de domaine complet du serveur NTP qui doit être utilisé pour la synchronisation. Vous ne pouvez ajouter qu'un seul serveur NTP à cette étape. Vous pouvez ajouter des serveurs NTP supplémentaires via l'interface de ligne de commande Cisco ISE après l'installation. Utilisez un serveur NTP valide et accessible, car cela est requis pour les opérations ISE.
- fuseau horaire : Saisissez un fuseau horaire, par exemple, EST/UTC. Il est recommandé de définir tous les noeuds Cisco ISE sur le fuseau horaire UTC (Coordinated Universal Time), en particulier si vos noeuds Cisco ISE sont installés dans un déploiement distribué. Cette procédure garantit que les horodatages des rapports et des journaux de divers noeuds de votre déploiement sont toujours synchronisés.
- password : configurez un mot de passe pour la connexion à Cisco ISE via l'interface utilisateur graphique. Le mot de passe que vous entrez doit être conforme à la politique de mot de passe Cisco ISE. Le mot de passe doit contenir entre 6 et 25 caractères et inclure au moins un chiffre, une lettre majuscule et une lettre minuscule. Le mot de passe ne peut pas être le même que le nom d'utilisateur ou son inverse (iseadmin ou nimdaesi), cisco ou ocsic. Les caractères spéciaux autorisés sont @~*!, +=_-. Reportez-vous à la section « Politique

de mot de passe utilisateur » du chapitre « Configuration de base » du Guide de l'administrateur Cisco ISE pour connaître votre version.

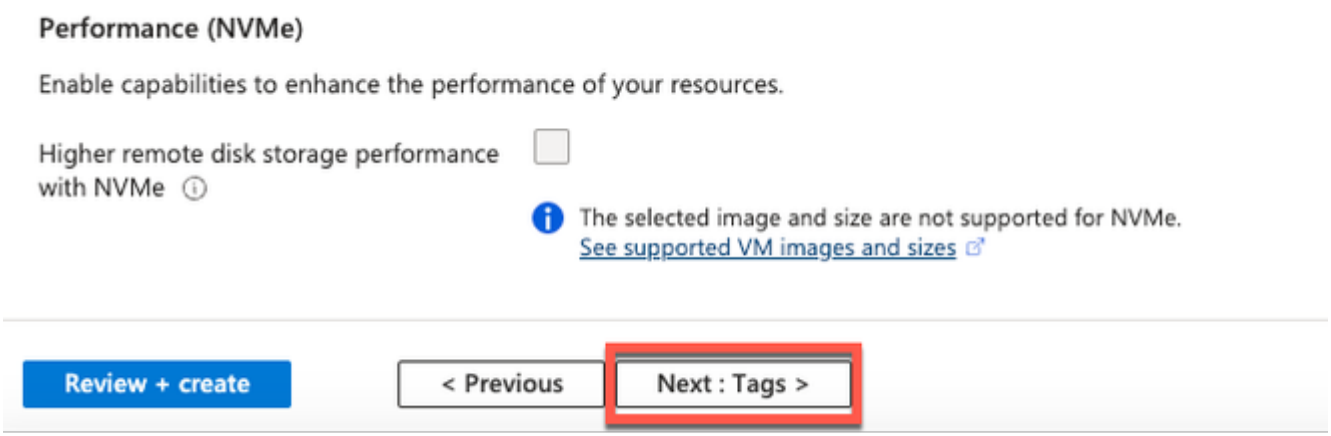
- ersapi : Entrez yes pour activer ERS ou no pour désactiver ERS.
- openapi : Entrez yes pour activer OpenAPI ou no pour désactiver OpenAPI.
- pxGrid : Entrez yes pour activer pxGrid ou no pour désactiver pxGrid.
- pxgrid_cloud : Entrez yes pour activer pxGrid Cloud ou no pour désactiver pxGrid Cloud. Pour activer pxGrid Cloud, vous devez activer pxGrid. Si vous désactivez pxGrid, mais activez pxGrid Cloud, les services pxGrid Cloud ne sont pas activés au lancement.



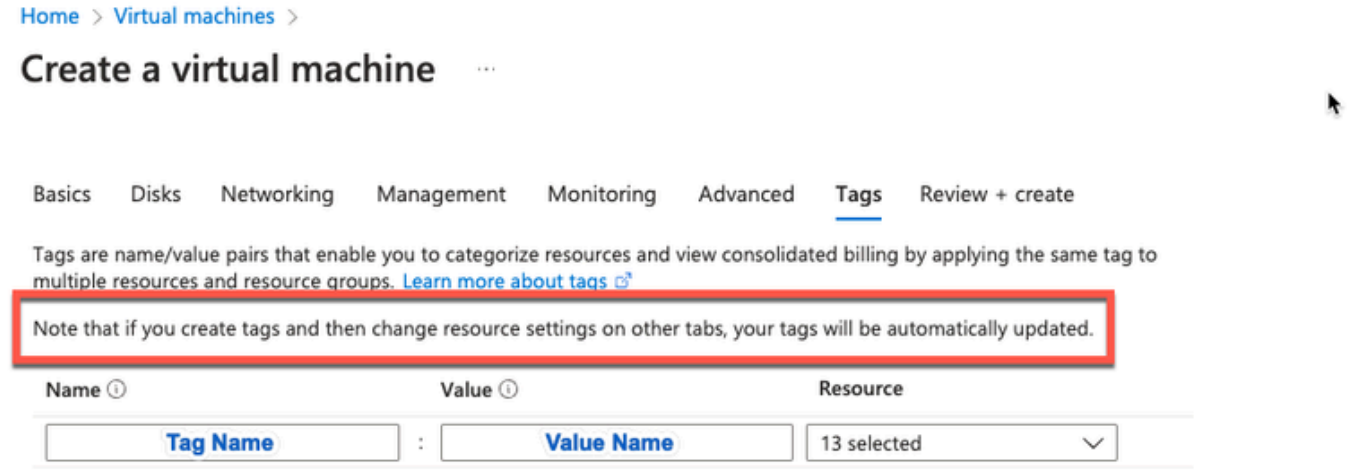
Section Données utilisateur

---

13. Cliquez sur Suivant : Étiquettes.



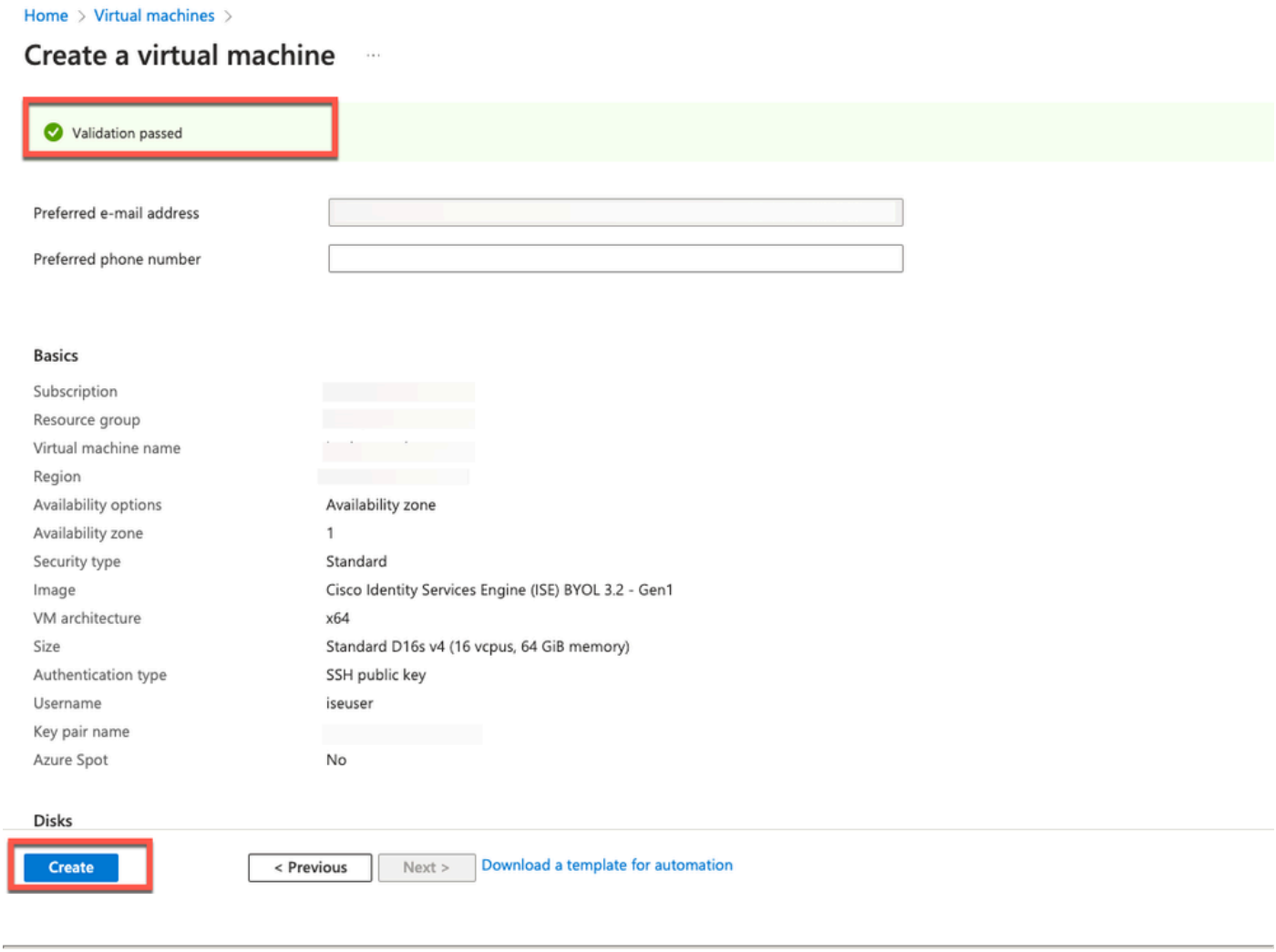
14. Créer des paires nom-valeur qui vous permettent de classer les ressources et de consolider plusieurs ressources et groupes de ressources ; saisissez des valeurs dans les champs Nom et Valeur.

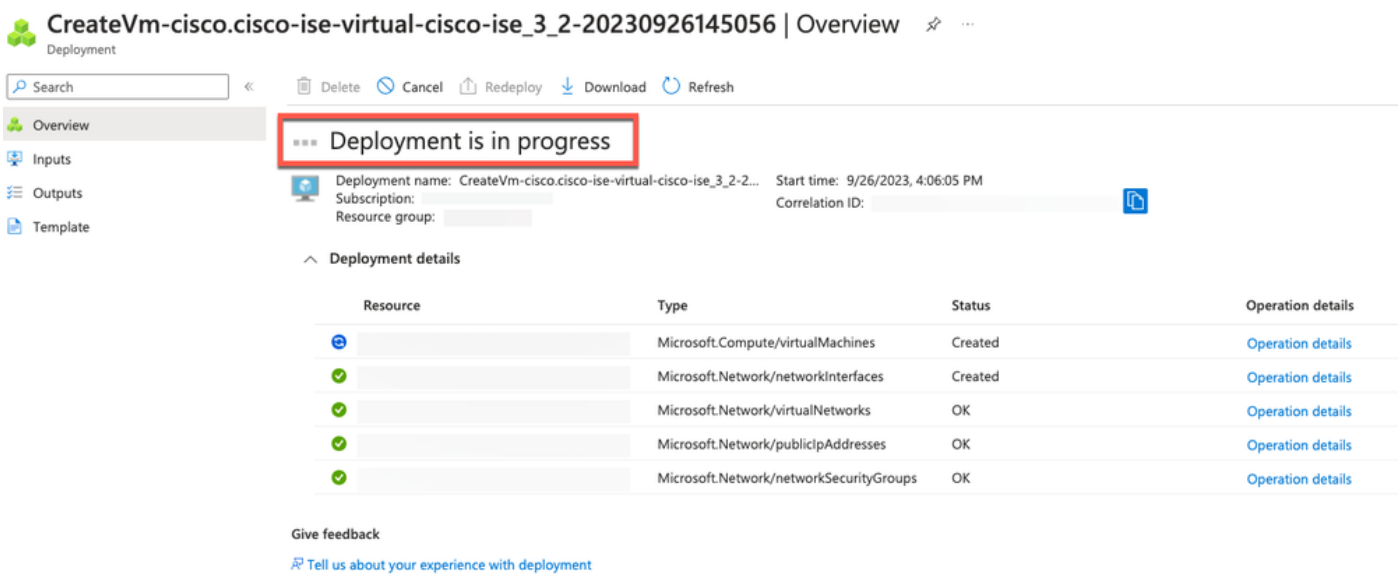


15. Cliquez sur Next : Vérifier + Créer.



16. Vérifiez les informations que vous avez fournies jusqu'à présent et cliquez sur Créer. La fenêtre Déploiement en cours s'affiche. Il faut environ 30 minutes pour que l'instance Cisco ISE soit créée et disponible. L'instance de machine virtuelle Cisco ISE est affichée dans la fenêtre Virtual Machines (utilisez le champ de recherche principal pour trouver la fenêtre).





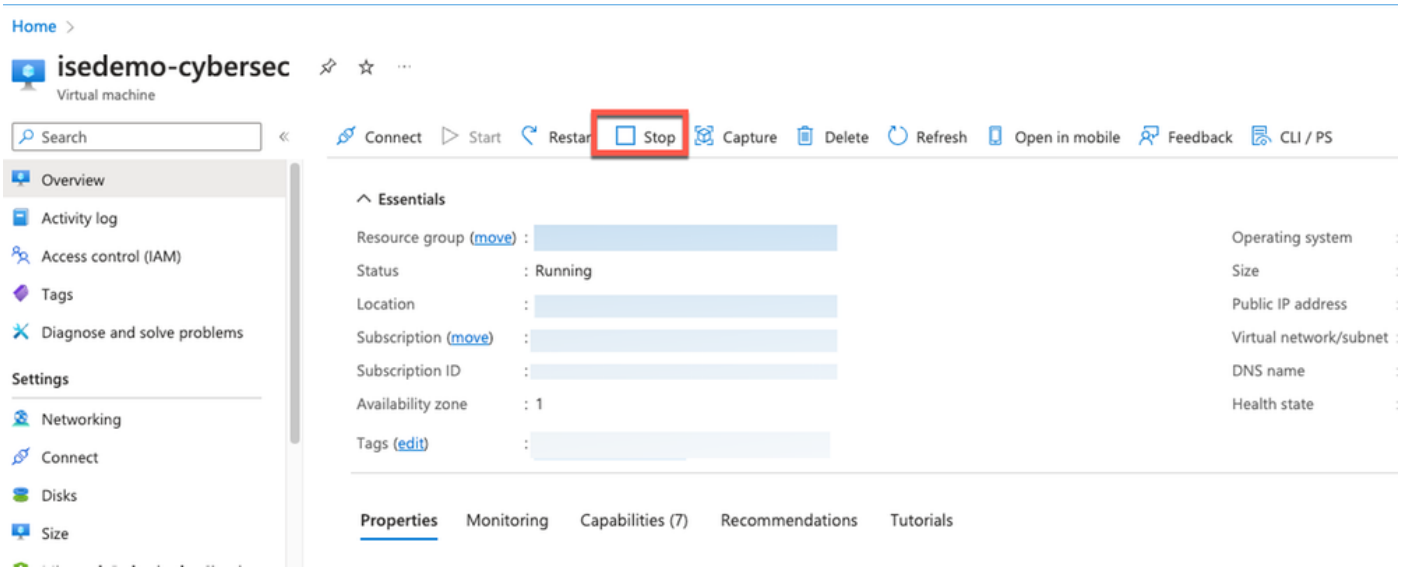
Que faire ensuite ?

En raison d'un paramètre Microsoft Azure par défaut, la machine virtuelle Cisco ISE que vous avez créée est configurée avec une taille de disque de 300 Go uniquement. Les noeuds Cisco ISE nécessitent généralement une taille de disque supérieure à 300 Go. Vous pouvez voir l'alarme Mémoire virtuelle insuffisante lorsque vous lancez Cisco ISE pour la première fois à partir de Microsoft Azure.

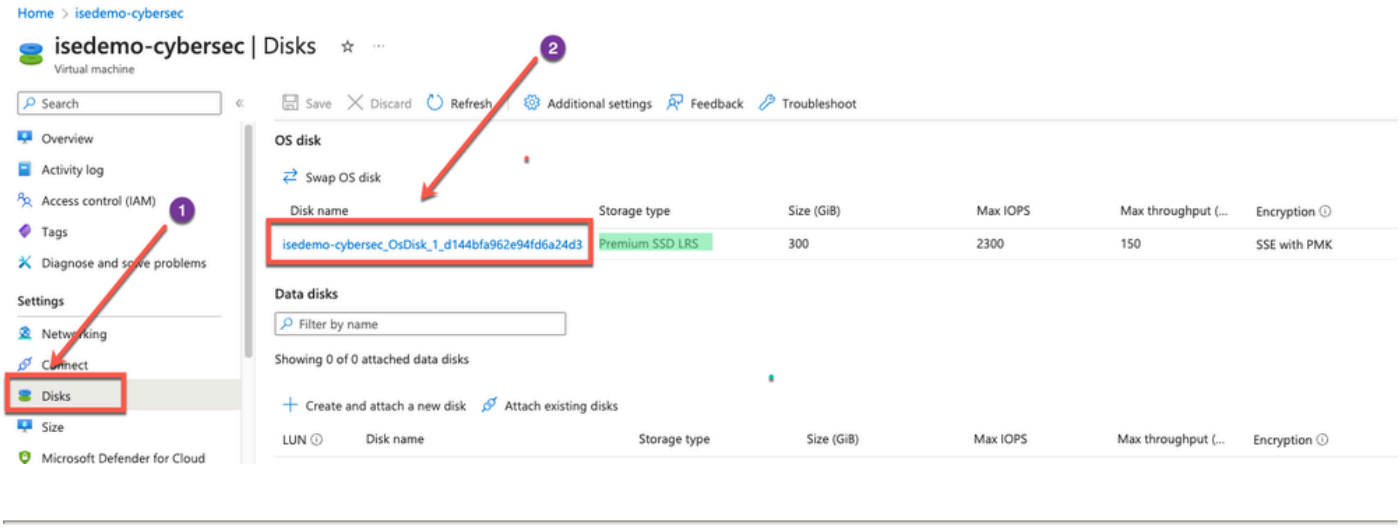
Une fois la création de la machine virtuelle Cisco ISE terminée, connectez-vous au portail d'administration Cisco ISE pour vérifier que Cisco ISE est configuré. Ensuite, dans le portail Microsoft Azure, effectuez les étapes suivantes dans la fenêtre Machines virtuelles pour modifier la taille du disque :

---

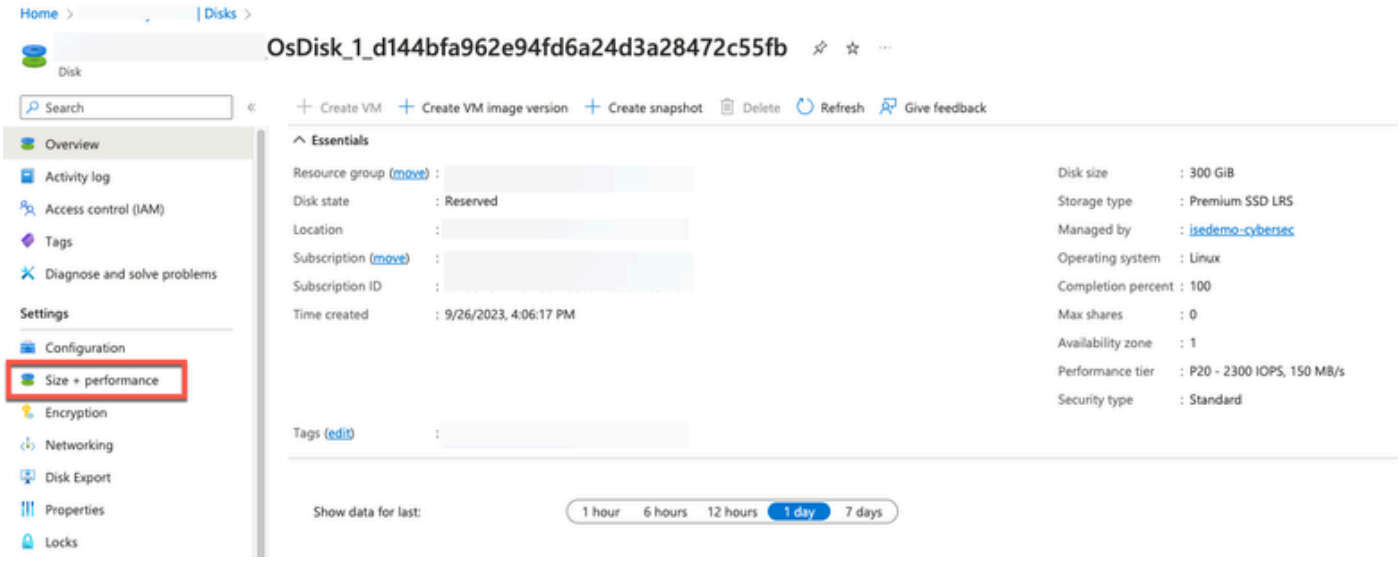
1. Arrêtez l'instance Cisco ISE.



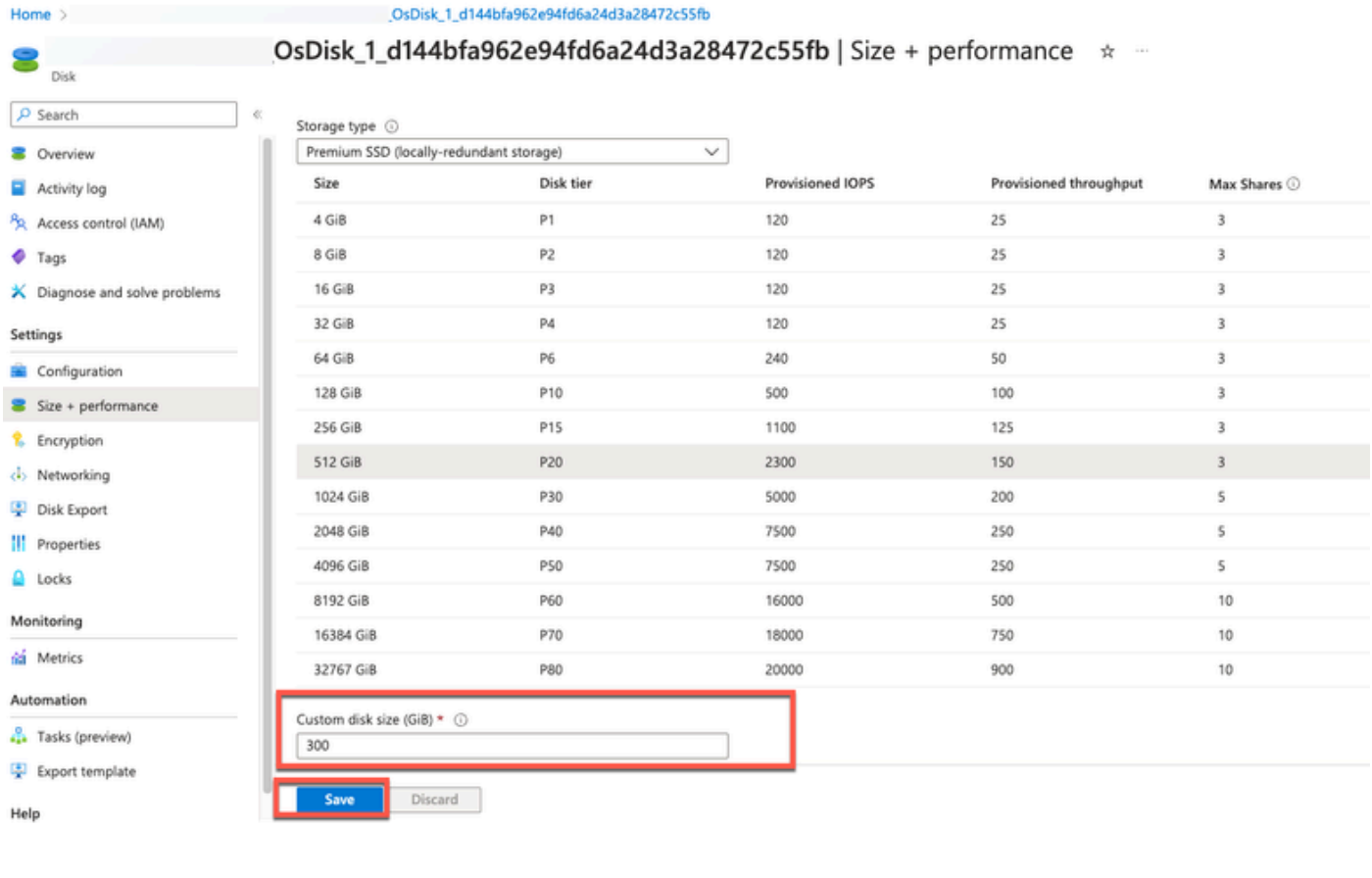
2. Cliquez sur Disk dans le volet de gauche et cliquez sur le disque que vous utilisez avec Cisco ISE.



3. Cliquez sur Taille + Performance dans le volet de gauche.



4. Dans le champ Taille de disque personnalisée, entrez la taille de disque souhaitée dans la base de données géographique.



Tâches post-installation

Pour obtenir des informations sur les tâches de post-installation que vous devez effectuer après la création d'une instance Cisco ISE, reportez-vous aux chapitres « Vérification de l'installation et tâches de post-installation » du Guide d'installation de Cisco ISE pour votre version de Cisco ISE.

Récupération et réinitialisation de mot de passe sur le cloud Azure

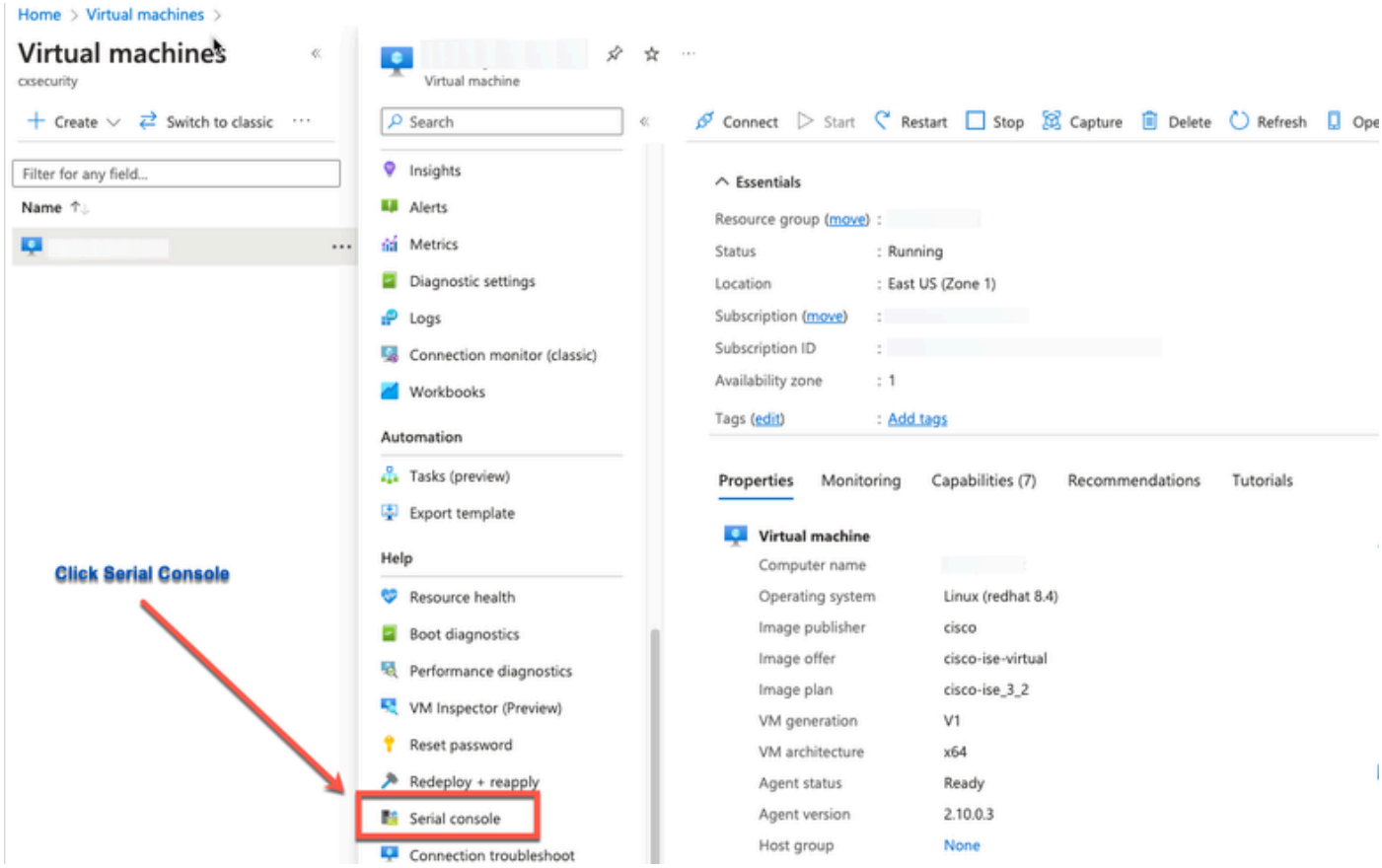
Effectuez les tâches qui vous aident à réinitialiser ou à récupérer votre mot de passe de machine virtuelle Cisco ISE. Choisissez les tâches dont vous avez besoin et suivez les étapes détaillées.

Réinitialiser le mot de passe de l'interface utilisateur Cisco ISE via la console série

1. Connectez-vous au cloud Azure et sélectionnez le groupe de ressources qui contient votre machine virtuelle Cisco ISE.

2. Dans la liste des ressources, cliquez sur l'instance Cisco ISE pour laquelle vous souhaitez réinitialiser le mot de passe.

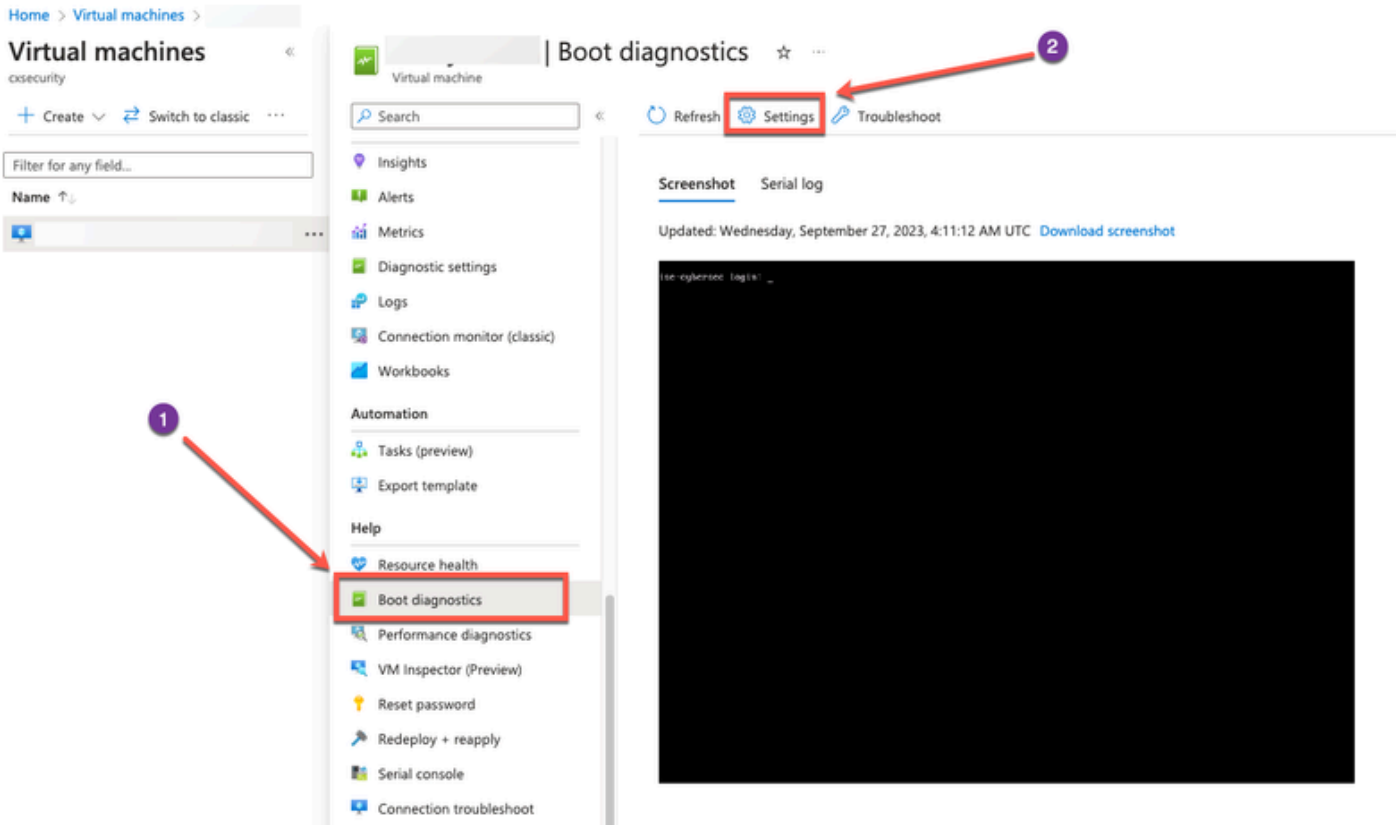
3. Dans le menu de gauche, dans la section Support + Troubleshooting, cliquez sur Serial Console.



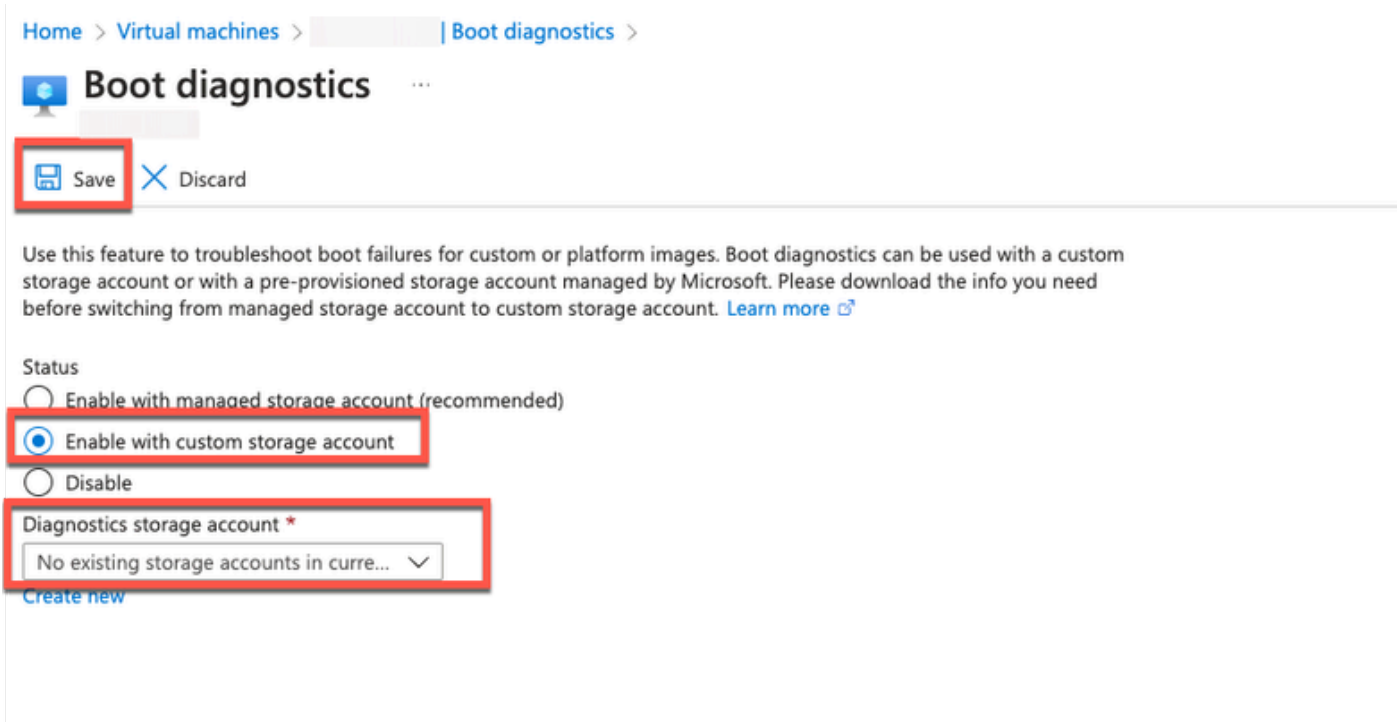
---

4. Si un message d'erreur s'affiche, vous devez activer les diagnostics de démarrage en procédant comme suit :

- Dans le menu de gauche, cliquez sur Boot Diagnostics.



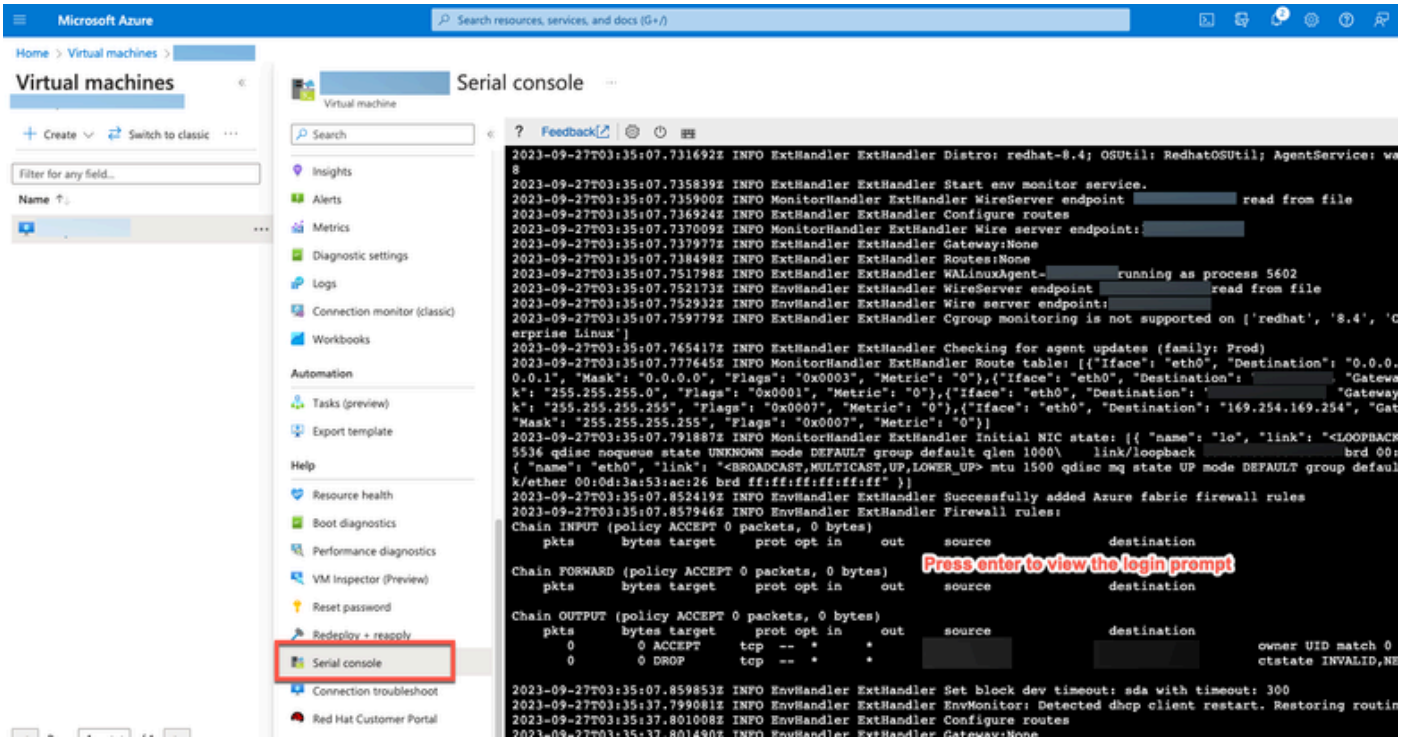
- Cliquez sur Activer avec un compte de stockage personnalisé. Cliquez sur Save.



---

5. Dans le menu de gauche, dans la section Support + Troubleshooting, cliquez sur Serial

Console. Azure Cloud Shell s'affiche dans une nouvelle fenêtre. Si l'écran est noir/vide, appuyez sur Entrée pour afficher l'invite de connexion.



---

6. Connectez-vous à la console série. Pour vous connecter à la console série, vous devez utiliser le mot de passe d'origine configuré lors de l'installation de l'instance.

---

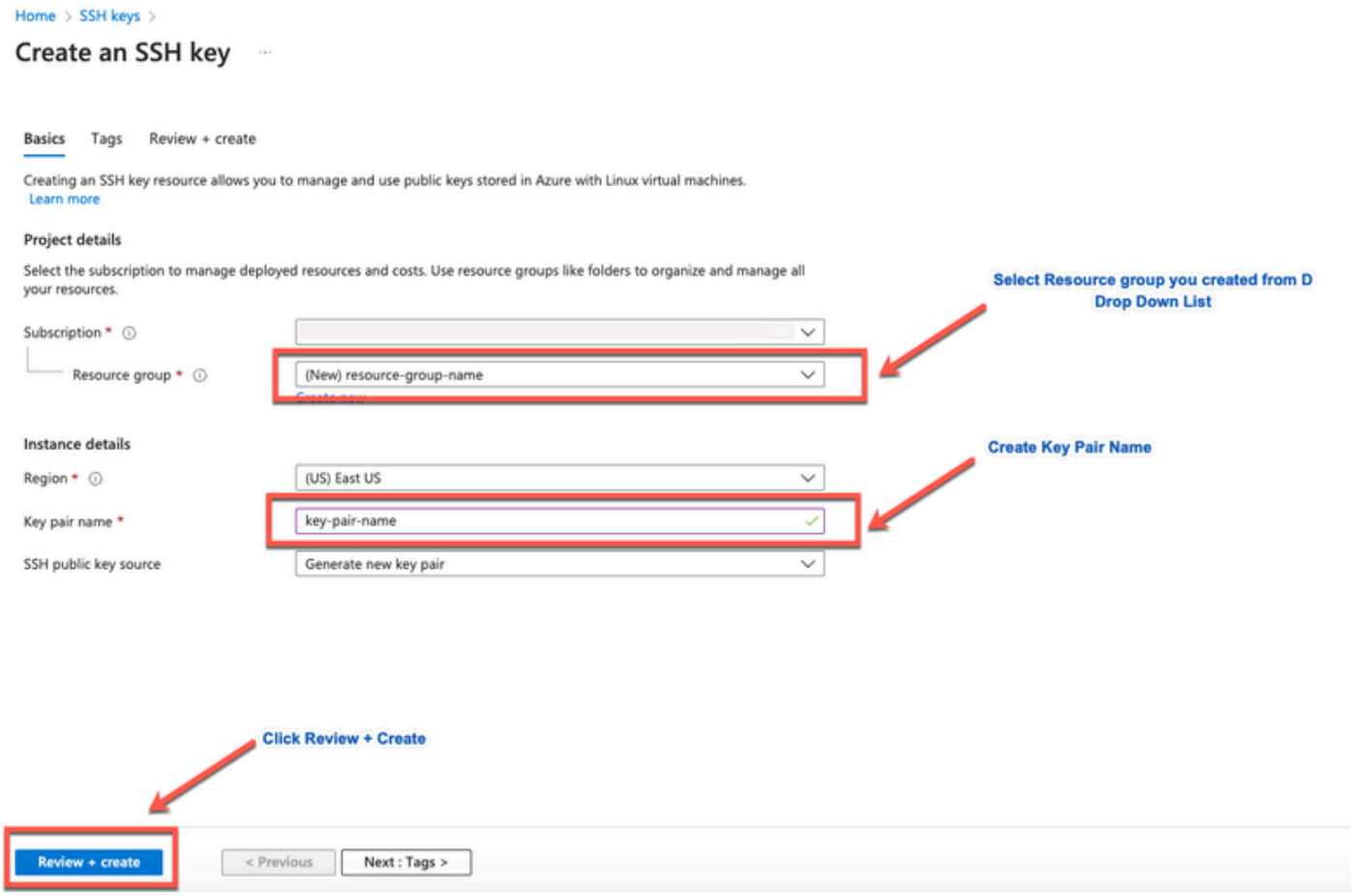
7. Exécutez la commande application reset-passwd ise iseadmin pour configurer un nouveau mot de passe GUI pour le compte iseadmin.

Créer une nouvelle paire de clés publiques pour l'accès SSH

Cette tâche vous permet d'ajouter des paires de clés supplémentaires à un référentiel. La paire de clés existante créée lors de la configuration de l'instance Cisco ISE n'est pas remplacée par la nouvelle clé publique que vous avez créée.

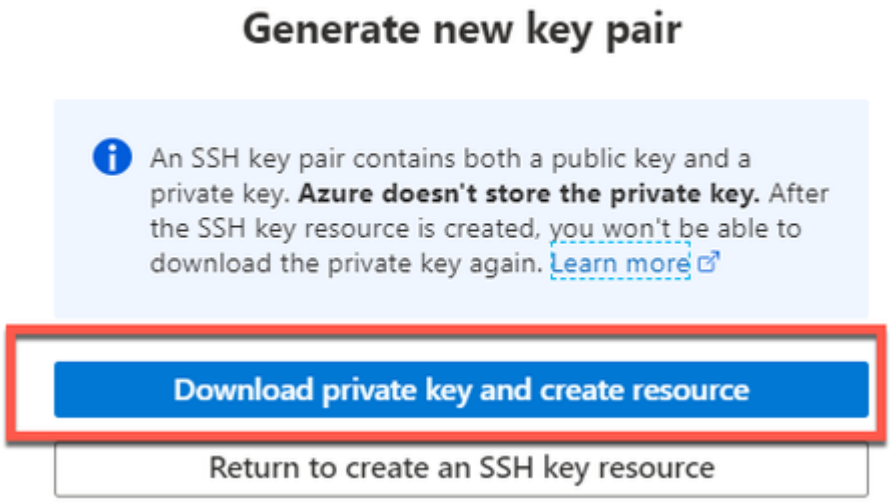
---

1. Créez une nouvelle clé publique dans le cloud Azure.



---

2. Vous recevez une fenêtre contextuelle pour choisir Télécharger la clé privée et Créer une ressource qui télécharge la clé SSH en tant que fichier .pem.



---

3. Pour créer un nouveau référentiel dans lequel enregistrer la clé publique, reportez-vous à la

documentation Azure Repos. Si vous disposez déjà d'un référentiel accessible via l'interface de ligne de commande, passez à l'étape 3.

---

4. Pour importer la nouvelle clé publique, exécutez la commande crypto key import <public key filename> repository <nom du référentiel>.

---

5. Une fois l'importation terminée, vous pouvez vous connecter à Cisco ISE via SSH à l'aide de la nouvelle clé publique.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.