

Réinitialiser les clés SSH pour Cisco ISE sur les machines virtuelles Azure

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment réinitialiser les clés SSH pour les machines virtuelles Azure ISE.

Conditions préalables

- Connaissances ISE de base
- Accès à la console ISE via Microsoft Azure
- Accès à l'interface ISE
- Privilèges pour créer de nouvelles paires de clés dans Microsoft Azure

Exigences

- Noeud Cisco ISE

Composants utilisés

- Cisco ISE 3.3

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.

Configurer

1. Dans Microsoft Azure, recherchez le service de clés SSH.



2. Cliquez sur Create pour créer une nouvelle clé SSH. Sélectionnez votre abonnement et votre groupe de ressources. Spécifiez un nom personnalisé pour votre nouvelle clé SSH. Pour le champ source de clé publique SSH, sélectionnez l'option pour Générer une nouvelle paire de clés et pour Type de clé SSH sélectionnez Format SSH RSA. Enfin, cliquez sur Vérifier + Créer pour valider et créer la clé.

Microsoft Azure

Search resources, services, and docs (G+/I)

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 *
[Create new](#)

Instance details

Region

Key pair name *

SSH public key source

SSH Key Type

☒ RSA SSH Format

☐ Ed25519 SSH Format

i Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.

Review + create < Previous Next : Tags >

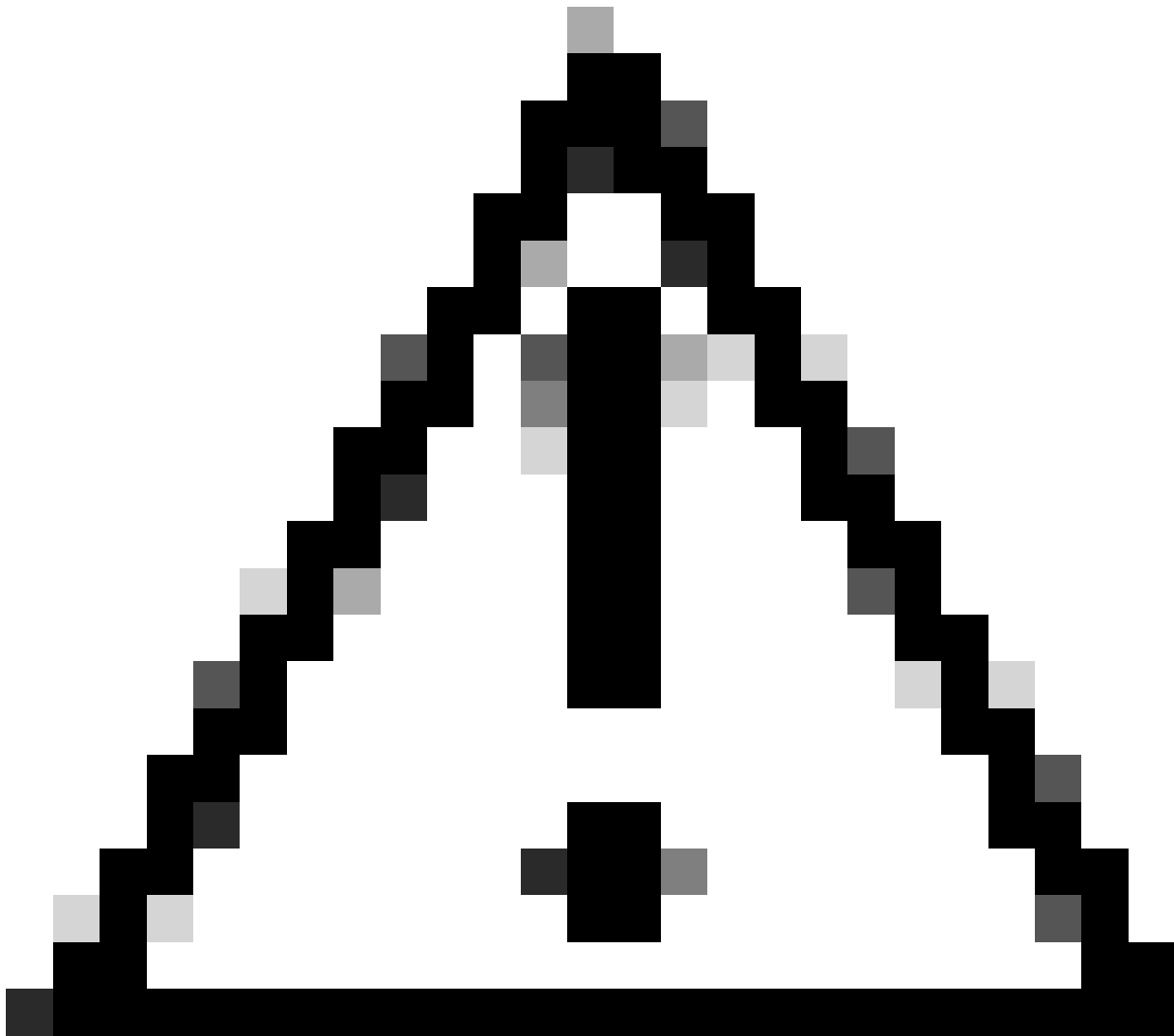
3. Lorsque la clé est créée, une nouvelle fenêtre s'affiche. Cliquez sur Télécharger la clé privée et créer une ressource.

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](#)



Mise en garde : Il est important de conserver cette clé privée en toute sécurité, car c'est le seul moment où Azure vous permet de télécharger cette clé privée. Azure ne stocke pas cette clé privée et ne peut pas être téléchargé ailleurs.

-
4. À présent, revenez au service SSH Keys et recherchez la clé que vous venez de créer, puis cliquez dessus pour la voir.

SSH keys



List all SSH keys using ARG.

How many SSH keys do I have in total?

Identify

[+ Create](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Open query](#) | [Assign tags](#)

[You are viewing a new version of Browse experience. Click here to access the old experience.](#)

[isnewkey](#) [X](#)

Subscription equals all

Resource Group equals all [X](#)

Location



Name ↑

Type



[ISEnewKey](#)



SSH key

5. Dans la vue d'ensemble de la clé, vous voyez la clé publique. Copiez ce texte et collez-le dans un éditeur de texte afin de pouvoir l'enregistrer en tant que fichier local avec l'extension .pem. Dans ce guide, le fichier est enregistré sous le nom public.pem .

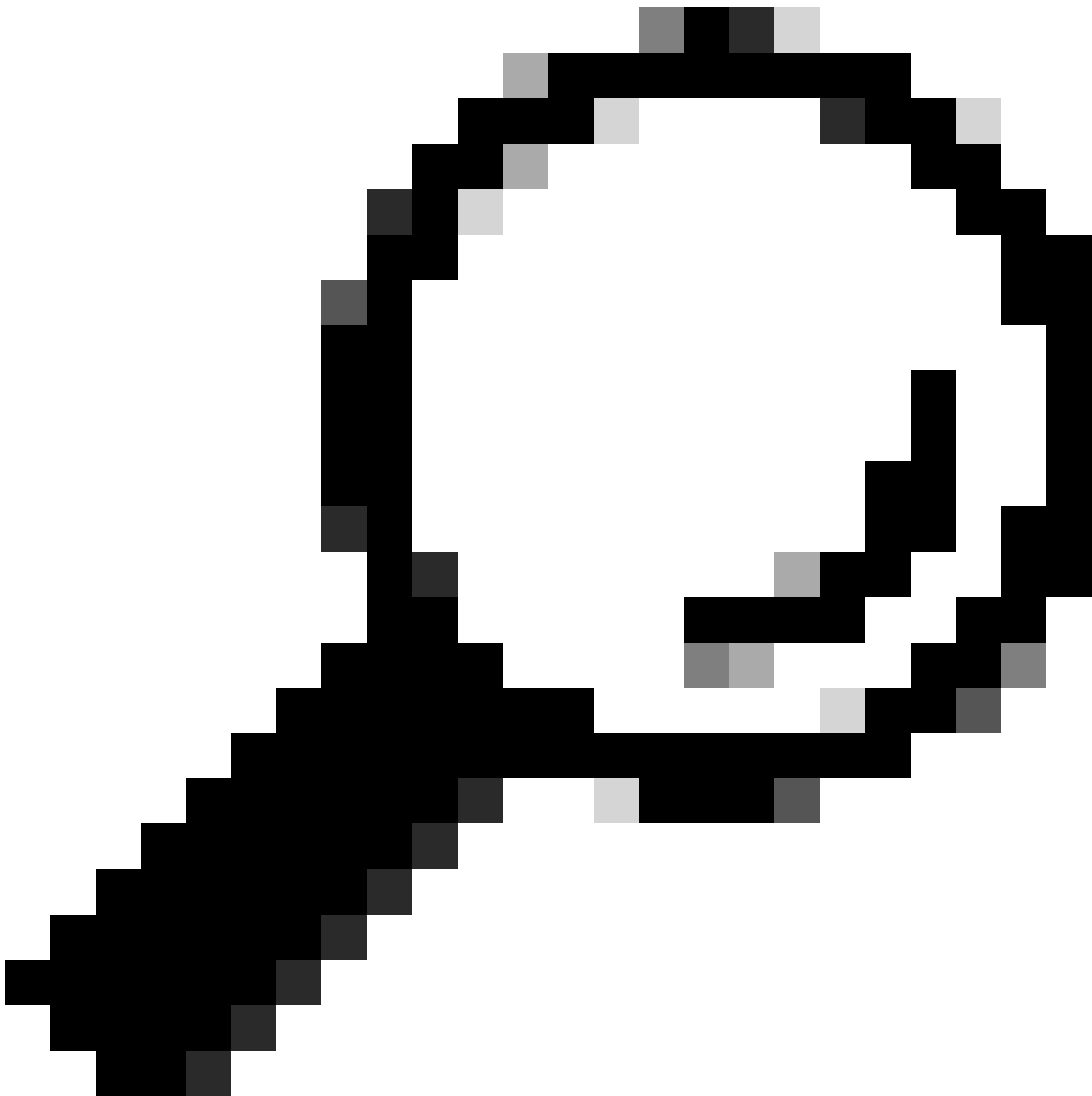
Public key

ssh-rsa

```
AAAA83NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrzLUV41tSEcOjdC2k4tyju1n/Xxs8/w7T2T33QDE6MjI7u+v8DI2HjWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF
4lupl8amyjFpqdPHJbOu90GkQSFICEbYVUJYpzuSdNYomxlB5J+tuSVQFscn3ht5SbXGLDEUTSPcntXeHdq+Zc/CPSoVwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1cOxyIglhRC
AnQ0wyJy3DhN+PJWZMqr8NqADF5SeGKXr1EgSgSlw3+fbW7gl+eZ8ZhwzX8EpRrHpKCTbjh9gtERXfKPt2Ik/HRctVU0xXY49noenL+QLCGUvN+3pD2BL3jsK5RCR2D5/9aH
14h0SqWRW/XknQHxLqXPXrWH5tE566Y9Y80J375HcyDtAjDu4S2LURZA3u+2Q75UXaQuquyXt0x9PSP1bm/dYQwY9dn+DKXWdlh2AFhUnlPU8M2A4/jj55Ucu
Wi0= generated-by-azure
```

Copy to clipboard



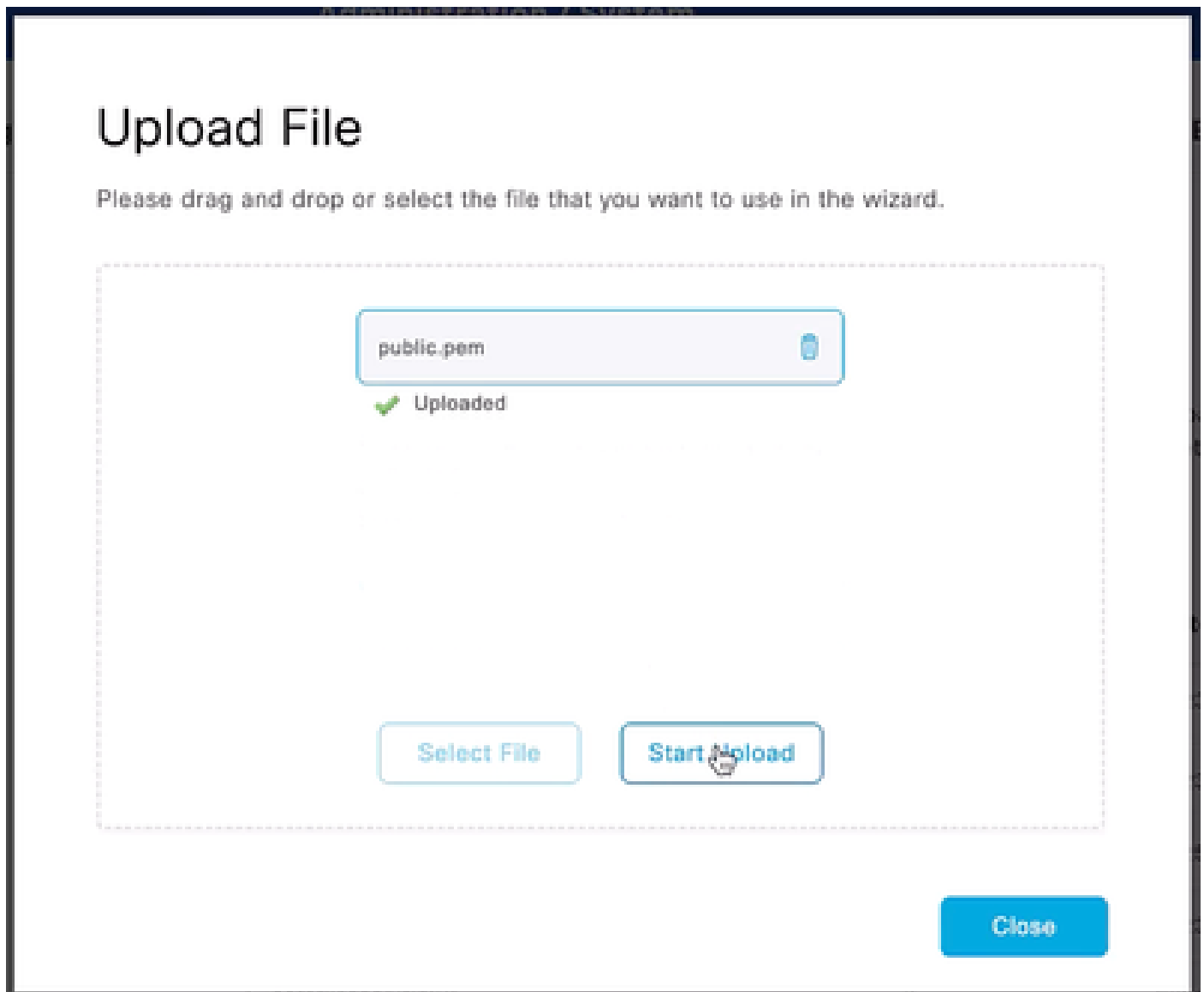


Conseil : Vous pouvez cliquer sur le bouton Copier dans le Presse-papiers pour copier la chaîne de clé publique.

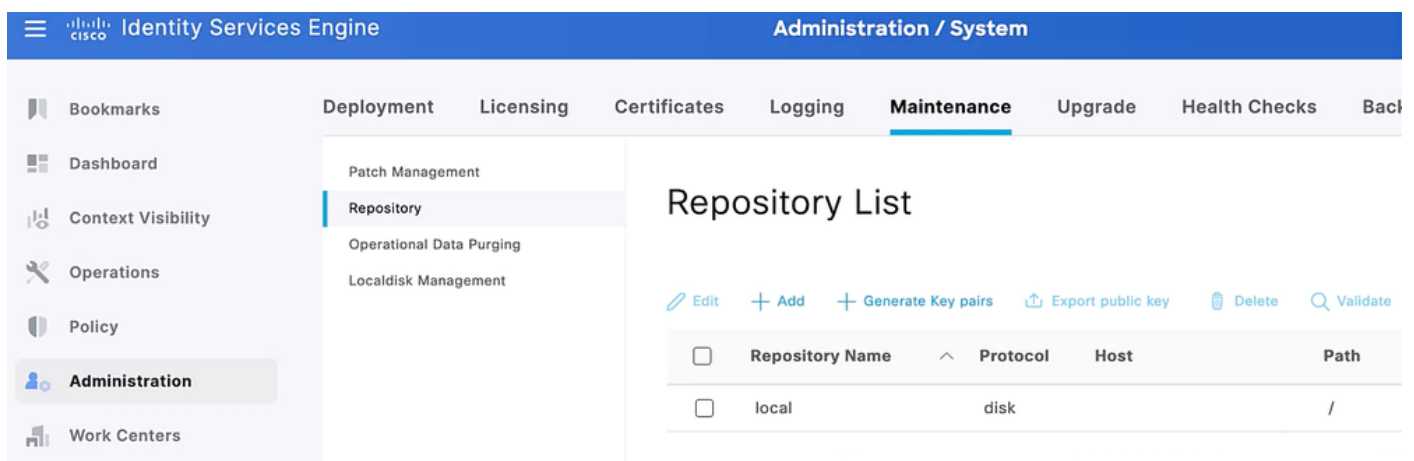
```
public.pem
1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrzLUV41tSEc0jdC2k4tyju1n/Xxs8/
w7T2T33QDE6MjJ7u+v8DI2HhjWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF4IupI8amyjFpqdPHJb0u90GkQSFLEbYVUJ
YpzUSdNYomxLB5J+tuSVQFscn3ht5SbXGLDEUTSPcntXeHdq+Zc/CPS0vwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1c0xy
IgkIlhRCAnQ0wyJy3DhN+PJWZMqrBNqADFS5eGKXr1EgSgSlw3+fbW7gl+eZ8ZhWzX8EpRrHpKCtbJh9gtERXfPt2Ik/
HRctVU0xXY49noenL+QLCGUvN+3pD2BL3jsK5RCR2D5/9aHUQ0fPkTojh4h0SqWRW/
XknQHkxLqXPXrWH5tE566Y9YB0J375HcyDtAjDu4S2LJRZA3u+2Q75UXaQuquyXt0x9PSP1bm/
dYQwY9dn+DKXWdLh2AFhUnlPU8M2A4/jJ55UcuvUWA+jWYWi0= generated-by-azure
```

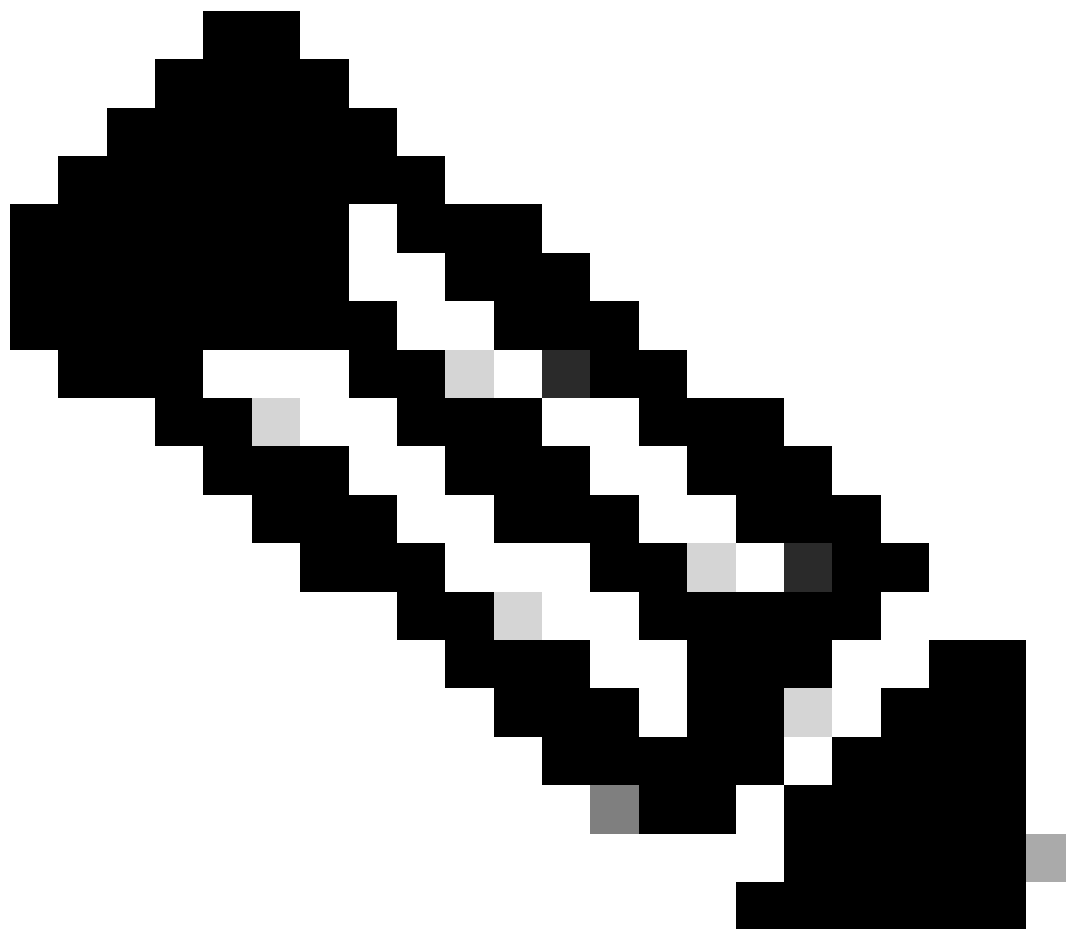
6. Téléchargez cette clé publique sur le disque local ISE. Pour ce faire, accédez à ISE > Administration > System > Maintenance > Local Disk Management. Cliquez sur votre nom d'hôte ISE, puis sur Télécharger et cliquez sur Sélectionner un fichier et recherchez et

sélectionnez la clé publique sur votre ordinateur local. Enfin, cliquez sur Start Upload .



7. Créez un référentiel qui pointe vers le disque local ISE afin que vous puissiez l'utiliser pour installer la clé publique. Dans cet exemple, notre référentiel est appelé local.

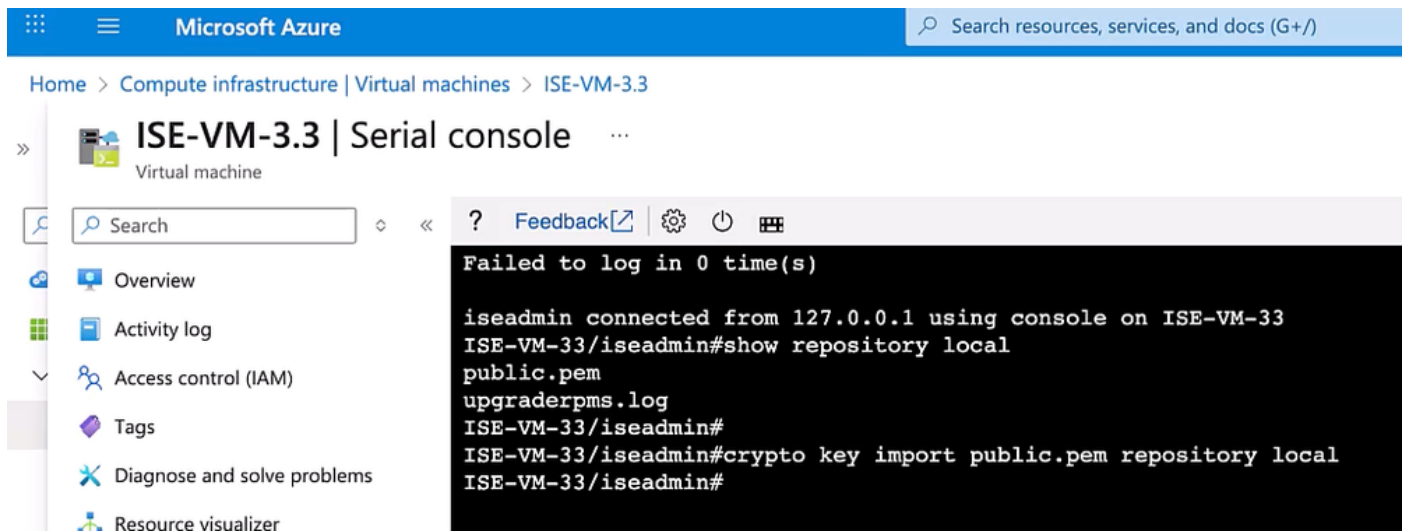




Remarque : Si vous le souhaitez, vous pouvez télécharger le fichier de clé publique vers un autre référentiel déjà créé sur ISE. Il n'est pas nécessaire qu'il s'agisse d'un disque local.

8. Connectez-vous à la console série ISE à partir d'Azure en utilisant le nom d'utilisateur pour lequel vous souhaitez réinitialiser la clé SSH.

9. Vérifiez que la clé publique (fichier .pem) se trouve correctement dans le référentiel et installez la clé à l'aide de la commande `crypto key import { nom du fichier de clé publique } référentiel { nom du référentiel }`.



Vérifier

Pour établir une connexion SSH vers ISE à l'aide des nouvelles paires de clés, vous devez utiliser la clé privée comme identification lors de la connexion.

1. Attribuez les autorisations appropriées à la clé privée (celle téléchargée à l'étape 3)

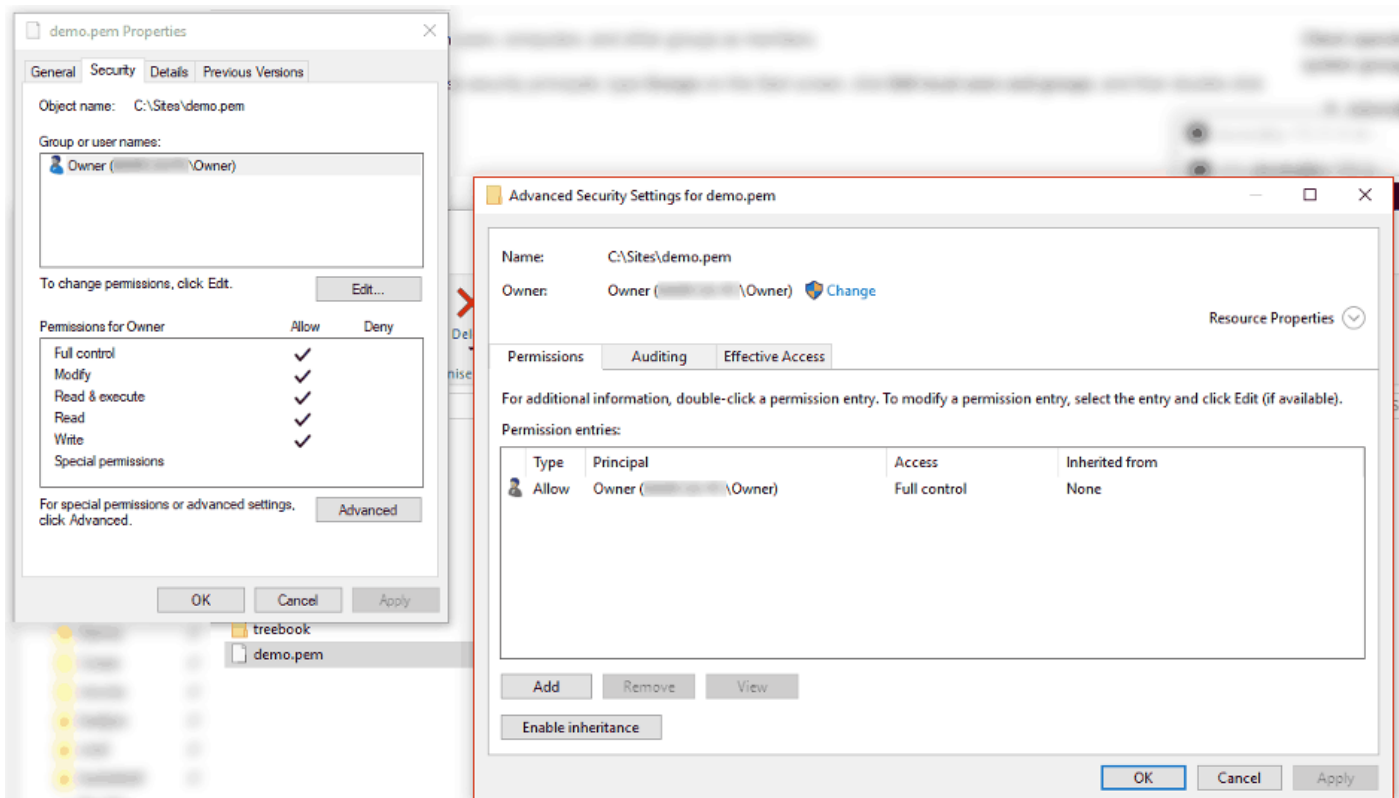
À partir du terminal macOS :

```
chmod 600 { fichier de clé privée }
```

Depuis Windows :

Recherchez le fichier dans l'Explorateur Windows, cliquez dessus avec le bouton droit de la souris, puis sélectionnez Propriétés. Accédez à l'onglet Security et cliquez sur Advanced.

Remplacez le propriétaire par vous, désactivez l'héritage et supprimez toutes les autorisations. Accordez-vous ensuite le contrôle total et enregistrez les autorisations.



2. Envoyez une requête SSH vers ISE en utilisant la nouvelle clé privée, le nom d'utilisateur ISE et l'adresse IP ISE ou le nom de domaine complet.

À partir du terminal macOS :

```
ssh -I { fichier de clé privée } { username }@{ IP ISE ou FQDN }
```

À partir de Windows CMD :

```
ssh -i "{ fichier de clé privée }" { username }@{ IP ISE ou FQDN }
```

Dépannage

- Veillez à copier le texte complet du fichier de clé publique dans votre fichier .pem.
- Assurez-vous que le référentiel contient le fichier de clé publique.
- Si la commande crypto ne parvient pas à installer la clé publique sur ISE, soulevez un ticket auprès du TAC Cisco afin que la clé puisse être installée manuellement à partir de la racine. L'erreur courante pour cette opération est « %Error : Impossible de mettre à jour le fichier de clé autorisé. »

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.