

SSH-sleutels opnieuw instellen voor Cisco ISE op Azure VM's

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u SSH-sleutels voor Azure ISE VM's kunt resetten.

Voorwaarden

- Basiskennis ISE
- Toegang tot ISE Console via Microsoft Azure
- Toegang tot de ISE GUI
- Privileges voor het maken van nieuwe sleutelparen in Microsoft Azure

Vereisten

- Cisco ISE-node

Gebruikte componenten

- Cisco ISE 3.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

1. Zoek in Microsoft Azure naar de service SSH-sleutels.



2. Klik op Maken om een nieuwe SSH-sleutel te maken. Selecteer uw abonnement en uw bronnengroep. Geef een aangepaste naam op voor de nieuwe SSH-sleutel. Selecteer in het bronveld van de openbare SSH-sleutel de optie Nieuw sleutelpaar genereren en selecteer voor SSH-sleuteltype de optie RSA SSH-indeling. Klik ten slotte op Bekijken + Maken om de sleutel te valideren en te maken.

A screenshot of the 'Create an SSH key' page in the Azure portal. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there is a breadcrumb trail: 'Home > SSH keys >'. The main heading is 'Create an SSH key'. There are three tabs: 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is selected. The page contains several sections: 'Project details' with a description and a 'Learn more' link; 'Subscription' and 'Resource group' dropdowns; 'Instance details' with 'Region' and 'Key pair name' dropdowns; 'SSH public key source' dropdown; and 'SSH Key Type' with radio buttons for 'RSA SSH Format' and 'Ed25519 SSH Format'. A note below the radio buttons states: '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.' At the bottom, there are three buttons: 'Review + create', '< Previous', and 'Next : Tags >'. A mouse cursor is hovering over the 'Review + create' button.

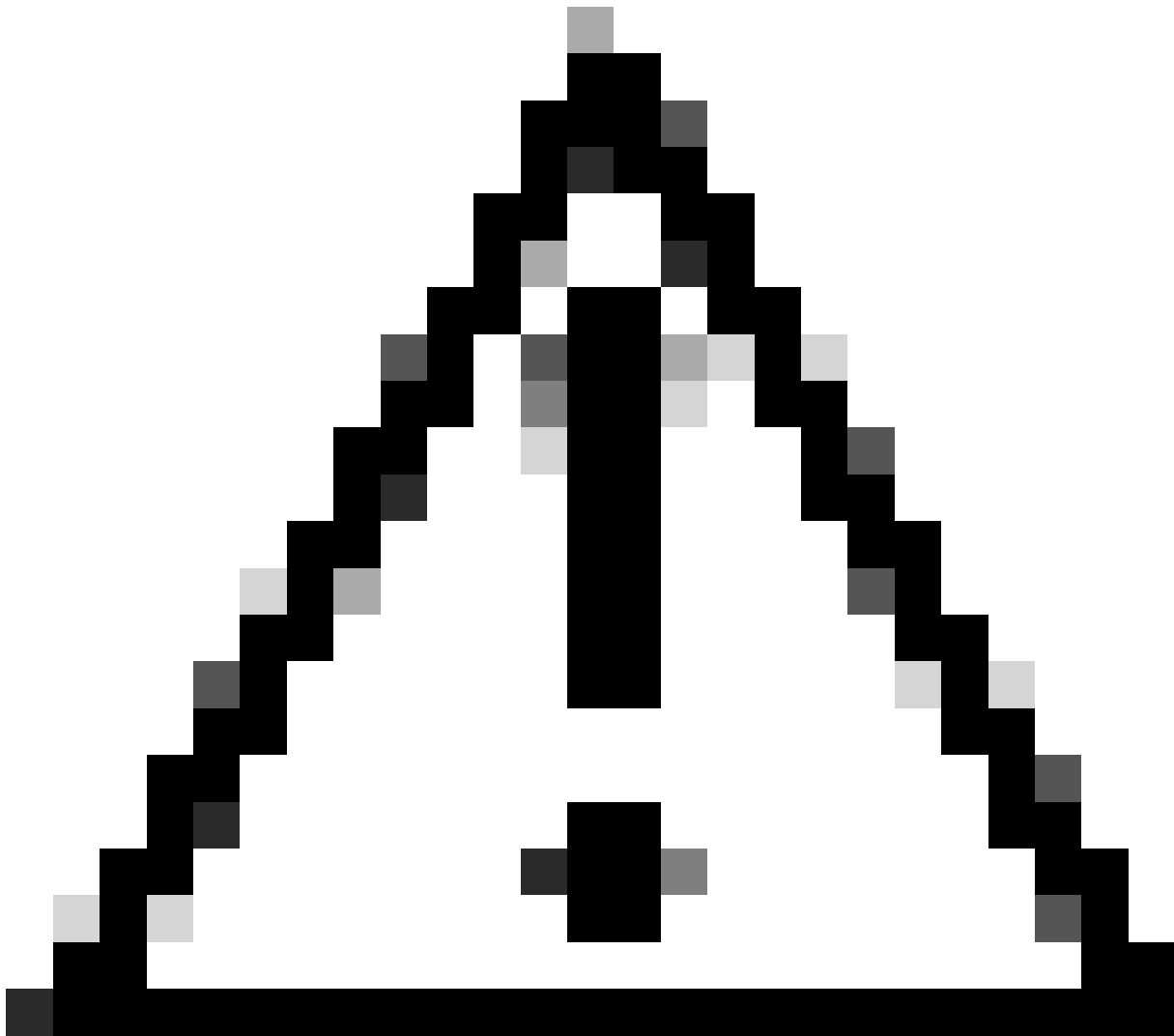
3. Wanneer de sleutel is gemaakt, verschijnt er een nieuw venster. Klik op Privésleutel downloaden en bron maken.

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](#)



Let op: Het is belangrijk om deze privésleutel veilig te bewaren, omdat dit het enige moment is waarop Azure u toestaat deze privésleutel te downloaden. Azure slaat deze privésleutel niet op en kan nergens anders worden gedownload.

-
4. Navigeer nu terug naar de SSH Keys-service en zoek naar uw nieuw gemaakte sleutel en klik erop om het overzicht te zien.

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.](#)

isenewkey

Subscription equals all

Resource Group equals all

Location



Name ↑

Type



[ISEnewKey](#)



SSH key

5. Op het overzicht van de sleutel ziet u de Public key. Kopieer deze tekst en plak deze op een teksteditor, zodat u deze kunt opslaan als een lokaal bestand met de extensie .pem. In deze handleiding wordt het bestand opgeslagen als public.pem.

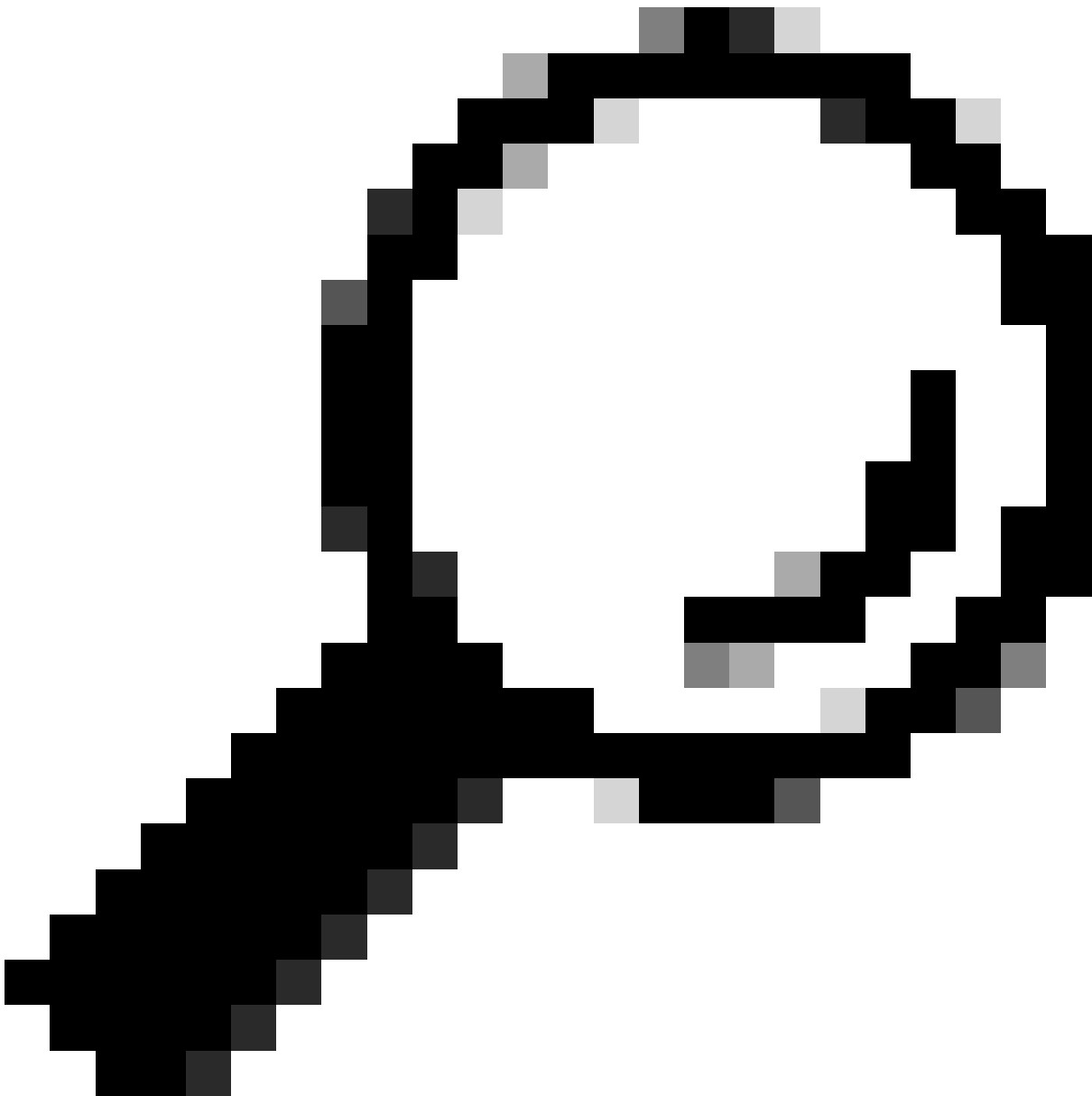
Public key

ssh-rsa

AAAA83NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrzLUV41tSEcOjdC2k4tyju1n/Xxs8/w7T2T33QDE6MjI7u+v8DI2HjWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF4lupl8amyjFpqdPHJbOu90GkQSFICEbYVUJYpzuSdNYomxlB5J+tuSVQFscn3ht5SbXGLDEUTSPcntXeHdq+Zc/CPSoVwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1cOxyIglhRCAnQ0wyJy3DhN+PJWZMqr8NqADF5SeGKXr1EgSgSlw3+fbW7gl+eZ8ZhwzX8EpRrHpKCbJh9gtERXfKPt2Ik/HRctVU0xXY49noenL+QLCGUvN+3pD2BL3jsK5RCR2D5/9aH14h0SqWRW/XknQHxLqXPXrWH5tE566Y9Y80J375HcyDtAjDu4S2LURZA3u+2Q75UXaQuquyXt0x9PSP1bm/dYQwY9dn+DKXWdlh2AFhUnlPU8M2A4/jj55UcuWi0= generated-by-azure

Copy to clipboard



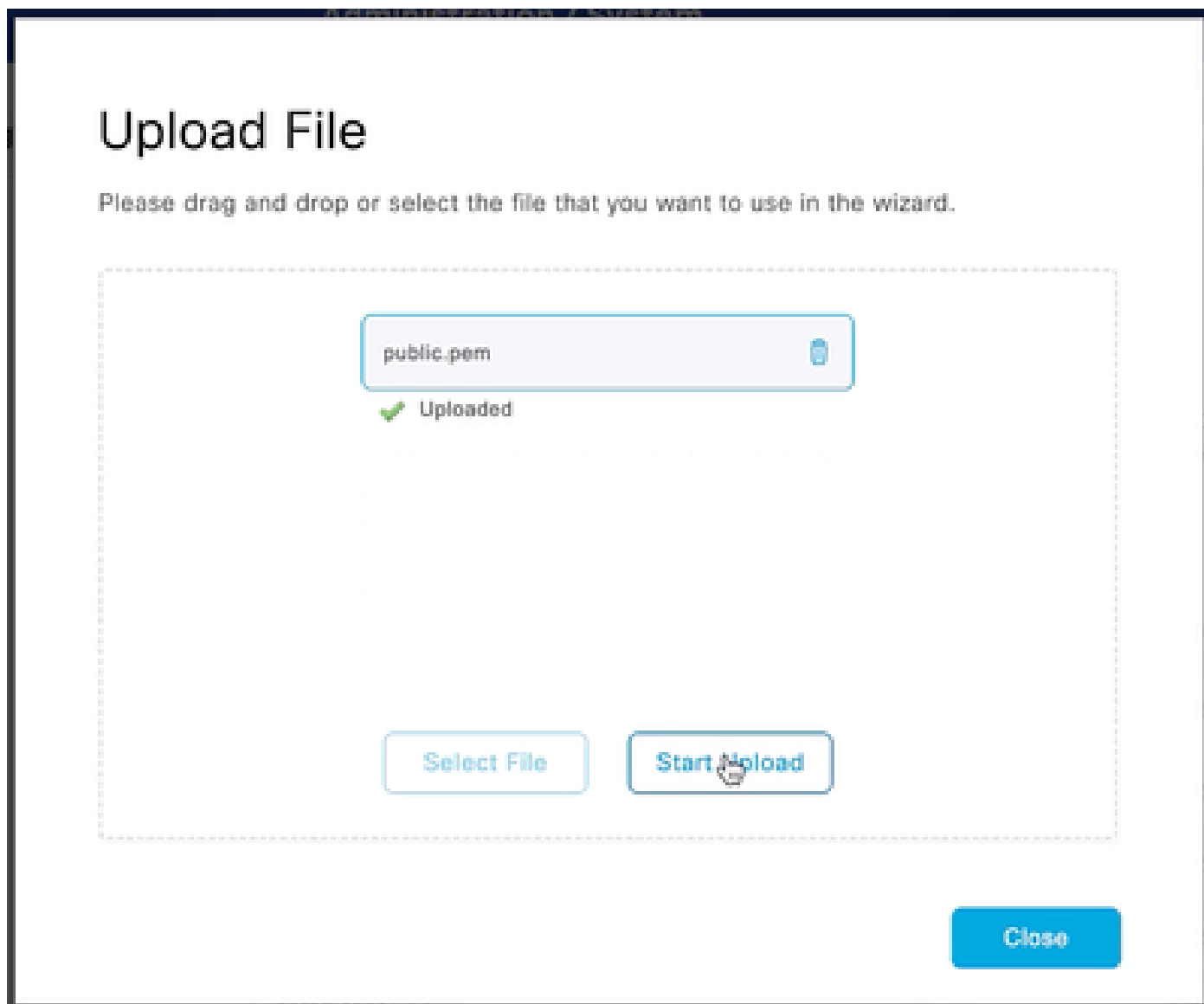


Tip: U kunt op de knop Kopiëren naar klembord klikken om de openbare sleutelreeks te kopiëren.

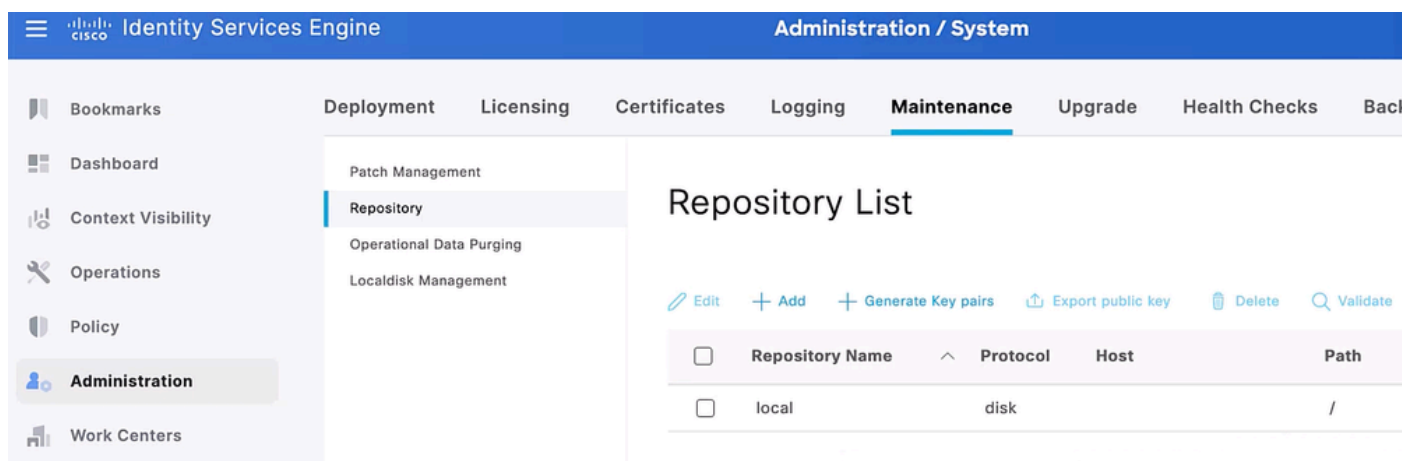
```
public.pem
1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrzLUV41tSEc0jdC2k4tyju1n/Xxs8/
w7T2T33QDE6MjJ7u+v8DI2HhjWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF4IupI8amyjFpqdPHJb0u90GkQSFLEbYVUJ
YpzUSdNYomxLB5J+tuSVQFscn3ht5SbXGLDEUTSPcntXeHdq+Zc/CPS0vwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1c0xy
IgakIhRCAnQ0wyJy3DhN+PJWZMqrBNqADFS5eGKXr1EgSgSlw3+fbW7gl+eZ8ZhwxX8EpRrHpKCtbJh9gtERXfPt2Ik/
HRctVU0xXY49noenL+QLCGUvN+3pD2BL3jsK5RCR2D5/9aHUQ0fPkTojh4h0SqWRW/
XknQHkxLqXPXrWH5tE566Y9YB0J375HcyDtAjDu4S2LJRZA3u+2Q75UXaQuquyXt0x9PSP1bm/
dYQwY9dn+DKXWdLh2AFhUnlPU8M2A4/jJ55UcuvUWA+jWYWi0= generated-by-azure
```

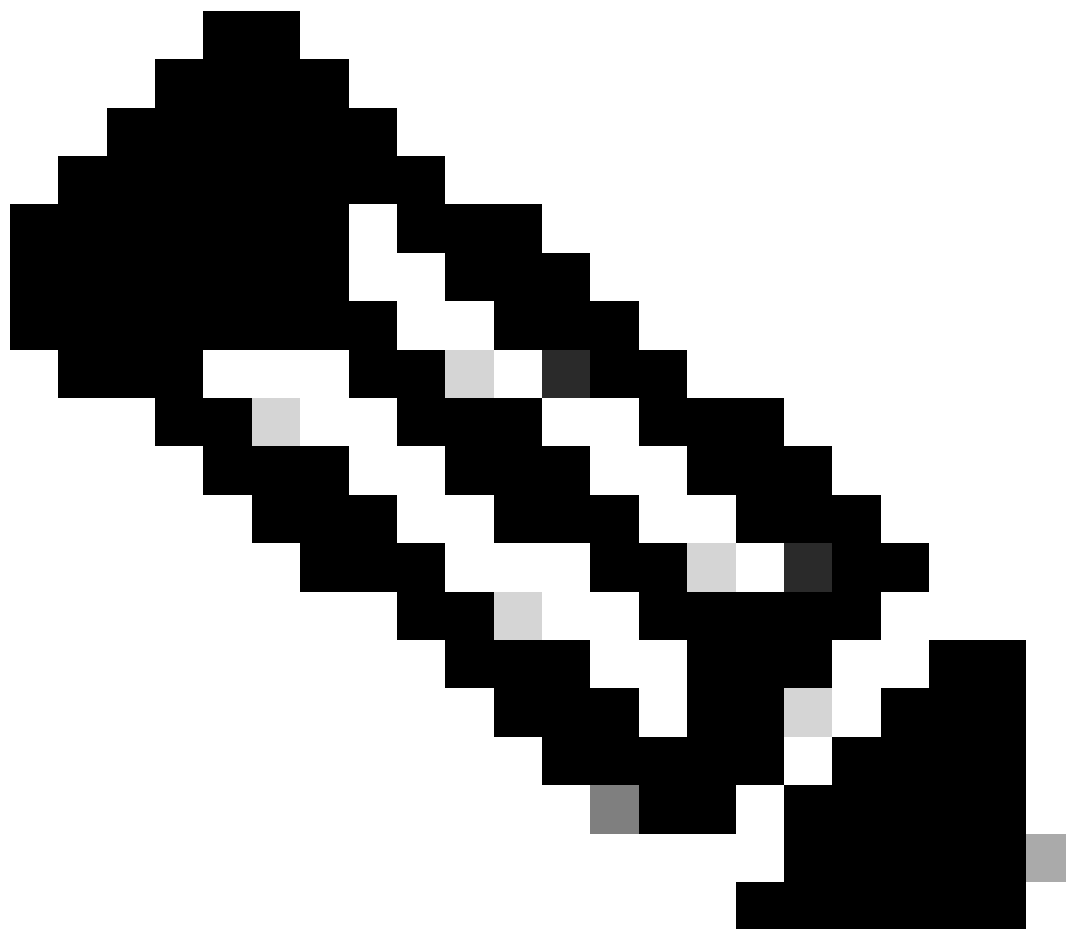
6. Upload deze publieke sleutel naar ISE localdisk. Ga hiervoor naar ISE > Beheer > Systeem > Onderhoud > Lokaal schijfbeheer. Klik op de ISE-hostnaam, klik vervolgens op Uploaden en klik vervolgens op Bestand selecteren en zoek de openbare sleutel op uw lokale

computer. Klik ten slotte op Uploaden starten.



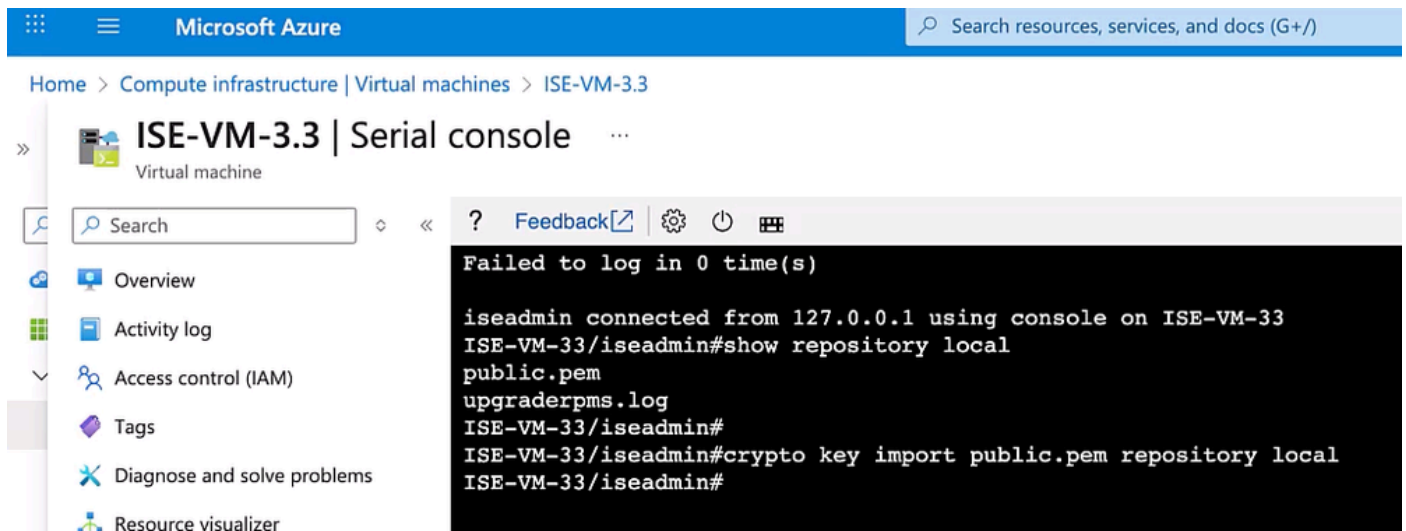
7. Maak een repository die verwijst naar de lokale ISE-schijf, zodat u deze kunt gebruiken om de openbare sleutel te installeren, in dit voorbeeld wordt onze repository lokaal genoemd.





Opmerking: Als u het bestand met de publieke sleutel wilt uploaden naar een andere repository die al op ISE is gemaakt, hoeft dit geen lokale schijf te zijn.

-
8. Meld u aan bij ISE Serial Console van Azure met behulp van de gebruikersnaam waarvoor u de SSH-sleutel wilt resetten.
 9. Controleer of de publieke sleutel (.pem-bestand) zich op de juiste manier in de repository bevindt en installeer de sleutel met de opdracht `crypto key import { naam van het public key-bestand } repository { naam van de repository }`.



Verifiëren

Om SSH in ISE te gebruiken met behulp van de nieuwe sleutelparen, moet u de privésleutel gebruiken als uw identificatie tijdens het inloggen.

1. Wijs de juiste rechten toe aan de privésleutel (degene die is gedownload in stap 3)

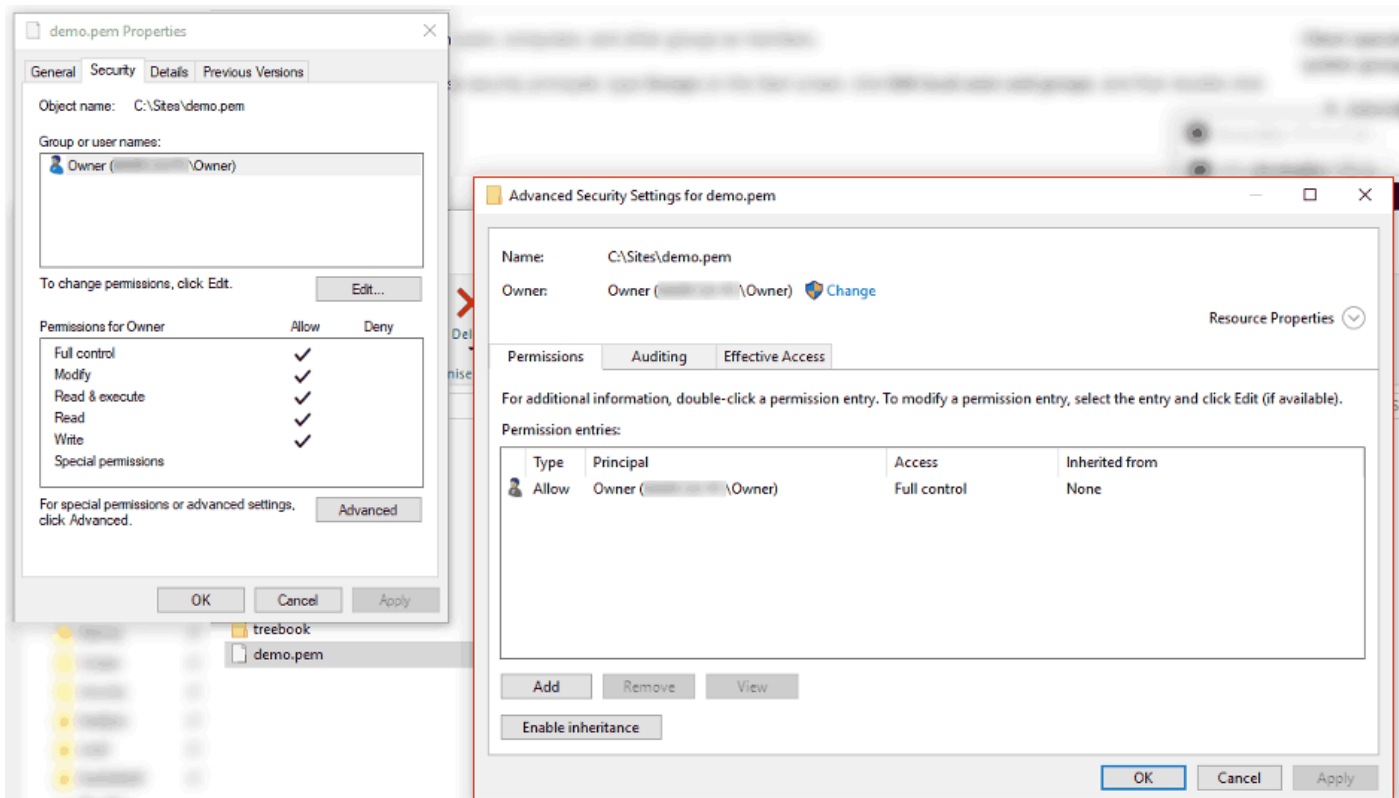
Vanaf macOS terminal:

```
CHMOD 600 { Privé-sleutelbestand }
```

Vanuit Windows:

Zoek het bestand in Windows Verkenner, klik er met de rechtermuisknop op en selecteer Eigenschappen. Navigeer naar het tabblad Beveiliging en klik op Geavanceerd.

Wijzig de eigenaar aan u, schakel overerving uit en verwijder alle machtigingen. Geef jezelf dan volledige controle en sla de machtigingen op.



2. SSH naar ISE met behulp van de nieuwe private key, de ISE-gebruikersnaam en het ISE IP-adres of FQDN.

Vanaf macOS terminal:

```
ssh -I { private key file } { gebruikersnaam } @{ ISE IP of FQDN }
```

Van Windows CMD:

```
ssh -i "{ private key file }" { gebruikersnaam } @{ ISE IP of FQDN }
```

Problemen oplossen

- Zorg ervoor dat u de volledige tekst van het bestand met de openbare sleutel naar uw .pem-bestand kopieert.
 - Zorg ervoor dat de repository het public key bestand bevat.
 - Als de crypto-opdracht de openbare sleutel niet op ISE installeert, verhoogt u een ticket met Cisco TAC, zodat de sleutel handmatig vanaf root kan worden geïnstalleerd.
- Veelvoorkomende fout voor deze bewerking is "% Fout: kan het geautoriseerde sleutelbestand niet bijwerken."

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.