

重置Azure VM上思科ISE的SSH金鑰

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何重置Azure ISE VM的SSH金鑰。

必要條件

- 基本ISE知識
- 通過Microsoft Azure訪問ISE控制檯
- 訪問ISE GUI
- 在Microsoft Azure中建立新金鑰對的許可權

需求

- Cisco ISE節點

採用元件

- Cisco ISE 3.3

本文中的資訊是根據特定實驗室環境內的裝置所建立。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。

設定

1. 在Microsoft Azure中，查詢SSH金鑰服務。



2. 按一下Create以建立新的SSH金鑰。選擇Subscription和Resource Group。請為新的SSH金鑰指定自定義名稱。對於SSH公鑰源欄位，選擇Generate new key pair選項，對於SSH Key Type選擇RSA SSH Format。最後，按一下Review + Create驗證並建立金鑰。

A screenshot of the 'Create an SSH key' wizard in the Azure portal. The wizard has three tabs: 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is selected. The page title is 'Create an SSH key'. Below the title, there is a description: 'Creating an SSH key resource allows you to manage and use public keys stored in Azure with Linux virtual machines. Learn more'. The 'Project details' section asks to 'Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.' It has two dropdown menus: 'Subscription' and 'Resource group'. The 'Resource group' dropdown is set to 'ISEresourceGroup'. The 'Instance details' section has four fields: 'Region' (set to '(US) East US'), 'Key pair name' (set to 'ISEnewKey'), 'SSH public key source' (set to 'Generate new key pair'), and 'SSH Key Type' (set to 'RSA SSH Format'). There is a note about Ed25519: '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.

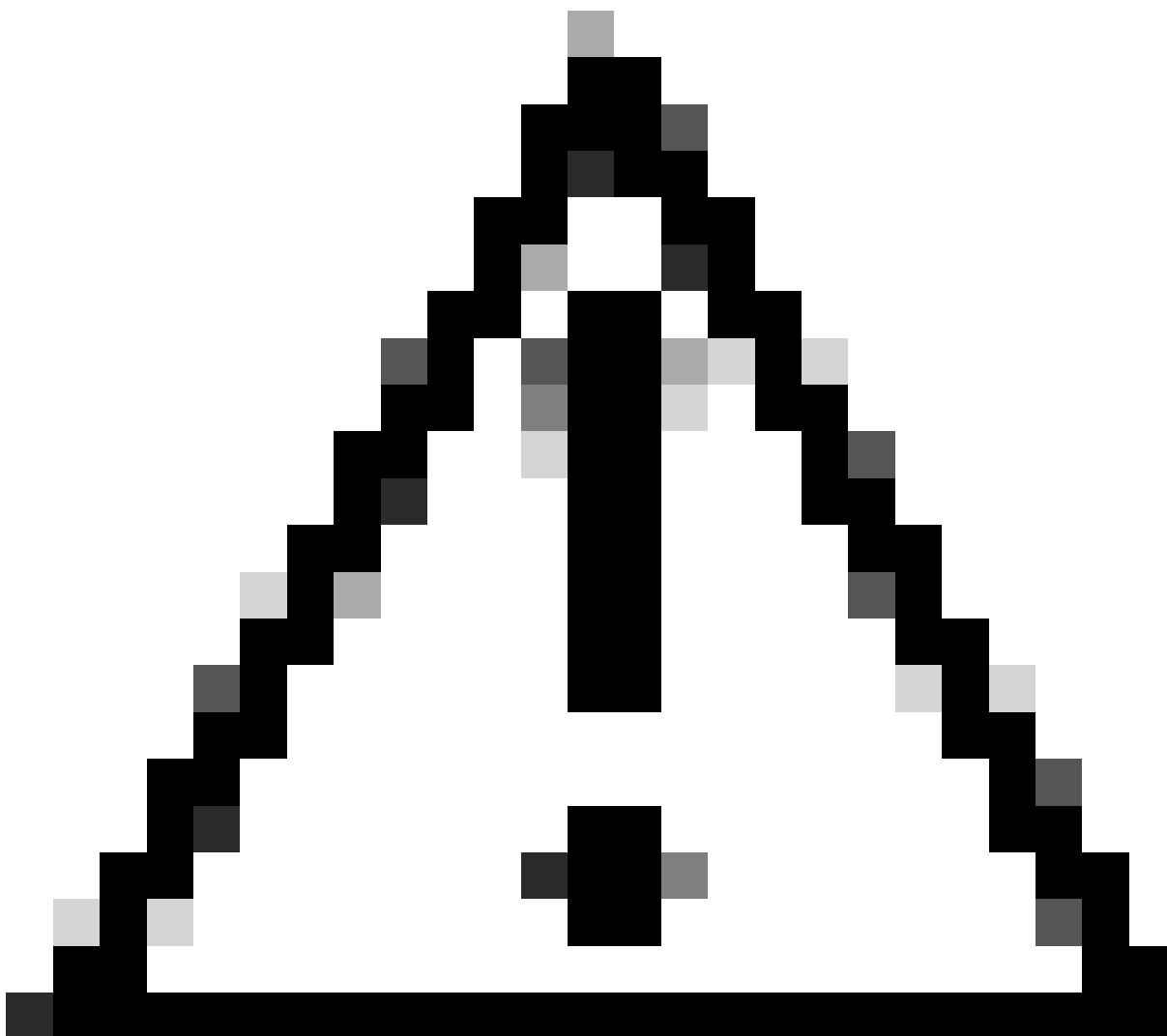
3. 建立金鑰後，將出現一個新視窗。按一下Download private key and create resource。

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](#)



注意：安全地儲存此私鑰很重要，因為這是Azure允許你下載此私鑰的唯一時刻。Azure不儲存此私鑰，無法從其他任何位置下載。

-
- 現在，導航回到SSH金鑰服務，查詢您新建立的金鑰，然後按一下它以檢視其概述。

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

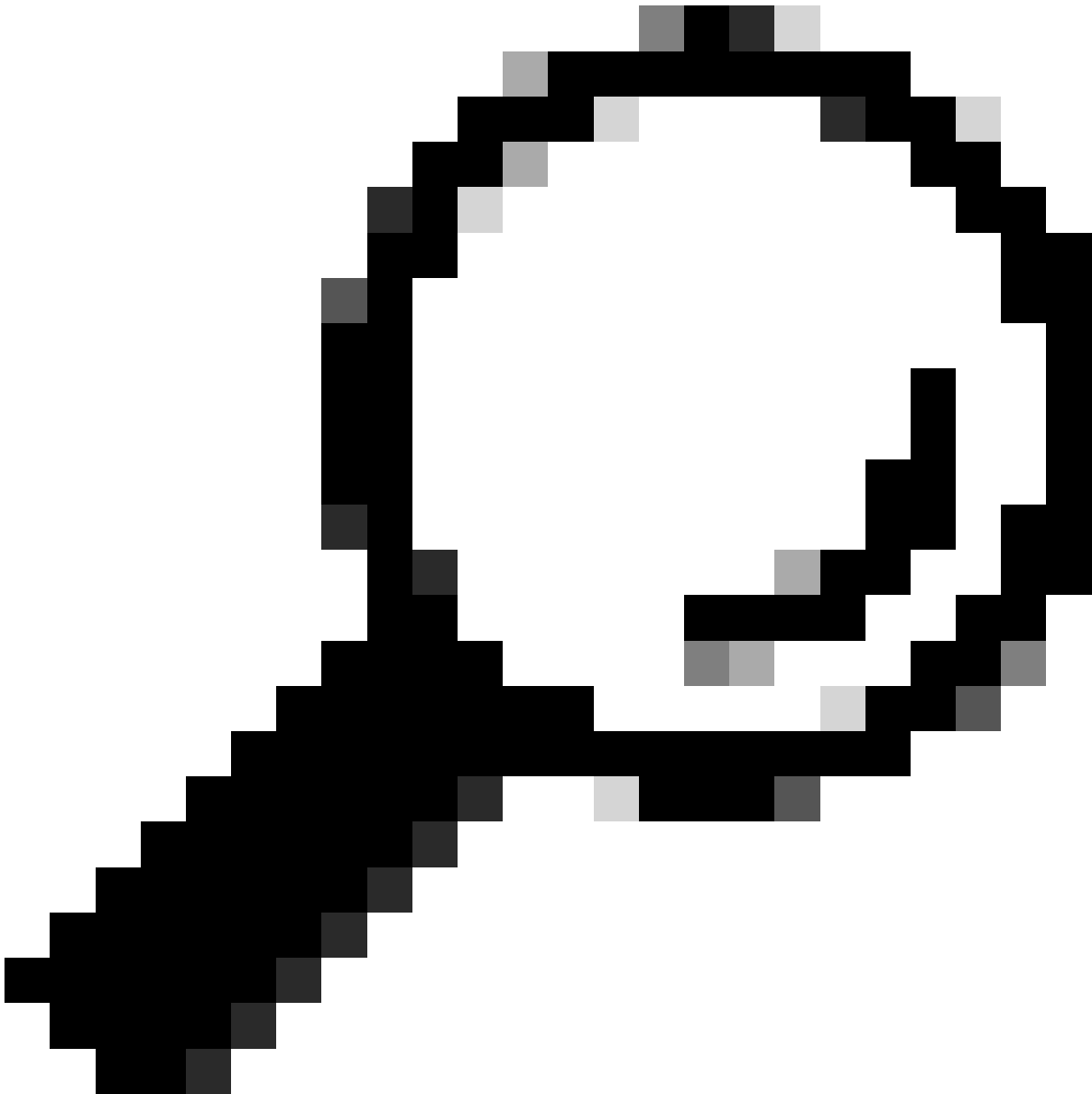
☐	Name ↑	Type
☐	 ISEnewKey	SSH key

5. 在金鑰的概述中，您將看到公鑰。複製此文本並將其貼上到文本編輯器上，以便將其另存為副檔名為.pem的本地檔案。在本指南中，檔案儲存為public.pem。

Public key

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrLUV41tSEcOjdC2k4tyju1n/Xxs8/w7T2T33QDE6MjJ7u+v8DI2HhJWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF4lupl8amyjFpqdPHJbOu90GkQSFICEbYVUJYpzUSdNYomxlB5J+tuSVQFscN3ht5SbXGLDEUTSPcntXeHdq+Zc/CPSoWwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1cOxylgkllhRCAnQ0wyJy3DhN+PJWZMqr8NqADFS5eGKXr1EgSgSlw3+fbW7gl+eZ8ZhWzX8EpRrHpKCtBjh9gtERXfkP12Ik/HRctVU0xXY49noenL+QLCGUvN+3pD28L3jsK5RCR2D5/9aHv4h0SqWRW/XknQHkxLqXPXrWH5tE566Y9YB0J375HcyDtAjDu4S2LJRZA3u+2Q75UXaQuquyXt0x9PSP1bm/dYQwyY9dn+DKXWdlh2AFhUnlPU8M2A4/jj55UcuWi0= generated-by-azure

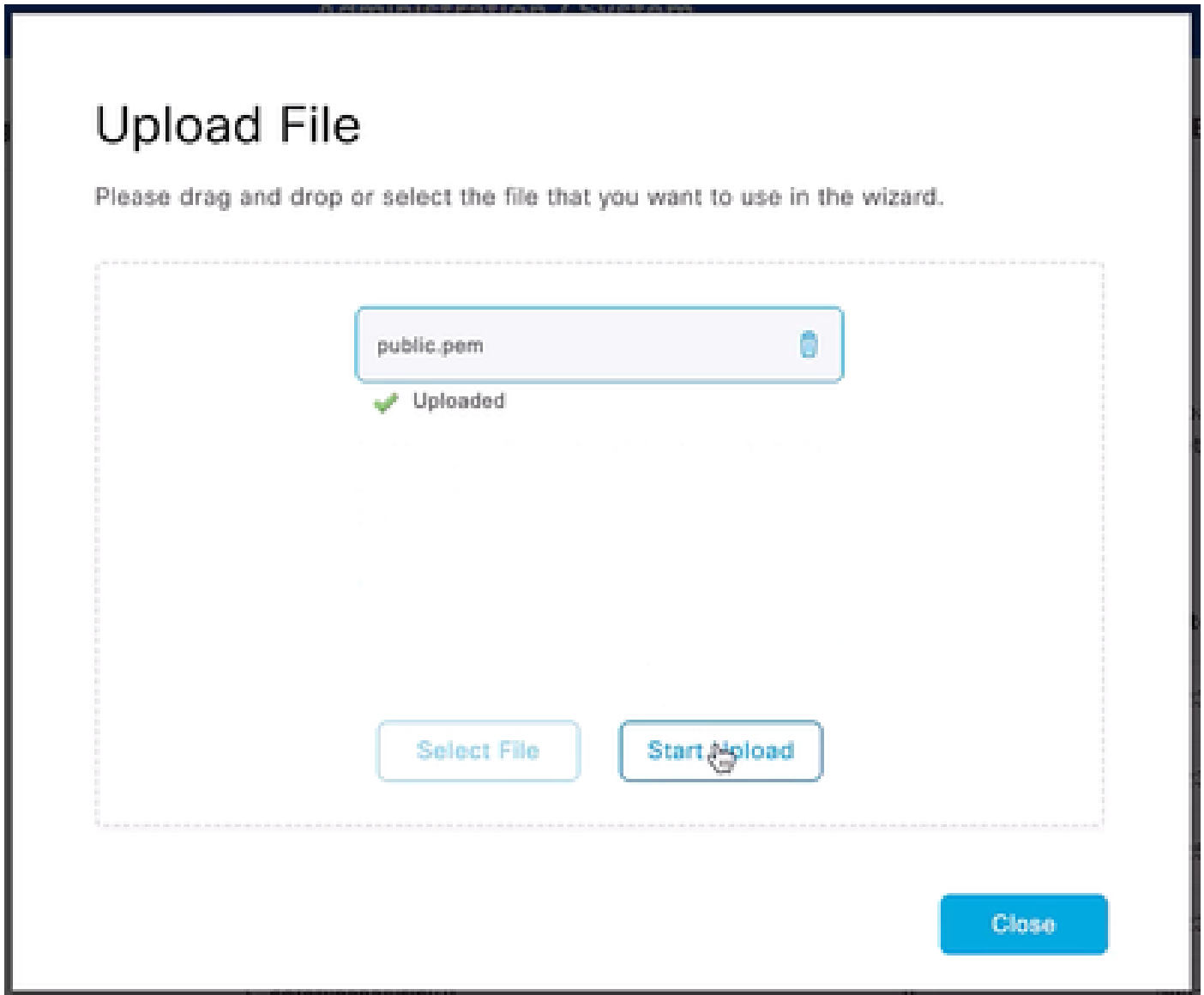
Copy to clipboard



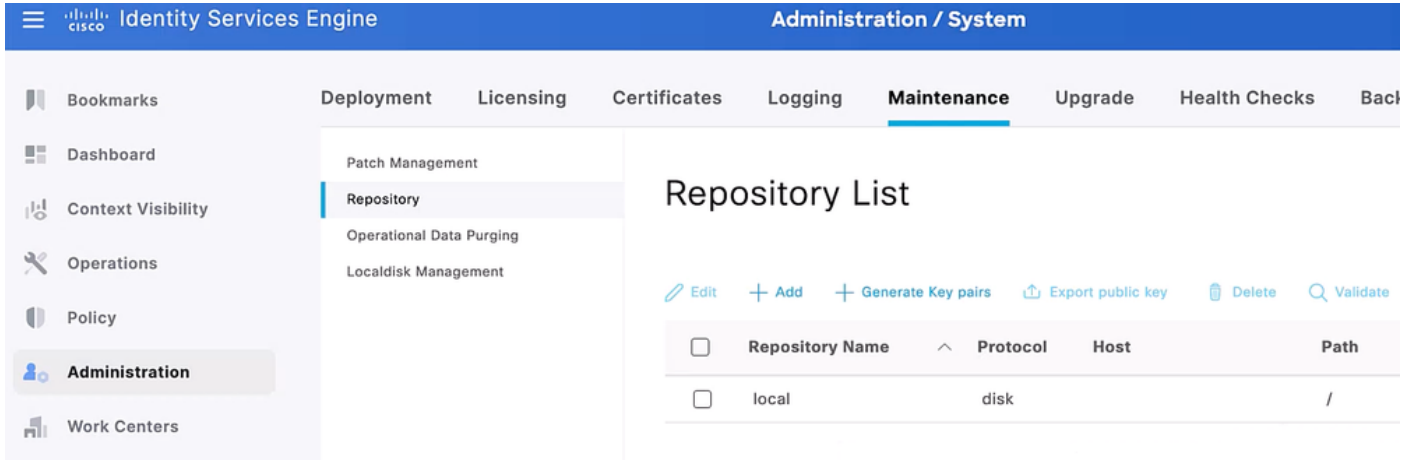
提示：您可以按一下Copy to clipboard按鈕複製公鑰字串。

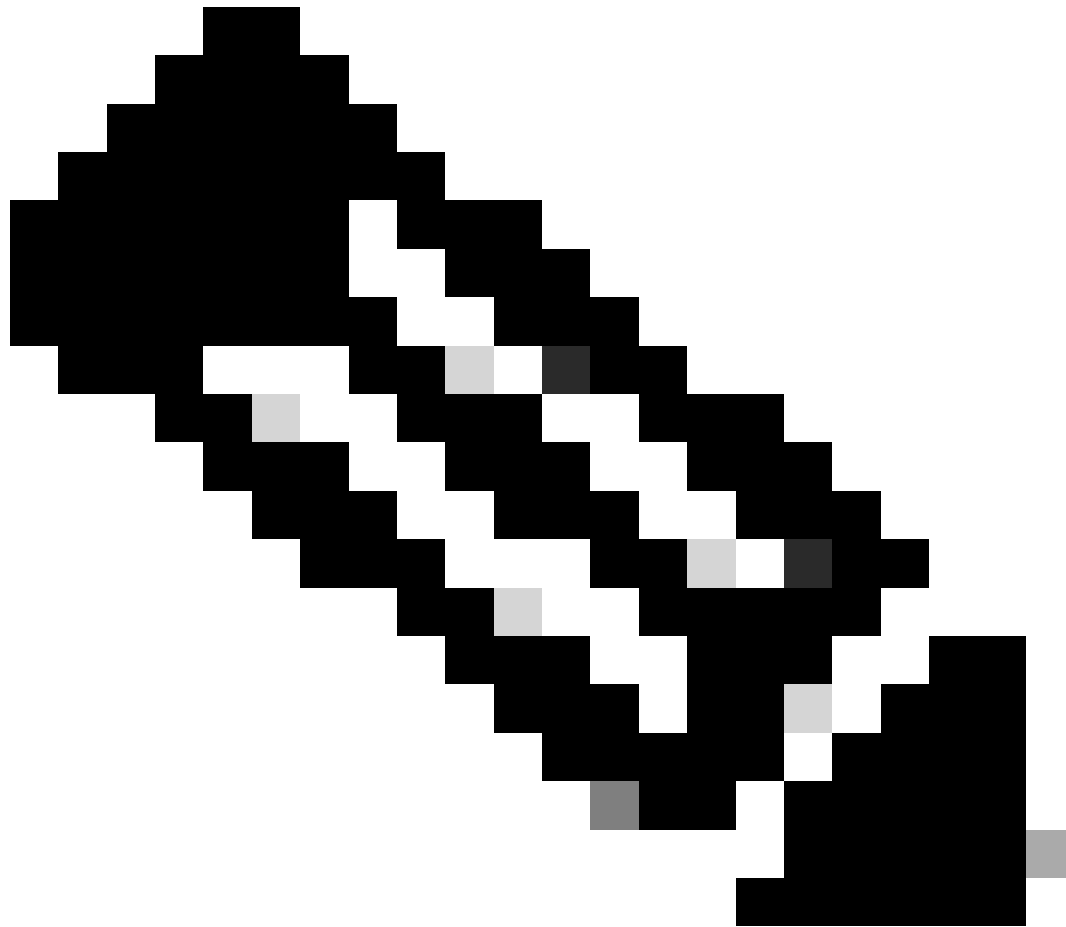
```
1 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCddpg4cnMpUsjrzLUV41tSEc0jdC2k4tyju1n/Xxs8/
w7T2T33QDE6MjJ7u+v8DI2HhjWwgMD2vi1a3Sooc2/VCYiNaVHHxhG10CKF4IupI8amyjFpqdPHJb0u90GkQSFLCEbYVUJ
YpzUSdNYomxLB5J+tuSVQFsc0N3ht5SbXGLDEUTSPcntXeHdq+Zc/CPS0vwyVQdesF/jaVMczRiT6xh2J3aPeRo5d1c0xy
IgakIhRCAnQ0wyJy3DhN+PJWZMqrBNqADFS5eGKXr1EgSgSlw3+fbW7gl+eZ8ZhWzX8EpRrHpKCtbJh9gtERXfKPt2Ik/
HRctVU0xXY49noenL+QLCGUvN+3pD2BL3jsK5RCR2D5/9aHUQ0fPkTojh4h0SqWRW/
XknQHkxLqXPXrWH5tE566Y9YB0J375HcyDtAjDu4S2LJRZA3u+2Q75UXaQuquyXt0x9PSP1bm/
dYQwY9dn+DKXWdlh2AFhUnlPU8M2A4/jJ55UcuvUWA+jWYWi0= generated-by-azure
```

6. 將此公鑰上傳到ISE本地磁碟。為此，請導航至ISE >管理>系統>維護>本地磁碟管理。按一下您的ISE主機名，然後按一下上傳，然後按一下選擇檔案，然後查詢並選擇您本地電腦中的公鑰。最後按一下Start Upload。



7. 建立一個指向ISE本地磁碟的儲存庫，以便您可以使用該儲存庫安裝公鑰，在本示例中，我們的儲存庫稱為local。

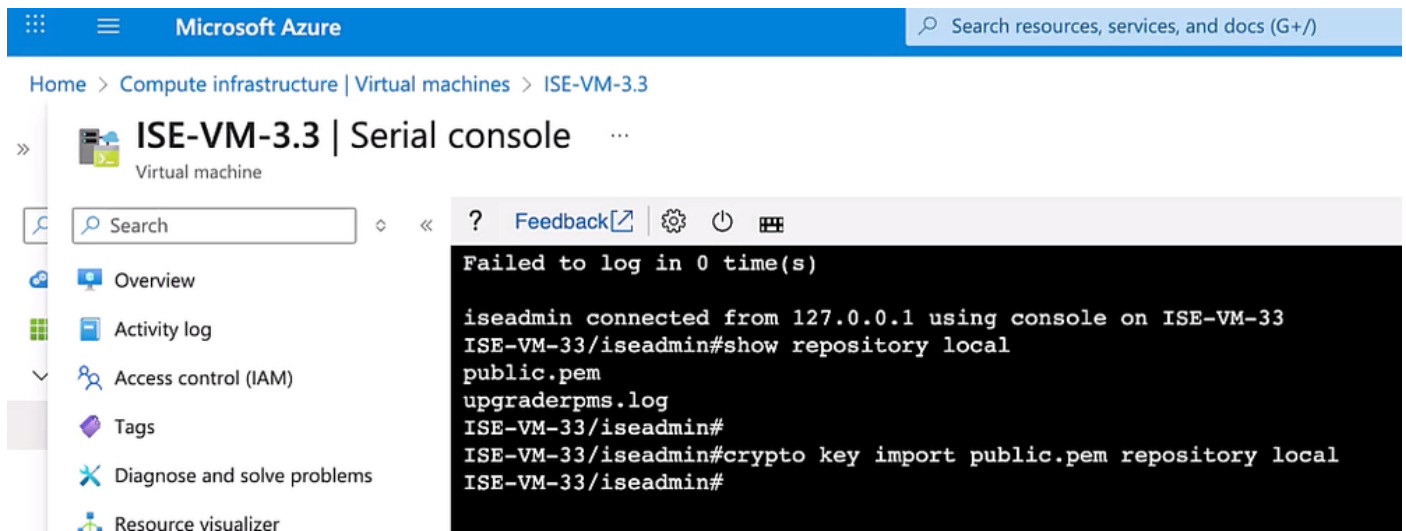




附註：如果您希望將公鑰檔案上傳到ISE上已建立的其他儲存庫，則不需要它是本地磁碟。

8. 使用要重置SSH金鑰的使用者名稱從Azure登入到ISE串列控制檯。

9. 驗證公鑰（.pem檔案）是否正確位於儲存庫中，並使用`crypto key import { name of the public key file } repository { name of the repository }`命令安裝該金鑰。



驗證

要使用新金鑰對SSH到ISE，您需要使用私鑰作為登入時的標識。

1. 為私鑰分配適當的許可權（步驟3中下載的私鑰）

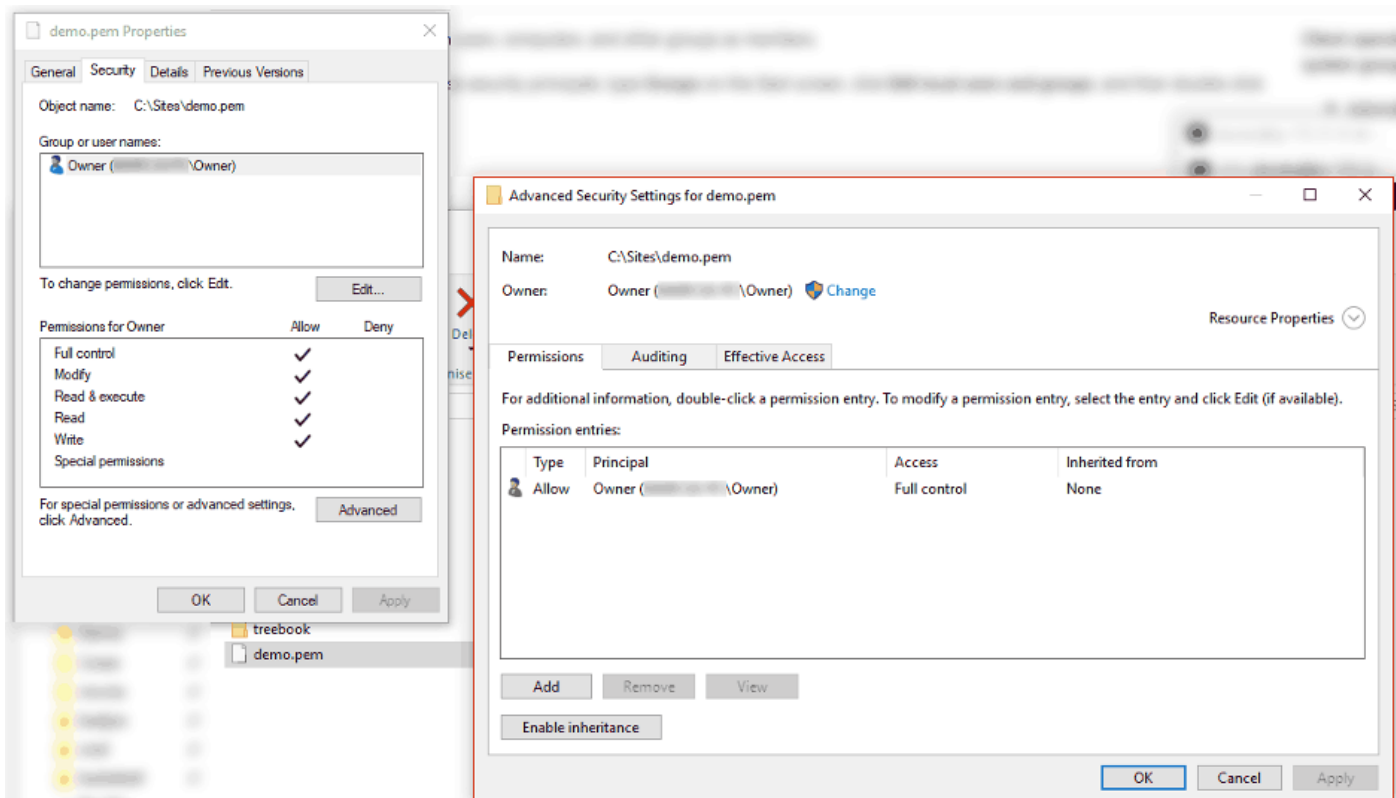
從macOS終端：

```
chmod 600 { private key file }
```

在Windows中：

在Windows資源管理器中查詢該檔案，按一下右鍵該檔案，然後選擇屬性。導覽至Security索引標籤，然後按一下Advanced。

將所有者更改為您，禁用繼承並刪除所有許可權。然後授予您自己「完全控制」並儲存許可權。



2. 使用新私鑰、ISE使用者名稱和ISE IP地址或FQDN通過SSH進入ISE。

從macOS終端：

```
ssh -I { private key file } { username }@{ ISE IP或FQDN }
```

在Windows CMD上：

```
ssh -i "{ private key file }" { username }@{ ISE IP或FQDN }
```

疑難排解

- 確保將公鑰檔案的完整文本複製到.pem檔案中。
- 確保儲存庫包含公鑰檔案。
- 如果crypto命令無法在ISE上安裝公鑰，請向Cisco TAC提交票證，以便可以從根手動安裝金鑰。此操作的常見錯誤為「% Error:無法更新授權金鑰檔案。」

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）。