Azure VMでのCisco ISEのSSHキーのリセット

内容

はじめに

- 前提条件
- 要件
- 使用するコンポーネント

設定

確認

トラブルシュート

はじめに

このドキュメントでは、Azure ISE VMのSSHキーをリセットする方法について説明します。

前提条件

- ISEの基礎知識
- Microsoft Azureを介したISEコンソールへのアクセス
- ISE GUIへのアクセス
- Microsoft Azureで新しいキーペアを作成する権限

要件

- Cisco ISEノード

使用するコンポーネント

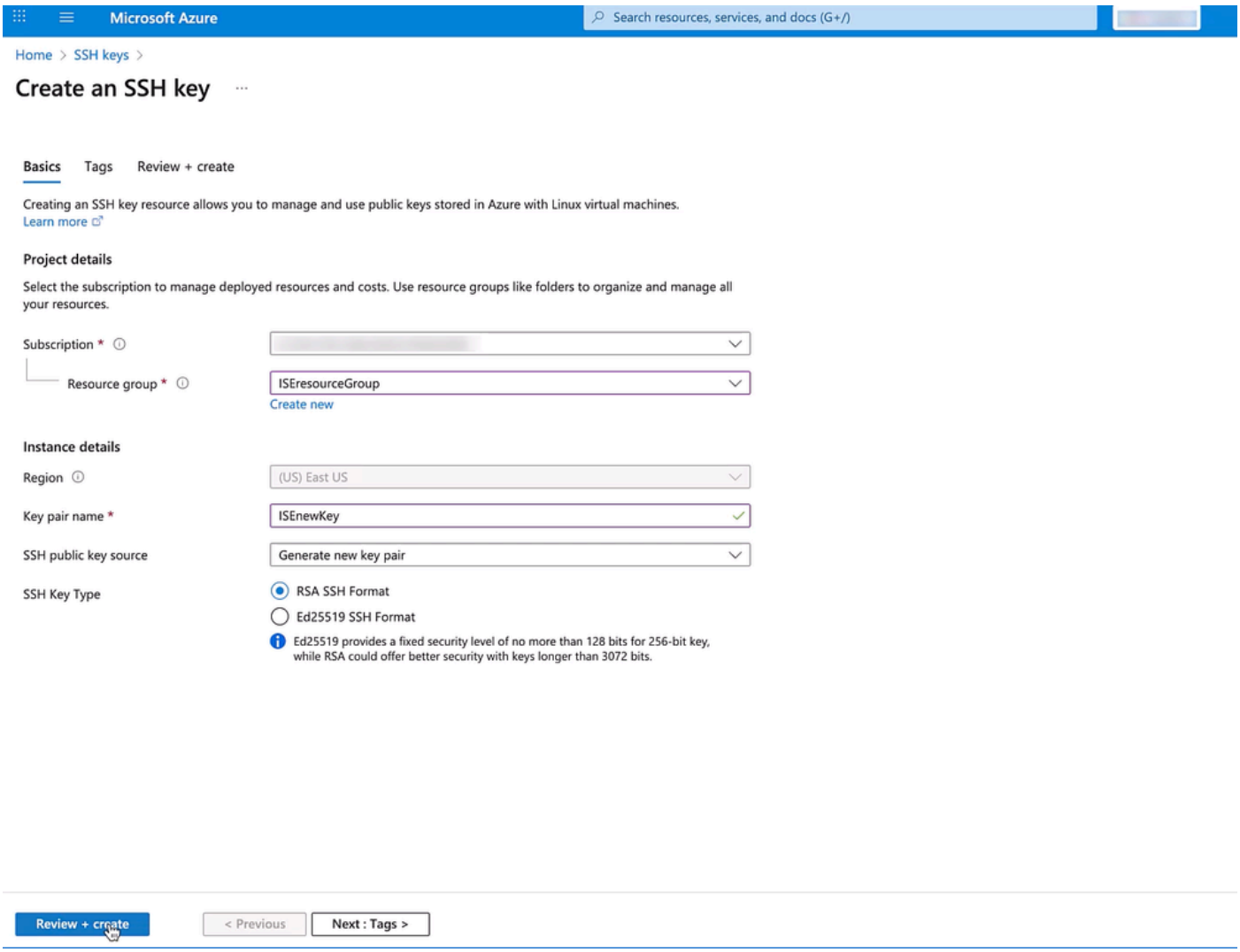
- Cisco ISE 3.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

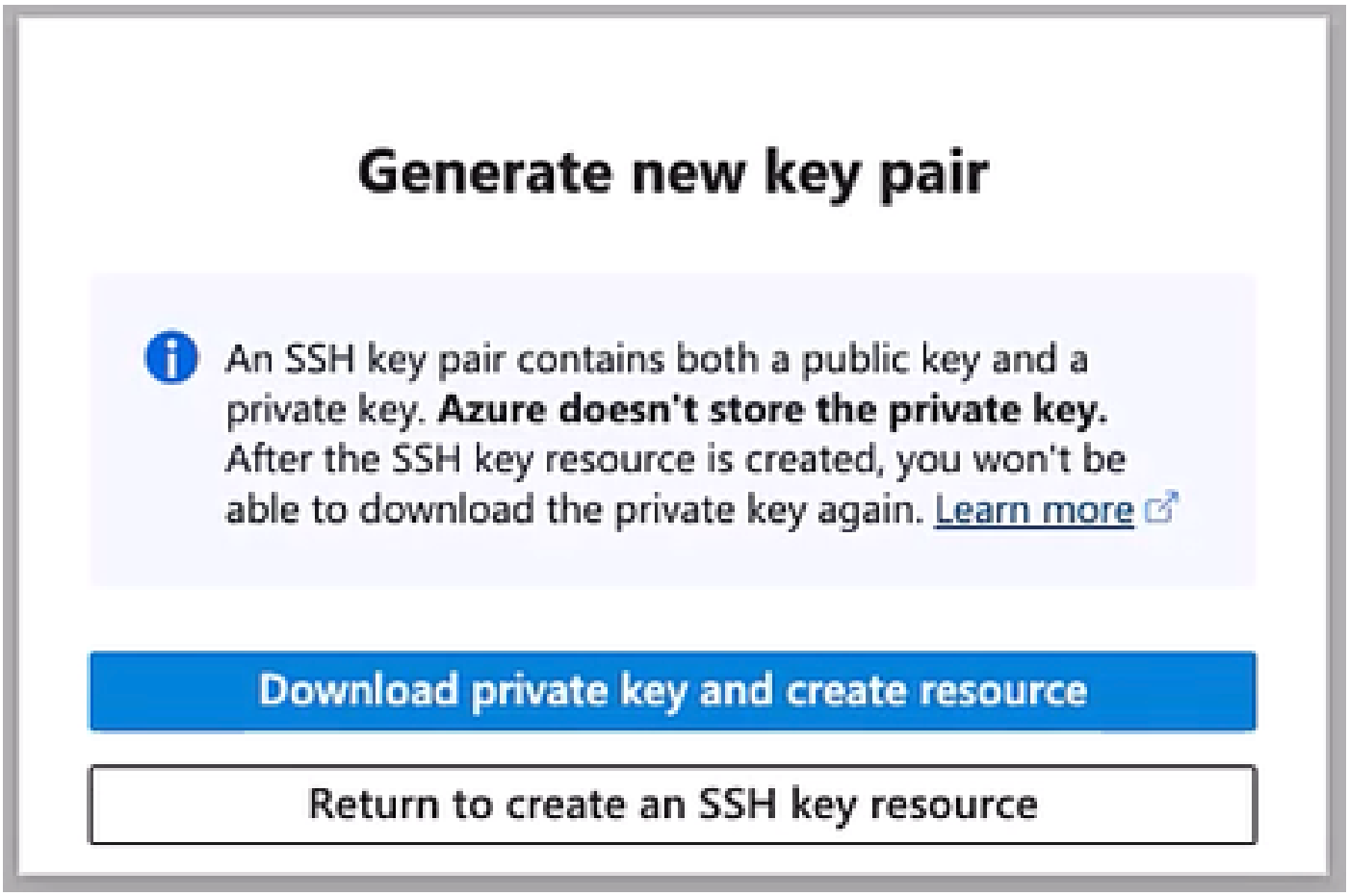
設定

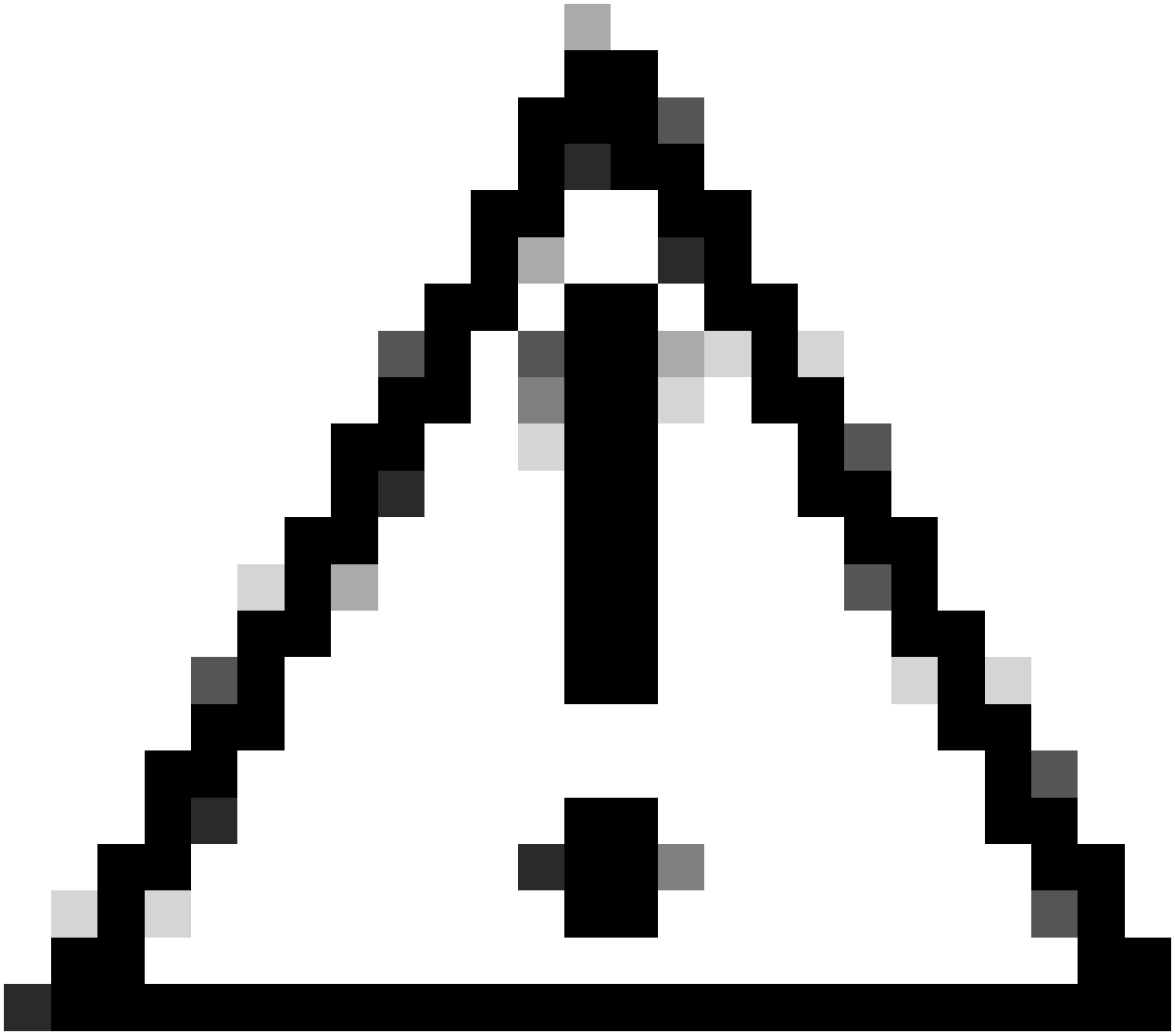
1. Microsoft Azureで、SSHキーサービスを探します。

2. Createをクリックして、新しいSSHキーを作成します。サブスクリプションとリソースグループを選択します。 新しいSSHキーのカスタム名を指定します。SSH public key sourceフィールドで、Generate new key pairのオプションを選択し、SSH Key TypeでRSA SSH Formatを選択します。 最後に、Review + Createをクリックしてキーを検証し、作成します。



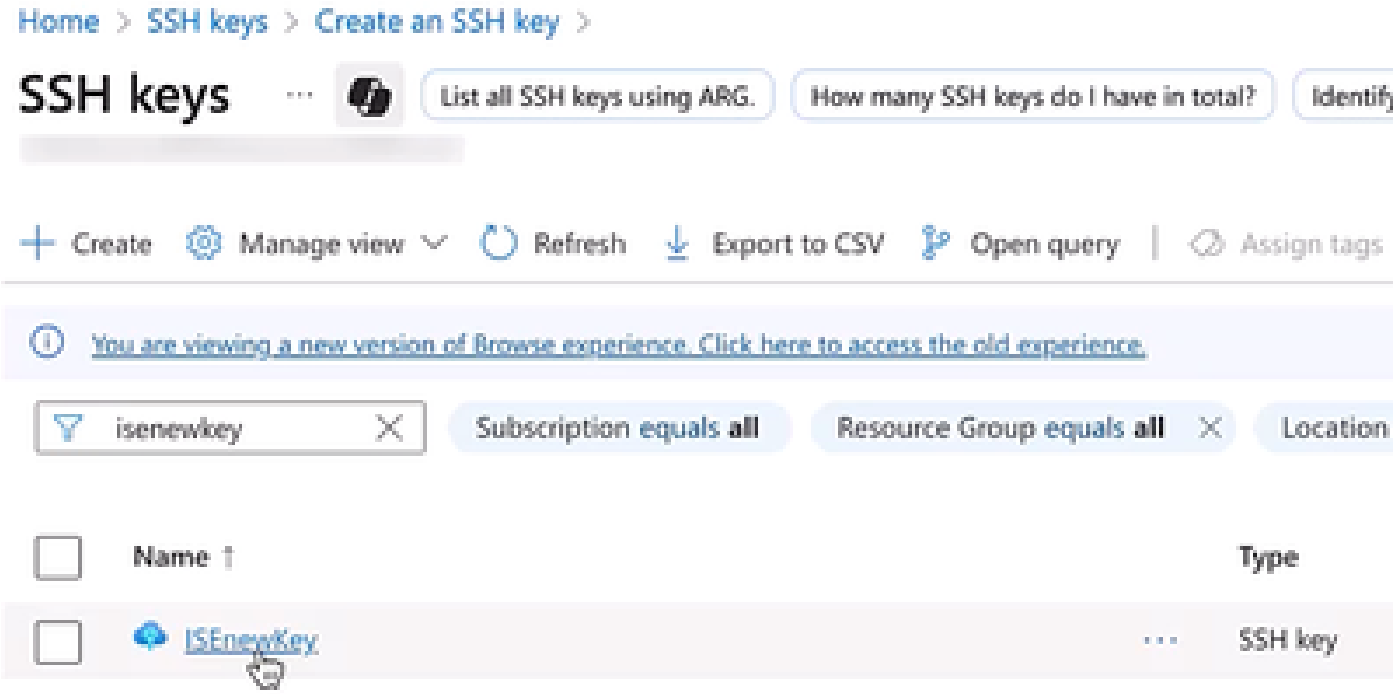
3. キーが作成されると、新しいウィンドウが表示されます。Download private key and create resourceをクリックします。



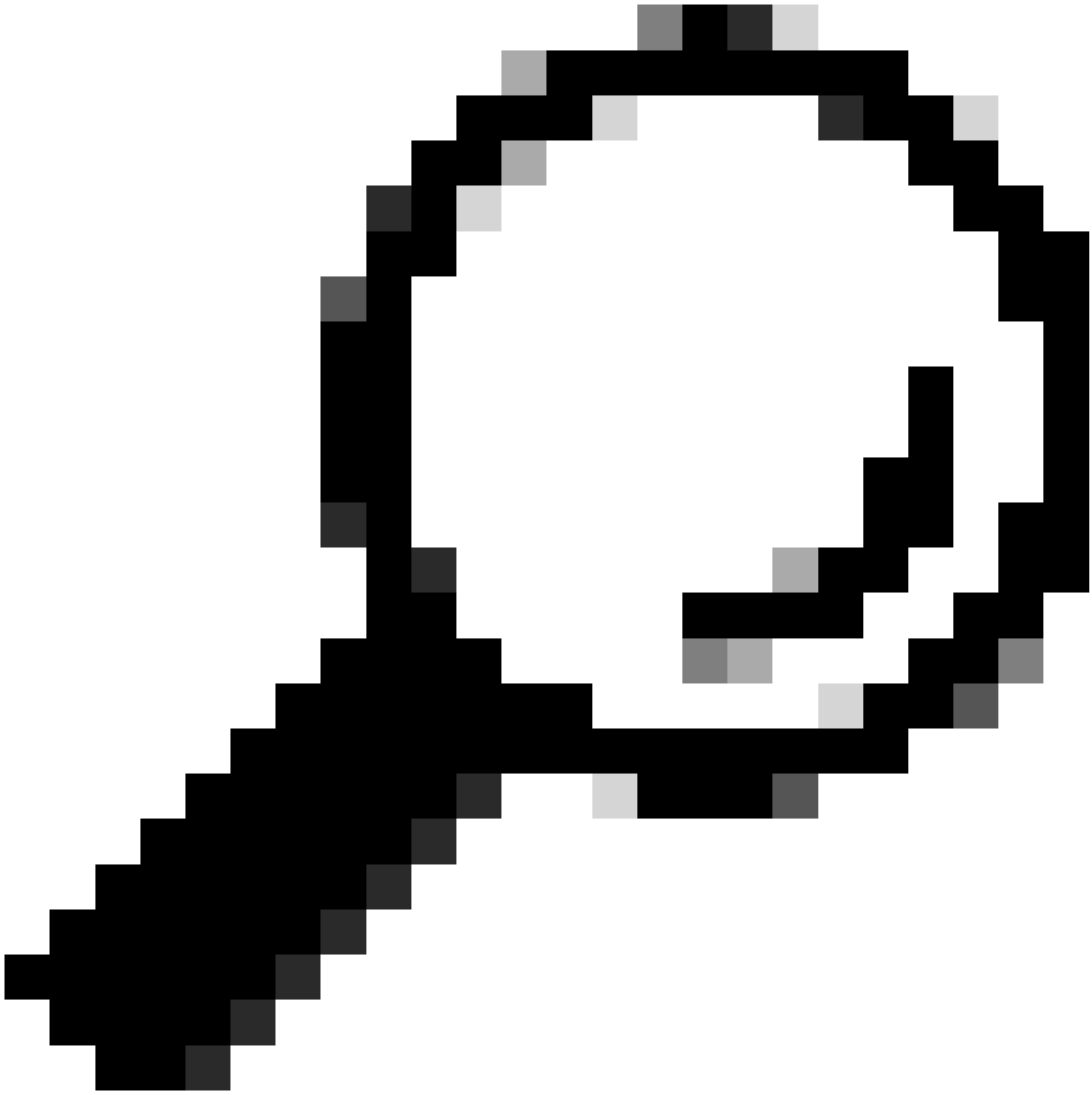


注意：この秘密キーを安全に保管することが重要です。これは、この秘密キーをダウンロードできる唯一のタイミングであるためです。Azureはこの秘密キーを保存しないため、他の場所からダウンロードできません。

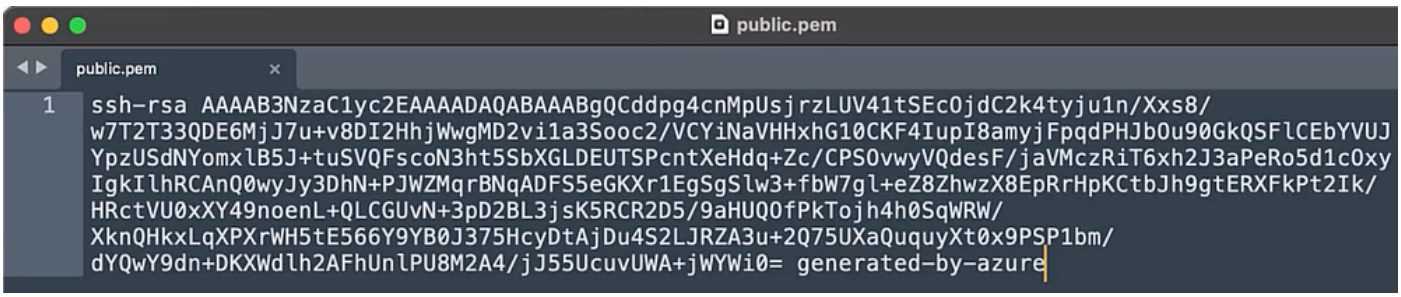
4. 次に、SSH Keysサービスに戻り、新しく作成したキーを探してクリックすると、その概要が表示されます。



5. キーの概要には、公開キーが表示されます。このテキストをコピーしてテキストエディタに貼り付け、.pem拡張子の付いたローカルファイルとして保存できるようにします。このガイドでは、このファイルはpublic.pem(pem)として保存されます。

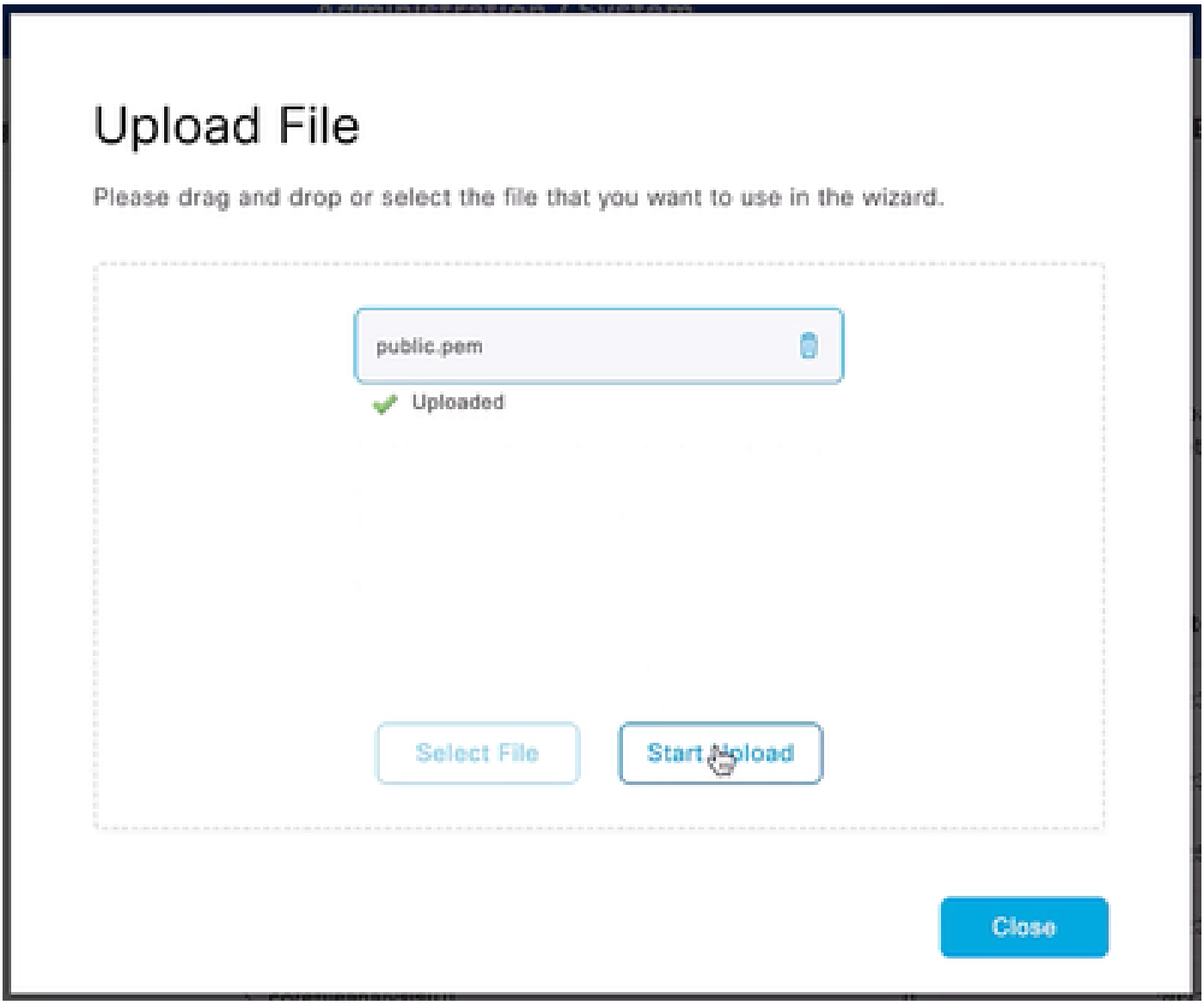


ヒント: [クリップボードにコピー] ボタンをクリックすると、公開キー文字列をコピーできます。

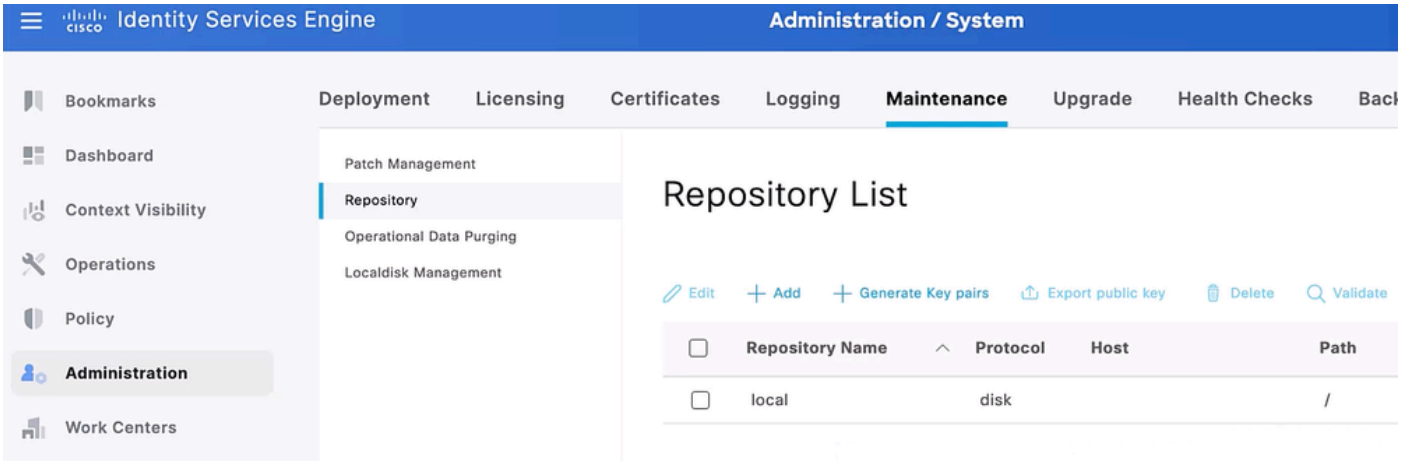


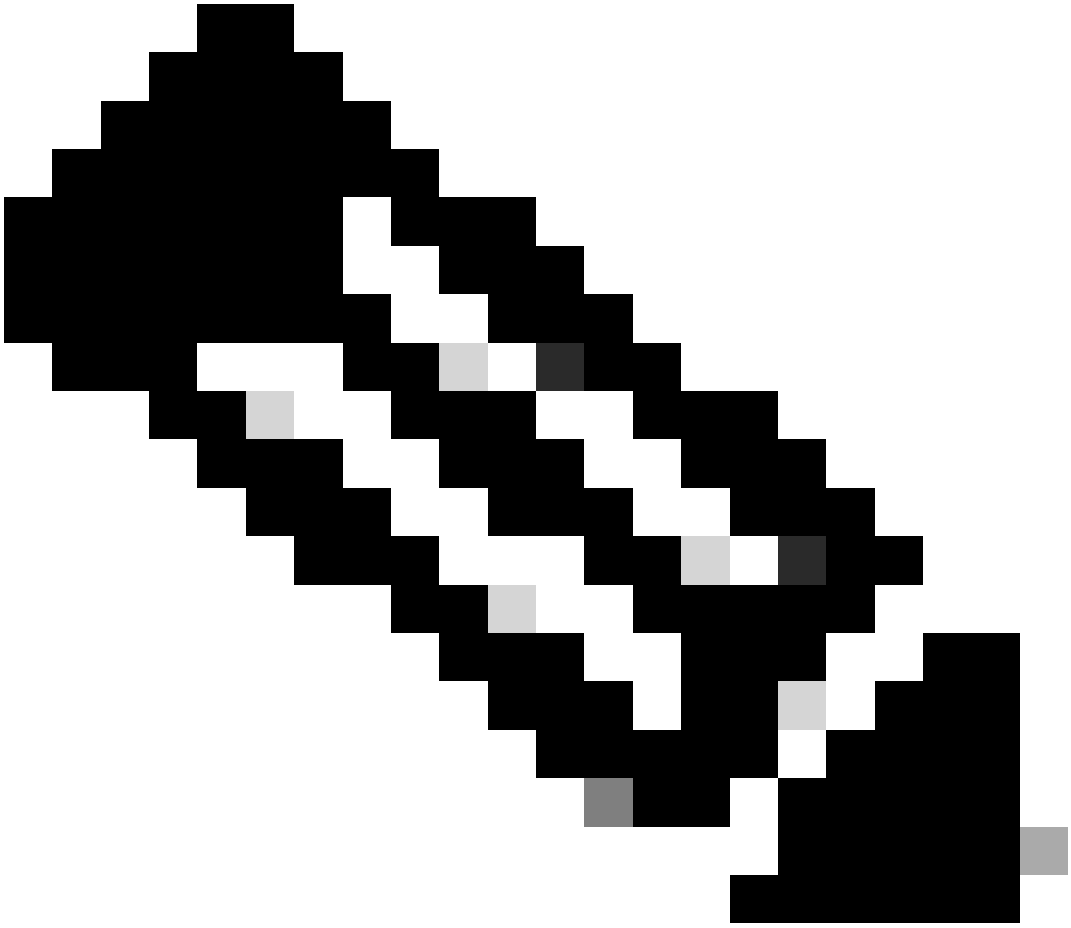
6. この公開キーをISEローカルディスクにアップロードします。それには、ISE > Administration > System > Maintenance > Local Disk Managementの順に選択します。ISEホスト名をクリックし、Uploadをクリックしてから Select Fileをクリックし、ローカル

コンピュータの公開キーを検索して選択します。最後に、Start Uploadをクリックします。



7. ISEローカルディスクを指すリポジトリを作成して、公開キーのインストールに使用できるようにします。この例では、リポジトリの名前はlocalです。

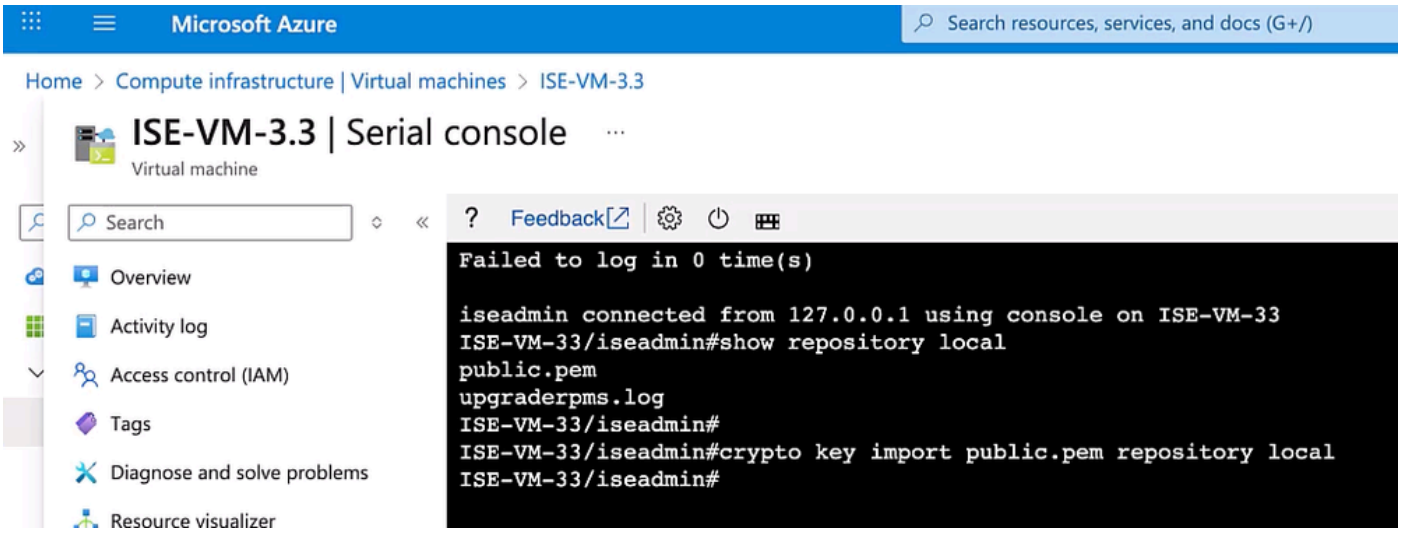




注:ISEですでに作成されている別のリポジトリに公開キーファイルをアップロードできるようにする場合は、ローカルディスクである必要はありません。

8. SSHキーをリセットするユーザ名を使用して、AzureからISEシリアルコンソールにログインします。

9. 公開キー（.pemファイル）がリポジトリに正しく配置されていることを確認し、コマンド crypto key import { public key file } repository { repository of the repository }を使用してキーをインストールします。



確認

新しいキーペアを使用してSSHからISEにログインするには、ログイン時にIDとして秘密キーを使用する必要があります。

1. 秘密キー（手順3でダウンロードした秘密キー）に適切な権限を割り当てます

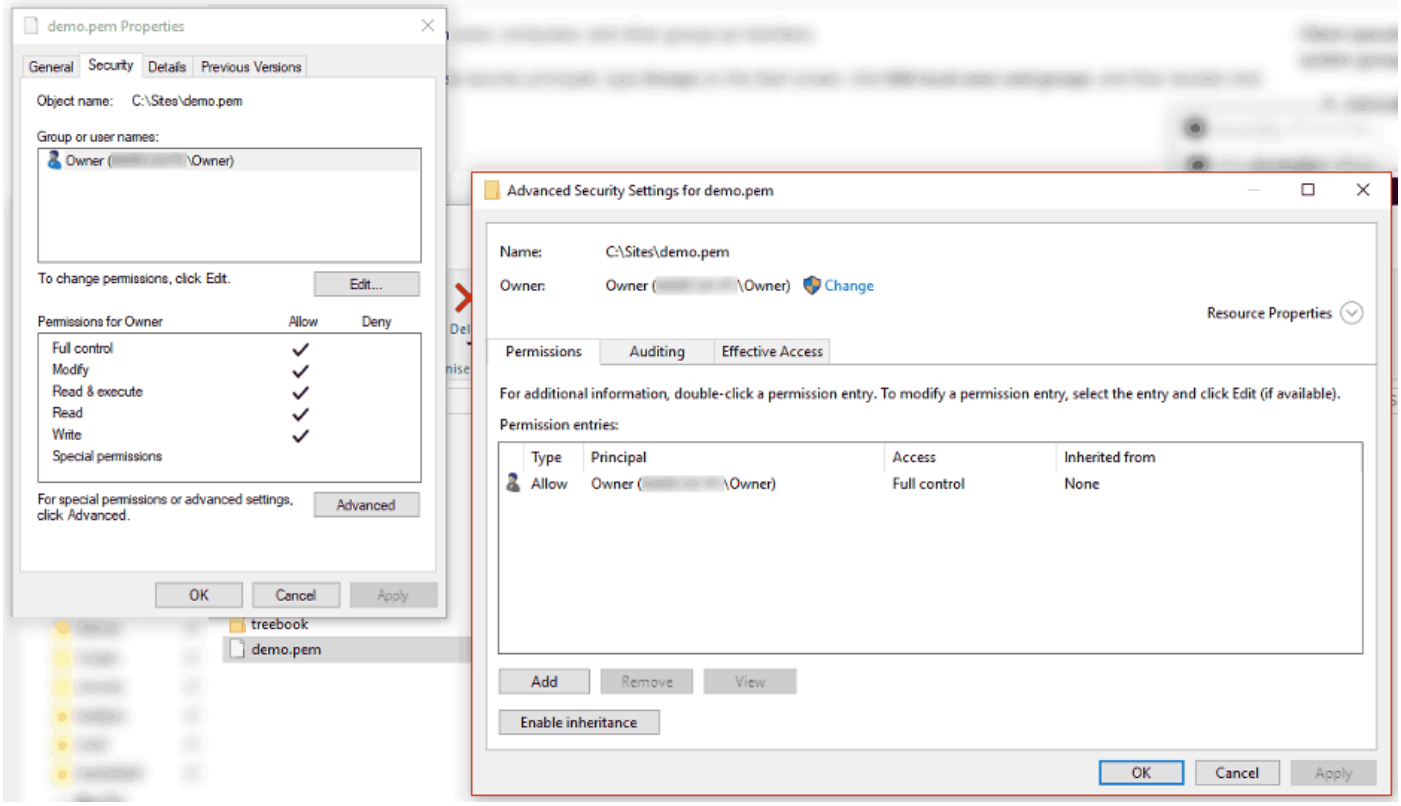
macOSターミナルから：

chmod 600 { private key file }

Windowsから：

Windowsエクスプローラでファイルを探し、右クリックしてPropertiesを選択します。Securityタブに移動し、Advancedをクリックします。

所有者を自分に変更し、継承を無効にし、すべてのアクセス許可を削除します。次に、フルコントロールを付与し、権限を保存します。



2. 新しい秘密キー、ISEユーザ名、およびISEのIPアドレスまたはFQDNを使用して、SSHからISEにアクセスします。

macOSターミナルから：

ssh -I { private key file } { username }@{ ISE IPまたはFQDN }

Windows CMDから：

ssh -i "{ private key file }" { username }@{ ISE IPまたはFQDN }

トラブルシュート

- 公開キーファイルの完全なテキストを.pemファイルにコピーしてください。
- リポジトリに公開キーファイルが含まれていることを確認します。
- cryptoコマンドを実行してもISEに公開キーをインストールできない場合は、Cisco TACにチケットを提出して、ルートから手動でキーをインストールできるようにします。この操作の一般的なエラーは「% Error: Unable to update authorized key file」です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。