SSH-Schlüssel für Cisco ISE auf Azure-VMs zurücksetzen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie SSH-Schlüssel für Azure ISE-VMs zurückgesetzt werden.

Voraussetzungen

- Grundlegendes ISE-Wissen
- Zugriff auf die ISE-Konsole über Microsoft Azure
- Zugriff auf die ISE-GUI
- Berechtigungen zum Erstellen neuer Schlüsselpaare in Microsoft Azure

Anforderungen

- Cisco ISE-Knoten

Verwendete Komponenten

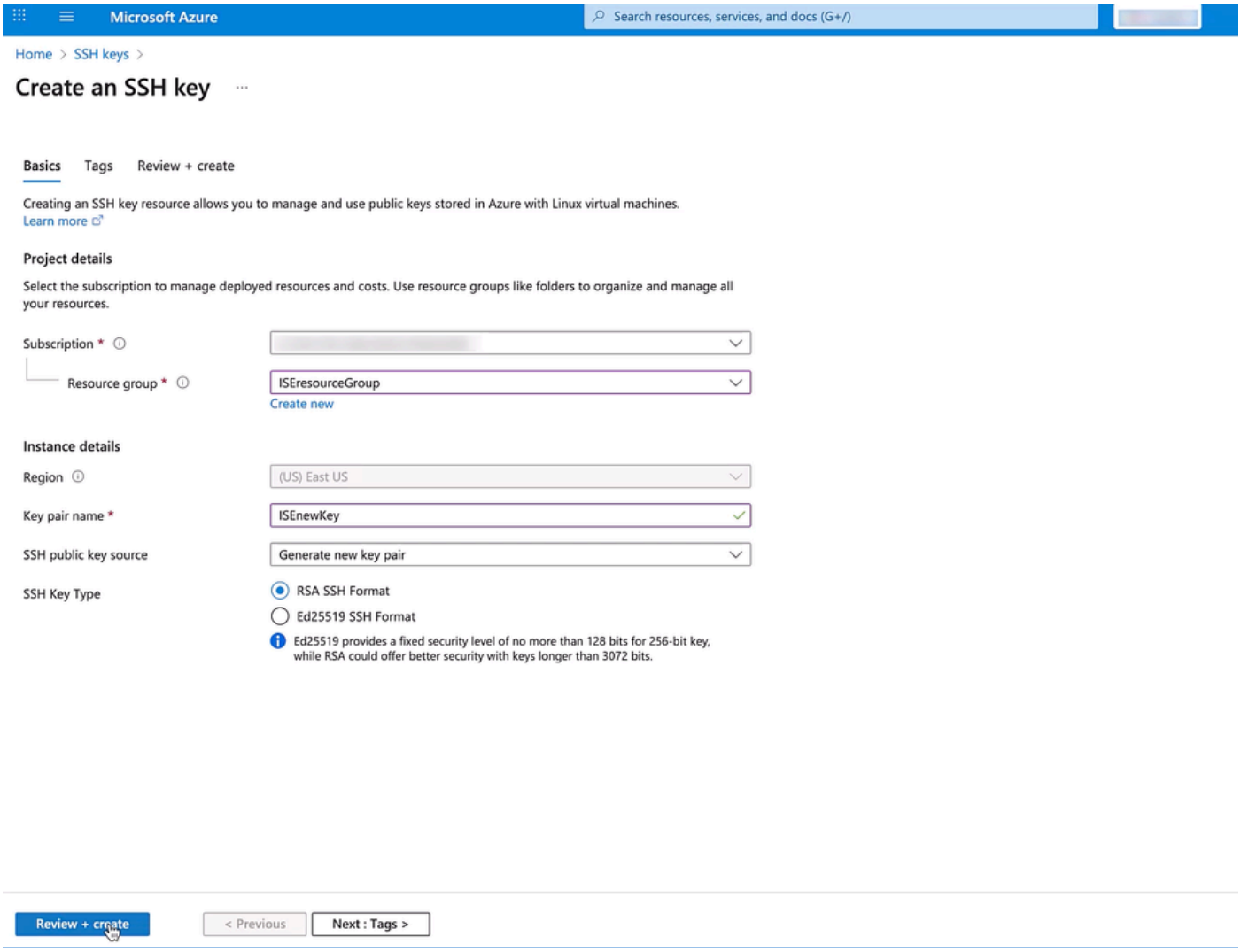
- Cisco ISE 3.3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

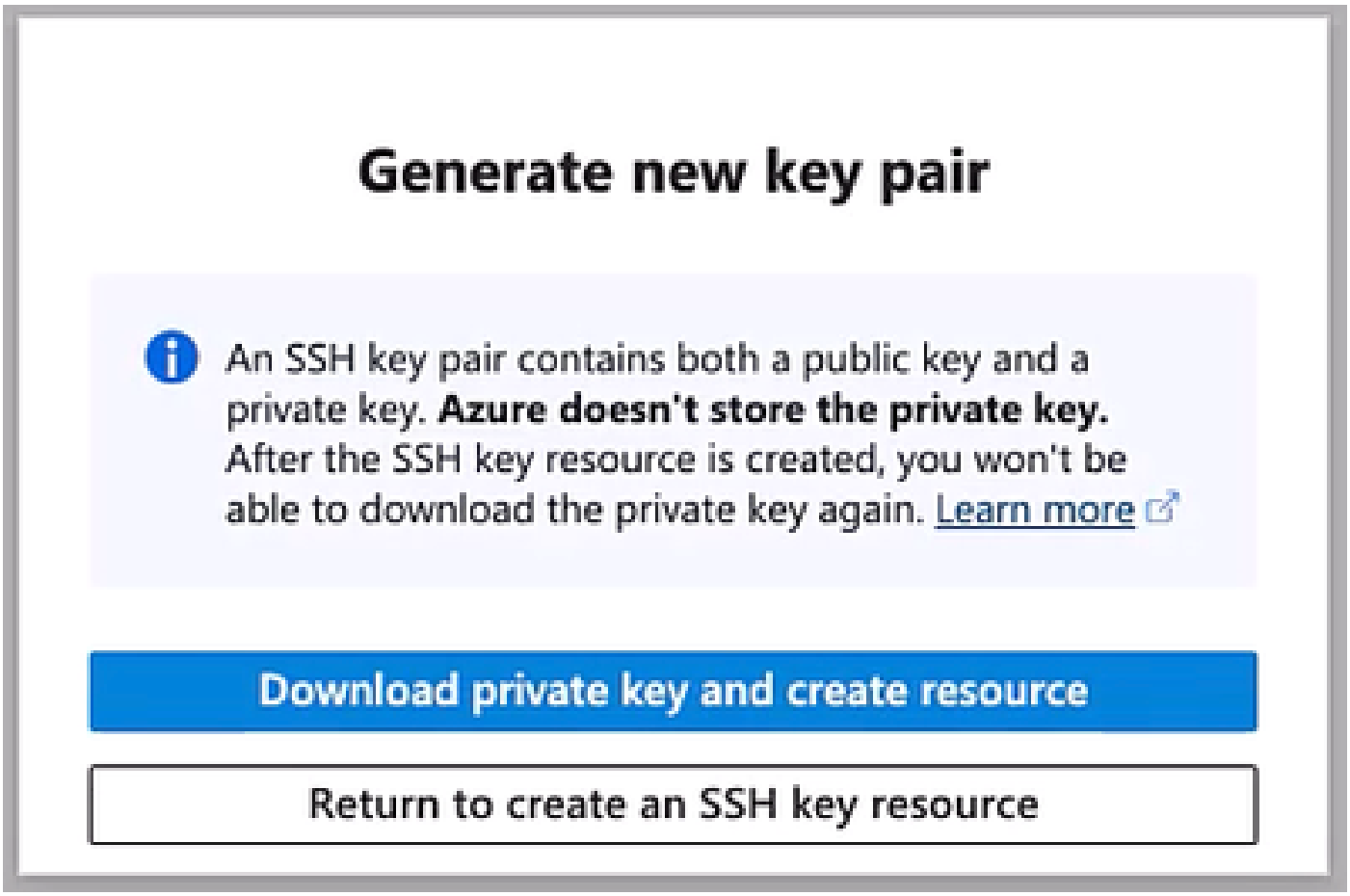
Konfigurieren

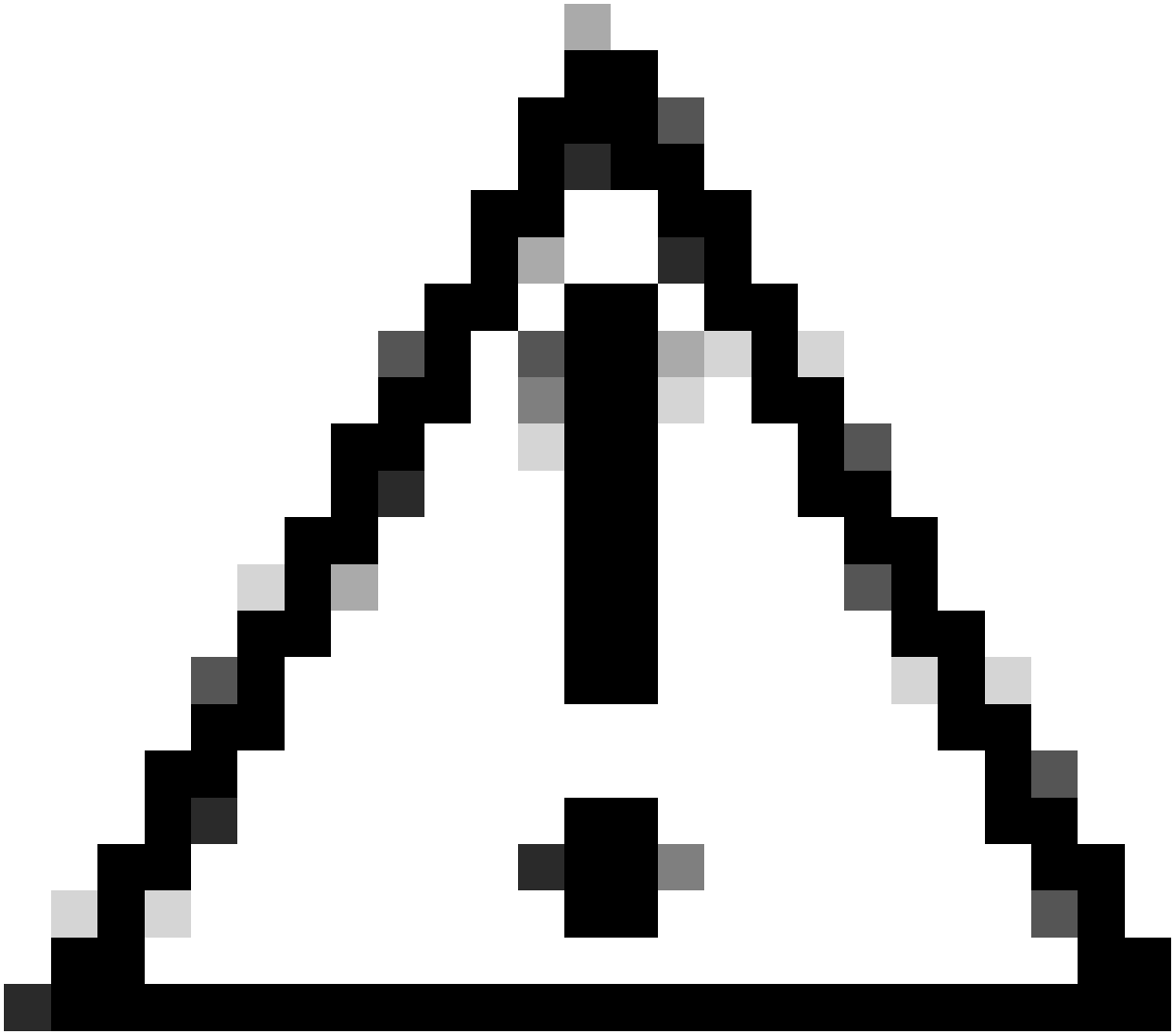
1. Suchen Sie in Microsoft Azure nach einem SSH-Schlüssel-Dienst.

2. Klicken Sie auf Erstellen, um einen neuen SSH-Schlüssel zu erstellen. Wählen Sie Ihr Abonnement und Ihre Ressourcengruppe aus. Geben Sie einen benutzerdefinierten Namen für den neuen SSH-Schlüssel an. Wählen Sie als Quellfeld für den öffentlichen SSH-Schlüssel die Option für Neues Schlüsselpaar generieren und für den SSH-Schlüsseltyp RSA SSH Format aus. Klicken Sie abschließend auf Prüfen + Erstellen, um den Schlüssel zu validieren und zu erstellen.



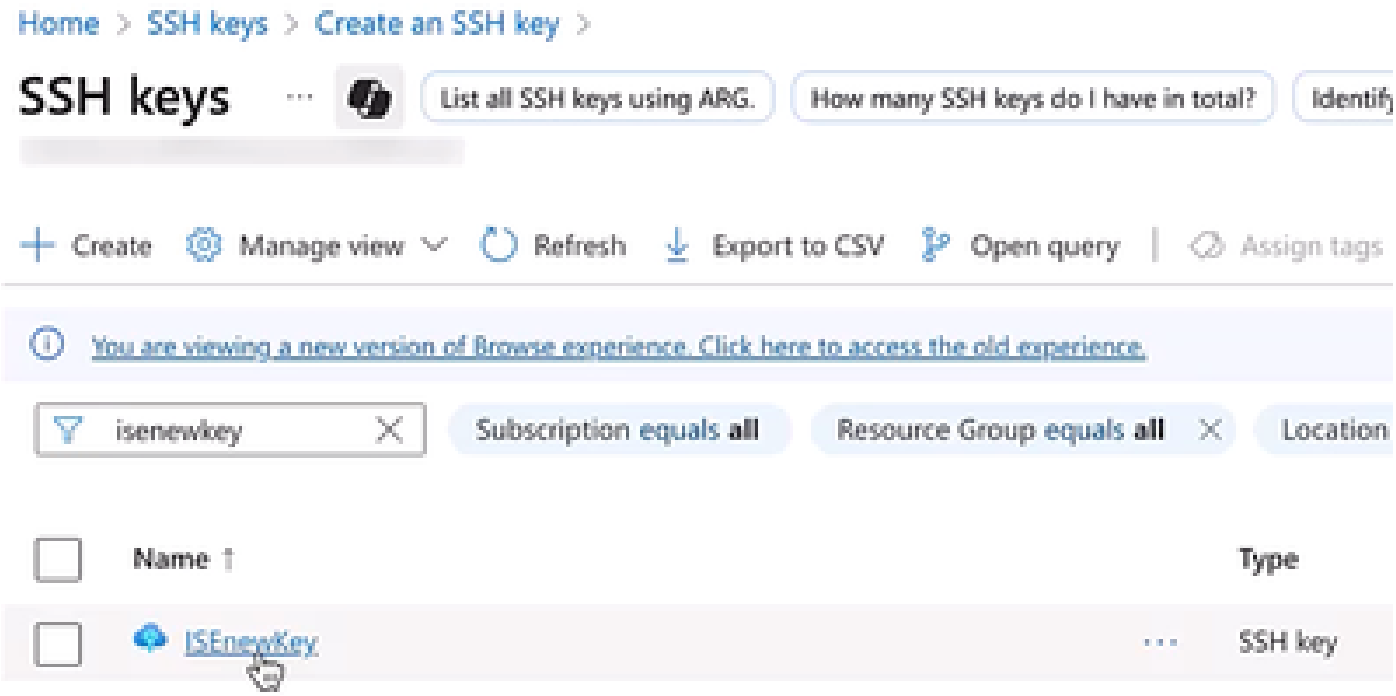
3. Wenn der Schlüssel erstellt wurde, wird ein neues Fenster angezeigt. Klicken Sie auf Privaten Schlüssel herunterladen und Ressource erstellen.


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

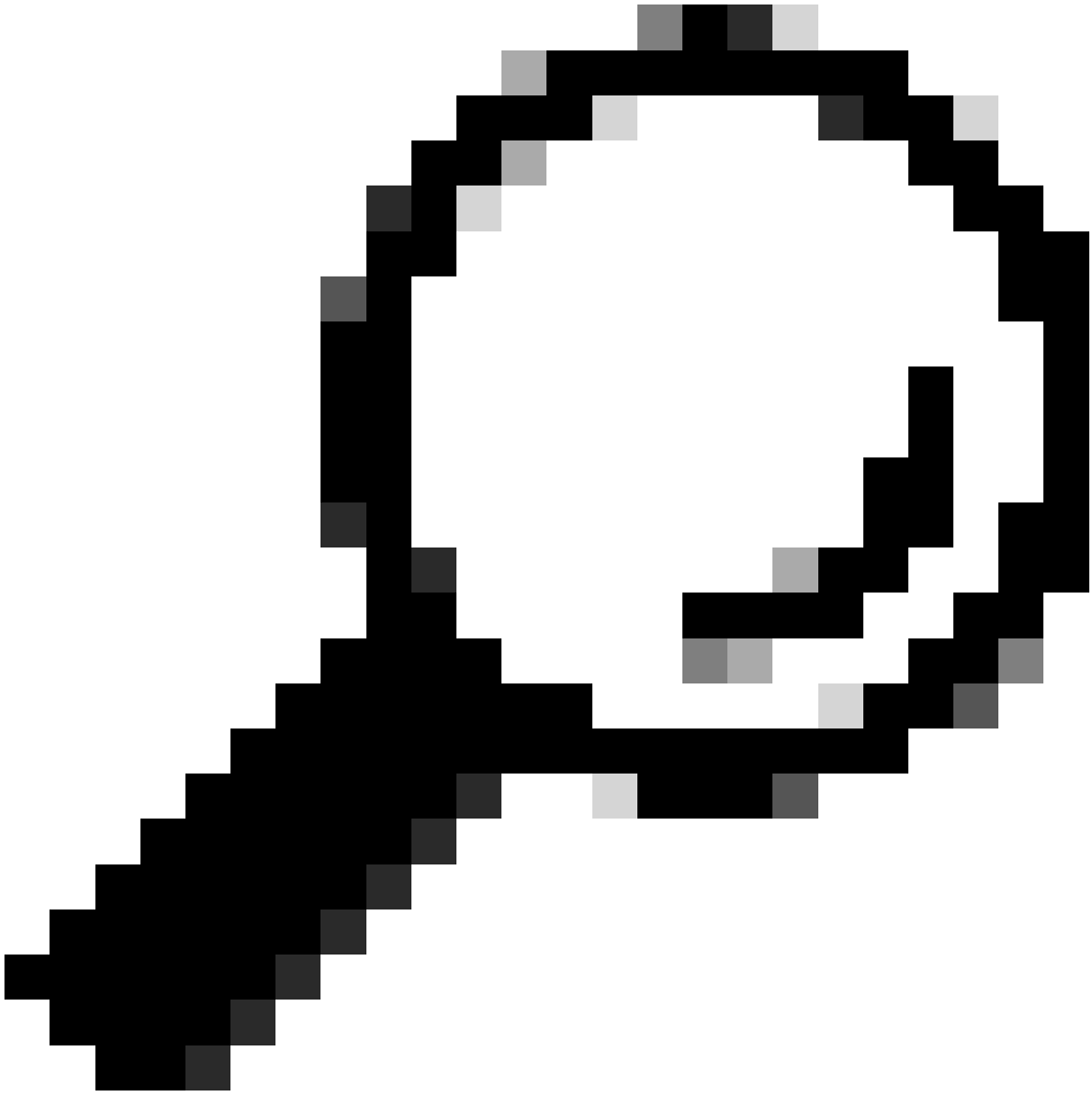


Vorsicht: Es ist wichtig, diesen privaten Schlüssel sicher zu halten, da dies der einzige Moment ist, in dem Azure Ihnen das Herunterladen dieses privaten Schlüssels ermöglicht. Azure speichert diesen privaten Schlüssel nicht und kann von keinem anderen Speicherort heruntergeladen werden.

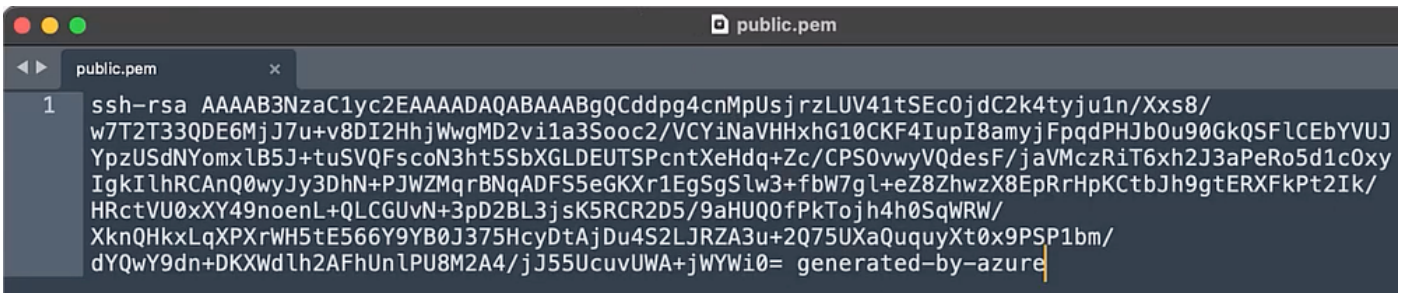
4. Navigieren Sie jetzt zurück zum SSH-Schlüsseldienst, suchen Sie nach dem neu erstellten Schlüssel, und klicken Sie darauf, um dessen Übersicht anzuzeigen.



5. In der Übersicht des Schlüssels wird der öffentliche Schlüssel angezeigt. Kopieren Sie diesen Text und fügen Sie ihn in einen Texteditor ein, sodass Sie ihn als lokale Datei mit der Erweiterung .pem speichern können. In diesem Handbuch wird die Datei als public.pem gespeichert.

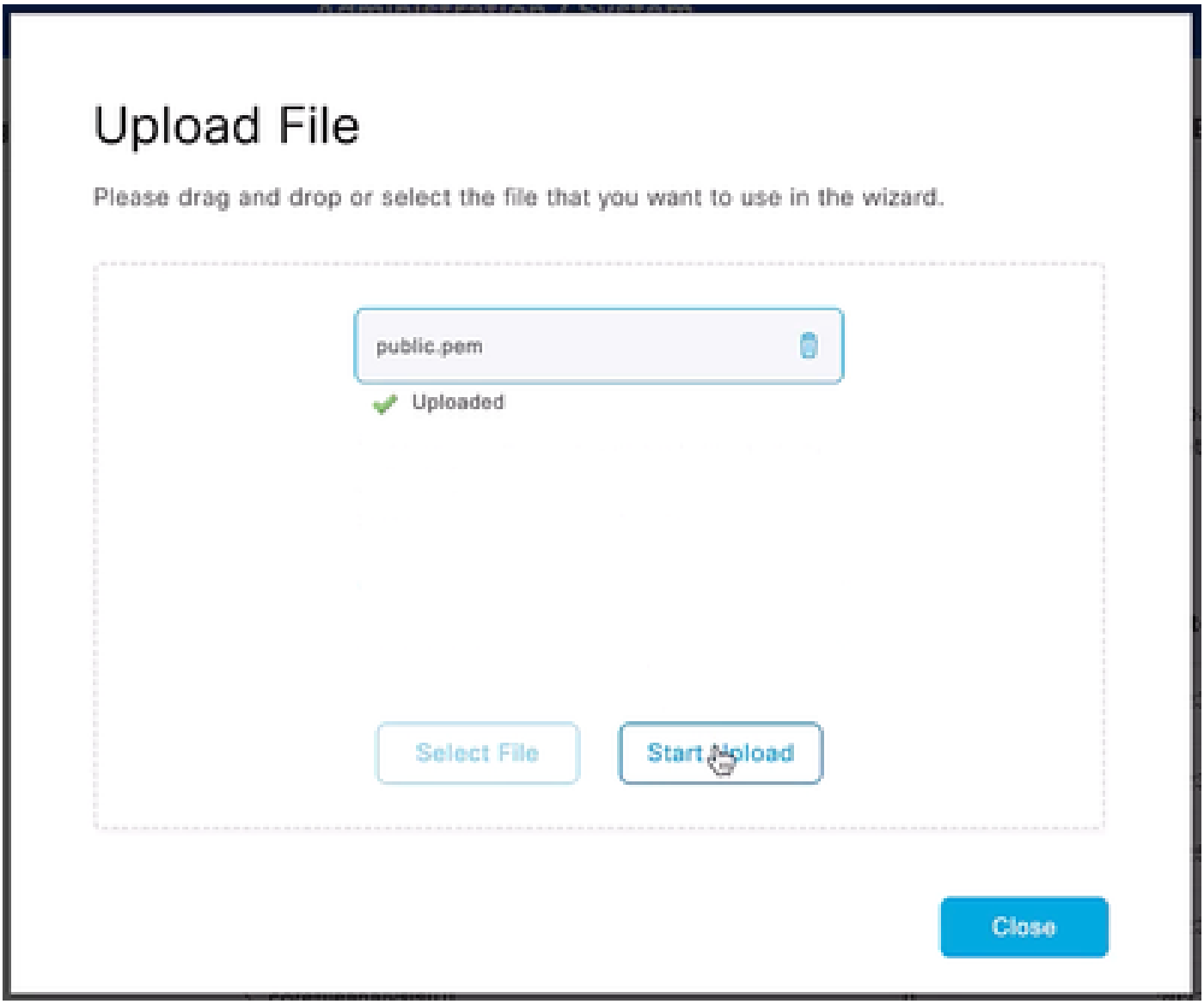


Tipp: Klicken Sie auf die Schaltfläche In Zwischenablage kopieren, um die Zeichenfolge des öffentlichen Schlüssels zu kopieren.

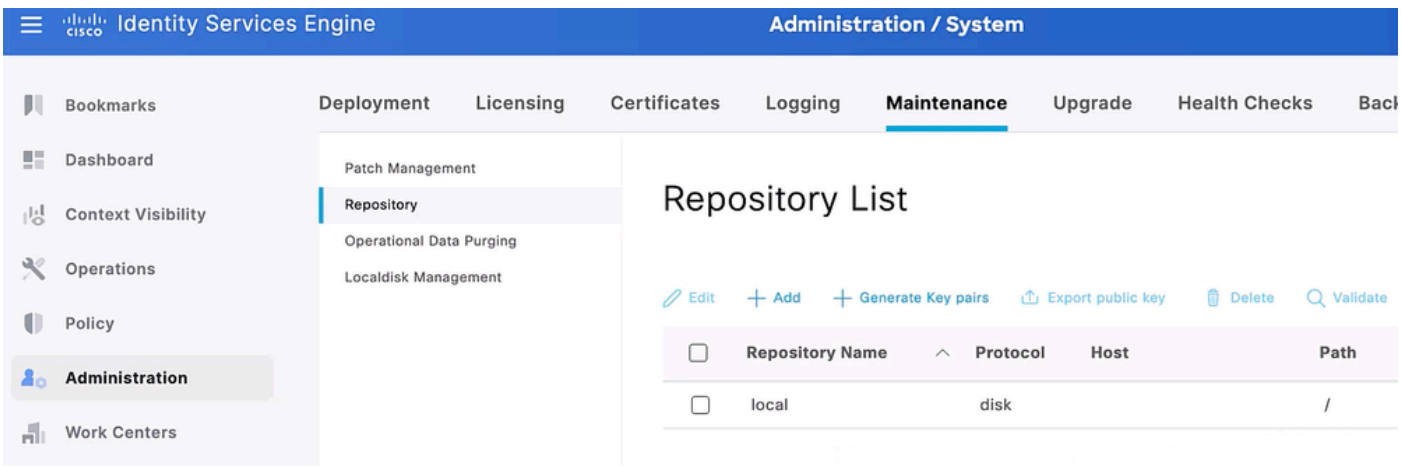


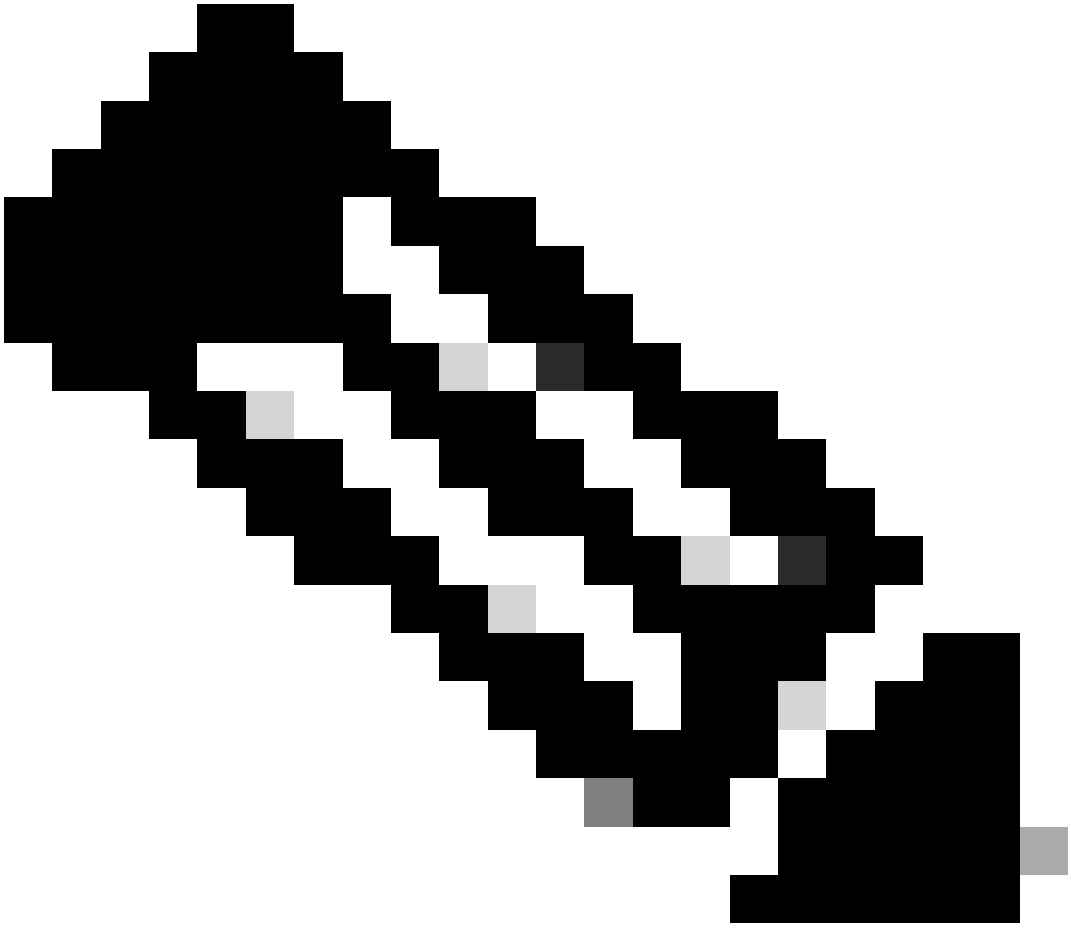
6. Laden Sie diesen öffentlichen Schlüssel auf die lokale ISE-Festplatte hoch. Navigieren Sie dazu zu ISE > Administration > System > Maintenance > Local Disk Management. Klicken Sie auf Ihren ISE-Hostnamen, dann auf Hochladen und dann auf Datei auswählen, suchen

Sie nach dem öffentlichen Schlüssel auf Ihrem lokalen Computer, und wählen Sie ihn aus. Klicken Sie abschließend auf Upload starten .



7. Erstellen Sie ein Repository, das auf die lokale ISE-Festplatte verweist, damit Sie damit den öffentlichen Schlüssel installieren können. In diesem Beispiel wird unser Repository als lokal bezeichnet.

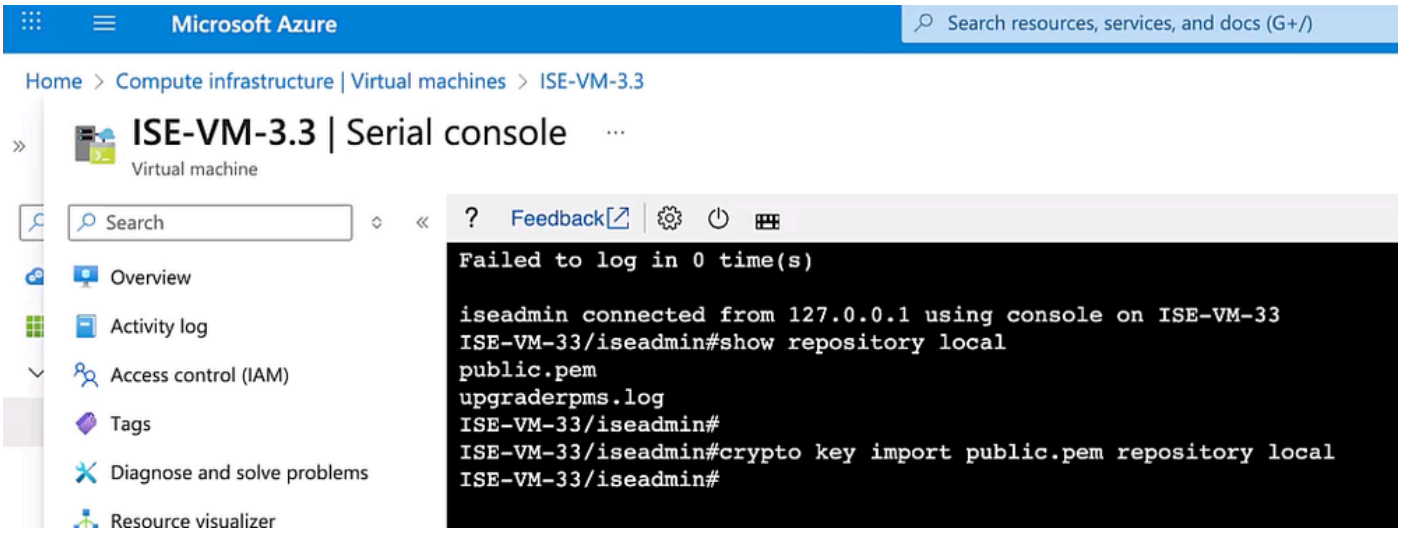




Anmerkung: Wenn Sie die Public-Key-Datei in ein anderes Repository hochladen möchten, das bereits auf der ISE erstellt wurde, muss es sich nicht um eine lokale Festplatte handeln.

8. Melden Sie sich von Azure aus bei der seriellen ISE-Konsole an, und verwenden Sie den Benutzernamen, für den Sie den SSH-Schlüssel zurücksetzen möchten.

9. Stellen Sie sicher, dass sich der öffentliche Schlüssel (.pem-Datei) im Repository befindet, und installieren Sie den Schlüssel mit dem Befehl crypto key import { name of the public key file } repository { name of the repository }.



Überprüfung

Um SSH mit den neuen Schlüsselpaaren in die ISE zu integrieren, müssen Sie bei der Anmeldung den privaten Schlüssel als Identifizierung verwenden.

1. Weisen Sie dem privaten Schlüssel (dem in Schritt 3 heruntergeladenen Schlüssel) die entsprechenden Berechtigungen zu.

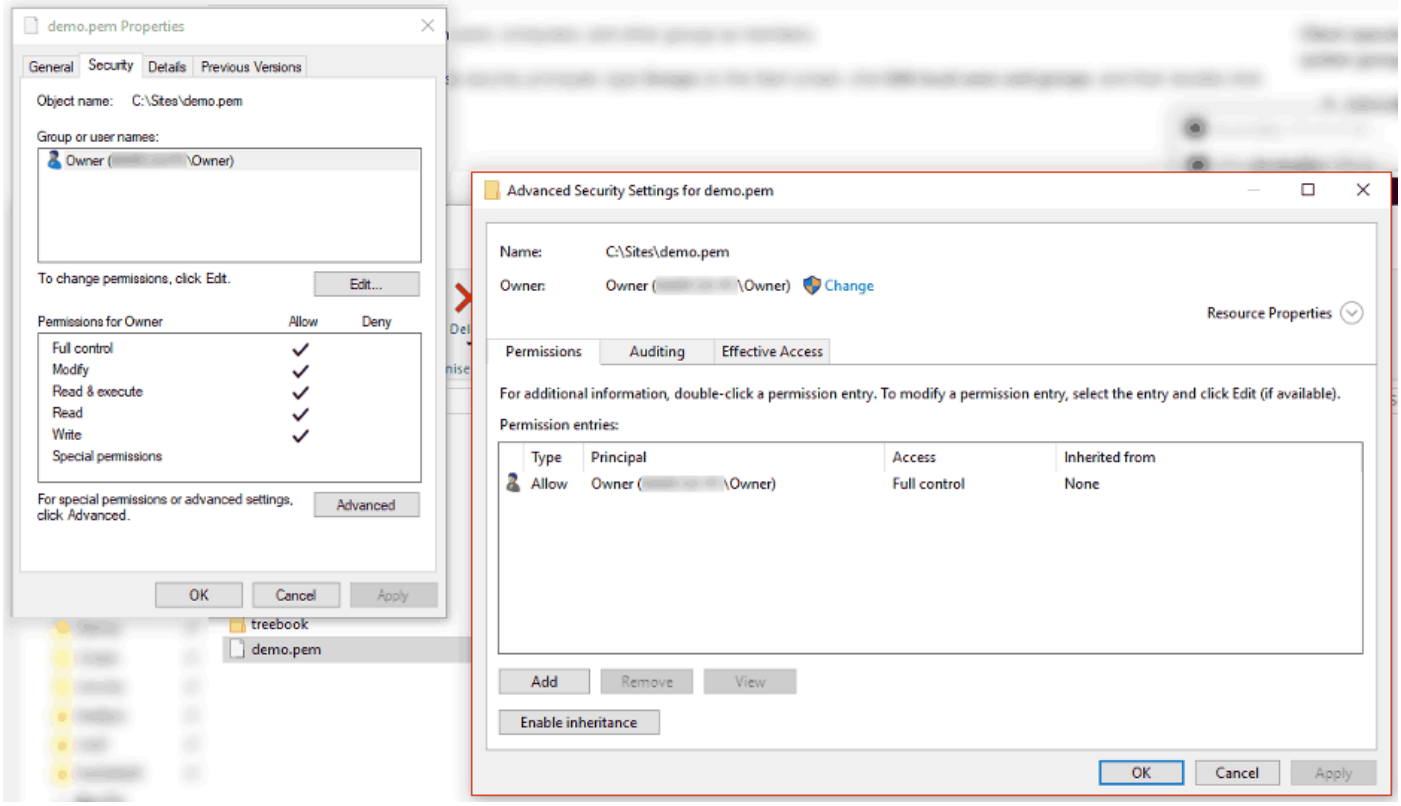
Vom MacOS-Terminal:

chmod 600 { private Schlüsseldatei }

Von Windows:

Suchen Sie die Datei im Windows-Explorer, klicken Sie mit der rechten Maustaste darauf, und wählen Sie dann Eigenschaften aus. Navigieren Sie zur Registerkarte Sicherheit, und klicken Sie auf Erweitert.

Ändern Sie den Besitzer zu Ihnen, deaktivieren Sie die Vererbung und löschen Sie alle Berechtigungen. Gewähren Sie sich dann die volle Kontrolle, und speichern Sie die Berechtigungen.



2. SSH in die ISE mithilfe des neuen privaten Schlüssels, des ISE-Benutzernamens und der ISE-IP-Adresse oder des FQDN.

Vom MacOS-Terminal:

ssh -I { private Schlüsseldatei } { Benutzername }@{ ISE IP or FQDN }

Von Windows CMD:

ssh -i "{ private Schlüsseldatei }" { Benutzername }@{ ISE IP or FQDN }

Fehlerbehebung

- Stellen Sie sicher, dass Sie den vollständigen Text der Datei mit dem öffentlichen Schlüssel in die PEM-Datei kopieren.
- Stellen Sie sicher, dass das Repository die Datei mit dem öffentlichen Schlüssel enthält.
- Wenn der Befehl crypto den öffentlichen Schlüssel nicht auf der ISE installiert, erstellen Sie ein Ticket beim Cisco TAC, damit der Schlüssel manuell vom Root installiert werden kann. Allgemeiner Fehler bei diesem Vorgang: "% Fehler: Autorisierte Schlüsseldatei konnte nicht aktualisiert werden."

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.