Konfigurieren von ISE SFTP mit zertifikatbasierter Authentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Linux-Server mit CentOS-Distribution als SFTP-Server (Secure File Transfer Protocol) mit PKI-Authentifizierung (Public Key Infrastructure) für Identity Services Engine (ISE) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Allgemeine ISE-Kenntnisse
- ISE-Repository-Konfiguration
- Allgemeine Linux-Kenntnisse

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE 2.2
- ISE 2.4
- ISE 2.6

- ISE 2.7
- ISE 3.0
- CentOS Linux Release 8.2.2004 (Core)

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 potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Um die Sicherheit für Dateiübertragungen durchzusetzen, kann die ISE über PKI-Zertifikate über SFTP authentifizieren, um einen sichereren Zugriff auf Repositorydateien zu gewährleisten.

Konfiguration

1. CentOS-Server konfigurieren

1.1 Erstellen Sie ein Verzeichnis als Stammbenutzer.

```
mkdir -p /cisco/engineer
```

1.2. Erstellen Sie eine Benutzergruppe.

```
groupadd tac
```

1.3. Mit diesem Befehl wird der Benutzer dem Hauptverzeichnis (Dateien) hinzugefügt, und der Benutzer gehört zu den **Technikern** der Gruppe.

```
useradd -d /cisco/engineer -s /sbin/nologin engineer
usermod -aG tac engineer
```

> **Hinweis:** Der **/sbin/nologin-**Teil des Befehls zeigt an, dass der Benutzer sich nicht über Secure Shell (SSH) anmelden kann.

1.4. Fahren Sie mit der Erstellung des Verzeichnisses zum Hochladen der Dateien fort.

```
mkdir -p /cisco/engineer/repo
```

1.4.1 Berechtigungen für die Verzeichnisdateien festlegen.

```
chown -R engineer:tac /cisco/engineer/repo
find /cisco/engineer/repo -type d -exec chmod 2775 {} \+
find /cisco/engineer/repo -type f -exec chmod 664 {} \+
```

1.5. Erstellen Sie das Verzeichnis und die Datei, in der der CentOS-Server die Prüfung auf Zertifikate durchführt.

Verzeichnis:

```
mkdir /cisco/engineer/.ssh
chown engineer:engineer /cisco/engineer/.ssh
chmod 700 /cisco/engineer/.ssh
```

Datei:

```
touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
```

1.6. Erstellen Sie die Anmeldeberechtigungen in der Systemdatei **sshd_config**.

Um die Datei zu bearbeiten, können Sie das **vim** Linux-Tool mit diesem Befehl verwenden.

```
vim /etc/ssh/sshd_config
```

1.6.1 Fügen Sie die unten angegebenen Zeilen hinzu.

```
#Subsystem sftp /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
Match Group tac
ChrootDirectory %h
X11Forwarding no
AllowTCPForwarding no
ForceCommand internal-sftp
```

1.7. Führen Sie den Befehl aus, um die Systemdateisyntaxis **sshd_config** zu überprüfen.

```
sshd -t
```

> **Hinweis:** Keine Ausgabe bedeutet, dass die Syntax der Datei korrekt ist.

1.8. Starten Sie den SSH-Dienst neu.

```
systemctl restart sshd
```

> **Hinweis:** Einige Linux-Server haben **selinux** Durchsetzung, um diesen Parameter zu bestätigen, können Sie den **getenforce-**Befehl verwenden. Wenn der **Durchsetzungsmodus aktiviert** ist, ändern Sie ihn als Empfehlung in **den Genehmigungsmodus.**

1.9. (optional) Bearbeiten Sie die Datei **semanage.conf**, um die Durchsetzung auf permissive festzulegen.

```
vim /etc/selinux/semanage.conf
```

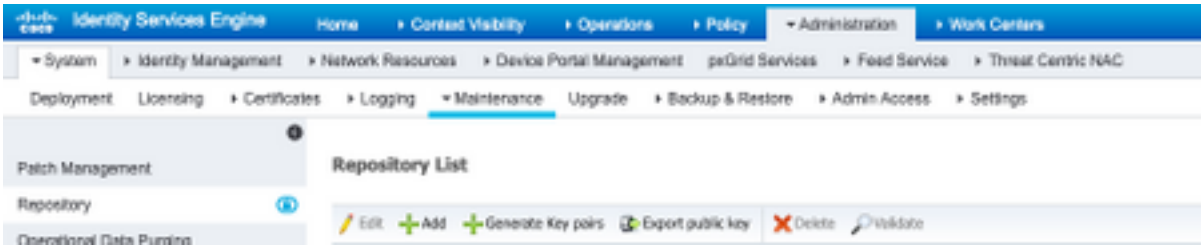
Fügen Sie den Befehl **setforce0 hinzu.**

```
setenforce0
```

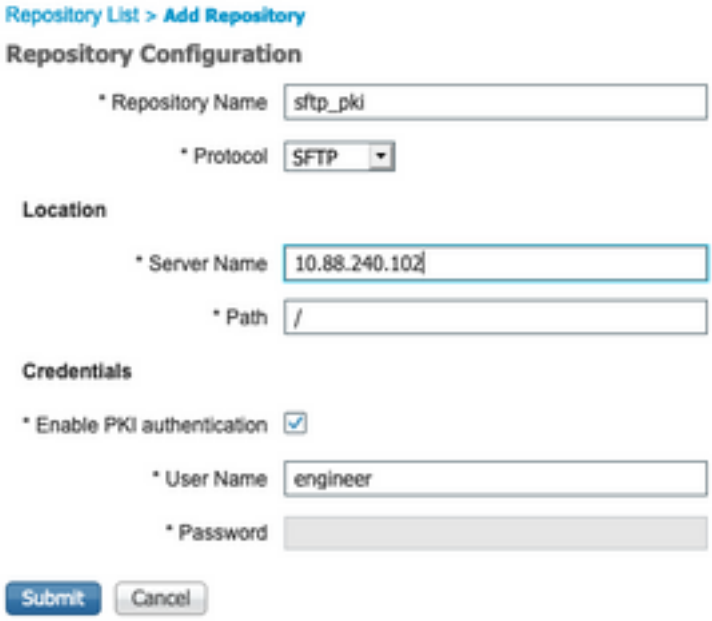
2. ISE-Repository konfigurieren

2.1. Setzen Sie das Repository über die grafische Benutzeroberfläche (GUI) der ISE ein.

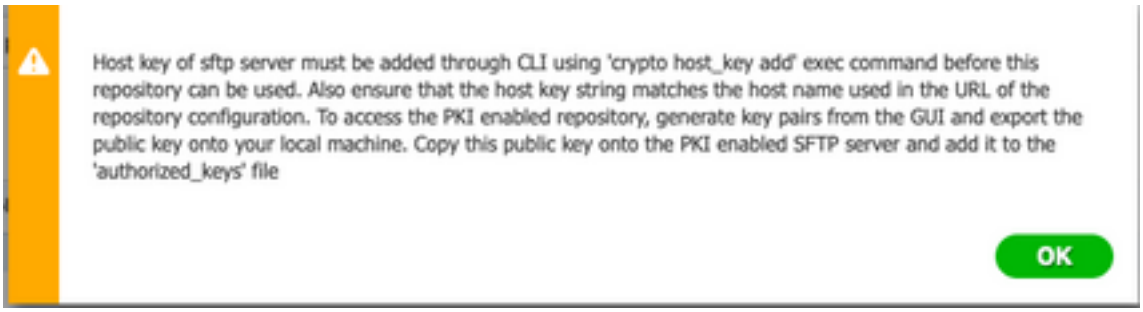
Navigieren Sie zu **Administration > System Maintenance > Repository > Add**



2.2. Geben Sie die richtige Konfiguration für Ihr Repository ein.



Hinweis: Wenn Sie Zugriff auf das Repo-Verzeichnis anstelle des Root-Verzeichnisses des Engineers benötigen, muss der Zielpfad /repo/ lauten.

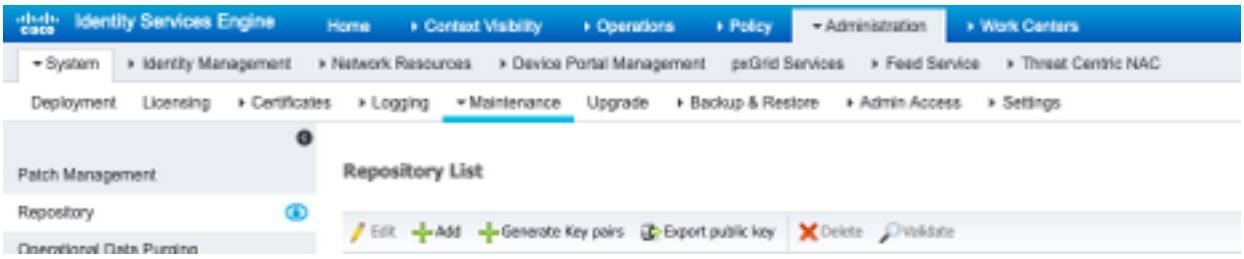


3. Generieren von Schlüsselpaaren auf dem ISE-Server

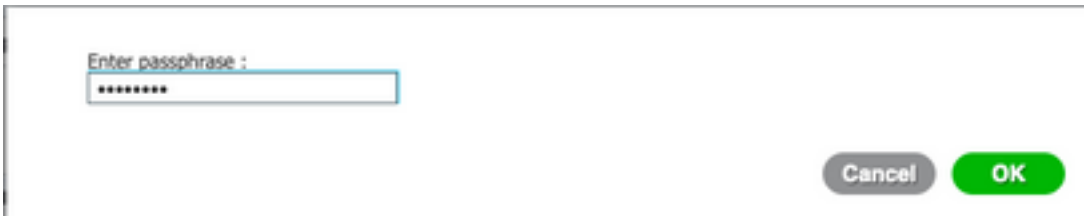
3.1. ISE-Benutzeroberfläche

Navigieren Sie zu **Administration>System Maintenance>Repository>Generate key pair** (**Schlüsselpaare generieren**), wie im Bild gezeigt.

Hinweis: Sie müssen Schlüsselpaare über die ISE-GUI und die Befehlszeilenschnittstelle (CLI) generieren, um vollständigen bidirektionalen Zugriff auf das Repository zu haben.



3.1.1. Geben Sie eine Passphrase ein. Dies ist erforderlich, um das Schlüsselpaar zu schützen.

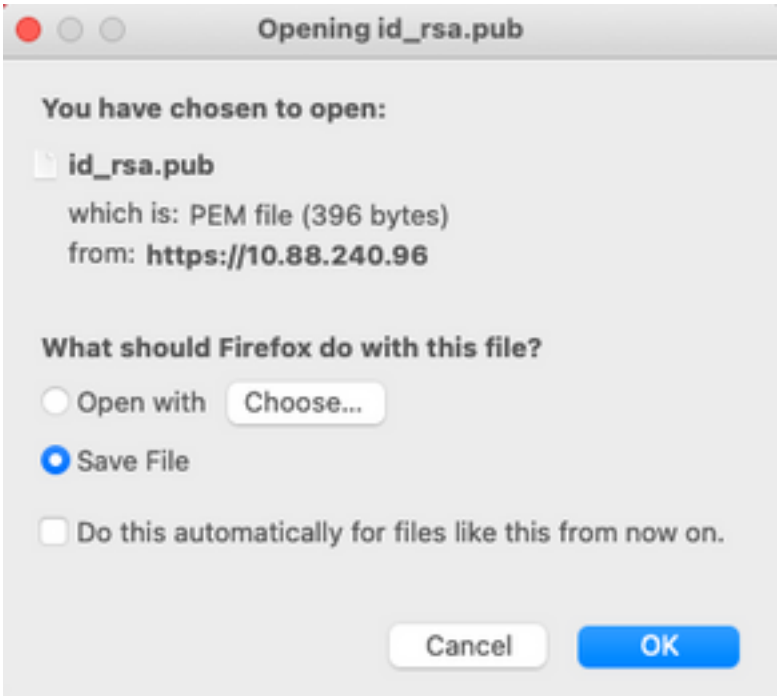


Hinweis: Generieren Sie zuerst die Schlüsselpaare, bevor die öffentlichen Schlüssel exportiert werden.

3.1.2. Exportieren Sie den öffentlichen Schlüssel weiter.

Navigieren Sie zu **Administration > System Maintenance > Repository > Export public key (Verwaltung > Systemwartung > Repository > Öffentlichen Schlüssel exportieren).**

Wählen Sie **Öffentlichen Schlüssel exportieren aus**. Eine Datei wird mit dem Namen **id_rsa.pub** generiert (stellen Sie sicher, dass diese für zukünftige Verweise gespeichert wird).



3.2. ISE-CLI

3.2.1. Navigieren Sie zur CLI des Knotens, in dem Sie die Konfiguration des Repositorys beenden möchten.

Hinweis: Ab diesem Zeitpunkt sind die nächsten Schritte für jeden Knoten erforderlich, dem mithilfe der PKI-Authentifizierung der Zugriff auf das SFTP-Repository gewährt werden soll.

3.2.2. Führen Sie diesen Befehl aus, um die IP-Adresse des Linux-Servers der Systemdatei **host_key** hinzuzufügen.

```
crypto host_key add host <Linux server IP>
```

```
ise24htts/admin# crypto host_key add host 10.88.240.102
host key fingerprint added
# Host 10.88.240.102 found: line 2
10.88.240.102 RSA SHA256:sFA1b+NujB8NxIx4zhS/7Fj1hyHRkJlKyLhJCIteSpE
```

3.2.3. Generieren Sie einen öffentlichen CLI-Schlüssel.

```
crypto key generate rsa passphrase <passphrase>
```

```
ise24htts/admin# crypto key generate rsa passphrase admin123
```

3.2.4. Exportieren Sie die öffentlichen Schlüsseldateien mit diesem Befehl aus der CLI der ISE.

```
crypto key export <name of the file> repository <repository name>
```

Hinweis: Sie müssen über ein zuvor zugängliches Repository verfügen, in das Sie die Datei des öffentlichen Schlüssels exportieren können.

```
ise24htts/admin# crypto key export public repository FTP
```

4. Integration

4.1. Melden Sie sich beim CentOS-Server an.

Navigieren Sie zu dem Ordner, in dem Sie die Datei **authorized_key** zuvor konfiguriert haben.

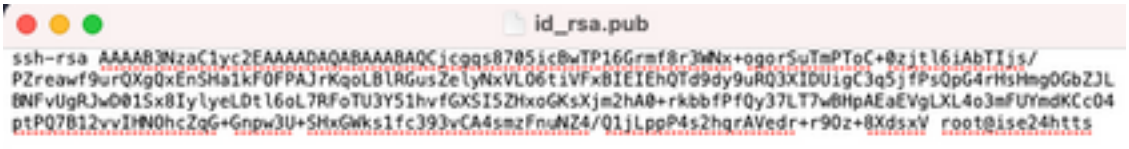
4.2. Bearbeiten Sie die autorisierte Schlüsseldatei.

Führen Sie den Befehl vim aus, um die Datei zu ändern.

```
vim /cisco/engineer/.ssh/authorized_keys
```

4.3. Kopieren Sie den in den Schritten **4** und **6** generierten Inhalt aus dem Abschnitt **Schlüsselpaare generieren,** und fügen Sie ihn ein.

Öffentlicher Schlüssel, der über die ISE-GUI generiert wird:



Öffentlicher Schlüssel, der von der ISE-CLI generiert wird:

Authorized_key-Datei auf dem Linux-Server:

4.4. Nachdem Sie die Tasten in die Datei eingefügt haben, drücken Sie ESC, fahren Sie fort, um das **wq!** um die Datei zu speichern.

Überprüfung

1. Führen Sie diesen Befehl vom Linux-Server als root aus.

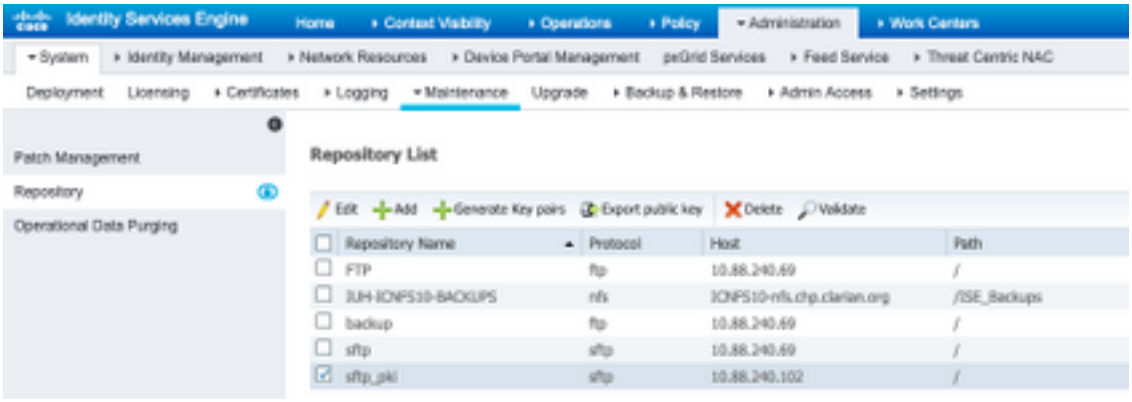
```
tail -f /var/log/secure
```

Die Ausgabe muss angezeigt werden, wie im Bild gezeigt.

2. Zur ISE-Verifizierung.

Navigieren Sie zu **Administration>System>Maintenance>Repository** in der GUI.

Wählen Sie das gewünschte Repository aus der **Repository-Liste aus** und wählen Sie **Validieren**.



In der unteren rechten Ecke des Bildschirms muss ein Popup-Fenster mit der Meldung **Server Response (Serverantwort)** angezeigt werden.

Führen Sie in der CLI den Befehl **show repo sftp_pki aus,** um die Schlüssel zu validieren.

```
ise24htts/admin# show repo sftp_pki
repo
```

Um die ISE weiter zu debuggen, führen Sie diesen Befehl in der CLI aus:

```
debug transfer 7
```

Die Ausgabe muss angezeigt werden, wie im Bild gezeigt:

```
ise24htts/admin# debug transfer 7
ise24htts/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] [admin]: sftp dir of repository sftp_pki requested
6 [16745]:[info] transfer: cars_xfer_util.c[2298] [admin]: resolved server to 10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[1027] [admin]: Running sftp command: 10.88.240.102 engineer *** /repo/ ls -l /repo/
6 [16745]:[info] transfer: sftp_handler.c[554] [admin]: DEBUG: local user: admin UID: 0 sftp_run_parent FD: 5 remote host: 10.88.240.102 remote user: engineer comma
nd: ls -l /repo/
7 [16747]:[debug] transfer: sftp_handler.c[268] [admin]: Executing SFTP command: 0 admin /usr/bin/sftp -oIdentityFile=/home/admin/.ssh/id_rsa -oUserKnownHostsFile=/
home/admin/.ssh/known_hosts -oPasswordAuthentication=no engineer@10.88.240.102
7 [16745]:[debug] transfer: sftp_handler.c[586] [admin]: fd is:5
7 [16745]:[debug] transfer: sftp_handler.c[461] [admin]: Found sftp prompt; No more data to read
7 [16745]:[debug] transfer: sftp_handler.c[917] [admin]: sftp parent status 0
7 [16745]:[debug] transfer: cars_xfer_util.c[2315] [admin]: ssh_list xfer succeeded
% Repository is empty
```

Zugehörige Informationen

https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_01011.html