# Konfigurieren von ISE SFTP mit zertifikatbasierter Authentifizierung

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfiguration 1. CentOS-Server konfigurieren 2. ISE-Repository konfigurieren 3. Generieren von Schlüsselpaaren auf dem ISE-Server 3.1. ISE-Benutzeroberfläche 3.2. ISE-CLI 4. Integration Überprüfung Zugehörige Informationen

## 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

| -dudu Identity           | Services Engine       | Home + Cont      | at Visibility + Operation | s + Policy                             | + Administration  | Work Centers              |
|--------------------------|-----------------------|------------------|---------------------------|--|-------------------|---------------------------|
| ≠ System ►               | identity Management   | Network Resource | s > Device Portal Manage  | iment pxGrid Ser                       | rvices > Feed Ser | vice > Threat Centric NAC |
| Deployment.              | Licensing + Certifica | tes + Logging    | Maintenance Upgrade       | <ul> <li>Backup &amp; Resto</li> </ul> | re + Admin Accer  | is → Settings             |
|                          | 0                     |                  |                           |  |                   |                           |
| Palch Management         |                       | Repository L     | ist                       |  |                   |                           |
| Repository               | 9                     | 100 1100         | L deserts for only 100    | Constantinion .                        | Anna Contan       |                           |
| Onerational Data Purging |                       | Add - Add        |                           | Export public key                      | Cooke Divestation |                           |

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

| Repository List > Add Reposito | ory           |  |  |  |
|--------------------------------|---------------|--|--|--|
| Repository Configuration       |               |  |  |  |
| * Repository Name              | sftp_pki      |  |  |  |
| * Protocol                     | SFTP -        |  |  |  |
| Location                       |               |  |  |  |
| * Server Name                  | 10.88.240.102 |  |  |  |
| * Path                         | 1             |  |  |  |
| Credentials                    |               |  |  |  |
| * Enable PKI authentication    |               |  |  |  |
| * User Name                    | engineer      |  |  |  |
| * Password                     |               |  |  |  |
| Submit Cancel                  |               |  |  |  |

**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.

| Identity Services E       | ngine          | ome + Context Visibility + Operations +       | Policy  Administration  Work Centers   |  |  |  |
|---------------------------|----------------|---|--|--|--|--|
| System       Identity Man | agement >      | ietwork Resources                             | prGrid Services                        |  |  |  |
| Deployment Licensing      | + Certificates | + Logging + Maintenance Upgrade + Back        | up & Restore + Admin Access + Settings |  |  |  |
|                           | 0              |   |  |  |  |  |
| Patch Management          |                | Repository List                               |  |  |  |  |
| Repository (1)            |                | 150 Last Louistic to only Observation         | Alekar Maine Online                    |  |  |  |
| Operational Data Puncing  |                | / con Trade To developer set pars & Export pu | and new Conter Provide                 |  |  |  |

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

| Enter passphrase : |        |    |
|--------------------|--------|----|
|                    | Cancel | ок |

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/7Fj1hyHRkJlKyLhJClteSpE

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:

id\_rsa.pub ssh-rsa\_AAAAB3NzaC1yc2EAAAADAQABAAABAQCjcgqs8705icBwTP16Grmf8r3WNx+ogorSwTmPToC+0zjtl6iAbTIjs/ PZreawf9wrQXgQxEn5Ha1kF0FPAJrKqoLB1RGwsZelyNxVL06t1VFx81E1EhQTd9dy9wRQ3XIDUigC3q5jfPs0p64rHsHmg0GbZ3L 8NFvUgR3wD01Sx8IylyeLDt16oL7RFoTU3Y51hvfGXSIS2HxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04 ptPQ7B12vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnwNZ4/Q1jLppP4s2hgrAVedr+r90z+8XdsxV\_root0se24htts

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



public

ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06s0+gSykTRrGfdMryIiitCMBs0bGsSyc9S8VKpLyyocsIvco4/ vF/pSHoTEIR3wrZTL1vCIUrGnngdQv4+8YnIbJ/f8EgZnX0+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/ HAyXQ/a9YR21L2906pjKSWyuTkbUxWvN9hx/ SESzpJ4pFr9opg+UaTNX0yYuuj328FGEFdKuFBSujAokP0nJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0cj6vMaV0L7G2dDI4NZHn7llpptqJFYAb65QB admingise24htts

Authorized\_key-Datei auf dem Linux-Server:

ish-rs: ALAUSNicativeZEAAAADAQBAAABAQGioqusTeSieBreisieBreisioBreisieBre

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.

```
[[root@localhost =]# tail =f /var/log/secure
Apr 12 21:37:53 localhost sshd[668112]: Accepted publickey for root from 10.24.140.234 port 61159 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaWFUue
GbKEW1EkcaeXU
Apr 12 21:37:53 localhost systemd[668117]: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668120]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668120]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaWFUue
GbKEW1EkcaeXU
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost systemd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: pam_unix(systemd-user:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: pam_unix(sstemd-user:session): session opened for user engineer by (uid=0)
```

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.

| dentity Services Engli      | NO Home +             | Context Visibility + Opr     | rations + Policy             | Administration     W        | ork Centers        |
|-----------------------------|-----------------------|------------------------------|------------------------------|-----------------------------|--------------------|
| + System + Identity Manager | ment > Network Re     | sources > Device Portal &    | lanagement petüris           | Services > Feed Service     | Threat Centric NAC |
| Deployment Licensing + 0    | Certificates + Loggin | ng + Maintenance Upgr        | ade 🔸 Backup & R             | estore + Admin Access +     | Settings           |
|                             | •                     |                              |                              |                             |                    |
| Patch Management            | Reposit               | ory List                     |                              |                             |                    |
| Repository                  | (i)                   | Lass Lances in solu          | (h for a bit in              | Marine Caster               |                    |
| Operational Data Purging    | / DDR -               | - Add - University Key point | Record by the set            | Kookee Prostate             |                    |
|                             | Repo                  | sitory Name                  | <ul> <li>Protocol</li> </ul> | Host                        | Path               |
|                             | C FTP                 |                              | fip .                        | 10.88.240.69                | /                  |
|                             | 204                   | IONF510-BACKUPS              | nfs                          | ICNFS10-rds.chp.clarian.org | /ISE_Backups       |
|                             | back                  | up                           | fo.                          | 10.88.240.69                | 1                  |
|                             | □ sftp                |                              | sto                          | 10.88.240.69                | 1                  |
|                             | 🖬 sftp.               | pki                          | sto                          | 10.88.240.102               | 1                  |

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:



## 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