Configurazione di ISE SFTP con autenticazione basata su certificato

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[1. Configurare il server CentOS](#)
[2. Configurazione del repository ISE](#)
[3. Generare una coppia di chiavi sul server ISE](#)
[3.1. INTERFACCIA GRAFICA DI ISE](#)
[3.2. ISE CLI](#)
[4. Integrazione](#)
[Verifica](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un server Linux con distribuzione CentOS come server SFTP (Secure File Transfer Protocol) con autenticazione PKI (Public Key Infrastructure) per Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze generali di ISE
- Configurazione del repository ISE
- Conoscenze generali di base di Linux

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE 2.2
- ISE 2.4
- ISE 2.6

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per garantire la sicurezza dei trasferimenti di file, ISE può eseguire l'autenticazione tramite i certificati PKI tramite SFTP per garantire un modo più sicuro di accedere ai file dei repository.

Configurazione

1. Configurare il server CentOS

1.1 Creare una directory come utente root.

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

1.2. Creare un gruppo di utenti.

```
groupadd tac
```

1.3. Questo comando aggiunge l'utente alla directory principale (file) e specifica che l'utente appartiene ai **tecnici** del gruppo**.**

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

> **Nota:** La parte **/sbin/nologin** del comando indica che l'utente non sarà in grado di accedere tramite Secure Shell (SSH).

1.4. Creare la directory per caricare i file.

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

1.4.1 Impostare le autorizzazioni per i file di directory.

```
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. Creare la directory e il file in cui il server CentOS esegue il controllo dei certificati.

Directory:

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

File:

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

1.6. Creare le autorizzazioni di accesso nel file di sistema **sshd_config**.

Per modificare il file, è possibile usare lo strumento **vim** Linux con questo comando.

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

1.6.1 Aggiungere le righe indicate di seguito.

```
#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. Eseguire il comando per verificare la sintassi del file di sistema **sshd_config**.

```
sshd -t
```

> **Nota:** Nessun output indica che la sintassi del file è corretta.

1.8. Procedere al riavvio del servizio SSH.

```
systemctl restart sshd
```

> **Nota:** Alcuni server Linux dispongono di imposizione **selinux**. Per confermare questo parametro, è possibile utilizzare il comando **getenforce**. Se è attiva la modalità di **imposizione**, è consigliabile modificarla in **permissiva.**

1.9. (facoltativo) Modificare il file **semanage.conf** per impostare l'imposizione su permissiva.

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

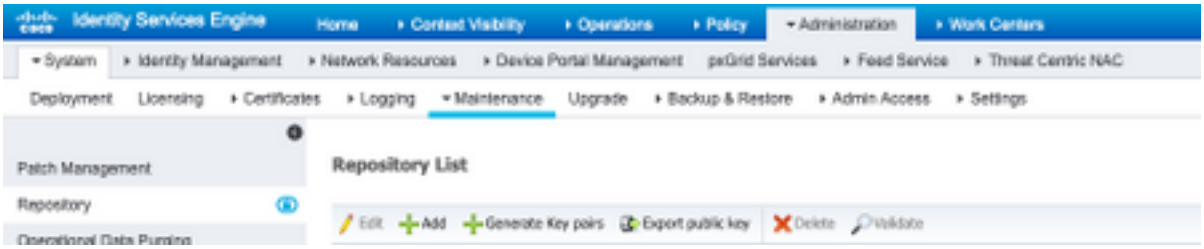
Aggiungere il comando **setenforce0.**

```
setenforce0
```

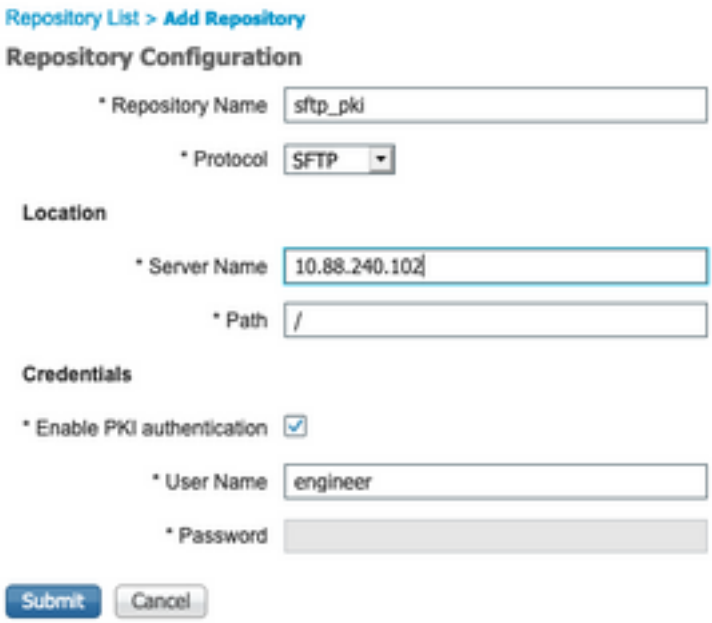
2. Configurazione del repository ISE

2.1. Continuare ad aggiungere il repository attraverso l'interfaccia grafica utente (GUI) di ISE.

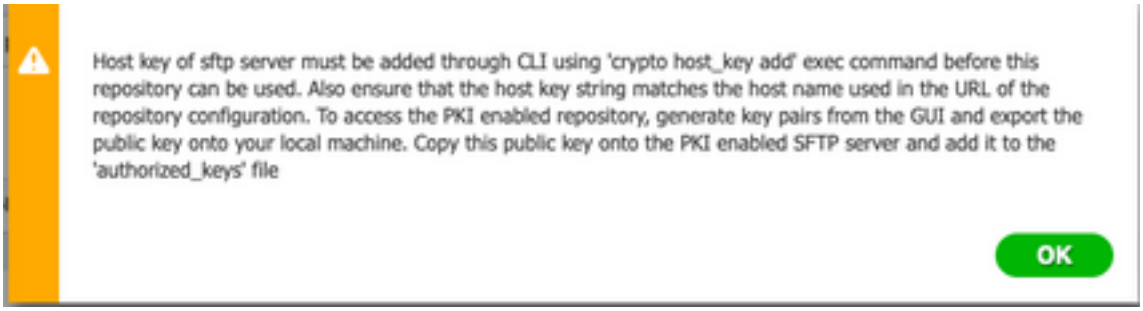
Selezionare **Amministrazione>Manutenzione sistema>Repository>Aggiungi**



2.2. Inserire la configurazione corretta per il repository.



Nota: Se è necessario accedere alla directory del repository anziché alla directory principale di engineer, il percorso di destinazione deve essere /repo/.

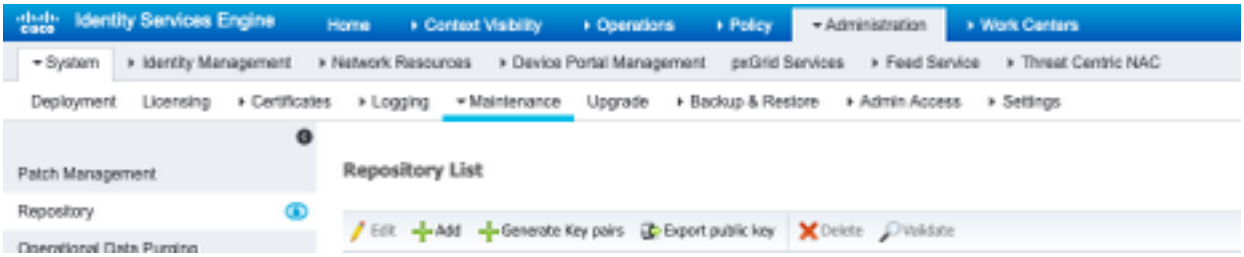


3. Generare una coppia di chiavi sul server ISE

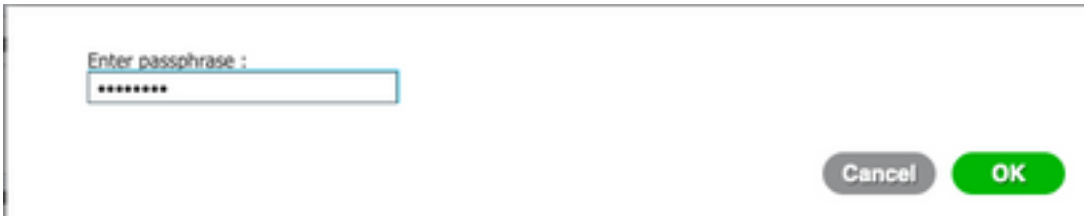
3.1. INTERFACCIA GRAFICA DI ISE

Passare a **Amministrazione>Manutenzione sistema>Repository>Genera coppie di chiavi**, come mostrato nell'immagine.

Nota: Per avere accesso bidirezionale completo al repository, è necessario generare una coppia di chiavi dalla GUI ISE e dall'interfaccia della riga di comando (CLI).



3.1.1. Inserire una passphrase. Questa operazione è necessaria per proteggere la coppia di chiavi.

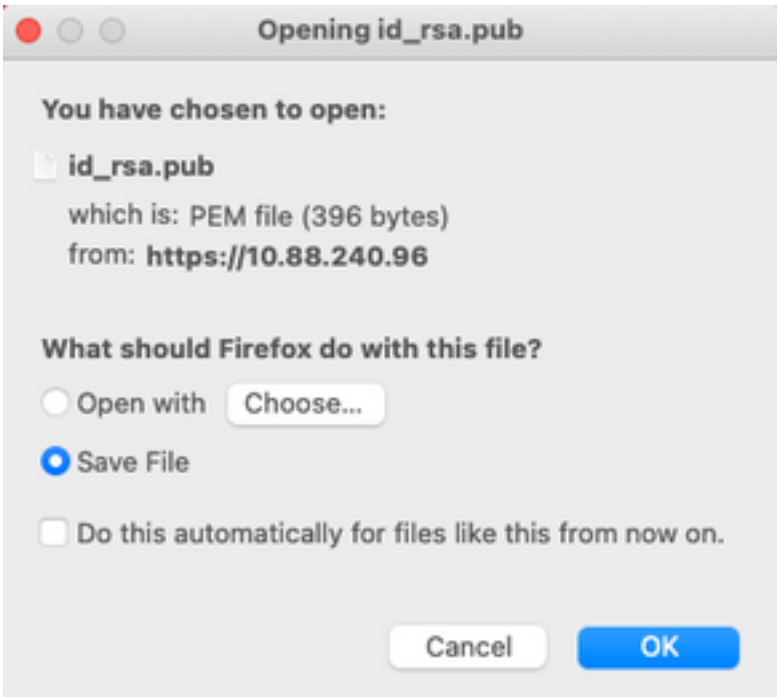


Nota: Generare le coppie di chiavi prima di esportare le chiavi pubbliche.

3.1.2. Procedere all'esportazione della chiave pubblica.

Passare a **Amministrazione>Manutenzione sistema>Repository>Esporta chiave pubblica.**

Selezionare **Esporta chiave pubblica**. Viene generato un file con il nome **id_rsa.pub** (assicuratevi che venga salvato per riferimenti futuri).



3.2. ISE CLI

3.2.1. Passare alla CLI del nodo in cui si desidera completare la configurazione del repository.

Nota: Da questo punto in poi, i passaggi successivi sono necessari su ogni nodo che si desidera consentire l'accesso al repository SFTP con l'uso dell'autenticazione PKI.

3.2.2. Eseguire questo comando per aggiungere l'indirizzo IP del server Linux al file di sistema **host_key**.

```
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. Generare la chiave CLI pubblica.

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

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

3.2.4. Esportare i file delle chiavi pubbliche dalla CLI di ISE con questo comando.

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

> **Nota:** È necessario disporre di un repository accessibile in precedenza in cui è possibile esportare il file della chiave pubblica.

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

4. Integrazione

4.1. Accedere al server CentOS.

Passare alla cartella in cui è stato precedentemente configurato il file **authorized_key**.

4.2. Modificare il file di chiave autorizzato.

Eseguire il comando vim per modificare il file.

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

4.3. Copiare e incollare il contenuto generato nei passaggi **4** e **6** dalla sezione **Generate key pair**.

Chiave pubblica generata dall'interfaccia utente di ISE:

Chiave pubblica generata dalla CLI di ISE:

File **Authorized_key** sul server Linux:

4.4. Dopo aver incollato i tasti sul file, premere ESC, procedere per eseguire il comando **wq!** per salvare il file.

Verifica

1. Dal server Linux eseguire questo comando come root.

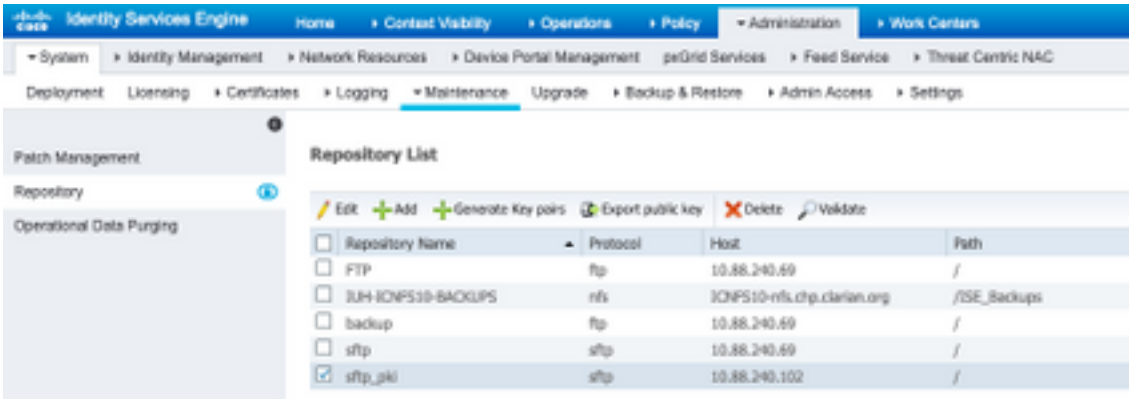
```
tail -f /var/log/secure
```

L'output deve essere visualizzato, come mostrato nell'immagine.

2. Per la verifica ISE.

Selezionare **Amministrazione>Sistema>Manutenzione>Repository** sulla GUI.

Selezionare il repository desiderato dall'**Elenco repository** e selezionare **Convalida**.



Ènecessario visualizzare un popup che indica la **risposta del server** nell'angolo inferiore destro dello schermo.

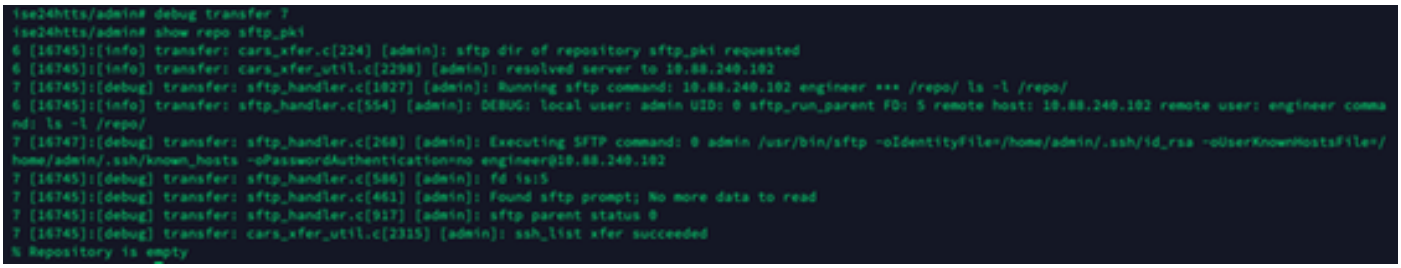
Dalla CLI, eseguire il comando **show repo sftp_pki** per convalidare le chiavi.

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

Per eseguire ancora il debug ISE, eseguire questo comando sulla CLI:

```
debug transfer 7
```

L'output deve essere visualizzato, come mostrato nell'immagine:



Informazioni correlate

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