# 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

-dude- Identity Services Engl	ine i	Home + Context Visib	illy + Operations	+ Policy	· Administration	Work Centers
System      identity Manage	ament >	Network Resources + I	Sevice Portal Manageme	nt petGrid Se	rvices > Feed Ser	vice > Threat Centric NAC
Deployment Licensing + (	Certificates	s → Logging - Mainte	nance Upgrade +	Backup & Resto	ore + Admin Accer	ss → Settings
	0					
Patch Management		Repository List				
Repository	۲	100 144 14	and the sale of the	at a difference of	Contra	
Onecotional Data Pursing			uence well house of othe	in point, key	Conter Contendado	

2.2. Inserire la configurazione corretta per il repository.

Repository List > Add Reposite	ory
Repository Configuration	on
* 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	

**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).

Identity Services En	gine :	Home + Context Visibility + Operations + Policy - Administration + Work Centers		
⇒ System     → Identity Mana	gement >	Network Resources -> Device Portal ManagementpxGrid Services -> Feed Service -> Threat Centric NAC		
Deployment Licensing	Certificates	Logging Maintenance Upgrade Backup & Restore Admin Access Settings		
	0			
Patch Management		Repository List		
Repository	۲	100 Latt L'annue farmin (h.Dantadirian Minist Oblight		
Operational Data Purging		Lear Linea Longeone web hous Recorder base web		

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).

• • •	Opening id_rsa.pub
You have cho	sen to open:
id_rsa.pub	
which is: PE	M file (396 bytes)
from: https	://10.88.240.96
What should	Firefox do with this file?
Open with	Choose
🔾 Save File	
Do this auto	omatically for files like this from now on.
	Cancel OK

## 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/7Fj1hyHRkJlKyLhJClteSpE

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:

id\_rsa.pub ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjcgqs8705icBwTP16Grmf8r3wNx+oqorSuTmPToC+0zjtl6iAbTIjs/ PZreawf9wrQXgQxEnSHa1kF0FPAJrKqoLB1RGusZelyNxVL06t1VFxBIEIEhQTd9dy9uRQ3XIDU1gC3q5jfPsQpG4rHsHmgOGbZ3L BNFvUgR3wD01Sx8IylyeLDt16oL7RFoTU3Y51hvfGXSI5ZHxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04 ptP07B12vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnuNZ4/Q1jLppP4s2hgrAVedr+r90z+8XdsxV root0ise24htts

Chiave pubblica generata dalla CLI di ISE:



public

ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06sQ+gSykTRrGfdMryIiitCWBs0bGs5yc9S8VKpLyyocsIvco4/ vF/pSHoTEIR3wrZTLlvCIUrGnngdQv4+8YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQ8086tknc40cmT/ HAyXQ/a9YRZ1L2906pjKSWyuTkbUxWvN9hx/ SE5zpJ4pFr9opg+UaTNXXQYTuuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0cj6vMaV0L7GzdDI4NZHn7LlpptqJFYAb65QB admingise24htts

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.

```
[[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
GbKEWIEkcaeXU
Apr 12 21:37:53 localhost systemd[668112]: 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[668201]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaW
FUueGbKEWIEkcaeXU
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(shd:session): session opened for user engineer by (uid=0)
```

2. Per la verifica ISE.

Selezionare Amministrazione>Sistema>Manutenzione>Repository sulla GUI.

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

-dude Identity Services Engli	10 Home +	Context Vaibility + Op	erations + Policy	- Administration + We	rk Centers
System + Identity Manager	ment > Network Res	ources + Device Portal M	lanagement petiri	d Services > Feed Service	Threat Centric NAC
Deployment Licensing + 0	Certificates + Logging	Maintenance Upg	rade 🔸 Backup & R	lestore + Admin Access +	Settings
	0				
Patch Management	Reposito	ry List			
Repository	<b>()</b>	And A descent for solution	( Charles Maria	Marian Californi	
Operational Data Purging	/ tot -	Add -Generate key pair	<ul> <li>Be extent brank wei</li> </ul>	Conte Diversione	
	Repos	itory Name	<ul> <li>Protocol</li> </ul>	Host	Path
	C FTP		fip .	10.88.240.69	/
	200-10	OVF510-BACKUPS	nfs	ICNFS10-rds.chp.clarian.org	/ISE_Backups
	backu	p	fo	10.88.240.69	/
	□ sftp		sto	10.88.240.69	1
	🗹 sftp.g	ki	sto	10.88.240.102	1

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.



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

debug transfer 7

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

isegunitsjaumina ueung transfer /
ise24htts/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] (admin): sftp dir of repository sftp_pki requested
6 [16745]:[inf0] transfer: cars_xfer_util.c[2208] [admin]: resolved server to 10.08.240.102
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
ndi la -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
N Repository is empty

# 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