# ISE SFTP configureren met op certificaten gebaseerde verificatie

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren 1. CentOS-server configureren 2. ISE-archiefbestand configureren 3. Generate key pairs op ISE server 3.1. ISE GUI 3.2. ISE CLI 4. Integratie Verifiëren Gerelateerde informatie

# Inleiding

Dit document beschrijft hoe u een Linux-server kunt configureren met CentOS-distributie als een Secure File Transfer Protocol (SFTP) server met PKI-verificatie (Public Key Infrastructuur) naar Identity Services Engine (ISE).

# Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Algemene ISE-kennis
- Configuratie ISE-opslaglocatie
- Algemene kennis van basisLinux

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE 2.2
- ISE 2.4
- ISE 2.6
- ISE 2.7

- ISE 3.0
- CentOS Linux release 8.2.2004 (Core)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, zorg er dan voor dat u de mogelijke impact van elke opdracht begrijpt.

## Achtergrondinformatie

Om beveiliging voor bestandsoverdrachten af te dwingen, kan ISE via PKI-certificaten via SFTP authenticeren om een veiligere manier te garanderen om bestanden van gegevensbanken te openen.

## Configureren

## 1. CentOS-server configureren

1.1 Een map als een root gebruiker maken.

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

1.2. Maak een gebruikersgroep.

groupadd tac

1.3. Deze opdracht voegt de gebruiker toe aan de hoofdmap (bestanden) en geeft aan welke gebruiker tot de groep **engineers** behoort.

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

**Opmerking:** Het gedeelte **/sbin/nologin** van de opdracht geeft aan dat de gebruiker niet via Secure Shell (SSH) kan inloggen.

1.4. Maak een directory om de bestanden te uploaden.

mkdir -p /cisco/engineer/repo
1.4.1 Stel permissies in voor de folder bestanden.

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. Maak de map en het bestand waarin de CentOS-server de controle van de certificaten uitvoert.

Map:

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

touch /cisco/engineer/.ssh/authorized\_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized\_keys
chmod 600 /cisco/engineer/.ssh/authorized\_keys
1.6. Maak de inlogrechten in het systeembestand sshd\_diskset.

U kunt het bestand bewerken met deze opdracht met het actieve Linux-gereedschap.

vim /etc/ssh/sshd\_config
1.6.1 Voeg de onderstaande regels toe.

```
#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. Start de opdracht om de syntaxis van het sshd_fig systeem te controleren.
```

sshd -t

Opmerking: Geen uitvoer betekent dat de syntaxis van het bestand juist is.

1.8. Start de SSH-service opnieuw.

systemctl restart sshd

**Opmerking:** Sommige Linux-servers hebben **selinux**-handhaving, om deze parameter te bevestigen, kunt u de **getenforce** opdracht gebruiken. Als het een aanbeveling is om de modus voor **handhaving** op te leggen, moet u deze wijzigen in **toestemming**.

1.9. (optioneel) Bewerk het bestand semanage.conf om de executie in te stellen op toestemming.

vim /etc/selinux/semanage.conf
Voeg de opdrachtinstelling toe:0.

setenforce0

## 2. ISE-archiefbestand configureren

2.1. Voeg de gegevensbank toe via de ISE Graphic User Interface (GUI).

#### Navigeren in beheer>Systeemonderhoud>Bewaarplaats>Toevoegen



2.2. Voer de juiste configuratie voor uw opslagplaats in.

Repository List > Add Repository						
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						

**Opmerking:** Als u toegang tot de repo folder nodig hebt in plaats van de root folder van ingenieur, moet het doelpad /repo/ zijn.



## 3. Generate key pairs op ISE server

#### 3.1. ISE GUI

Navigeren in **op** beheer>**Systeemonderhoud>Bewaarplaats>Generate sleutelparen**, zoals in de afbeelding wordt getoond.

**Opmerking:** U moet belangrijke paren van de ISE GUI en de Opdracht Line Interface (CLI) genereren om volledige bidirectionele toegang tot de gegevensbank te hebben.

Identity Services Engine		Home + Context Visibility + Operations + Policy - Administration + Work Centers	
- System + Identity Management	£ >	Network Resources > Device Portal Management peGrid Services > Feed Service > Threat Centric NAC	
Deployment Licensing + Cert	ficates	Logging Maintenance Upgrade Backup & Restore Admin Access Settings	
	0		
Patch Management		Repository List	
Repository	۲	150 Last Linearis Security (b. Destandinismo Minister Oblights	
Operational Data Purging		Lett And Aneware we have the phase we have been been and the second	

3.1.1. Voer een wachtwoord in. Dit is nodig om het sleutelpaar te beschermen.

Enter passphrase :		

**Opmerking:** genereren eerst de sleutelparen voordat de openbare sleutels geëxporteerd worden.

3.1.2. Uitvoeren van de openbare sleutel.

Navigeren in om te schakelen>Systeemonderhoud>Bewaarinstelling>Openbare sleutel exporteren.

Selecteer **Openbare sleutel exporteren**. Er wordt een bestand gegenereerd met de naam **id\_rsa.pub** (controleer of dit wordt opgeslagen voor toekomstige referenties).



#### 3.2. ISE CLI

3.2.1. Navigeer naar de CLI van het knooppunt waarin u de configuratie van de gegevensbank wilt voltooien.

**Opmerking:** Vanaf dit punt vooruit zijn de volgende stappen nodig op elk knooppunt dat u toegang tot de SFTP-opslagplaats wilt toestaan met het gebruik van de PKI-verificatie.

3.2.2. Start deze opdracht om IP van de Linux-server toe te voegen aan het systeembestand **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. genereren van een openbare CLI-toets.

crypto key generate rsa passphrase <passphrase>
ise24htts/admin# crypto key generate rsa passphrase admin123

3.2.4. Exporteren van de openbare sleutelbestanden van de CLI van ISE met deze opdracht.

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

**Opmerking:** U moet beschikken over een eerder toegankelijke opslagplaats waaraan u het openbare sleutelbestand kunt exporteren.

ise24htts/admin# crypto key export public repository FTP

#### 4. Integratie

4.1. Meld u aan bij uw CentOS-server.

navigeren naar de map waarin u eerder het geautoriseerde\_key bestand hebt ingesteld.

4.2. Bewerk het geautoriseerde sleutelbestand.

Start de vim opdracht om het bestand aan te passen.

vim /cisco/engineer/.ssh/authorized\_keys

4.3. Kopieer en plak de inhoud die op de stappen **4** en **6** is gegenereerd uit de sectie **Generate** sleutelparen.

Openbare sleutel van ISE GUI:

id\_rsa.pub sh-rsa AAAAB3WzaC1yc2EAAAADAQABAAABAQCjcgqs8705icBwTP16Grmf8r3WNx+oqorSwTmPToC+0zit16iAbTIjs/ P2reawf9wrQXgQxEnSHa1kF0FPAJrKqoLB1RGwsZe1yNxVL06tjVFxB1E1Eh0Td9dy9wRQ3X1DUigC3q5jfPsQp64rHsHmg0GbZJL BNFvUgRJwD01Sx8Iy1yeLDt16oL7RFoTU3Y51hvfGXSI5ZHxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04 ptP07B12vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnvNZ4/Q1jLppP4s2hqrAVedr+r90z+8XdsxV root0ise24htts

Openbare sleutel gegenereerd door ISE CLI:



public

ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06sQ+gSykTRrGfdMryIiitCMBsObGsSyc9S8VKpLyyocsIvco4/ vF/pSHoTEIR3wrZTLlvCIUrGnngdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/ HAyXQ/a9YRZ1L2906pjKSWyuTkbUXWvN9hx/ SESzpJ4pFr9opg+UaTNX0yYuuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0cj6vMaV0L7GzdDI4NZHn7llpptqJFYAb65QB admingise24htts

Authorized\_key file op de Linux server:

4.4. Nadat u de toetsen op het bestand hebt geplakt, drukt u op ESC, om de **q** uit te voeren! opdracht om het bestand op te slaan.

# Verifiëren

1. Voer deze opdracht vanuit de Linux-server uit als wortel.

tail -f /var/log/secure

De uitvoer moet worden weergegeven, zoals in de afbeelding.

```
[[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:MNHNp2AtVXO8ObTswgPLKOGBaWFUue
ObKEWELKeaxU
Apr 12 21:37:53 localhost sshd[668112]: pam_unix(systemd-user:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[66812]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[66812]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXO8DbTswgPLKOGBaW
FUueDbXEWIEkcaeXU
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[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668201]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
```

2. Voor ISE-verificatie.

Navigeren in op Administratie>Systeem>Onderhoud>Bewaarinstelling op de GUI.

Selecteer de gewenste opslagplaats in de lijst Bewaarinstelling en selecteer Valideren.

dude Identity Services Engine	Home + Context Visibility + Operat	ions + Policy - Administration + W	wit Centers				
System + Identity Management + Network Resources + Davice Portal Management peDrid Services + Feed Service + Threat Centric N4C							
Deployment Licensing + Certificate	s + Logging + Maintenance Upgrad	Backup & Restore      Admin Access	Settings				
0							
Patch Management	Repository List						
Repository 💿	In Lui Linner train	Anna Cutta					
Operational Data Puncing							
	<ul> <li>Repository Name</li> </ul>	Protocol Host	Path				
	C FTP	Rp 10.88.240.69	1				
	UH-IONFS10-BACKUPS	nfs ICNPS10-nfs.chp.clarian.org	/ISE_Backups				
	backup	ftp 10.88.240.69	1				
	□ sftp	sftp 10.88.240.69	1				
	🗹 sftp_pki	sftp 10.88.240.102	1				

U moet een pop-up zien waarin de **Reactie van de Server** op de rechteronderhoek van het scherm staat.



Vanuit CLI voert u de opdracht show repo sftp\_pki uit om de keys te valideren.



Om ISE verder te zuiveren, voert u deze opdracht op CLI uit:

debug transfer 7

De uitvoer moet worden weergegeven, zoals in het beeld:



## Gerelateerde informatie

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