Configurer ISE SFTP avec authentification basée sur les certificats

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration 1. Configurer le serveur CentOS 2. Configurer le référentiel ISE 3. Générer des paires de clés sur le serveur ISE 3.1. Interface utilisateur ISE 3.2. CLI ISE 4. Intégration Vérification Informations connexes

Introduction

Ce document décrit comment configurer un serveur Linux avec une distribution CentOS en tant que serveur SFTP (Secure File Transfer Protocol) avec une authentification PKI (Public Key Infrastructure) vers Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances ISE générales
- Configuration du référentiel ISE
- Connaissances générales Linux de base

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ISE 2.2
- ISE 2.4
- ISE 2.6

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de toute commande.

Informations générales

Pour renforcer la sécurité des transferts de fichiers, ISE peut s'authentifier via des certificats PKI via SFTP afin d'assurer un accès plus sécurisé aux fichiers des référentiels.

Configuration

1. Configurer le serveur CentOS

1.1 Créez un répertoire en tant qu'utilisateur racine.

mkdir -p /cisco/engineer

1.2. Créez un groupe d'utilisateurs.

groupadd tac

1.3. Cette commande ajoute l'utilisateur au répertoire principal (fichiers), il spécifie que l'utilisateur appartient aux **ingénieurs** du groupe.

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

Note: La partie **/sbin/nologin** de la commande indique que l'utilisateur ne pourra pas se connecter via Secure Shell (SSH).

1.4. Créez le répertoire pour télécharger les fichiers.

mkdir -p /cisco/engineer/repo
1.4.1 Définition des autorisations pour les fichiers du répertoire

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. Créez le répertoire et le fichier dans lequel le serveur CentOS effectue la vérification des certificats.

Répertoire :

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

touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
1.6. Créez les autorisations de connexion dans le fichier système sshd_config.

Afin de modifier le fichier, vous pouvez utiliser l'outil vim Linux avec cette commande.

vim /etc/ssh/sshd_config
1.6.1 Ajouter les lignes spécifiées ci-dessous.

```
#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. Exécutez la commande afin de vérifier la syntaxe du fichier système sshd_config.
```

sshd -t

Note: Aucune sortie signifie que la syntaxe du fichier est correcte.

1.8. Redémarrez le service SSH.

systemctl restart sshd

Note: Certains serveurs Linux ont **selinux** application, pour confirmer ce paramètre, vous pouvez utiliser la commande **getEnforcement**. En tant que recommandation, s'il est en mode **d'application**, changez-le en **mode** d'**autorisation**.

1.9. (facultatif) Modifiez le fichier semanage.conf pour définir l'application sur permissive.

vim /etc/selinux/semanage.conf Ajoutez la commande **setfont0**.

setenforce0

2. Configurer le référentiel ISE

2.1. Ajoutez le référentiel via l'interface utilisateur graphique ISE (GUI).

Accédez à Administration>Maintenance du système>Référentiel>Ajouter

-dude- case Identity Services Engin	ine i	Home + Contas	d Visibility + Operatio	ons + Policy	+ Administration	Work Centers
System Identity Manager	ment >	Network Resources	> Device Portal Mana	gement petärid S	iervices > Feed Ser	vice > Threat Centric NAC
Deployment Licensing + 0	Certificates	s → Logging +1	Maintenance Upgrade	 Backup & Ret 	tore + Admin Acces	ss → Settings
	0					
Patch Management		Repository Lis	it.			
Repository	۲	100	- Liferante Receptor - D	Constantinion	Marian Canton	
Operational Data Russian		1 con	- concrete wey points in	Codest Broak stak	× 00000 10 000000	

2.2. Entrez la configuration appropriée pour votre référentiel.

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	

Note: Si vous avez besoin d'accéder au répertoire repo au lieu du répertoire racine de l'ingénieur, le chemin cible doit être /repo/.



3. Générer des paires de clés sur le serveur ISE

3.1. Interface utilisateur ISE

Accédez à Administration>Maintenance du système>Référentiel>Générer des paires de clés, comme l'illustre l'image.

Note: Vous devez générer des paires de clés à partir de l'interface utilisateur graphique ISE et de l'interface de ligne de commande (CLI), afin d'avoir un accès bidirectionnel complet au référentiel.

durby Identity Services En	gine i	ome + Context Visibility	Operations	+ Policy	Administration	Work Centers
System Identity Management	gement >	ietwork Resources > Device	a Portai Management	peGrid Servi	ices > Feed Ser	vice Threat Centric NAC
Deployment Licensing	Certificales	+ Logging - Maintenance	Upgrade → Ba	sokup & Restore	+ Admin Acces	as → Settings
	0					
Patch Management		Repository List				
Repository	۲	100 144 10000	New pairs - The Depart	aublic law	Dates Ontes	
Operational Data Purging		/ cor made moderate	s well boils . Proport	ризк ксу	Deele Press	

3.1.1 . Entrez une phrase de passe, cette opération est requise afin de protéger la paire de clés.

Enter passphrase :		
	Cancel	ок

Note: Tout d'abord, générez les paires de clés avant l'exportation des clés publiques.

3.1.2 . Passez à l'exportation de la clé publique.

Accédez à Administration>Maintenance du système>Référentiel>Exporter la clé publique.

Sélectionnez **Exporter la clé publique**. Un fichier est généré avec le nom **id_rsa.pub** (assurez-vous qu'il est enregistré pour les références futures).

000	Opening id_rsa.pub
You have cho	osen to open:
id_rsa.pub	
which is: P	EM file (396 bytes)
from: http:	://10.88.240.96
What should	Firefox do with this file?
Open with	Choose
🔾 Save File	
Do this aut	comatically for files like this from now on.
	Cancel

3.2. CLI ISE

3.2.1 . Accédez à l'interface de ligne de commande du noeud dans lequel vous voulez terminer la configuration du référentiel.

Note: À partir de ce stade, les étapes suivantes sont nécessaires sur chaque noeud que vous souhaitez autoriser l'accès au référentiel SFTP avec l'utilisation de l'authentification

PKI.

3.2.2 . Exécutez cette commande afin d'ajouter l'adresse IP du serveur Linux au fichier système **host_key**.



3.2.3 . Générer une clé CLI publique.

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

3.2.4 . Exportez les fichiers de clé publique à partir de l'interface de ligne de commande d'ISE à l'aide de cette commande.

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

Note: Vous devez disposer d'un référentiel précédemment accessible auquel vous pouvez exporter le fichier de clé publique.

ise24htts/admin# crypto key export public repository FTP

4. Intégration

4.1. Connectez-vous à votre serveur CentOS.

Accédez au dossier dans lequel vous avez précédemment configuré le fichier Authorized_key.

4.2. Modifiez le fichier de clé autorisé.

Exécutez la commande vim afin de modifier le fichier.

vim /cisco/engineer/.ssh/authorized_keys

4.3. Copiez et collez le contenu généré sur les étapes **4** et **6** à partir de la section **Générer les paires de clés**.

Clé publique générée à partir de l'interface utilisateur ISE :



Clé publique générée à partir de l'interface de ligne de commande ISE :



public

ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06sQ+gSykTRrGfdMryIiitCWBs0bGs5yc9S8VKpLyyocsIvco4/ vF/pSHoTEIR3wrZTLlvCIUrGnngdQv4+8YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/ HAyXQ/a9YRZ1L2906pjKSWyuTkbUxWvN9hx/ SE5zpJ4pFr9opg+UaTNXXVYTuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0cj6vMaV0L7GzdDI4NZHn7LlpptqJFYAb65QB admingise24htts

Fichier Authorized_key sur le serveur Linux :

4.4. Après avoir collé les touches sur le fichier, appuyez sur Échap, exécutez le **wq !** afin d'enregistrer le fichier.

Vérification

1. À partir du serveur Linux, exécutez cette commande en tant que root.

tail -f /var/log/secure

Le résultat doit être affiché, comme le montre l'image.

```
[[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:MNHNp2AtVXD8ObTswgPLKOGBaWFUue
GbXEWIEkcaeXU
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[668121]: 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:MNHNp2AtVXD8DbTswgPLKOGBaWFUue
GbXEWIEkcaeXU
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[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. Pour la vérification ISE.

Accédez à Administration>System>Maintenance>Repository sur l'interface utilisateur graphique.

Sélectionnez le référentiel souhaité dans la liste de référentiels et sélectionnez Valider.

dada Identity Services Engine	Home + Context Vability + Ope	rations + Policy + Administration + V	Nork Centers
System + Identity Management	Network Resources Device Portal M	anagement petirid Services + Feed Service	Threat Centric NAC
Deployment Licensing + Certil	loates + Logging - Maintenance Upgr	ide + Backup & Restore + Admin Access	 Settings
	•		
Palch Management	Repository List		
Repository	Area 1 44 1 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	Annual Marine Conten	
Operational Data Purging	/ ER	Coppet public key Cooker Divergence	
	Repository Name	 Protocol Host 	Path
	C FTP	Rp 10.88.240.69	/
	UH-IOVES10-BACKUPS	nfs ICNPS10-nfs.chp.clarian.org	/ISE_Backups
	backup	ftp 10.88.240.69	1
	🗆 sftp	sftp 10.88.240.69	1
	🗹 sftp.jski	sftp 10.88.240.102	1

Vous devez voir une fenêtre contextuelle qui indique la **réponse du serveur** dans le coin inférieur droit de l'écran.



Àpartir de l'interface de ligne de commande, exécutez la commande **show repo sftp_pki** afin de valider les clés.



Afin de déboguer ISE plus avant, exécutez cette commande sur CLI :

debug transfer 7

Le résultat doit être affiché, comme le montre l'image :



Informations connexes

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