# 証明書ベース認証を使用したISE SFTPの設定

## 内容

概要 <u>前提条件</u> 要件 使用するコンポーネント 背景説明 設定 <u>1. CentOSサーバの設定</u> <u>2. ISEリポジトリの設定</u> <u>3. ISEサーバでキーペアを生成する</u> <u>3.1. ISE GUI</u> <u>3.2. ISE CLI</u> <u>4.統合</u> 確認 関連情報

### 概要

このドキュメントでは、CentOSディストリビューションを使用するLinuxサーバを、Identity Services Engine(ISE)に対する公開キーインフラストラクチャ(PKI)認証を使用したSecure File Transfer Protocol(SFTP)サーバとして設定する方法について説明します。

# 前提条件

#### 要件

次の項目に関する知識があることが推奨されます。

- 一般的なISEの知識
- ISEリポジトリの設定
- Linuxの基本的な一般知識

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ISE 2.2
- ISE 2.4
- ISE 2.6
- ISE 2.7
- ISE 3.0
- CentOS Linuxリリース8.2.2004 (コア)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。ネットワークが稼働中の場合は、コマンドの潜在的な影響について理解しておいてください。

### 背景説明

ファイル転送のセキュリティを強化するために、ISEはSFTPを介してPKI証明書を使用して認証 し、リポジトリファイルへのより安全なアクセス方法を確保できます。

### 設定

#### 1. CentOSサーバの設定

1.1ルートディレクトリをルートユーザとして作成します。

mkdir -p /cisco/engineer

1.2.ユーザグループの作成

groupadd tac

1.3.このコマンドは、ユーザーをメインディレクトリ(ファイル)に追加し、ユーザーがグルー プエンジニアに属することを指定**しま**す。

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

**注**:コマンドの/sbin/nologin部分は、ユーザがセキュアシェル(SSH)を介してログインできないことを示しています。

1.4.ファイルをアップロードするディレクトリの作成に進みます。

mkdir -p /cisco/engineer/repo
1.4.1ディレクトリファイルの権限を設定する。

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. CentOSサーバが証明書のチェックを実行するディレクトリとファイルを作成します。

ディレクトリ:

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. sshd\_configシステムファイルにログイン権限を作成します。

このファイルを編集するには、このコマンドでvim Linuxツールを使用します。

vim /etc/ssh/sshd\_config 1.6.1指定した行を次に追加します。

#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. sshd configシステムファイルの同期を確認するために、コマンドを実行します。

sshd -t

**注**:出力は、ファイルの構文が正しいことを意味します。

1.8. SSHサービスの再起動に進みます。

systemctl restart sshd

**注**:一部のLinuxサーバには**selinuxが**適用されており、このパラメータを確認するには、 getenforceコマンドを使用できます。強制モードの場合はpermissiveに変更することをお勧 **めします。** 

1.9. (オプション) semanage.confファイルを編集して、強制をpermissiveに設定します。

vim /etc/selinux/semanage.conf コマンドsetenforce0を追加します。

setenforce0

#### 2. ISEリポジトリの設定

2.1. ISEグラフィックユーザインターフェイス(GUI)を使用してリポジトリを追加します。

[管理(Administration)] > [システムメンテナンス(System Maintenance)] > [リポジトリ(Repository)] > [追加(Add)]に移動します

-dude- Identity Services Er	ngine	Home + Context \	faibility + Operations	+ Policy	+ Administration	Work Centers
System > Identity Mana	agement >	Network Resources	Device Portal Managem	ent petürid Se	ervices > Feed Se	rvice + Threat Centric NAC
Deployment Licensing	Certificates	s ≻ Logging - Ma	intenance Upgrade	Backup & Rest	ore + Admin Acce	ss → Settings
	0					
Patch Management		Repository List				
Repository	۲	too Jaw J	- Cananda Kay solar (Ph.D.)	out a dela lana	Voice Ontes	
Operational Data Purging		/ COX - MOD -	- developer wey bors	pert guark key	Coole Press	20

#### 2.2.リポジトリの適切な設定を入力します。

Repository List > Add Reposit	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	

**注**:エンジニアのルートディレクトリではなくrepoディレクトリにアクセスする必要がある 場合は、ターゲットパスは/repo/である必要があります。



### 3. ISEサーバでキーペアを生成する

3.1. ISE GUI

図に示すように、[管理] > [システムメンテナンス] > [リポジトリ] > [キーペアの生成]に移動しま す。

注:リポジトリへの完全な双方向アクセスを実現するには、ISE GUIおよびコマンドライン インターフェイス(CLI)からキーペアを生成する必要があります。

their Identity Services Engine	Home +	Context Visibility	+ Operations	+ Policy	+ Administration	Work Centers
+ System + Identity Management	> Network Real	ources > Device	Portal Managemer	nt perGirid S	ervices > Feed Se	rvice > Threat Centric NAC
Deployment Licensing + Certifi	cales > Logging	Maintenance	Upgrade + E	lackup & Res	Iore + Admin Acce	ss → Settings
	0					
Patch Management	Reposito	ry List				
Repository		Let Country	Karanta di Dana	4 - 07 - Los	Maria Carro	
Operational Data Purging	/ eax -	Add Generate	key pairs 🖉 Expo	rt public key	Cente Presso	2

3.1.1.パスフレーズを入力します。これは、キーペアを保護するために必要です。

Enter passphrase :	
•••••	
	Cancel 0

**注**:公開キーをエクスポートする前に、まずキーペアを生成します。

3.1.2.公開キーのエクスポートに進みます。

[管理(Administration)] > [システムメンテナンス(System Maintenance)] > [リポジトリ(Repository)] > [公開キーのエクスポート(Export public key)]に移動します。

[Export public key]を選択します。id\_rsa.pubという名前のファイルが生成されます(これ以降の参照のために保存してください)。

• • •	Opening id_rsa.pub					
You have chosen to open:						
id_rsa.put	2					
which is: P	EM file (396 bytes)					
from: http	s://10.88.240.96					
What should	Firefox do with this file?					
On on with	Change					
Open with	choose					
Save File						
Do this au	tomatically for files like this from now on.					
	Cancel OK					

#### 3.2. ISE CLI

3.2.1.リポジトリの設定を終了するノードのCLIに移動します。

**注**:この時点から、PKI認証を使用してSFTPリポジトリへのアクセスを許可する各ノード で、次の手順が必要になります。 3.2.2.このコマンドを実行して、LinuxサーバのIPをhost\_keyシステムファイルに追加します。

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.パブリックCLIキーを生成する。

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

3.2.4.次のコマンドを使用して、ISEのCLIから公開キーファイルをエクスポートします。

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

**注**:公開キーファイルをエクスポートできる、以前にアクセス可能なリポジトリが必要です。

ise24htts/admin# crypto key export public repository FTP

#### 4.統合

4.1. CentOSサーバにログインします。

authorized\_keyファイルを以前に構成したフォルダに移動します。

4.2.認証キーファイルの編集

vimコマンドを実行して、ファイルを変更します。

vim /cisco/engineer/.ssh/authorized\_keys 4.3. 「キーペアの生成」セクションのステップ4および6で生成されたコンテンツをコピーして貼 り付けます。

ISE GUIから生成された公開キー:

id\_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCicggs8705icBwTP16Grmf8r3WNx+ogorSwTmPToC+0zitl6iAbTIis/
PZreawf9wrQXgQxEnSHa1kF0FPAJrKqoLB1RGwsZelyNxVL06t1VFxBIEIEhQTd9dy9wRQ3XIDUigC3q5jfPsQpG4rHsHmgOGbZ3L
BNFvUgR3wD01Sx8IylyeLDt16oL7RFoTU3Y51hvfGXSI5ZHxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04
ptP07B12vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnwNZ4/Q1jLppP4s2hgrAVedr+r90z+8XdsxV root0ise24htts

ISE CLIから生成された公開キー:



public

AAAAB3NzaC1yc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06s0+gSykTRrGfdMryIiitCMBs0bGsSyc9S8VKpLyyocsIvco4/ vF/pSHoTE1R3wrZTL1vCTUrGnnqdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQ8086tkno40cmT/ HAyXQ/a9YRZ1L2906pjKSWyuTkbUxWvN9hx/ SE5zpJ4pFr9opg+UaTNXQyYuuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0Cj6vMaV0L7GZdDI4NZHn7llpptqJFYAb65QB admingise24htts

#### Linuxサーバ上のAuthorized\_keyファイル:

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjcgqs8705ic8wTP16Grmf8r3WNx+ogorSuTmPToC+0zjtl6iAbT1js/PZreawf9urQXgQxEnSHa1kF0FPAJrKqoLB1RGusZelyNxVLO6ti VFxBEIEhQTd9dy9uRQ3XIDUigC3q5jfPsQpG4rHsHmgOGbZJLBNFVUGP3W0015x81y1yeLD16oL7RFoTU3Y51hvfGXSI5ZHxoGKsXjm2hA0+rkbbfPfQy37LT7w8HpAEaEVgLXL4o3mFUYm dKCcO4ptPQ7812vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnuNZ4/Q1jLppP4s2hqrAVedr+r90z+8XdsxV root9ise24htts ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCaH+SANATb47+NXFyuz06s0+g5ykTRtGfdMry1iitCWBsDGb5Syc958VKDLyyosIvco4/vF/pSHoTE1R3wrZTL1vCIUrGnnqdQv4+0YnIb J/f8EgZnXQ+fLK8oyLeVxPgdBcewL3HMV8giQHLizAdXtQD086stkno40cmT/HAyXQ/a9YRZ112906pjK5WyuTkbUxWvN9hx/5E5zp34pFr9opq+UaTNX0yYuuj328FGEFdKuFBSujAokPOnJT LN80dLAQ6x4kkkcXWXKT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm00Cj6vMaV0L7GZdDI4NZHn7llpptq3FYAb65Q8 admin8ise24htts



1

4.4.ファイルにキーを貼り付けた後、Escキーを押し、wqを実行しま**す!**コマンドを発行して、 ファイルを保存します。

# 確認

1. Linuxサーバから、このコマンドをrootとして実行します。

tail -f /var/log/secure

図に示すように、出力を表示する必要があります。

```
[[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:MNHNp2AtVXD8DbTswgPLKOG8aWFUue
ObKEVEKtoacxU
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(shd:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668120]: pam_unix(shd:session): session opened for user root by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOG8aW
FUue0ExtEmt[kcaeXU
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[668201]: 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(sshd:session): session opened for user engineer by (uid=0)
Apr 12 21:38:27 localhost sshd[668208]: pam_unix(sshd:session): session opened for user engineer by (uid=0)
```

2. ISE検証の場合。

GUIで[Administration] > [System] > [Maintenance] > [Repository]に移動します。

リポジトリ・リストから目的のリポジトリを選択し、「検証」を選択します。

deale Identity Services Engine	Home + Context Vability + Opera	dons + Policy + Administration + W	Aris Centers			
System      Identity Management      Network Resources      Device Portal Management      peDrid Services      Feed Service      Threat Centric NAC						
Deployment Licensing + Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings						
0						
Patch Management	Repository List					
Repository 💿	In Lui Linner to de	A Contraction Marine Contract				
Contractional Data Puncting						
	<ul> <li>Repository Name</li> </ul>	Protocol Host	Path			
	C FTP	Rp 10.88.240.69	1			
	UH-IONF510-BACKUPS	nfs ICNFS10-nfs.chp.clarian.org	/ISE_Backups			
	backup	Rp 10.88.240.69	1			
	sftp	sftp 10.88.240.69	1			
	🖬 sftp_pki	sftp 10.88.240.102	1			

画面の右下隅に[Server Response]というポップアップが表示されます。



CLIから、show repo sftp\_pkiコマンドを実行して、キーを検証します。



ISEをさらにデバッグするには、CLIで次のコマンドを実行します。

debug transfer 7 次の図に示すように、出力を表示する必要があります。



# 関連情報

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