Configurar o ISE SFTP com autenticação baseada em certificado

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Configurar 1. Configurar servidor CentOS 2. Configurar o repositório do ISE 3. Gerar pares de chaves no servidor ISE 3.1. GUI do ISE 3.2. CLI ISE 4. Integração Verificar Informações Relacionadas

Introduction

Este documento descreve como configurar um servidor Linux com distribuição CentOS como um servidor Secure File Transfer Protocol (SFTP) com autenticação PKI (Public Key Infrastructure) em direção ao Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento geral do ISE
- configuração de repositório ISE
- Conhecimento geral básico do Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

- ISE 3.0
- CentOS Linux versão 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. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Para reforçar a segurança das transferências de arquivos, o ISE pode autenticar-se através de certificados PKI através do SFTP, a fim de garantir uma maneira mais segura de acessar arquivos de repositórios.

Configurar

1. Configurar servidor CentOS

1.1 Crie um diretório como usuário raiz.

mkdir -p /cisco/engineer

1.2. Crie um grupo de usuários.

groupadd tac

1.3. Esse comando adiciona o usuário ao diretório principal (arquivos), especifica que o usuário pertence aos **engenheiros** do grupo.

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

Note: A parte do comando /sbin/nologin indica que o usuário não poderá fazer login por meio do Secure Shell (SSH).

1.4. Prossiga para criar o diretório para carregar os arquivos.

mkdir -p /cisco/engineer/repo
1.4.1 Defina permissões para os arquivos de diretório.

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. Crie o diretório e o arquivo no qual o servidor CentOS executa a verificação dos certificados.

Diretório:

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

touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
1.6. Crie as permissões de login no arquivo do sistema sshd_config.

Para editar o arquivo, você pode usar a ferramenta vim Linux com esse comando.

vim /etc/ssh/sshd_config
1.6.1 Adicione as linhas especificadas abaixo.

```
#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. Execute o comando para verificar a sintaxe do arquivo do sistema sshd_config.
```

sshd -t

Note: Nenhuma saída significa que a sintaxe do arquivo está correta.

1.8. Continue para reiniciar o serviço SSH.

systemctl restart sshd

Note: Alguns servidores Linux têm aplicação **selinux**. Para confirmar esse parâmetro, você pode usar o comando **getforce**. Como recomendação, se estiver no modo **de aplicação**, altere-o para **permissivo**.

1.9. (opcional) Edite o arquivo **semage.conf** para definir a aplicação como permissiva.

vim /etc/selinux/semanage.conf
Adicione o comando setforce0.

setenforce0

2. Configurar o repositório do ISE

2.1. Prossiga para adicionar o repositório por meio da Interface Gráfica do Usuário (GUI) do ISE.

Navegue até Administração>Manutenção do sistema>Repositório>Adicionar

-dub- tere Identity Services Engine		Home + Context	Visibility +	Operations	+ Policy	 Administration 	Work Centers
System Hentity Manageme	nt >	Network Resources	Device Par	tai Management	petGrid S	ervices > Feed Se	rvice > Threat Centric NAC
Deployment Licensing + Cer	ificates	+ Logging + M	laintenance (Jpgrade + Ba	ckup & Res	tore + Admin Acce	ss > Settings
	0						
Patch Management		Repository List					
Repository	۲	100	L Gananda Kay	mir Prinet	a dik kec	Volume Constant	
Onerotional Data Purging		Cost Trian	Concrete wey	boas @ optor	public key	A Deole Press	0

2.2. Digite a configuração apropriada para o repositório.

Repository List > Add Repository				
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: Se você precisar de acesso ao diretório repo em vez do diretório raiz do engenheiro, o caminho de destino precisa ser /repo/.



3. Gerar pares de chaves no servidor ISE

3.1. GUI do ISE

Navegue até Administração>Manutenção do sistema>Repositório>Gerar pares de chaves, como mostrado na imagem.

Note: Você deve gerar pares de chaves da GUI do ISE e da CLI (Command Line Interface, interface de linha de comando), para ter acesso bidirecional total ao repositório.

Identity Services Engin	19	Home + Context Visibility	Operations	Policy -	Administration	Work Centers
+ System + Identity Manager	ment >	Network Resources > Dev	ice Portal Management	peGrid Servic	es > Feed Ser	vice + Threat Centric NAC
Deployment Licensing + 0	Certificales	s → Logging → Maintenar	ice Upgrade + Bac	kup & Restore	+ Admin Acces	as → Settings
	0					
Patch Management		Repository List				
Repository	۲	100 144 1000	te Key ester - 🕩 Depart e	alie kase 💙 I	ulas Obstan	
Operational Data Purging		Cox manage models	ade key pars - 🖉 Export p	ubik key 👗	1002 100000	

3.1.1. Insira uma senha, que é necessária para proteger o par de chaves.

Enter passphrase :	
•••••	
	Oursel OV
	Cancel

Note: Primeiro, gere os pares de chaves antes que as chaves públicas sejam exportadas.

3.1.2. Prossiga para exportar a chave pública.

Navegue até Administração>Manutenção do sistema>Repositório>Exportar chave pública.

Selecione **Exportar chave pública**. Um arquivo é gerado com o nome **id_rsa.pub** (certifique-se de que ele seja salvo para referências futuras).

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

3.2. CLI ISE

3.2.1. Navegue até a CLI do nó em que deseja concluir a configuração do repositório.

Note: A partir desse ponto, as próximas etapas são necessárias em cada nó que você gostaria de permitir acesso ao repositório SFTP com o uso da autenticação PKI.

3.2.2. Execute este comando para adicionar o IP do servidor Linux ao arquivo do 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. Gerar chave CLI pública.

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

3.2.4. Exporte os arquivos de chave pública da CLI do ISE com este comando.

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

Note: Você deve ter um repositório previamente acessível para o qual possa exportar o arquivo de chave pública.

ise24htts/admin# crypto key export public repository FTP

4. Integração

4.1. Faça login no servidor CentOS.

Navegue até a pasta na qual você configurou anteriormente o arquivo authorized_key.

4.2. Edite o arquivo de chave autorizada.

Execute o comando vim para modificar o arquivo.

vim /cisco/engineer/.ssh/authorized_keys

4.3. Copie e cole o conteúdo gerado nas etapas 4 e 6 da seção Gerar pares de chaves.

Chave pública gerada pela GUI do ISE:

id_rsa.pub ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCicggs8785icBwTP16Grmf8r3WNx+ogorSwTmPToC+&zitl6iAbTIis/ P2reawf9wrQXgQxEnSHa1kF0FPAJrKqoLB1RGusZelyNxVL06t1VFxB1EIEh0Td9dy9uRQ3XIDU1gC3q5jfPsQpG4rHsHmg0GbZJL BNFvUgR3wD01Sx8IylyeLDt16oL7RFoTU3Y51hvfGXSISZHxoGKsXjm2hA&+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04 ptP07812vvIHN0hcZqG+Gnpw3U+SHxGWks1fc393vCA4smzFnuNZ4/Q1jLppP4s2hgrAVedr+r90z+8XdsxV root8ise24htts

Chave pública gerada pela CLI do ISE:



public

ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06s0+gSykTRrGfdMryIiitCMBs0bGsSyc958VKpLyyocsIyco4/ vF/pSHoTEIR3wrZTL1vCIUrGnngdQv4+8YnIbJ/f8EgZnX0+fLK8oyLeVxPgd8cewL3HMV8g1QHLizAdXtQ8886tkno40cmT/ HAyXQ/a9YRZ1L2906pjKSWyuTkbUxWvN9hx/ SE5zpJ4pFr9opg+UaTNX0yYuuj328FGEFdKuFBSujAokP0nJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G8zm D0cj6vMaV8L7G2dDI4NZHn7LlpptgJFYAb65QB admingise24htts

Arquivo Authorized_key no servidor Linux:

4.4. Depois de colar as teclas no arquivo, pressione ESC, continue para executar a **wq!** para salvar o arquivo.

Verificar

1. No servidor Linux, execute esse comando como raiz.

tail -f /var/log/secure

A saída deve ser exibida, como mostrado na imagem.

```
[[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[668112]: pam_unix(sshd:session): session opened for user root by (uid=0)
Apr 12 21:37:53 localhost sshd[668120]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaWFUue
Apr 12 21:38:27 localhost sshd[668208]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaW
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(ssted:session): session opened for user engineer by (uid=0)
```

2. Para verificação do ISE.

Navegue até Administration>System>Maintenance>Repository na GUI.

Selecione o repositório desejado na Lista de repositórios e selecione Validar.

-dude Identity Services Engl	NO Home +	Context Visibility + 0	perations + Policy	Administration	Vork Centers
System Hentity Manage	ment > Network Res	ources + Davice Portal	Management petitri	d Services + Feed Service	Threat Centric NAC
Deployment Licensing + 0	Certificates > Loggin	g + Maintenance Up	grade 🔸 Backup & P	lestore + Admin Access +	• Settings
	•				
Patch Management	Reposito	ry List			
Repository	(i)	Last descents the sec	. A factor and the	Martin Ontern	
Operational Data Purging	/ CDK -	- wad - Generate wey be	as Reportation vo	Coone prosant	
	Report	itory Name	 Protocol 	Host	Path
	C FTP		fp	10.88.240.69	/
	III.	ONFS10-BACKUPS	nfs	ICNPS10-nfs.chp.clarian.org	/ISE_Backups
	backs	p	fo	10.88.240.69	/
	🗆 sftp		sto	10.88.240.69	/
	🗹 sftp.j	phi .	sto	10.88.240.102	/

Você deve ver um pop-up que indica a Resposta do servidor no canto inferior direito da tela.



Na CLI, execute o comando show repo sftp_pki para validar as chaves.



Para melhor depurar o ISE, execute este comando na CLI:

debug transfer 7

A saída deve ser exibida, como mostrado na imagem:

ise24htts/admin# show repo sftp_pki
6 [16745]:[info] transfer: cars_xfer.c[224] [admin]: sftp dir of repository sftp_pki requested
6 [16745]:[info] transfer: cars_xfer_util.c[2200] (admin): resolved server to 10.00.240.102
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 1s -1 /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 ~ePasswordAuthentication=no engineerQ10.88.240.102
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_sfer_util.c[2315] (admin): ssh_list xfer succeeded
S Repository is empty

Informações Relacionadas

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