使用基於證書的身份驗證配置ISE SFTP

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>設定</u> <u>1.配置CentOS伺服器</u> <u>2.配置ISE儲存庫</u> <u>3.在ISE伺服器上生成金鑰對</u> <u>3.1. ISE GUI</u> <u>3.2. ISE CLI</u> <u>4.一體化</u> <u>驗證</u> 相關資訊

簡介

本文描述如何將使用CentOS分發的Linux伺服器配置為使用面向身份服務引擎(ISE)的公鑰基礎架構 (PKI)身份驗證的安全檔案傳輸協定(SFTP)伺服器。

必要條件

需求

思科建議您瞭解以下主題:

- 一般ISE知識
- ISE儲存庫配置
- Linux基礎常識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- ISE 2.2
- ISE 2.4
- ISE 2.6
- ISE 2.7
- ISE 3.0
- CentOS Linux版本8.2.2004(核心)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

為了對檔案傳輸實施安全性,ISE可以通過PKI證書通過SFTP進行身份驗證,以確保更安全地訪問 儲存庫檔案。

設定

1. 配置CentOS伺服器

1.1以根使用者身份建立目錄。

mkdir -p /cisco/engineer

1.2.建立使用者組。

groupadd tac

1.3.此命令將使用者新增到主目錄(檔案),它指定使用者屬於組工程師。

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

附註:命令的/**sbin/nologin**部分表示使用者將無法通過安全殼層(SSH)登入。

1.4.繼續建立用於上傳檔案的目錄。

mkdir -p /cisco/engineer/repo
1.4.1設定目錄檔案的許可權。

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.建立CentOS伺服器在其中執行證書檢查的目錄和檔案。

目錄:

mkdir /cisco/engineer/.ssh
chown engineer:engineer /cisco/engineer/.ssh
chmod 700 /cisco/engineer/.ssh
檔案:

chown engineer:engineer /cisco/engineer/.ssh/authorized_keys chmod 600 /cisco/engineer/.ssh/authorized_keys 1.6.在sshd config系統檔案中建立登入許可權。

若要編輯檔案,可以透過此命令使用vim Linux工具。

vim /etc/ssh/sshd_config 1.6.1在下面新增指定的行。

#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.運行命令以驗證sshd_config**系統檔案語法。

sshd -t

附註:無輸出表示檔案的語法正確。

1.8.繼續重新啟動SSH服務。

systemctl restart sshd

附註:某些Linux伺服器具有**selinux**實施,要確認此引數,可以使用**getenforce**命令。作為建 議,如果處於**enforce**模式,請將其更改為**permissive。**

1.9.(可選)編輯semanage.conf檔案,將實施設定為允許執行。

vim /etc/selinux/semanage.conf 新增命令setenforce0。

setenforce0

2.配置ISE儲存庫

2.1.繼續通過ISE圖形使用者介面(GUI)新增儲存庫。

導航到管理>系統維護>儲存庫>新增

Identity Services Er	ngine i	Home + Contact Visibility	+ Operations + Policy	Administration Work Centers
+ System > Identity Mana	agement >	Network Resources + Device	Portal Management petirid 5	lervices + Feed Service + Threat Centric NAC
Deployment Licensing	Certificates	s + Logging + Maintenance	Upgrade + Backup & Res	tore + Admin Access + Settings
	0	Reporting List		
Parch Management		Repository List		
Repository	۲	/ ErR +Add +Generate	Key pairs 🕃 Export public key	Cekte Dividate
Operational Data Purging				

2.2. 輸入儲存庫的正確配置。

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				

附註:如果您需要訪問回購目錄而不是工程師的根目錄,則目標路徑需要為/repo/。



3.在ISE伺服器上生成金鑰對

3.1. ISE GUI

導覽至Administration>System Maintenance>Repository>Generate key對,如下圖所示。

附註:必須通過ISE GUI和命令列介面(CLI)生成金鑰對,才能對儲存庫進行完全雙向訪問。

Identity Services En	igine i	Home + Conte	ot Visibility + Open	ations + Policy	· Administration	Work Centers
System → identity Mana	gement >	Network Resource	s > Device Portal Ma	nagement pxGrid S	Services > Feed Ser	vice > Threat Centric NAC
Deployment Licensing + Certificates + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings						
	0					
Patch Management		Repository Li	st			
Repository	۲	100 1.00	- Casarda Kasarda	The Department of the Inter-	Voia Ontes	
Operational Data Purging		Cor Tried	Cenerate key pars	Protost branc vok	COULD PARADO	c

3.1.1.輸入密碼短語,這是保護金鑰對所必需的。

Enter passphrase :	
	Cancel

附註:首先生成金鑰對,然後匯出公鑰。

3.1.2.繼續匯出公鑰。

導航到管理>系統維護>儲存庫>匯出公鑰。

選擇**匯出公鑰**。將生成一個名為id_rsa.pub的檔案(確保儲存該檔案以供將來參考)。

00	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	l Firefox do with this file?				
 Open with 	Choose				
🔾 Save File					
Do this automatically for files like this from now on.					
	Cancel				

3.2. ISE CLI

3.2.1.導航到要在其中完成儲存庫配置的節點的CLI。

附註:從此以後,您需要在使用PKI身份驗證允許訪問SFTP儲存庫的每個節點上執行後續步 驟。

3.2.2.運行此命令,以便將Linux伺服器的IP新增到host_key系統檔案中。

crypto host_key add host <linux ip="" server=""></linux>	
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/7Fj1hyHRkJlKyLhJC	lteSpE

3.2.3.生成公共CLI金鑰。

crypto key generate rsa passphrase <passphrase>

ise24htts/admin# crypto key generate rsa passphrase admin123

3.2.4.使用此命令從ISE的CLI匯出公鑰檔案。

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

附註:必須具有一個以前可以訪問的儲存庫,您可以將公鑰檔案匯出到該儲存庫。

ise24htts/admin# crypto key export public repository FTP

4.一體化

4.1.登入您的CentOS伺服器。

導航到您先前配置了authorized_key檔案的文件夾。

4.2.編輯授權金鑰檔案。

執行vim命令以修改檔案。

vim /cisco/engineer/.ssh/authorized_keys 4.3.從生成金鑰對部分複製並貼上在步驟4和步驟6上生成的內容。

從ISE GUI生成的公鑰:

● ● ● ● id_rsa.pub ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAABAQCicggs8705icBwTP16Grmf8r3wNx+ogor5wTmPToC+0zitl6iAbTIjs/ PZreawf9wrQXgQxEn5HaikF0FPAJrKgoLBLRGwsZelyMxVL06t1VF#BIEIEh0Td9dy9wRQ3XIDUigC3q5jfPs0pG4rHsHmgOGbZ3L BNFvUgR3wD015x8IylyeLDt16oL7RFoTU3Y51hvfGXSI52HxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUrmdKCc04 ptP07B12vvIHN0hcZqG+Gnpw3U+5HxGWks1fc393vCA4smzFnuNZ4/01jLppP4s2hgrAVedr+r90z+8XdsxV root0ise24htts 從ISE CLI生成的公鑰:

public

ssh-rsa
AAAAB3WzaC1yc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06s0+gSykTRr6fdMryIiitCWBs0bGs5yc9S8VKpLyyocsIvc04/
vF/pSHoTE1R3wrZTL1vCIUrGnngdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8g10HLizAdXt08086tkno40cmT/
HAyX0/a9YRZ1L2906pjKSWyuTkbUxWvN9hx/
5E5zpJ4pFr9opg+UaTNX0yYuuj328FGEFdKuFBSujAokP0nJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm
D0Cj6vMaV0L7GZdDI4NZHn7llpptgJFYAb6508 admingise24htts

Linux伺服器上的authorized_key檔案:



4.4.將鍵貼上到檔案後,按ESC,繼續運行wq!命令以儲存檔案。

驗證

1.從Linux伺服器以root使用者身份執行此命令。

tail -f /var/log/secure 必須顯示輸出.如下圖所示。

```
[[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[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: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 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(shd: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.用於ISE驗證。

在GUI上導航到管理>系統>維護>儲存庫。

從Repository List中選擇所需的資料庫,然後選擇Validate。

Identity Services Engine	Home + Context Vaibility + Open	nors + Poley + Administration + V	Vork Centers	
System → identity Management	Network Resources Portal Ma	nagement petitid Services > Feed Service	Threat Centric NAC	
Deployment Licensing + Certificati	es + Logging - Maintenance Upgrad	le + Backup & Restore + Admin Access	 Settings 	
0				
Patch Management	Repository List			
Repository 💿	In Las Law a survey	A Contraction Marine Contract		
Correlational Data Puncing / Edit + Add + Generate Key parts @ Export publick key X Delete / Veldate				
	 Repository Name 	Protocol Host	Path	
	C FTP	ftp 10.88.240.69	/	
	UH-RONFS10-BACKUPS	nfs ICNPS10-nfs.ctp.clarian.org	/ISE_Backups	
	backup	Rp 10.88.240.69	/	
	□ sftp	sftp 10.88.240.69	1	
	sftp_pki	sftp 10.88.240.102	1	

您必須在螢幕右下角看到Server Response彈出視窗。



在CLI中,執行show repo sftp_pki 指令以驗證金鑰。



為了進一步調試ISE,請在CLI上執行以下命令:

debug transfer 7 必須顯示輸出,如下圖所示:



相關資訊

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