使用基于证书的身份验证配置ISE SFTP

目录

简<u>介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>配置</u> <u>1.配置CentOS服务器</u> <u>2.配置ISE存储库</u> <u>3.在ISE服务器上生成密钥对</u> <u>3.1. ISE GUI</u> <u>3.2. ISE CLI</u> <u>4.一体化</u> <u>验证</u> 相关信息

简介

本文档介绍如何将具有CentOS分发的Linux服务器配置为具有面向身份服务引擎(ISE)的公钥基础设施(PKI)身份验证的安全文件传输协议(SFTP)服务器。

先决条件

要求

Cisco 建议您了解以下主题:

- 一般ISE知识
- ISE存储库配置
- •基本Linux常识

使用的组件

本文档中的信息基于以下软件和硬件版本:

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始(默认)配置。如果您的网络处于活动状态,请确保您了解任何命令的潜在影响。

背景信息

为了对文件传输实施安全性,ISE可以通过SFTP通过PKI证书进行身份验证,以确保访问存储库文 件的更安全方式。

配置

1.配置CentOS服务器

1.1以根用户身份创建目录。

mkdir -p /cisco/engineer

1.2.创建用户组。

groupadd tac

1.3.此命令将用户添加到主目录(文件),它指定用户属于组工程师。

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

注意:命**令的/**sbin/nologin部分表示用户无法通过安全外壳(SSH)登录。

1.4.继续创建目录以上传文件。

mkdir -p /cisco/engineer/repo
1.4.1设置目录文件的权限。

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.创建CentOS服务器在其中执行证书检查的目录和文件。

目录:

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

chown engineer:engineer /cisco/engineer/.ssh/authorized_keys chmod 600 /cisco/engineer/.ssh/authorized_keys 1.6.在sshd config系统文件中创建登录权限。

要编辑文件,可以使用vim Linux工具和此命令。

vim /etc/ssh/sshd_config 1.6.1在下面添加指定行。

#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.运行命令以验证sshd_config系统文件同步。**

sshd -t

注意:没有输出表示文件的语法正确。

1.8.继续重新启动SSH服务。

systemctl restart sshd

注意:某些Linux服务器具**有selinux**实施,要确认此参数,可以使用**getenforce**命令。作为建 议,如果它处于强制**模式**,请将其更改为允**许。**

1.9.(可选)编辑semanage.conf文件,将强制设置为允许。

vim /etc/selinux/semanage.conf 添加命令setenforce0。

setenforce0

2.配置ISE存储库

2.1.继续通过ISE图形用户界面(GUI)添加存储库。

导航至"管理">"系统维护">"存储库">"添加"

which Identity Services I	Engine	Home + Contact Visibility	y + Operations +	Policy - Administration	Work Centers
System Identity Mar	nagement >	Network Resources > De	rice Portal Management	petGrid Services + Feed Se	rvice > Threat Centric NAC
Deployment Licensing	+ Certificates	s → Logging - Maintena	nce Upgrade + Back	ap & Restore + Admin Acce	ss → Settings
Patch Management	0	Repository List			
Repository	۲	ten tun ten			
Operational Data Purging		/ EDE + Add + Gene	ate Key pairs 🕃 Export put	sik key X Dekte Division	10

2.2.输入存储库的正确配置。

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	

注意:如果您需要访问repo目录而不是工程师的根目录,则目标路径必须是/repo/。



3.在ISE服务器上生成密钥对

3.1. ISE GUI

导航至管理>系统维护>存储库>生成密钥对,如图所示。

注意:您必须从ISE GUI和命令行界面(CLI)生成密钥对,才能对存储库进行完全双向访问。

Identity Services Er	igine i	Home + Conte	at Visibility + Operation	ons + Policy	· Administration	Work Centers
System Identity Mana	gement >	Network Resource	 > Device Portal Mana 	gement pxGrid S	ervices > Feed Se	vice + Threat Centric NAC
Deployment Licensing	 Certificates 	s → Logging →	Maintenance Upgrade	 Backup & Rest 	ore + Admin Acce	ss → Settings
	9					
Patch Management		Repository List				
Repository	۲	100	L Casardo Kay onlos - C	- Connet sublic law	Voia Ontra	
Operational Data Purging		COX THOU	- cenerate key pars @	Eddout brank wei	Coole Presso	c

3.1.1.输入密码,这是保护密钥对所必需的。

•••••	Enter passphrase :	

注意:在导出公钥之前,首先生成密钥对。

3.1.2.继续导出公钥。

导航至"管理">"系统维护">"存储库">"导出公钥"。

选择**导出公钥**。将生成名为id_rsa.pub**的文件**(确保保存该文件以备将来参考)。

00	Opening id_rsa.pub
You have ch	osen to open:
id_rsa.pul	b
which is: P	EM file (396 bytes)
from: http	s://10.88.240.96
What should	I 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. ISE CLI

3.2.1.导航至要在其中完成存储库配置的节点的CLI。

注意:从此开始,您需要在您希望允许使用PKI身份验证访问SFTP存储库的每个节点上执行 后续步骤。

3.2.2.运行此命令以将Linux服务器的IP添加到host_key系统文件中。

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/7Fj1hyHRkJlKyLh	ClteSpE

3.2.3.生成公共CLI密钥。

crypto key generate rsa passphrase <passphrase>

ise24htts/admin# crypto key generate rsa passphrase admin123

3.2.4.使用此命令从ISE的CLI导出公钥文件。

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

_**注意:**您必须拥有以前可访问的存储库,可以将公钥文件导出到该存储库。

ise24htts/admin# crypto key export public repository FTP

4.一体化

4.1.登录CentOS服务器。

导航至之前在其中配置了authorized_key文件的文件夹。

4.2.编辑授权密钥文件。

运行vim命令以修改文件。

vim /cisco/engineer/.ssh/authorized_keys 4.3.从"生成密钥对"部分复制并粘贴在步骤4和6中生成的内容。

从ISE GUI生成的公钥:

AAAAB3NzaC1yc2EAAAADAQABAAABAQCaH+SANAYb47+NXFyuz06sQ+gSykTRrGfdMryIiitCMBs0bGs5yc9S8VKpLyyocsIvc04/ vF/pSHoTE1R3wrZTL1vCIUrGnnqdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXt0B086tkno40cmT/ HAyX0/a9YRZ1L2906pjK5WyuTkbUxHvN9hx/ 5E5zpJ4pFr9opq+UaTNX0yYuuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm D0Cj6vMaV0L7GZdDI4NZHn7llpptgJFYAb65QB admingise24htts

Linux服务器上的Authorized_key文件:



4.4.将密钥粘贴到文件上后,按ESC键,继续运行wq!命令以保存文件。

验证

1.从Linux服务器以root身份执行此命令。

tail -f /var/log/secure 必须显示输出,如图所示。

[[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[668208]: Accepted publickey for engineer from 10.24.140.234 port 61164 ssh2: RSA SHA256:MNHNp2AtVXD8DbTswgPLKOGBaW FUueObKEWIEkcaeXU 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(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)

2.用于ISE验证。

在GUI上导航至Administration > System > Maintenance > Repository。

从"存储库列表"中选择所需**的存储**库,然后**选择验证**。

-dude Identity Services Engli	10 Home +	Context Vaibility + Op	erations + Policy	- Administration + We	rk Centers
System + Identity Manager	ment > Network Res	ources + Device Portal M	lanagement petiri	d Services > Feed Service	Threat Centric NAC
Deployment Licensing + 0	Certificates + Logging	Maintenance Upg	rade 🔸 Backup & R	lestore + Admin Access +	Settings
	0				
Patch Management	Reposito	ry List			
Repository	()	And A descent for solution	(A Contraction	Marian Californi	
Operational Data Purging	/ tot -	Add -Generate key pair	 Be extent brank wei 	Conte Diversione	
	Repos	itory Name	 Protocol 	Host	Path
	C FTP		fip .	10.88.240.69	/
	200-10	OVF510-BACKUPS	nfs	ICNFS10-rds.chp.clarian.org	/ISE_Backups
	backu	p	fo	10.88.240.69	/
	□ sftp		sto	10.88.240.69	1
	🗹 sftp.g	ki	sto	10.88.240.102	1

您必须看到一个弹出窗口,该弹出窗口在屏**幕右**下角显示"服务器响应"。



在CLI中,运行命令show repo sftp_pki以验证密钥。



要进一步调试ISE,请在CLI上执行以下命令:

debug transfer 7 必须显示输出,如图所示:



相关信息

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