인증서 기반 인증으로 ISE SFTP 구성

목차

소개

이 문서에서는 CentOS 배포가 있는 Linux 서버를 ISE(Identity Services Engine)에 대한 PKI(Public Key Infrastructure) 인증을 사용하는 SFTP(Secure File Transfer Protocol) 서버로 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 일반 ISE 지식
- ISE 저장소 구성
- 기본 Linux 일반 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 2.2
- ISE 2.4
- ISE 2.6
- ISE 2.7
- ISE 3.0
- CentOS Linux 릴리스 8.2.2004(코어)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우, 모든 명령의 잠재적 영향을 이해해야 합니다.

배경 정보

파일 전송에 보안을 적용하기 위해 ISE는 SFTP를 통해 PKI 인증서를 통해 인증하여 저장소 파일에 더 안전하게 액세스할 수 있습니다.

구성

1. CentOS 서버 구성

1.1 루트 사용자로 디렉토리를 생성합니다.

```
mkdir -p /cisco/engineer
```

1.2. 사용자 그룹을 생성합니다.

```
groupadd tac
```

1.3. 이 명령은 사용자를 Main 디렉터리(파일)에 추가하고 사용자가 그룹 **엔지니어**에 속하도록 지정합니다**.**

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

> **참고:**명령의 /sbin/nologin 부분은 사용자가 SSH(Secure Shell)를 통해 로그인할 수 없음을 나타냅니다.

1.4. 계속해서 파일을 업로드할 디렉토리를 생성합니다.

```
mkdir -p /cisco/engineer/repo
```

1.4.1 디렉토리 파일에 대한 권한을 설정합니다.

```
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 서버가 인증서 확인을 수행하는 디렉토리와 파일을 만듭니다.

디렉터리:

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

파일:

```
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** 시스템 파일에 로그인 권한**을** 생성합니다.

파일을 편집하려면 **vim** Linux 툴을 이 명령과 함께 사용할 수 있습니다.

```
vim /etc/ssh/sshd_config
```

1.6.1 아래에 지정된 행을 추가합니다.

```
#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** 시스템 파일 동기화를 확인하려면 명령을 실행합니다.

```
sshd -t
```

참고:출력 없음은 파일의 구문이 정확함을 의미합니다.

1.8. SSH 서비스를 다시 시작합니다.

```
systemctl restart sshd
```

참고:일부 Linux 서버에는 **seleclinux**가 적용되어 있으므로 이 매개변수를 확인하려면 getenforce 명령**을** 사용할 수 있습니다.권장 사항으로, **시행** 모드인 경우 허용으로 **변경합니다** .

1.9. (선택 사항) **semanage.conf** 파일을 편집하여 시행이 허용되도록 설정합니다.

```
vim /etc/selinux/semanage.conf
```

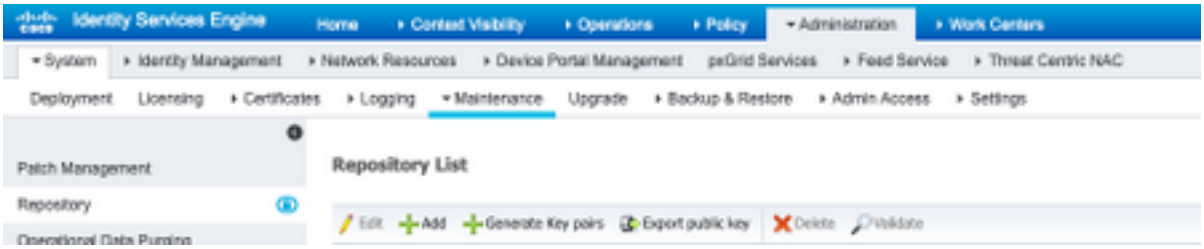
setenforce **0** 명령을 **추가합니다.**

```
setenforce0
```

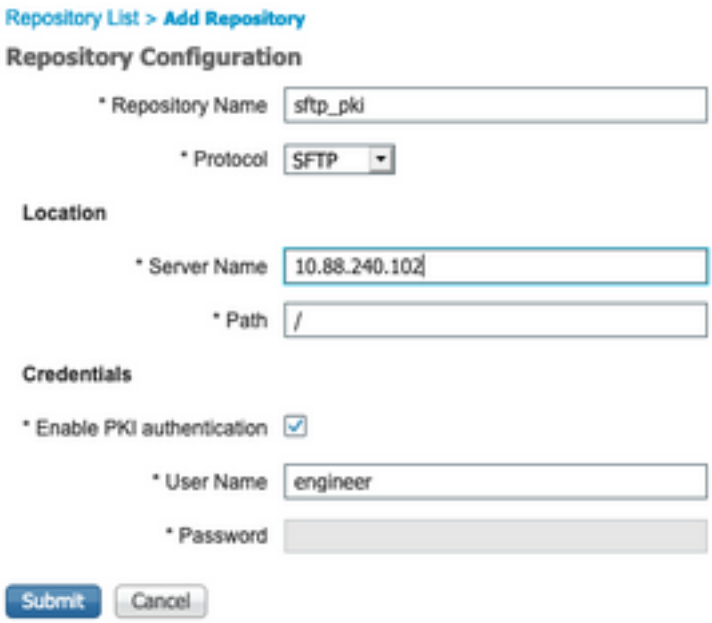
2. ISE 저장소 구성

2.1. ISE 그래픽 사용자 인터페이스(GUI)를 통해 저장소를 계속 추가합니다.

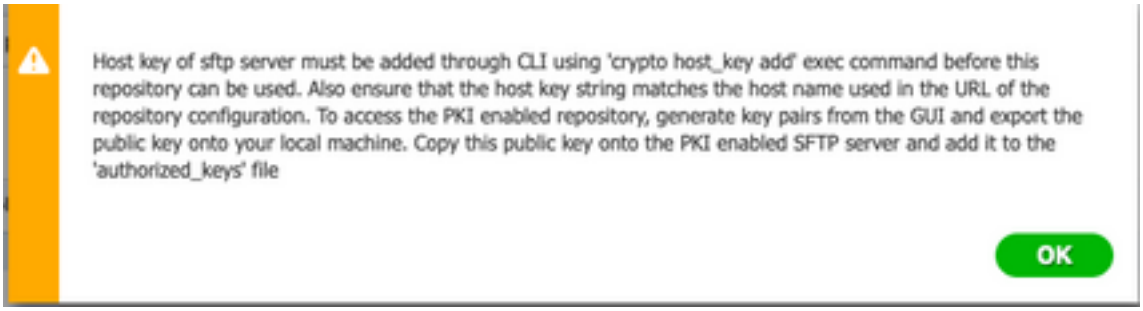
관리**>시스템 유지 관리>저장소>추가를 선택합니다.**



2.2. 저장소에 적합한 구성을 입력합니다.



참고:엔지니어의 루트 디렉토리 대신 repo 디렉토리에 액세스해야 하는 경우 대상 경로는 /repo/여야 합니다.

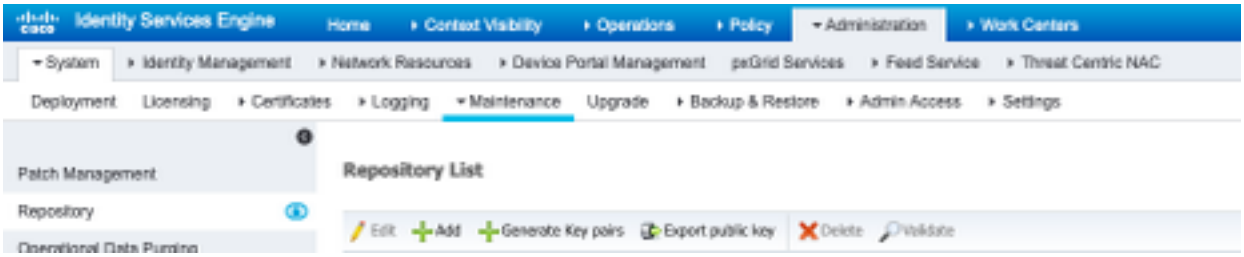


3. ISE 서버에서 키 쌍을 생성합니다.

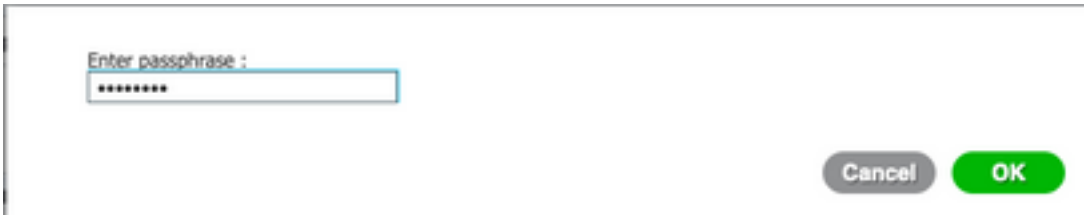
3.1. ISE GUI

이미지에 표시된 대로 **Administration>System Maintenance>Repository>Generate 키 쌍**으로 이동합니다.

참고:저장소에 대한 전체 양방향 액세스를 얻으려면 ISE GUI 및 CLI(Command Line Interface)에서 키 쌍을 생성해야 합니다.



3.1.1. 키 쌍을 보호하기 위해 필요한 암호 문구를 입력합니다.

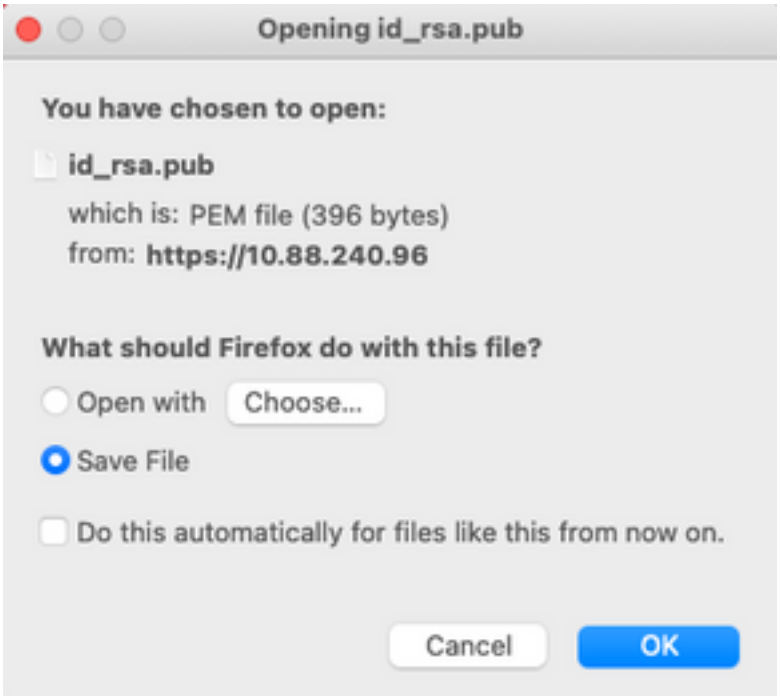


참고:공개 키를 내보내기 전에 먼저 키 쌍을 생성합니다.

3.1.2. 공개 키를 내보냅니다.

관리>**시스템 유지 관리>저장소>공개 키 내보내기로 이동합니다.**

공개 키 내보내기를 선택합니다.id_rsa.pub라는 이름으로 파일이 생성됩니다(나중에 참조할 수 있도록 저장되었는지 확인).



3.2. ISE CLI

3.2.1. 저장소 구성을 완료할 노드의 CLI로 이동합니다.

참고:이 시점부터 PKI 인증을 사용하여 SFTP 저장소에 대한 액세스를 허용하려는 각 노드에 다음 단계가 필요합니다.

3.2.2. Linux 서버의 IP를 **host_key** 시스템 파일에 추가하려면 이 명령을 실행합니다.

```
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/7Fj1hyHRkJlKyLhJCIteSpE
```

3.2.3. 공용 CLI 키를 생성합니다.

```
crypto key generate rsa passphrase <passphrase>
```

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

3.2.4. 이 명령을 사용하여 ISE의 CLI에서 공개 키 파일을 내보냅니다.

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

참고:공개 키 파일을 내보낼 수 있는 이전에 액세스 가능한 저장소가 있어야 합니다.

```
ise24htts/admin# crypto key export public repository FTP
```

4. 통합

4.1. CentOS 서버에 로그인합니다.

이전에 authorized_**key** 파일을 구성한 폴더**로** 이동합니다.

4.2. 인증된 키 파일을 편집합니다.

파일을 수정하려면 vim 명령을 실행합니다.

```
vim /cisco/engineer/.ssh/authorized_keys
```

4.3. Generate key pairs 섹션에서 **4** 및 **6** 단계에서 생성된 내용**을** 복사하여 붙여넣습니다.

ISE GUI에서 생성된 공개 키:

id_rsa.pub

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjcgqs8705ic8wTP16Grmf8r3WNx+ogorSuTmPToC+0zjtl6iAbTIjs/
PZreawf9urQXgQxEnSHa1kF0FPAJrKqoLBlRGusZelyNxVL06tiVFxBIEIEhQTd9dy9uRQ3XIDUigC3q5jfPsQpG4rHsHmgOGbZJL
8NFvUgRJwO01Sx8IylyeLDtl6oL7RFoTU3Y51hvfGXSI5ZHxoGKsXjm2hA0+rkbbfPfQy37LT7wBHpAEaEVgLXL4o3mFUYmdKCc04
ptPQ7B12vvIMNOhcZqG+Gnpw3U+SHxGWks1fcJ93vCA4smzFnuNZ4/Q1jLppP4s2hqrAVedr+r90z+8XdsxV root@ise24htts
```

ISE CLI에서 생성된 공개 키:

public

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCaH+5ANAYb47+NXFyuzO6sQ+gSykTRrGfdMryIiitCWBsObGs5yc9S8VKpLyyocsIvco4/
vF/pSHoTE1R3wrZTL1vCIUrGnnqdQv4+0YnIbJ/f8EgZnXQ+fLK8oyLeVxPgd8cewL3HMV8giQHLizAdXtQB0B6tkno4OcmT/
HAyXQ/a9YRZ1l29D6pjK5WyuTkbUxWvN9hx/
5E5zpJ4pFr9opq+UaTNXOyYuuj328FGEFdKuFBSujAokPOnJTLN8GdLAQ6x4kkkcXWXkT8F1saPZwyJuqY8FNWtyiFIVY5Ct5G0zm
D0Cj6vMaV0L7GZdDI4NZHn7llpptqJFYAb65QB admin@ise24htts
```

Linux 서버의 **authorized_key** 파일:

4.4. 파일에 키를 붙여넣은 후 Esc 키를 누르고 wq를 계속 **실행합니다!**명령을 사용하여 파일을 저장합니다.

다음을 확인합니다.

1. Linux 서버에서 이 명령을 루트로 실행합니다.

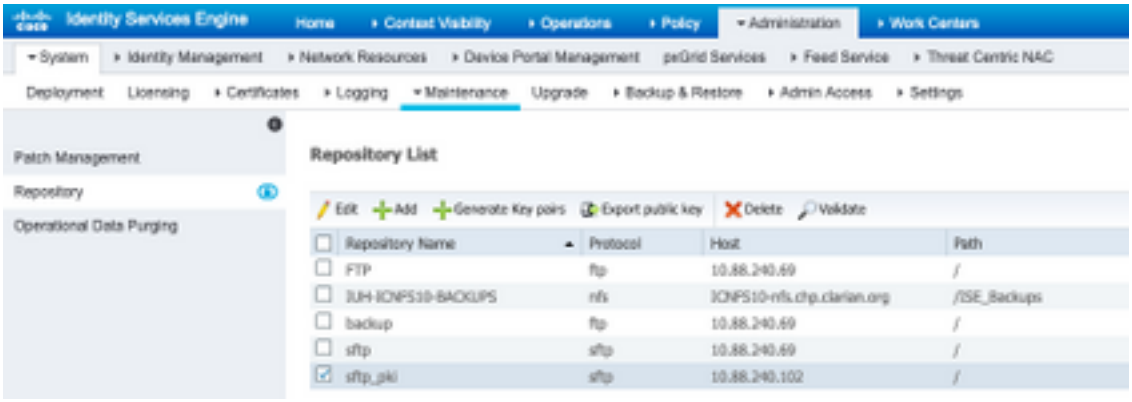
```
tail -f /var/log/secure
```

이미지에 표시된 대로 출력이 표시되어야 합니다.

2. ISE 확인용

GUI에서 **Administration>System>Maintenance>Repository**로 이동합니다.

저장소 목록에서 원하는 저장소**를** 선택하고 **검증**을 **선택합니다**.



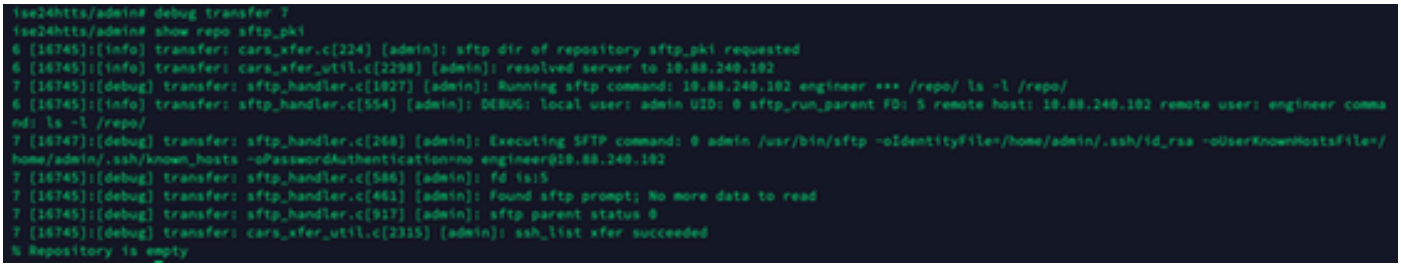
화면 오른쪽 하단에 **Server Response(서버 응답)**가 표시된 팝업이 표시되어야 합니다.

CLI에서 show repo sftp **_pki** 명령을 실행하여 키를 검증합니다.

ISE를 추가로 디버깅하려면 CLI에서 다음 명령을 실행합니다.

```
debug transfer 7
```

이미지에 표시된 대로 출력이 표시되어야 합니다.



관련 정보

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