تكوين ISE SFTP بمصادقة مستندة إلى شهادة

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين خادم Linux مع توزيع CentOS كخادم برروتوكول نقل الملفات الآمن (SFTP) باستخدام مصادقة البنية الأساسية للمفتاح العام (PKI) والوصول إلى محرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معلومات عامة عن ISE
- تكوين مستودع ISE
- معرفة Basic Linux العامة

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISE 2.2
- ISE 2.4
- ISE، الإصدار 2.6
- ISE، الإصدار 2.7

- ISE 3.0
- CentOS Linux، الإصدار 8.2.2004 (Core)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فيرجى التأكد من فهم للتأثير المحتمل لأي أمر.

معلومات أساسية

ولفرض الأمان لعمليات نقل الملفات، يمكن أن يقوم ISE بالمصادقة عبر شهادات PKI من الخالل SFTP لضمان طريقة أكثر أمانا للوصول إلى ملفات المستودعات.

التكوين

1. تكوين خادم CentOS

1.1 إنشاء دليل كمستخدم جذري.

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

1.2. إنشاء مجموعة مستخدمين.

```
groupadd tac
```

1.3. يضيف هذا الأمر المستخدم إلى الدليل الرئيسي (الملفات)، ويحدد المستخدم بأنه ينتمي إلى **مهندسي** المجموعة.

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

> **ملاحظة**: يشير جزء **/sbin/nologin** من الأمر إلى أن المستخدم لن يتمكن من تسجيل الدخول من خالل طبقة الأمان (SSH).

1.4. انتقل إلى إنشاء الدليل لتحميل الملفات.

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

1.4.1 تعيين الأذونات لملفات الدليل.

```
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. قم بإنشاء الدليل والملف الذي يقوم فيه خادم CentOS بالتحقق من الشهادات.

الدليل:

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

```
touch /cisco/engineer/.ssh/authorized_keys
chown engineer:engineer /cisco/engineer/.ssh/authorized_keys
chmod 600 /cisco/engineer/.ssh/authorized_keys
```
1.6. قم بإنشاء نسخة احتياطية من ملف تكوين الخادم **sshD_config**.

in order to تحرير الملف، أنت تستطيع استخدام **vim** Linux أداة مع هذا الأمر.

```
vim /etc/ssh/sshd_config
```
1-6-1 إضافة البنود المحددة أدناه.

```
#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. قم بتشغيل الأمر للتحقق من مزامنة ملف تكوين **ssh**_config.

```
sshd -t
```

ملاحظة: لا يوجد إخراج يعني أن صياغة الملف صحيحة.

1.8. قم بالمتابعة لإعادة تشغيل خدمة SSH.

```
systemctl restart sshd
```

ملاحظة: تحتوي بعض خوادم Linux على تطبيق **Selinux**، لتأكيد هذه المعلمة، يمكنك إدخال الأمر **getenforce**. وتوصية، إذا كانت في وضع **الإنفاذ**، فإنها تغيرها إلى **التسامح**.

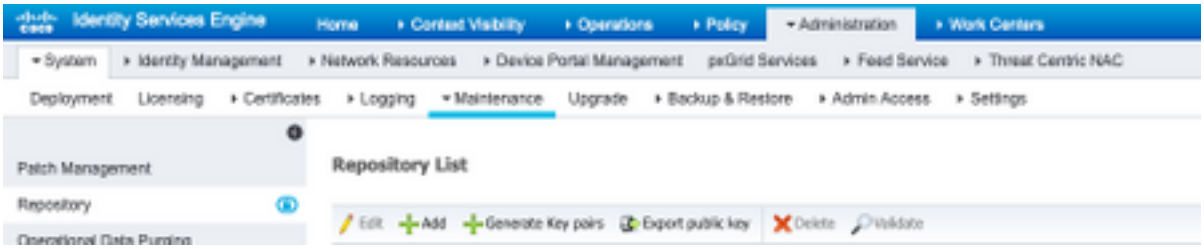
1.9. (إختياري) قم بتحرير ملف **semanage.conf** لتعيين عملية الإنفاذ على السماح.

```
vim /etc/selinux/semanage.conf
```
قم بإضافة الأمر **setenforce0.**

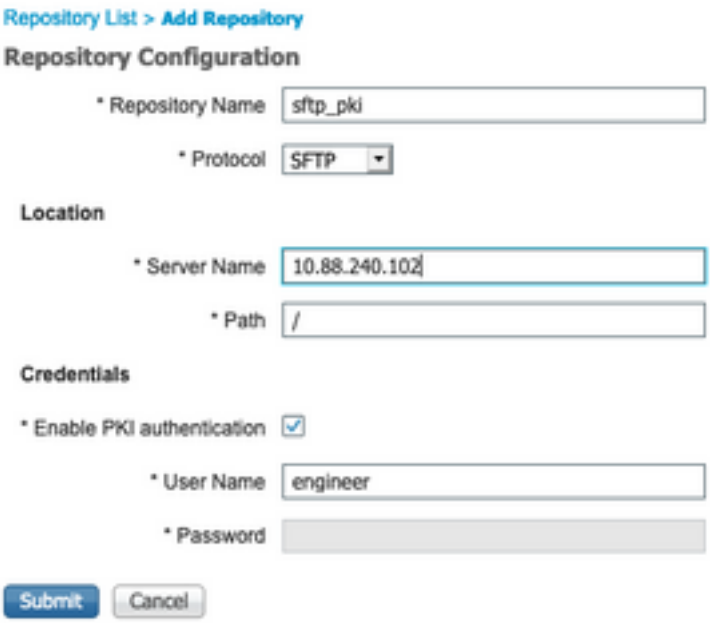
```
setenforce0
```
2. تكوين مستودع ISE

2.1. انتقل إلى إضافة المستودع من خلال واجهة المستخدم الرسومية ISE (GUI).

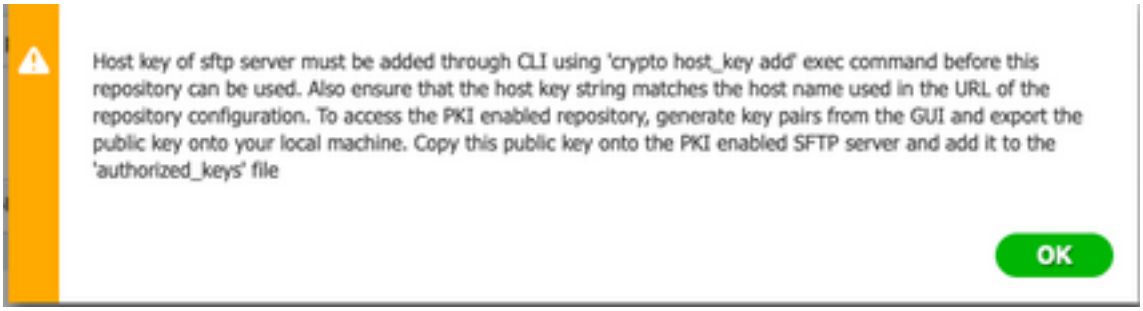
انتقل إلى **الإدارة>صيانة النظام>إضافة مستودع>Add**



2.2. أدخل التكوين المناسب للمستودع.



ملاحظة: إذا كنت بحاجة إلى الوصول إلى دليل إعادة الشراء بدلا من الدليل الجذر للمهندس، يجب أن يكون المسار الهدف /repo/.

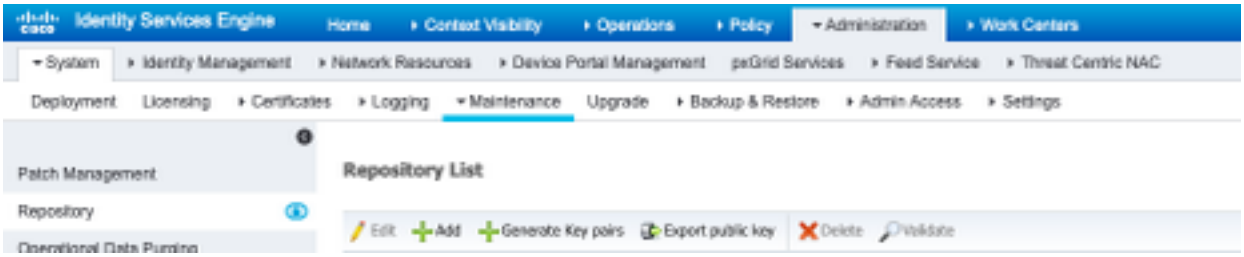


3. إنشاء أزواج مفاتيح على خادم ISE

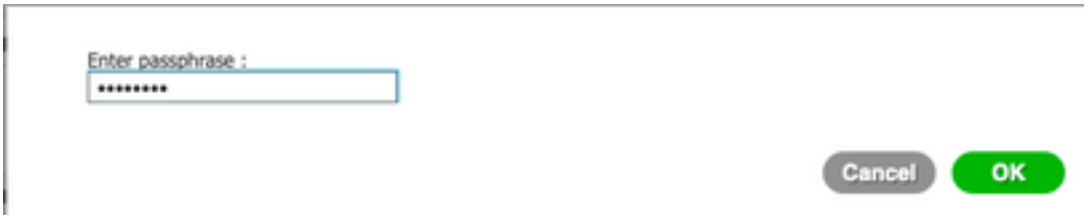
3-1 ISE GUI

انتقل إلى **إدارة>صيانة النظام>المستودع>قم بإنشاء أزواج المفاتيح**، كما هو موضح في الصورة.

ملاحظة: يجب عليك إنشاء أزواج مفاتيح من واجهة المستخدم الرسومية (ISE) وواجهة سطر الأوامر (CLI)، للحصول على وصول ثنائي الإتجاه كامل إلى المستودع.



3.1.1. أدخل عبارة مرور، وهذا مطلوب لحماية زوج المفاتيح.

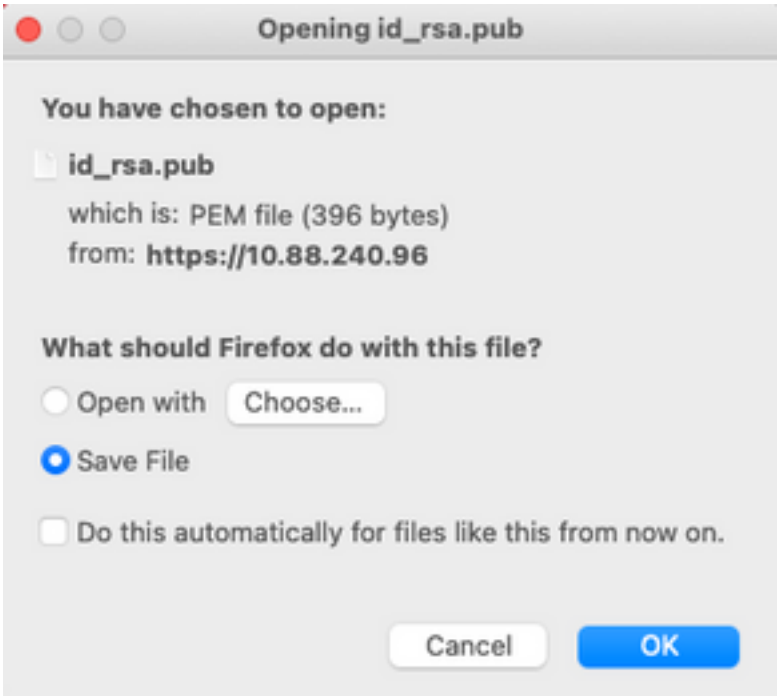


ملاحظة: قم أولا بإنشاء أزواج المفاتيح قبل تصدير المفاتيح العامة.

3-1-2- المضي قدما في تصدير المفتاح العام.

انتقل إلى **الإدارة>صيانة النظام>المستودع>تصدير المفتاح العام.**

حدد **تصدير المفتاح العام**. يتم إنشاء ملف باسم **id_rsa.pub** (تأكد من حفظ هذا الأمر للمراجع المستقبلية).



3-2 ISE CLI

3.2.1. انتقل إلى CLI الخاص بالعقدة التي تريد إنهاء تكوين المستودع فيها.

ملاحظة: من هذه النقطة فصاعدا، يلزم إتخاذ الخطوات التالية على كل عقدة ترغب في السماح بالوصول إلى مستودع SFTP باستخدام مصادقة PKI.

3.2.2. قم بتشغيل هذا الأمر من أجل إضافة عنوان IP الخاص بخادم Linux إلى ملف نظام **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/7Fj1hyHRkJlKyLhJCIteSpE
```

3.2.3. إنشاء مفتاح CLI عام.

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

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

3.2.4. تصدير ملفات المفاتيح العامة من CLI الخاص ب ISE باستخدام هذا الأمر.

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

ملاحظة: يجب أن يكون لديك مستودع يمكن الوصول إليه مسبقا والذي يمكنك تصدير ملف المفاتيح العام إليه.

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

4 - التكامل

4.1. سجل الدخول إلى خادم CentOS.

انتقل إلى المجلد الذي قمت فيه مسبقا بتكوين الملف **authorized_key**.

4-2- تحرير ملف المفاتيح المعتمد.

قم بتشغيل الأمر vim لتعديل الملف.

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

4.3. انسخ المحتوى الناتج عن الخطوات **4** و**6** ولصقه من قسم **إنشاء أزواج المفاتيح**.

تم إنشاء المفاتيح العام من واجهة المستخدم الرسومية (GUI) الخاصة ب ISE:

المفتاح العام الذي تم إنشاؤه من واجهة سطر الأوامر ISE:

Authorized_key file على خادم ليونكس:

4.4. بعد أن تقوم بلصق المفاتيح في الملف، اضغط مفتاح ESC، انتقل إلى تشغيل الأمر **wq!** لحفظ الملف.

التحقق من الصحة

1. من خادم ليونكس قم بتنفيذ هذا الأمر كجذر.

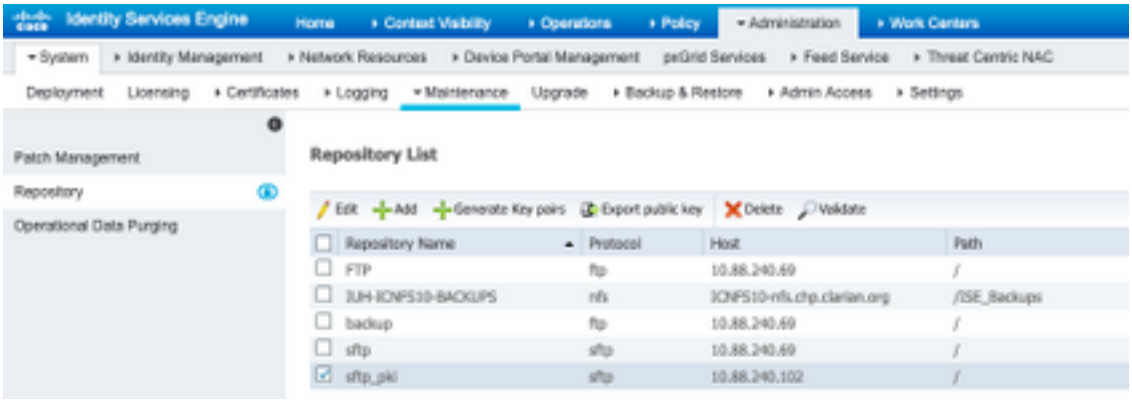
```
tail -f /var/log/secure
```

يجب عرض الإخراج، كما هو موضح في الصورة.

2. للتحقق من إخصاصات محرك خدمات الهوية.

انتقل إلى **Administration>System>Maintenance>مستودع** على واجهة المستخدم الرسومية.

حدد المستودع المرغوب فيه من **قائمة المستودع** وحدد **التحقق من الصحة**.



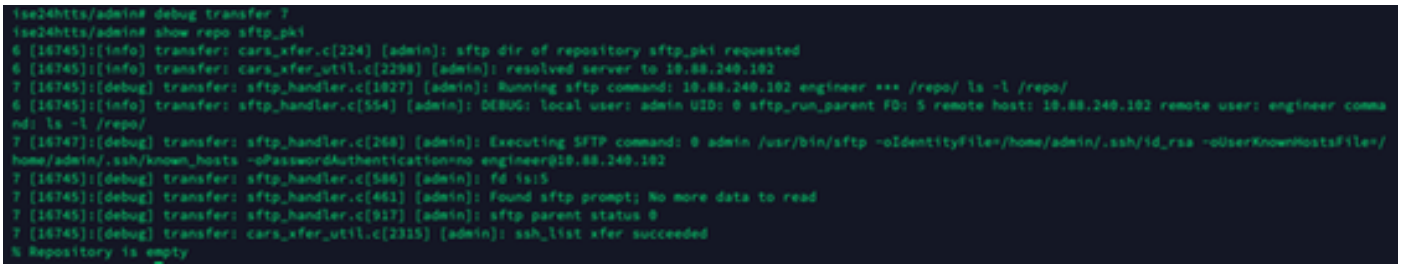
يجب أن ترى منبثقة توضح **إستجابة الخادم** في أسفل الزاوية اليمنى من الشاشة.

من واجهة سطر الأوامر (CLI)، قم بتشغيل الأمر **show repo sftp_pki** للتحقق من صحة المفاتيح.

in order to إضافي صححت ISE، نفذت هذا أمر على CLI:

```
debug transfer 7
```

يجب عرض الإخراج، كما هو موضح في الصورة:



معلومات ذات صلة

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).