

使用 Cisco pxGrid 部署证书

证书颁发机构 (CA) 签名的 ISE pxGrid 节点和 CA 签名的 pxGrid 客户端

目录

关于本文档	3
简介	4
证书配置示例	5
CA 签名的 ISE pxGrid 节点证书和 pxGrid 角色配置	5
pxGrid 客户端证书配置	7
测试 pxGrid 客户端和 ISE pxGrid 节点	12
查看密钥库条目	13
故障排除	21

关于本文档

本文档说明使用证书颁发机构配置 pxGrid 客户端和 ISE pxGrid 节点所需的配置步骤。本文档面向部署 Cisco pxGrid 的思科现场工程师、技术营销工程师、合作伙伴和客户。读者需要熟悉 pxGrid。

如果读者不熟悉 pxGrid，请参阅 [Configure_and_Test_Integration_with_Cisco_pxGrid.pdf](#)：

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

pxGrid sdk 可从思科客户团队获取。

本文档假设已安装思科身份服务引擎 (ISE) 1.3。对于 pxGrid 客户端，可以使用运行 OSX 10.8.5 的 MAC，或者 Linux 操作系统。此外，pxGrid 客户端需要具备 Oracle Java Development Kit 7 或 8。

在《*使用证书部署 pxGrid*》系列中还有两个文档：

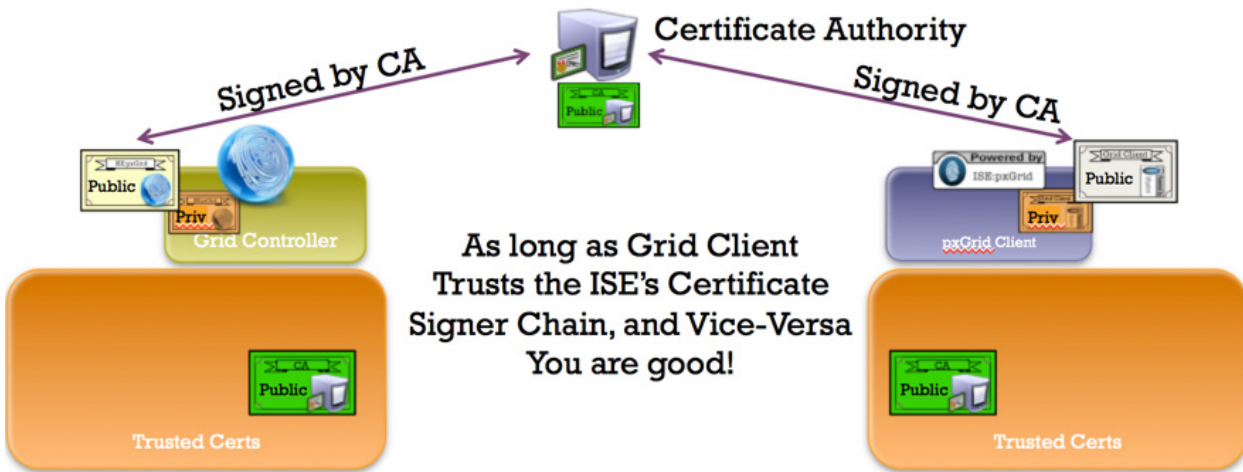
- 将自签名证书与 ISE pxGrid 节点和 pxGrid 客户端配合使用
- 使用证书颁发机构 (CA) 签名的 pxGrid 客户端和自签名 ISE pxGrid 节点证书

简介

本节详细介绍 ISE 独立部署中 pxGrid 客户端和 ISE pxGrid 节点的证书颁发机构 (CA) 签名证书配置。ISE pxGrid 节点和 pxGrid 客户端将从 Microsoft Enterprise CA 2008 R2 机构获取签名证书。请注意，必须创建具有同时用于客户端身份验证 (1.3.6.5.5.7.3.2) 和服务端身份验证 (1.3.6.1.5.5.7.3.1) 的增强型密钥使用 (EKU) ISO 定义的对象标识符 (OID) 的自定义 pxGrid 模板。ISE pxGrid 节点会将 CA 根证书下载到其受信任证书库，而 pxGrid 客户端会将根证书下载到受信任密钥库。

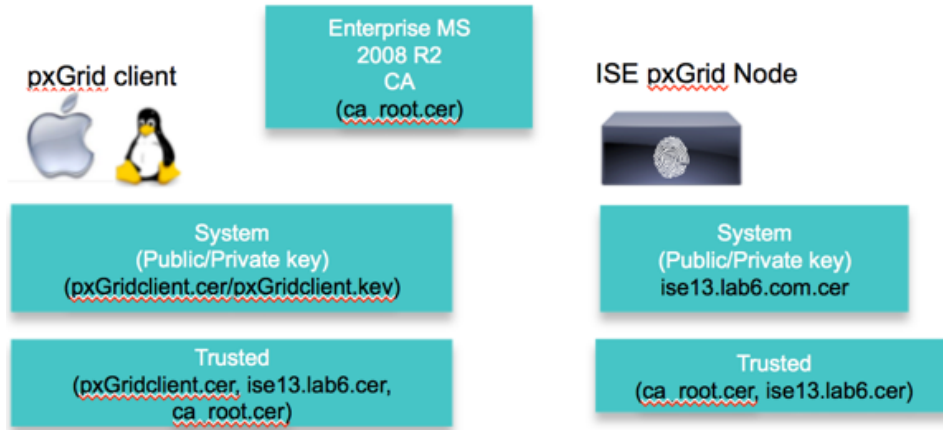
当 pxGrid 客户端连接到 ISE pxGrid 节点时，为使 pxGrid 连接成功，两个公共证书对于简单身份验证和安全层 (SASL) 而言都将是受信任的。

下图显示证书信息流。



证书配置示例

本文中使用的证书示例如下：

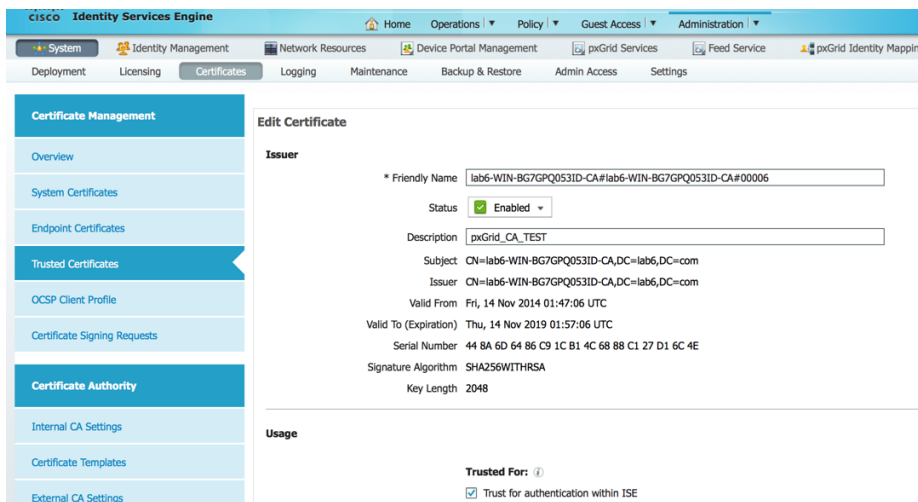


Keystore values:
 pxGridclient.iks- used for keystoreFilename in pxGrid script
 root3.jks- used for truststoreFilename in pxGrid script

CA 签名的 ISE pxGrid 节点证书和 pxGrid 角色配置

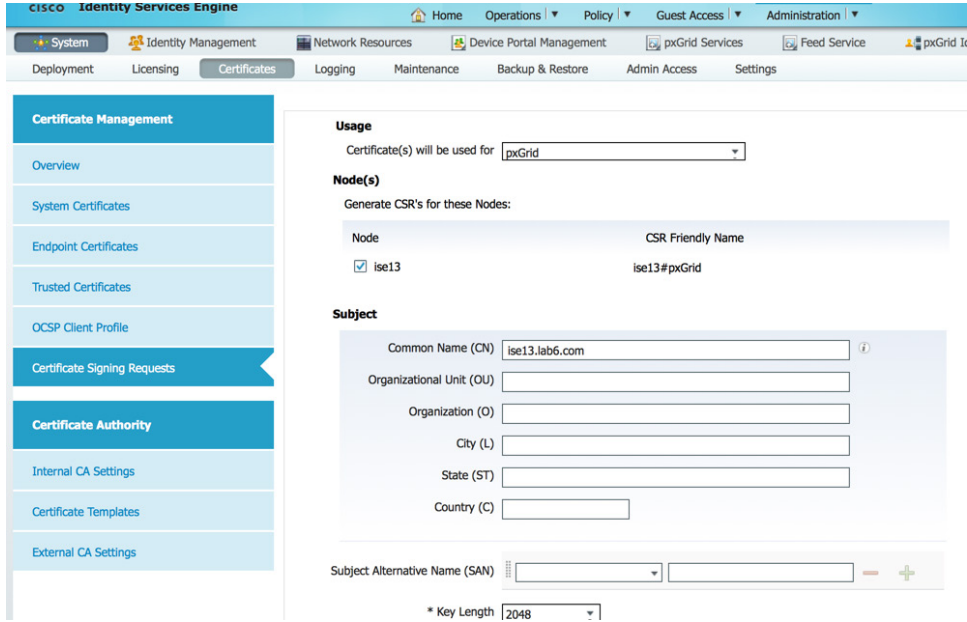
本节详细介绍 CA 签名的 ISE pxGrid 证书过程及如何将 CA 根证书导入到 ISE 受信任证书库中。将 CA 证书上传到受信任库并且 ISE 证书绑定到 CSR 请求后，即可在 ISE 节点上启用 pxGrid 角色并将其设为主用。

步骤 1 下载 CA root 证书并将其上传至 ISE 受信任证书库中，然后启用 Trust for ISE communication。



步骤 2 生成需要向 CA 机构提出的使用 pxGrid 的 ISE CSR 请求。必须为客户端身份验证和服务器身份验证的 EKU 配置 pxGrid 模板，以便为用户证书请求提供服务。

Administration -> System -> Certificates -> Certificate Signing Requests -> 生成具有 ISE FQDN 的 CSR 并设置用于 pxGrid。



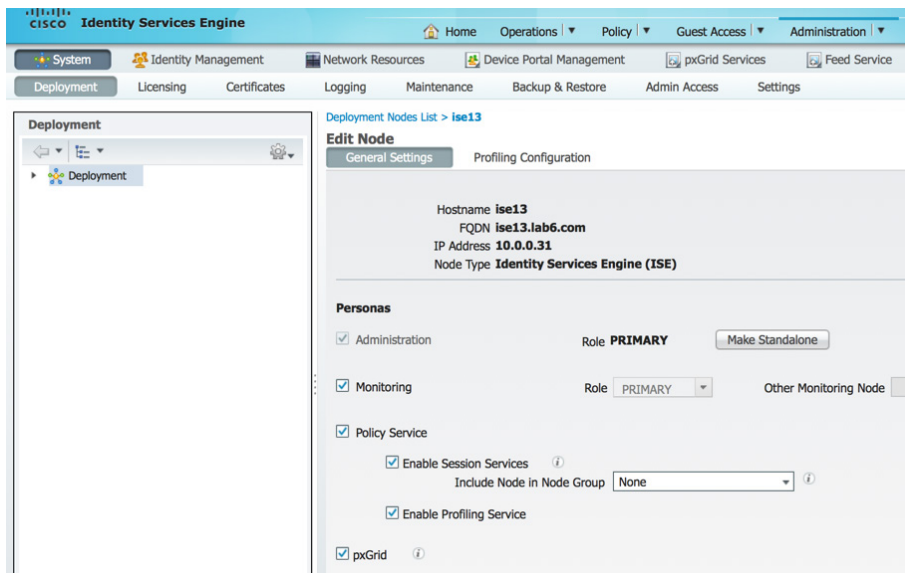
The screenshot shows the 'Certificate Signing Requests' configuration page in the ISE Administration console. The left sidebar is expanded to 'Certificate Management' > 'Certificate Signing Requests'. The main content area is titled 'Usage' and 'Node(s)'. Under 'Usage', 'Certificate(s) will be used for' is set to 'pxGrid'. Under 'Node(s)', 'Generate CSR's for these Nodes:' is checked, and a table lists the node 'ise13' with the CSR Friendly Name 'ise13#pxGrid'. The 'Subject' section contains several input fields: 'Common Name (CN)' is 'ise13.lab6.com', 'Organizational Unit (OU)', 'Organization (O)', 'City (L)', 'State (ST)', and 'Country (C)' are all empty. Below the subject fields is a 'Subject Alternative Name (SAN)' field with a dropdown menu and a '+' button. At the bottom, the '* Key Length' is set to '2048'.

步骤 3 从 CA 下载证书并绑定证书。

Administration -> Certificates -> Certificate Signing Requests -> 绑定证书。

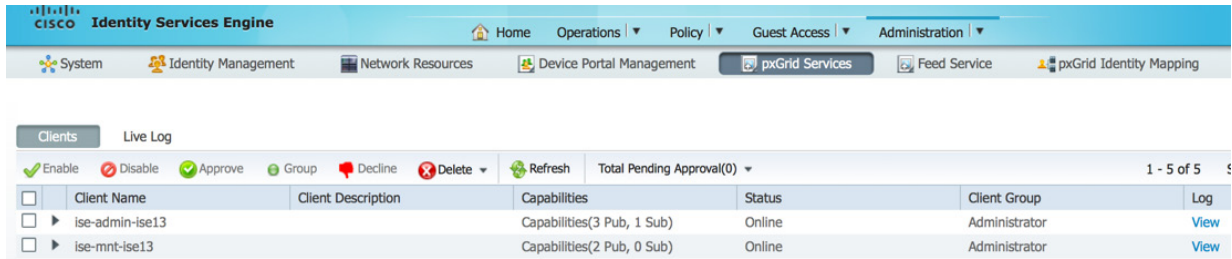
步骤 4 在 ISE 上启用 pxGrid。

Administration -> System -> Deployment -> 启用 pxGrid 并设为主用。



The screenshot shows the 'Deployment' configuration page for node 'ise13' in the ISE Administration console. The left sidebar is expanded to 'Deployment' > 'Deployment'. The main content area is titled 'Edit Node' and 'General Settings'. The node information is: Hostname 'ise13', FQDN 'ise13.lab6.com', IP Address '10.0.0.31', and Node Type 'Identity Services Engine (ISE)'. Under 'Personas', 'Administration' is checked with Role 'PRIMARY' and a 'Make Standalone' button; 'Monitoring' is checked with Role 'PRIMARY' and an 'Other Monitoring Node' field; 'Policy Service' is checked with 'Enable Session Services' checked and 'Include Node in Node Group' set to 'None'; 'Enable Profiling Service' is checked; and 'pxGrid' is checked.

步骤 5 您应该看到 pxGrid 服务已启动。
Administration -> pxGrid Services。



注：在 ISE 发布节点出现之前，可能会有延迟。在启用 pxGrid 角色之前，必须安装证书。

pxGrid 客户端证书配置

本节分步完成 pxGrid 客户端 CA 签名证书过程。生成公钥/私钥对后，将根据私钥 pxGridClient.key 生成 PKCS12 文件。

该 PKCS12 文件将导入到身份密钥库 pxGridClient.jks 中。此身份密钥库和关联的密码将用作 pxGrid 脚本中的 keystoreFilename 和 keystorePassword。pxGrid 客户端证书 pxGridClient.cer 也将添加到密钥库。

批量下载会话所需的 ISE 身份证书 isemnt 及 CA 根证书都将添加到信任密钥库 root3.jks。此信任密钥库和关联的密码将用作 pxGrid 脚本中的 truststoreFilename 和 truststorePassword。

步骤 1 为 pxGrid 客户端生成私钥（例如 pxGridClient.key）。

```
openssl genrsa -out pxGridClient.key 4096

Generating RSA private key, 4096 bit long modulus
.....++
.....++
e is 65537 (0x10001)
```

步骤 2 生成需要向 CA 机构提出的 CSR 请求（例如 pxGridClient.csr）。提供质询密码（例如 cisco123）

```
openssl req -new -key pxGridClient.key -out pxGridClient.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
```

```
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:Eppich, Inc
```

注：确保本文档各处的密码相同，这样更易于维护，并可减少错误。

步骤 3 CA 机构必须使用具有客户端身份验证和服务器身份验证的 EKU 的 pxGrid 模板为用户证书提供服务。

注：由于已选择 Windows 2003 的 CA 模板，所以它会出现在下拉列表中。使用客户端身份验证和服务器身份验证的 EKU 复制了用户模板。

Microsoft Active Directory Certificate Services -- lab6-WIN-BG7GPQ053ID-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 request by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

LOCAQEAXjh+u8GMpwxadhin6yxCwKY18YhOY5jrURxf
wcs4Joq7PY4tQ6a/1Gik3chergzdBkQMyXVzhXZhg
Prz3cMqOCyAsTxhn8NlfsvLZYk5ayPpmuah3iL3
Hm+6thRTVhrKOC61ejxFd+0lzQxEn19YMov7sRSWFU1
jlf+Z+ptK87AYGzPYWw/ki86b8TG1hSuMMF+Aglcn
0Q23iwmr4qgVabyhP6nmku4iQ8g==
-----
JEST-----

```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

步骤 4 根据 pxGridClient 证书（例如 pxGridClient.cer）中的私钥创建 pxGrid 客户端 .pkcs12 文件（pxGridClient.p12）。此文件将用于密钥库管理，并且其文件名可以是扩展名为 .p12 的随机文件名，包括 CA 根文件（例如 ca_root）。

```
openssl pkcs12 -export -out pxGridClient.p12 -inkey pxGridClient.key -in pxGridClient.cer -chain -CAfile
ca_root.cer
```

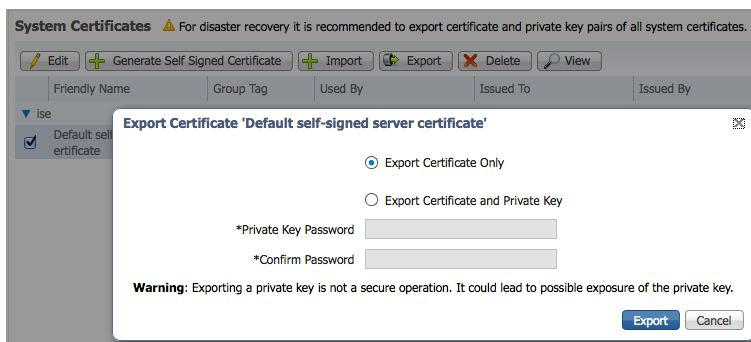
```
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```


步骤 5 创建 pxGrid 客户端身份密钥库（例如 pxGridClient.jks）。此密钥库将成为 pxGrid 客户端身份密钥库。其文件名可以是扩展名为 .jks 的随机文件名，它将用作 pxGrid 脚本示例中的密钥库文件名和关联密钥库密码。

```
keytool -importkeystore -srckeystore pxGridClient.p12 -destkeystore pxGridClient.jks -srcstoretype PKCS12

Enter destination keystore password: cisco123
Re-enter new password: cisco123
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

步骤 6 仅将公共 ISE 身份证书导出到 pxGrid 客户端中，请注意导出文件将采用 .pem 格式。您可以重命名扩展名为 .pem 的文件，使其更易于读取。在本示例中，该文件已重命名为 isemnt.pem。



步骤 7 将 .pem 文件转换为 .der 格式。

```
openssl x509 -outform der -in isemnt.pem -out isemnt.der
```

步骤 8 将 ISE 身份证书添加到信任密钥库（例如 root3.jks），此密钥库将是受信任密钥库。其文件名可以是扩展名为 .jks 的随机文件名。这将成为 pxGrid 脚本中使用的信任库文件名和信任库密码。

```
keytool -import -alias isemnt -keystore root3.jks -file isemnt.der

Enter keystore password: cisco123
Re-enter new password: cisco123

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d76000000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
    MD5: 2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
    SHA1: BD:18:C0:DD:4D:DD:43:80:CA:CA:3B:F6:DC:1E:6E:46:93:59:FE:B7
    SHA256:
F9:11:FC:EC:BC:0F:0F:84:36:F1:26:BC:5A:09:B7:2B:3C:D1:1B:AC:FC:1A:F1:AB:6D:00:8D:11:F8:26:93:FF
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ..0...*.H.....
```

```

0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ..0...+....0...*
0030: 86 48 86 F7 0D 03 07 .H.....

#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0.
0010: 06 08 2B 06 01 05 05 07 03 02 30 0A 06 08 2B 06 ..+.....0...+.
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 .....0...+.....
0030: 37 0A 03 04 7...

#3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false
0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.%+.....7.....
0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF 40 02 01 64 02 01 03 ^...#...@.d...

#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
    accessMethod: caIssuers
    accessLocation: ldap:///CN=lab6-WIN-BG7GPQ053ID-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?cACertificate?base?objectCla
ss=certificationAuthority
  ]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
]

#6: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-
BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint]
  ]]

#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
  [ ] ]
]

#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
]

#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`..
0010: AF D8 07 09 ....
]
]

```

```
Trust this certificate? [no]: yes  
Certificate was added to keystroke
```

步骤 9 将 pxGrid 客户端证书导入到身份密钥库中。

```
keytool -import -alias pxGridMAC -keystore pxGridClient.jks -file  
pxGridClient.cer
```

```
Enter keystore password: cisco123  
Certificate already exists in keystore under alias <1>  
Do you still want to add it? [no]: yes  
Certificate was added to keystore
```

注：如果您收到表明证书已添加到预先存在的密钥库的消息，则可以选择“no”，而操作仍然正常。我选择了“yes”，因此我们可以验证后来是否添加了证书。

步骤 10 将 CA 根证书添加到受信任密钥库，CA 根证书也需要受信任。

```
keytool -import -alias ca_root1 -keystore root3.jks -file ca_root.cer
```

```
Enter keystore password: cisco123  
Owner: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com  
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com  
Serial number: 448a6d6486c91cb14c6888c127d16c4e  
Valid from: Thu Nov 13 20:47:06 EST 2014 until: Wed Nov 13 20:57:06 EST 2019  
Certificate fingerprints:  
    MD5: 41:10:8A:F5:36:76:79:9C:2C:00:03:47:55:F8:CF:7B  
    SHA1: 9D:DA:06:AF:06:3F:8F:5E:84:C7:F4:58:50:95:03:22:64:48:96:9F  
    SHA256:  
DB:28:50:D6:47:CA:C0:6A:E9:7B:87:B4:0E:9C:3A:C1:A2:61:EA:D1:29:8B:45:B4:76:4B:DA:2A:F1:D8:E0:A3  
    Signature algorithm name: SHA256withRSA  
    Version: 3  
  
Extensions:  
  
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false  
0000: 02 01 00 ...  
  
#2: ObjectId: 2.5.29.19 Criticality=true  
BasicConstraints:[  
    CA:true  
    PathLen:2147483647  
]  
  
#3: ObjectId: 2.5.29.15 Criticality=false  
KeyUsage [  
    DigitalSignature  
    Key_CertSign  
    Crl_Sign  
]  
  
#4: ObjectId: 2.5.29.14 Criticality=false  
SubjectKeyIdentifier [  
KeyIdentifier [  
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...  
0010: 6A C8 79 2C j.y,  
]  
]  
]
```

```
Trust this certificate? [no]: yes
Certificate was added to keystore
```

步骤 11 将身份密钥库 (pxGridClient.jks) 和信任密钥库 (root3.jks) 复制到 ../samples/bin/.. 文件夹中。

测试 pxGrid 客户端和 ISE pxGrid 节点

系统将运行 pxGrid 脚本 register.sh 和 session download.sh 来确保 pxGrid 客户端连接和 pxGrid 注册。会话下载将确保 ISE MNT 证书和 pxGrid 客户端没有问题。

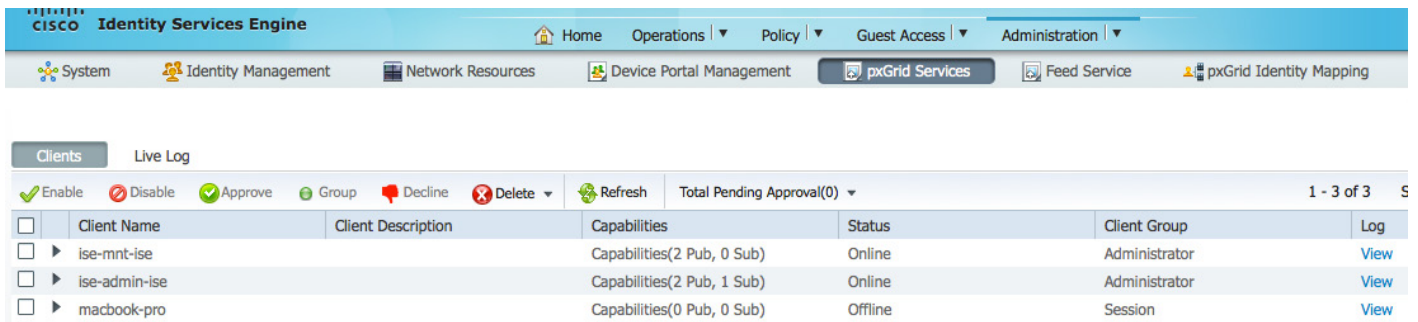
步骤 1 注册 pxGrid 客户端。

```
./register.sh -keystoreFilename pxGridClient.jks -keystoreFilename cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -group Session -description test -username MacBook-Pro -hostname 10.0.0.96

----- properties -----
version=1.0.0
hostnames=10.0.0.96
username=MacBook-Pro
descriptipon=test
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
-----
registering...
connecting...
account enabled
connected.
done registering.
connection closed
```

注：“Account enabled”意味着 pxGrid 管理员已启用帐户。

验证 pxGrid 客户端是否已注册到 pxGrid 控制器。



Client Name	Client Description	Capabilities	Status	Client Group	Log
<input type="checkbox"/> ▶ ise-mnt-ise		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ ise-admin-ise		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
<input type="checkbox"/> ▶ macbook-pro		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

步骤2 运行会话下载。

```
./session_download.sh -keystoreFilename pxGridClient.jks -keystoreFilename cisco123 -truststoreFilename
root3.jks -truststorePassword cisco123 -username MacBook-Pro -hostname 10.0.0.96

----- properties -----
version=1.0.0
hostnames=10.0.0.96
username=MacBook-Pro
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
filter=null
start=null
end=null
-----
connecting...
connected.
starting at Wed Dec 10 18:44:49 EST 2014...

session (ip=10.0.0.18, Audit Session Id=0A0000020000000B006E1086, User Name=jepich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:D1:8D:90, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint
Profile=VMWare-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-
Id=00000002], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Dec 10 16:41:48 EST
2014 )... ending at: Wed Dec 10 18:44:49 EST 2014

-----
downloaded 1 sessions in 26 milliseconds
-----

connection closed
```

查看密钥库条目

通过查看密钥库条目，可以查看身份和信任密钥库的受信任证书条目。

步骤1 验证信任密钥库 root3.jks。

```
keytool -list -v -keystore root3.jks
Enter keystore password: cisco123

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: ca_root1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 448a6d6486c91cb14c6888c127d16c4e
Valid from: Thu Nov 13 20:47:06 EST 2014 until: Wed Nov 13 20:57:06 EST 2019
Certificate fingerprints:
    MD5: 41:10:8A:F5:36:76:79:9C:2C:00:03:47:55:F8:CF:7B
    SHA1: 9D:DA:06:AF:06:3F:8F:5E:84:C7:F4:58:50:95:03:22:64:48:96:9F
    SHA256:
DB:28:50:D6:47:CA:C0:6A:E9:7B:87:B4:0E:9C:3A:C1:A2:61:EA:D1:29:8B:45:B4:76:4B:DA:2A:F1:D8:E0:A3
    Signature algorithm name: SHA256withRSA
    Version: 3
```

```

Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
...

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&...7..Z.6&...
0010: 6A C8 79 2C j.Y,
]
]

*****
*****

Alias name: isemnt1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d7600000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
  MD5: 2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
  SHA1: BD:18:C0:DD:4D:DD:43:80:CA:CA:3B:F6:DC:1E:6E:46:93:59:FE:B7
  SHA256:
F9:11:FC:EC:BC:0F:0F:84:36:F1:26:BC:5A:09:B7:2B:3C:D1:1B:AC:FC:1A:F1:AB:6D:00:8D:11:F8:26:93:FF
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:
#1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ..0...*.H.....
0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ..0...+....0...*
0030: 86 48 86 F7 0D 03 07 .H.....

#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0.
0010: 06 08 2B 06 01 05 05 07 03 02 30 0A 06 08 2B 06 ..+.....0...+.
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 .....0...+.....
0030: 37 0A 03 04 7...

#3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false
0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.%+.....7.....
0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF 40 02 01 64 02 01 03 ^...#...@..d...

```

```

#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
    accessMethod: caIssuers
    accessLocation: URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?cACertificate?base?objectCla
ss=certificationAuthority
  ]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
]

#6: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-
BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint]
  ]]

#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
  [] ]
]

#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
]

#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Key_Encipherment
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`..
0010: AF D8 07 09 ....]
]

*****
*****

Alias name: isemnt
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d76000000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
  MD5: 2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
  SHA1: BD:18:C0:DD:4D:DD:43:80:CA:CA:3B:F6:DC:1E:6E:46:93:59:FE:B7

```

```

    SHA256:
F9:11:FC:EC:BC:0F:0F:84:36:F1:26:BC:5A:09:B7:2B:3C:D1:1B:AC:FC:1A:F1:AB:6D:00:8D:11:F8:26:93:FF
    Signature algorithm name: SHA256withRSA
    Version: 3

Extensions:

#1: ObjectID: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ..0...*.H.....
0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ..0...+.....0...*
0030: 86 48 86 F7 0D 03 07 .H.....

#2: ObjectID: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0.
0010: 06 08 2B 06 01 05 05 07 03 02 30 0A 06 08 2B 06 ..+.....0...+.
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 .....0...+.....
0030: 37 0A 03 04 7...

#3: ObjectID: 1.3.6.1.4.1.311.21.7 Criticality=false
0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-..%+.....7.....
0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF 40 02 01 64 02 01 03 ^...#...@..d...

#4: ObjectID: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
    accessMethod: caIssuers
    accessLocation: URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?cACertificate?base?objectCla
ss=certificationAuthority
  ]
]

#5: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
]

#6: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-
BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint]
  ]]

#7: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
  [ ] ]
]

#8: ObjectID: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
]

#9: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

```



```
#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`..
0010: AF D8 07 09          ....
]
]

*****
*****

Johns-MacBook-Pro:bin jeppich$
```

步骤 2 验证身份密钥库 pxGridclient.jks。

```
keytool -list -v -keystore pxGridClient.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: pxgridmac
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 6101649b00000000000e
Valid from: Wed Dec 10 17:01:25 EST 2014 until: Sat Dec 10 17:11:25 EST 2016
Certificate fingerprints:
    MD5: 0F:3C:57:64:7E:BD:D9:0A:7B:C2:25:64:84:F2:E3:FA
    SHA1: 65:9C:A8:8D:52:B0:CF:C6:1B:46:7E:41:80:D3:7B:96:40:B1:E3:68
    SHA256:
3D:8A:72:6B:9D:7F:12:5A:AF:A7:CC:A6:E2:F7:E9:9A:F9:D8:BE:89:55:12:87:30:F8:17:3B:91:29:EB:6A:8E
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ..0...*.H.....
0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ..0...+...0...*
0030: 86 48 86 F7 0D 03 07          .H.....

#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0.
0010: 06 08 2B 06 01 05 05 07 03 02 30 0A 06 08 2B 06 ..+.....0...+.
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 .....0...+.....
0030: 37 0A 03 04          7...

#3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false
0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.%+.....7.....
0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF 40 02 01 64 02 01 03 ^...#...@..d...

#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
]
```

```

    accessMethod: caIssuers
    accessLocation: URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?cACertificate?base?objectCla
ss=certificationAuthority
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
]

#6: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
[DistributionPoint:
[URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-
BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint]
]]

#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
[CertificatePolicyId: [2.5.29.32.0]
[] ]
]

#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
clientAuth
emailProtection
1.3.6.1.4.1.311.10.3.4
]

#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
DigitalSignature
Key_Encipherment
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E6 87 7E 18 67 25 03 29 12 B4 56 F8 51 78 A1 94 ....g%.)..V.Qx..
0010: 78 88 D2 94 x...
]
]

*****
*****

Alias name: 1
Creation date: Dec 10, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 6101649b00000000000e
Valid from: Wed Dec 10 17:01:25 EST 2014 until: Sat Dec 10 17:11:25 EST 2016
Certificate fingerprints:
MD5: 0F:3C:57:64:7E:BD:D9:0A:7B:C2:25:64:84:F2:E3:FA
SHA1: 65:9C:A8:8D:52:B0:CF:C6:1B:46:7E:41:80:D3:7B:96:40:B1:E3:68

```

```

SHA256:
3D:8A:72:6B:9D:7F:12:5A:AF:A7:CC:A6:E2:F7:E9:9A:F9:D8:BE:89:55:12:87:30:F8:17:3B:91:29:EB:6A:8E
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectID: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ..0...*.H.....
0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ..0...+...0...*
0030: 86 48 86 F7 0D 03 07 .H....

#2: ObjectID: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0.
0010: 06 08 2B 06 01 05 05 07 03 02 30 0A 06 08 2B 06 ..+.....0...+
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 .....0...+.....
0030: 37 0A 03 04 7...

#3: ObjectID: 1.3.6.1.4.1.311.21.7 Criticality=false
0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.%+....7....
0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF 40 02 01 64 02 01 03 ^...#...@.d...

#4: ObjectID: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
    accessMethod: caIssuers
    accessLocation: URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?cACertificate?base?objectCla
ss=certificationAuthority
  ]
]

#5: ObjectID: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
]

#6: ObjectID: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-
BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati
onList?base?objectClass=cRLDistributionPoint]
  ]]

#7: ObjectID: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
  [] ]
]

#8: ObjectID: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
]

#9: ObjectID: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

```

```
]
#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E6 87 7E 18 67 25 03 29 12 B4 56 F8 51 78 A1 94 ....g%).V.Qx..
0010: 78 88 D2 94 x...
]
]

Certificate[2]:
Owner: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 448a6d6486c91cb14c6888c127d16c4e
Valid from: Thu Nov 13 20:47:06 EST 2014 until: Wed Nov 13 20:57:06 EST 2019
Certificate fingerprints:
MD5: 41:10:8A:F5:36:76:79:9C:2C:00:03:47:55:F8:CF:7B
SHA1: 9D:DA:06:AF:06:3F:8F:5E:84:C7:F4:58:50:95:03:22:64:48:96:9F
SHA256:
DB:28:50:D6:47:CA:C0:6A:E9:7B:87:B4:0E:9C:3A:C1:A2:61:EA:D1:29:8B:45:B4:76:4B:DA:2A:F1:D8:E0:A3
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00 ...

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
DigitalSignature
Key_CertSign
Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.Y,
]
]

*****
*****
```

故障排除

本节介绍一些故障排除提示：

- 通过验证 pxGrid 客户端主机名和 ISE pxGrid 节点是否可通过 DNS 进行可解析，避免出现 pxGrid 脚本错误消息。
- 如果信任库有更改，并且收到类似的错误消息，请从 ISE VM 停止并重新启动 ISE 应用。

```
./register.sh -keystoreFilename pxGridClient.jks -keysrePassword cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -username pxGridclient -hostname 10.0.0.96 -group Session -description test1
----- properties -----
version=1.0.0
hostnames=10.0.0.96
username=pxGridclient
descriptipon=test1
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
-----
registering...
connecting...
javax.net.ssl.SSLHandshakeException: Received fatal alert: unknown_ca
    at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
    at sun.security.ssl.Alerts.getSSLException(Alerts.java:154)
    at sun.security.ssl.SSLSocketImpl.recvAlert(SSLSocketImpl.java:1991)
    at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1104)
    at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1343)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1371)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1355)
    at org.jivesoftware.smack.XMPPConnection.proceedTLSReceived(XMPPConnection.java:806)
    at org.jivesoftware.smack.PacketReader.parsePackets(PacketReader.java:267)
    at org.jivesoftware.smack.PacketReader.access$000(PacketReader.java:43)
    at org.jivesoftware.smack.PacketReader$1.run(PacketReader.java:70)
Exception in thread "main" com.cisco.pxgrid.GCLEException: SASL authentication failed:
    at com.cisco.pxgrid.GridConnection.connect(GridConnection.java:197)
    at com.cisco.pxgrid.samples.ise.Register.main(Register.java:99)
Caused by: SASL authentication failed:
    at org.jivesoftware.smack.SASLAuthentication.authenticate(SASLAuthentication.java:281)
    at org.jivesoftware.smack.XMPPConnection.login(XMPPConnection.java:206)
    at com.cisco.pxgrid.Configuration.connect(Configuration.java:194)
    at com.cisco.pxgrid.GridConnection.connect(GridConnection.java:134)
    ... 1 more
```

- 重新启动 ISE 服务。

```
application stop ise
application start ise
```

步骤 3 如果您看到类似的错误消息，则需要将根证书添加到 truststoreFilename 密钥库，在本例中为 root3.jks。

```
./register.sh -keystoreFilename pxGridClient.jks -keystorePassword cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -group Session -description MACBOOK -username Macbook_PRO -hostname 10.0.0.96

----- properties -----
version=1.0.0
hostnames=10.0.0.96
username=Macbook_PRO
descriptipon=MACBOOK
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
-----
registering...
connecting...
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: root certificate not trusted of
[ise.lab6.com]
    at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
    at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1917)
    at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:301)
    at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:295)
    at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1471)
    at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:212)
    at sun.security.ssl.Handshaker.processLoop(Handshaker.java:936)
    at sun.security.ssl.Handshaker.process_record(Handshaker.java:871)
    at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1043)
    at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1343)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1371)
    at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1355)
    at org.jivesoftware.smack.XMPPConnection.proceedTLSReceived(XMPPConnection.java:806)
    at org.jivesoftware.smack.PacketReader.parsePackets(PacketReader.java:267)
    at org.jivesoftware.smack.PacketReader.access$000(PacketReader.java:43)
    at org.jivesoftware.smack.PacketReader$1.run(PacketReader.java:70)
Caused by: java.security.cert.CertificateException: root certificate not trusted of [ise.lab6.com]
    at org.jivesoftware.smack.ServerTrustManager.checkServerTrusted(ServerTrustManager.java:144)
    at sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:865)
    at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1453)
    ... 11 more
```