

在 ISE 分布式环境中配置 pxGrid

草稿

目录

关于本文档	4
简介	5
使用 pxGrid 角色的 ISE 分布式部署简介	6
pxGrid 角色配置	8
配置 Microsoft CA 2008 R2 企业版 pxGrid 模板	8
不含 pxGrid 主用-备用配置的 pxGrid 节点配置	10
生成 CA 签名的节点证书	10
在主要 PAN 节点和 MnT 节点中导出 pxGrid 节点公钥/私钥	14
批量会话下载	17
为分布式环境注册 ISE 节点	18
pxGrid 客户端管理	20
pxGrid 客户端配置	22
pxGrid Java sdk 安装	22
pxGrid 客户端 SDK Java 密钥库简介	23
pxGrid 客户端证书配置	24
pxGrid 客户端主用-备用配置示例	29
在 ISE 分布式环境中测试 xGrid 客户端	37
查看密钥库条目	38
采用 pxGrid 主用-备用配置的 ISE 分布式部署简介	46
为分布式环境 pxGrid 主用-备用配置注册 ISE 节点	47
在 ISE 分布式环境 pxGrid 主用-备用配置中测试 pxGrid 客户端	51
测试 pxGrid 主用-备用配置	52
基本操作	52
测试故障切换	55
恢复主要节点	58
ISE 自签名身份证书	61
SDK 中的样本证书	65
测试 pxGrid 客户端	67

参考资料	68
附录	69
故障排除.....	69
在 Centos 6.5 中删除 Java 和安装 JDK 8.0	70
删除 Java 早期版本	70
安装 JDK 8.0	70

关于本文档

本文档面向在思科身份服务引擎 (ISE) 1.3 生产环境中部署 pxGrid 的思科工程师、合作伙伴和客户。读者应熟悉 ISE 和 pxGrid。

本文档重点介绍如何为 ISE pxGrid 节点和 pxGrid 客户端部署外部 CA 签名的证书。

以下系列文档将详细介绍有关证书部署的其他注意事项（例如自签名 ISE 身份证书和 pxGrid 样本证书）：
《使用 Cisco pxGrid 部署证书》

- 证书颁发机构 (CA) 签名的 pxGrid ISE 节点和 CA 签名的 pxGrid 客户端
- 证书颁发机构 (CA) 签名的 pxGrid 客户端和自签名的 ISE pxGrid 节点证书
- 自签名证书与 ISE pxGrid 节点和 pxGrid 客户端

有关在测试环境中配置 pxGrid 的信息，请参阅以下参考资料：

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

本文档将介绍分布式 ISE 环境中的外部 ISE pxGrid 节点配置和 pxGrid 主用-备用配置。用于测试这些配置的 pxGrid 客户端是运行 OSX 10.8.5 的 MacBook Pro 和适用于 pxGrid java SDK 的 Oracle Java Development Kit (jdk-8u-20-macos-x64.dmg)。如果您运行的是其他版本的 Linux，请参阅

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

本文档还将介绍如何使用 POC 部署中所用的自签名证书和样本证书来配置 pxGrid ISE 节点。不过，如欲了解详细信息，还请参阅相关文档。

Microsoft Enterprise 2008 CA R2 企业版服务器用于证书颁发机构 (CA)，pxGrid 客户端证书、pxGrid 节点证书和 ISE 节点证书均由其签名。

简介

思科平台交换架构 (pxGrid) 可在 IT 基础设施的不同部分（例如安全监控和网络检测系统、网络平台、资产和配置管理、身份和访问管理平台，以及几乎所有其他 IT 运营平台）之间实现跨平台的多供应商网络系统协作。当出现相应的业务或运营需求时，生态系统合作伙伴可以使用 pxGrid 通过发布/订用方法，与使用 pxGrid 的思科平台及使用 pxGrid 的任何其他生态系统交换情景信息。

pxGrid 主要由三个部分组成：发布方、pxGrid 客户端和 pxGrid 控制器（即思科身份服务引擎 [ISE] pxGrid 节点）。

- pxGrid 客户端要订用的信息主题的 pxGrid 发布方 - 在思科身份服务引擎 (ISE) 1.3 版中，ISE 是此信息（也称为功能）的唯一发布方。
- pxGrid 客户端 - 可以是支持的思科安全平台、pxGrid 生态系统合作伙伴或者运行 pxGrid SDK 的 Linux 或 MAC 主机，均需订用发布的信息。
- pxGrid 控制器 - 思科身份服务引擎 (ISE) pxGrid 节点，用于控制客户端注册/管理和主题/订用流程。

ISE 将发布以下信息主题：

- SessionDirectory - 已经过身份验证的 802.1X 会话的会话属性
- EndpointProtectionService - 自适应网络控制 (ANC) 隔离/取消隔离缓解操作
- TrustsecMetadataCapability - 安全组标记 (SGT) 信息
- EndpointProfileMetadata - ISE 策略信息
- IdentityGroup - 组和分析信息

pxGrid 客户端将订用这些主题并获取 ISE 情景信息。

ISE 部署于分布式环境中，此环境中的所有节点都有不同的角色：主要 PAN（策略 Admin 节点），主要 MnT（监控）节点，PSN（策略服务节点）。pxGrid 节点也会作为不同的角色进行部署，而且在 CA（证书颁发机构）签名的环境中需要使用自定义的 pxGrid 模板。本文档将介绍在这种 ISE 分布式环境中对 ISE pxGrid 节点和 ISE pxGrid 客户端都使用 CA 签名的证书进行 pxGrid 配置的程序步骤。

此外，本文档还将介绍 pxGrid 主用-备用配置。

在本文档中，运行 OSX 10.8.5 的 MAC 将用作 pxGrid 客户端。

Microsoft Enterprise CA (Certificate Authority) 2008 R2 服务器将用作指定的 CA 服务器。请注意，用于 pxGrid 的自定义模板将同时具有客户端身份验证和服务器身份验证的增强型密钥用法 (EKU)。EKU 用于定义证书的用途，且以 ISO 定义的对象标识符 (OID) 来定义；在此使用案例中，一个用于客户端身份验证 (1.3.6.1.5.5.7.3.2)，另一个用于服务器身份验证 (1.3.6.1.5.5.7.3.1)。

使用 pxGrid 角色的 ISE 分布式部署简介

将 Windows 2008 R2 Enterprise CA 服务器用作 CA 机构。将 CA 根证书导入到每个 ISE 节点的受信任系统证书库中。CA 将使用 ISE 节点（pxGrid 节点除外）中定义的 Web 服务器模板和管理员 “usage” 证书为 CSR 节点请求提供服务。

pxGrid 节点则使用自定义模板，同时包含用于客户端身份验证和服务器身份验证的 EKU。

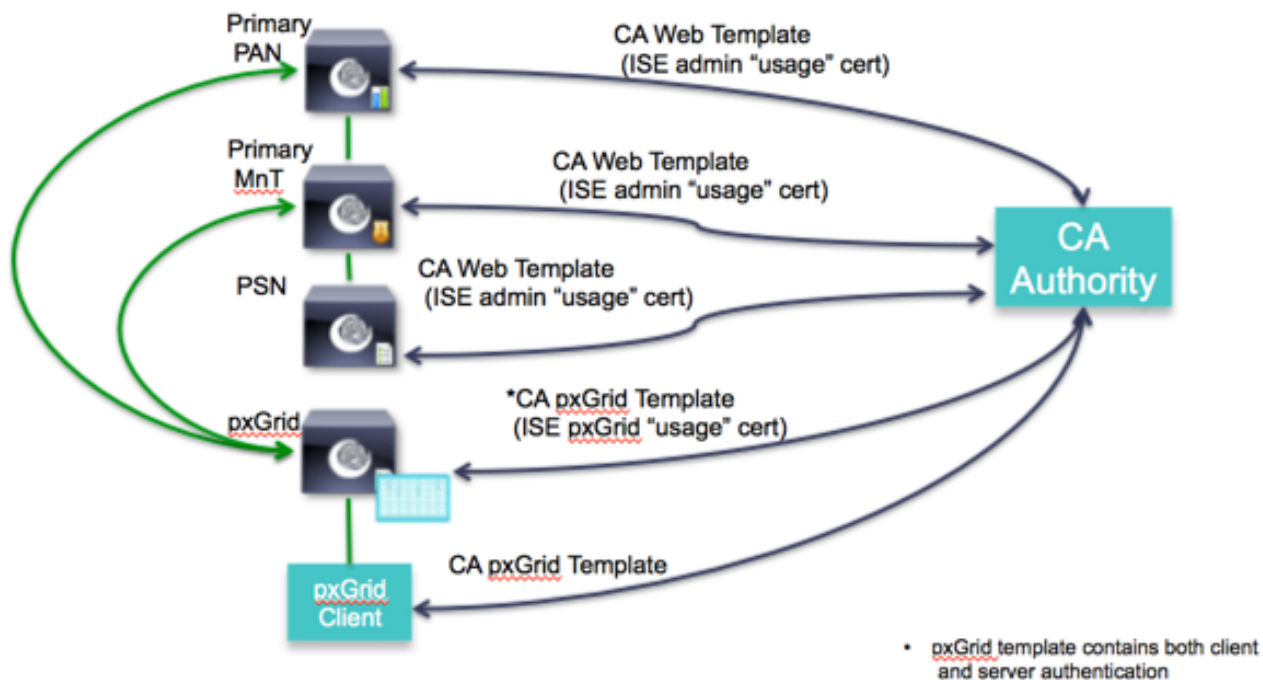
注： pxGrid 模板既可以是 Windows 2003 格式的用户模板的副本，也可以是添加了同时用于客户端身份验证和服务器身份验证的 EKU 的用户模板的副本。

必须将 pxGrid 节点的公钥/私钥对复制到每个主要 PAN（管理员）节点和主要 MnT（监控）节点的系统证书库，pxGrid 操作才能成功。

注： 如果是主用-备用 pxGrid 配置，则要将第一个 pxGrid 节点（主要 pxGrid 节点）的公钥/私钥对导出到主要 PAN 节点和主要 MnT 节点中。将第二个 pxGrid 节点（辅助 pxGrid 节点）的公钥/私钥对导出到辅助 PAN 节点或辅助 MnT 节点中。

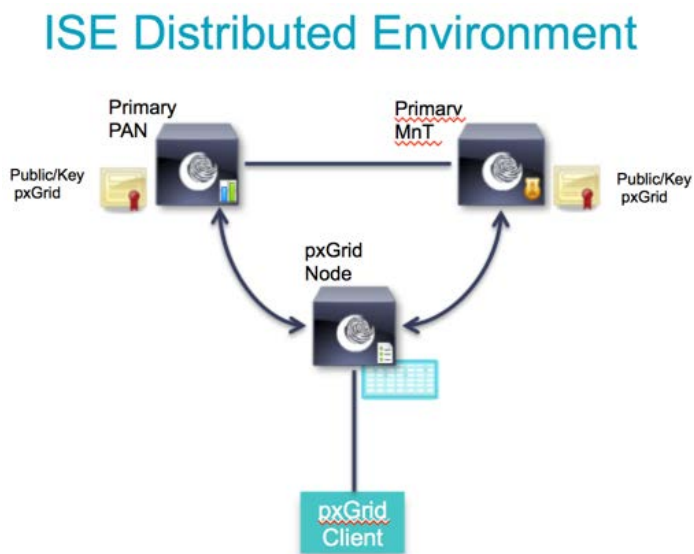
下图显示了典型的 ISE 分布式环境中各种不同 ISE 节点的证书生成情况。请注意，管理员 “usage” 证书用于除 pxGrid 节点外所有 ISE 节点的 CSR 请求生成过程。CA 服务器将使用 “Web server” 模板为这些请求提供服务。而 pxGrid “usage” 证书则用于 pxGrid 节点 CSR 请求，由自定义 pxGrid 模板提供服务。

pxGrid In Distributed ISE Deployment



下图显示了分布式 ISE 环境中的 pxGrid 节点配置。pxGrid 节点在所有生产环境中都是外部节点。

需要将 pxGrid 节点的公钥/私钥同时复制到主要 PAN 节点和主要 MnT 节点的系统证书库后才能启用 pxGrid 控制器。



pxGrid 角色配置

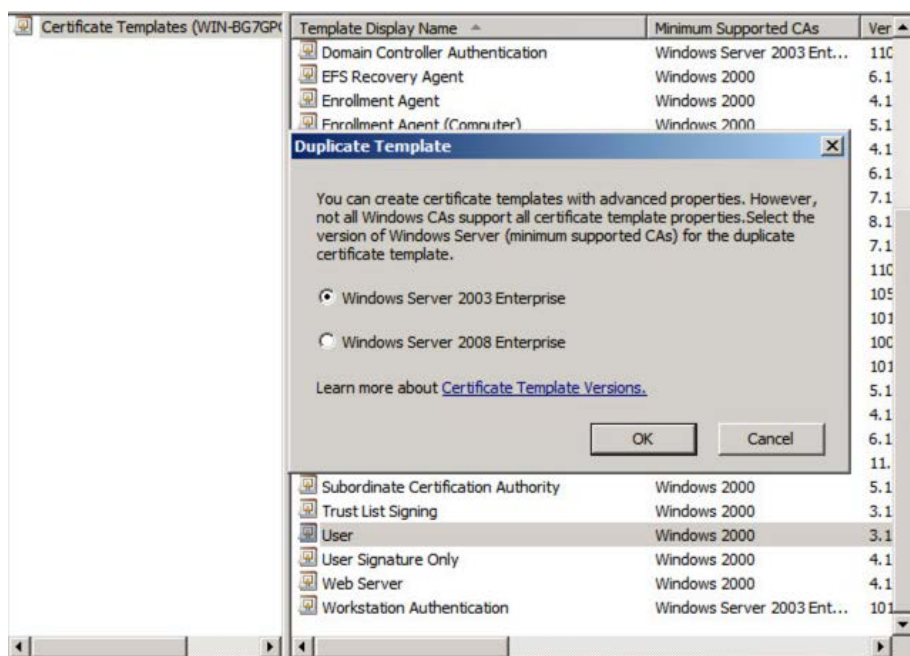
配置 Microsoft CA 2008 R2 企业版 pxGrid 模板

本节介绍 pxGrid 证书模板的配置。pxGrid 模板必须同时包含用于客户端身份验证和服务器身份验证的 EKU。

创建 pxGrid 模板的步骤如下：

步骤 1 Select -> Administrative Tools -> Certificate Authority -> CA 服务器旁的“+”下拉列表 -> 右键点击 Certificate Templates -> Manage

步骤 2 右键点击 User 模板并选择 Duplicate -> Select -> Windows 2003 Enterprise -> OK

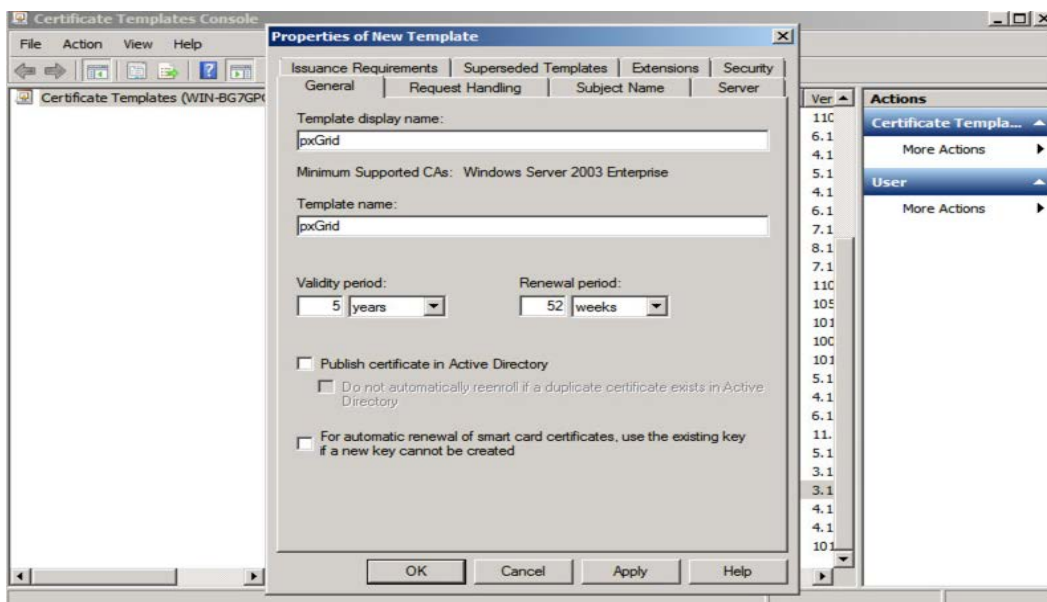


注： 选择 Windows Server 2003 Enterprise 让其显示于模板 CA 窗口下拉列表中。

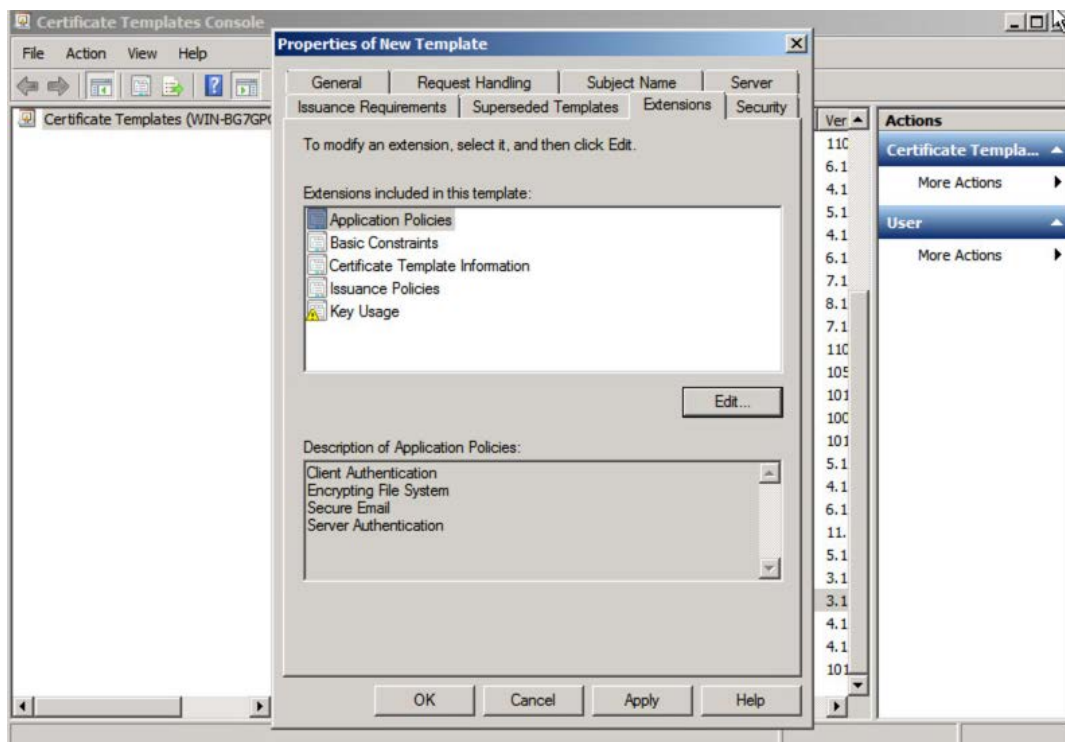
Certificate Template:

pxGrid

步骤 3 输入证书模板的名称，取消选中“Publish certificate in Active Directory”，提供有效期和续约期。



步骤 4 点击 Extensions -> Add -> Server Authentication -> OK -> Apply



不含 pxGrid 主用-备用配置的 pxGrid 节点配置

本节说明定义 ISE 节点、生成 CSR 请求以及从 CA 机构获取证书的步骤。这是所有 ISE 分布式部署的典型过程。此过程先在独立模式下进行配置，然后从主要 Admin 节点加入节点。

pxGrid 节点会将 ISE pxGrid “usage” 证书用于初始 CSR 请求，并由此前定义的 MS CA “pxGrid” 模板提供服务。返回的证书将与初始 pxGrid CSR 请求绑定。

将公钥/私钥对从 pxGrid 节点导出，然后导入到主要 PAN 节点和主要 MnT 节点中。

注：在 pxGrid 主用-备用配置中，要将第二个节点或辅助 pxGrid 节点的公钥/私钥对导入到辅助 PAN 节点和辅助 MnT 节点中。

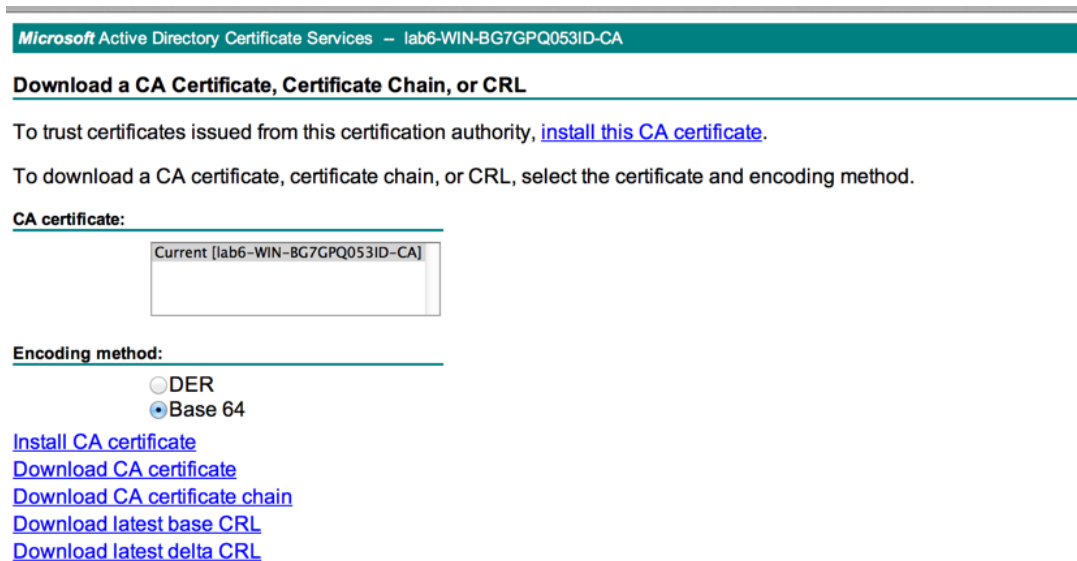
下载 Microsoft CA 根证书并将其导入到每个 ISE 节点的受信任系统证书库中，然后启用 “Trust for Authentication within ISE”。

生成 CA 签名的节点证书

以下步骤概述下载 CA 根证书、生成 ISE 节点 CSR 请求以及将证书与 CSR 请求绑定的步骤。

注：下载 CA 根证书和其他接受服务的证书请求时，应选择 base 64 格式

步骤 1 下载 base 64 格式的 CA 根证书。



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

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [lab6-WIN-BG7GPQ053ID-CA]

Encoding method:

DER

Base 64

[Install CA certificate](#)

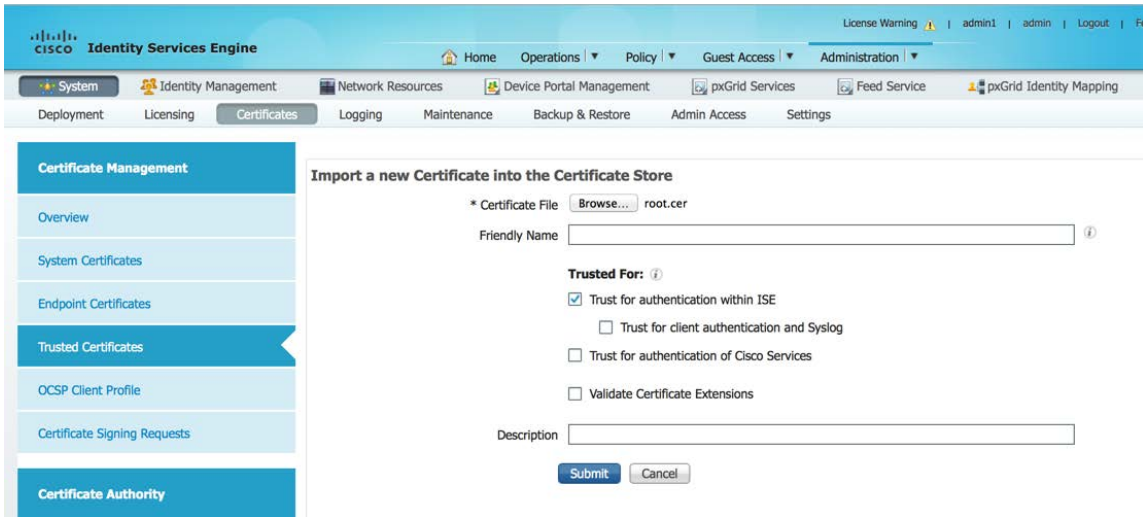
[Download CA certificate](#)

[Download CA certificate chain](#)

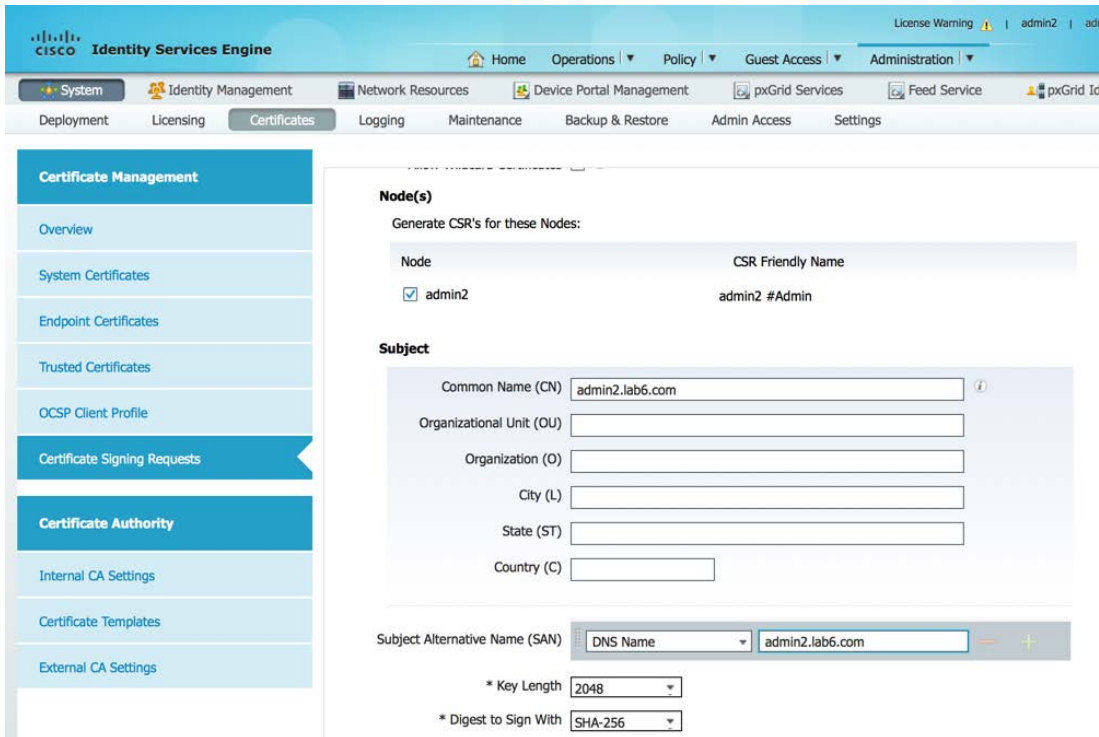
[Download latest base CRL](#)

[Download latest delta CRL](#)

步骤 2 导入到受信任的证书库中
Administration -> System -> Certificates -> Trusted Certificates



步骤 3 在独立环境中为所需的 Admin 节点、MnT 节点和 PSN 节点生成 CSR。
Administration -> System -> Certificates -> Certificate Signing Requests - “admin” 证书用法



步骤 4 使用 MS CA “Web Server” 模板为 Admin 节点、MnT 节点和 PSN 节点的证书请求提供服务。

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 PI Request box.

Saved Request:

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

```
lv9Z9LI5OnlaKmRjyfSg7O7fGw+zWRF1HSg+XYik91K
ycDLj4KDhrcTL819CFy+UIA4Ib2HmcuvMFGAFkXT+rr
CCB4RmUjLmiCP+SckXmTYqU9aloxkZseFpXnbMuSt9I
/6rNcWzbWxBSJqTwlwl+RwoSrUvjdvVwbDhjMlzFn5D2
60yMH0pELvPJYkR1xBbS5tRlXAQM
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

步骤 5 下载 base 64 编码格式的证书

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

Certificate Issued

The certificate you requested was issued to you.

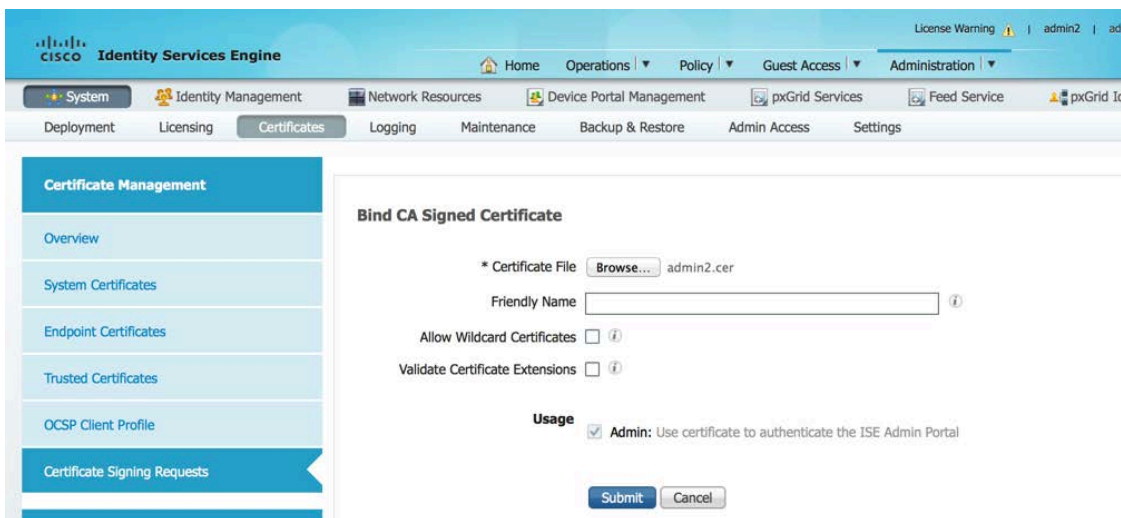
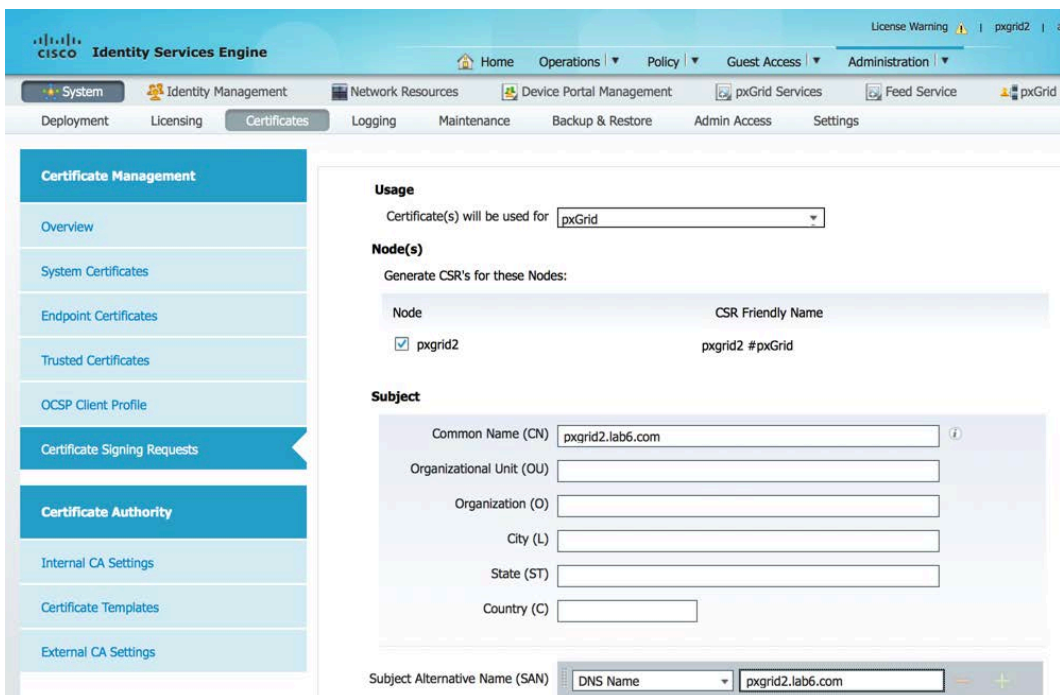
DER encoded or Base 64 encoded

[Download certificate](#)
[Download certificate chain](#)

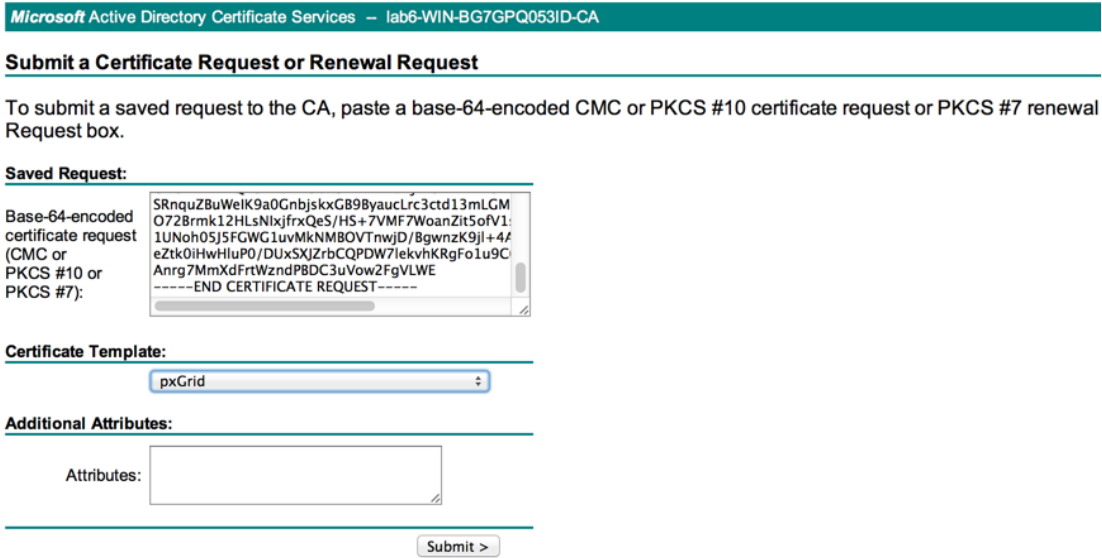
步骤 6 将证书分别与每个 ISE 节点的 CSR 请求绑定。（例如：Admin 节点、MnT 节点和 PSN 节点） Administration -> System -> Certificates -> Certificate Signing Requests -> 选择证书并绑定

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Certificates > Certificate Signing Requests. The page title is "Certificate Signing Requests". There is a "Generate Certificate Signing Requests (CSR)" button. Below it, a message states: "A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click 'export' to download one or more CSRs so that they may be signed by an external authority. A request has been signed, click 'bind' to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list." There are buttons for "View", "Export", "Delete", and "Bind Certificate". A table lists the requests:

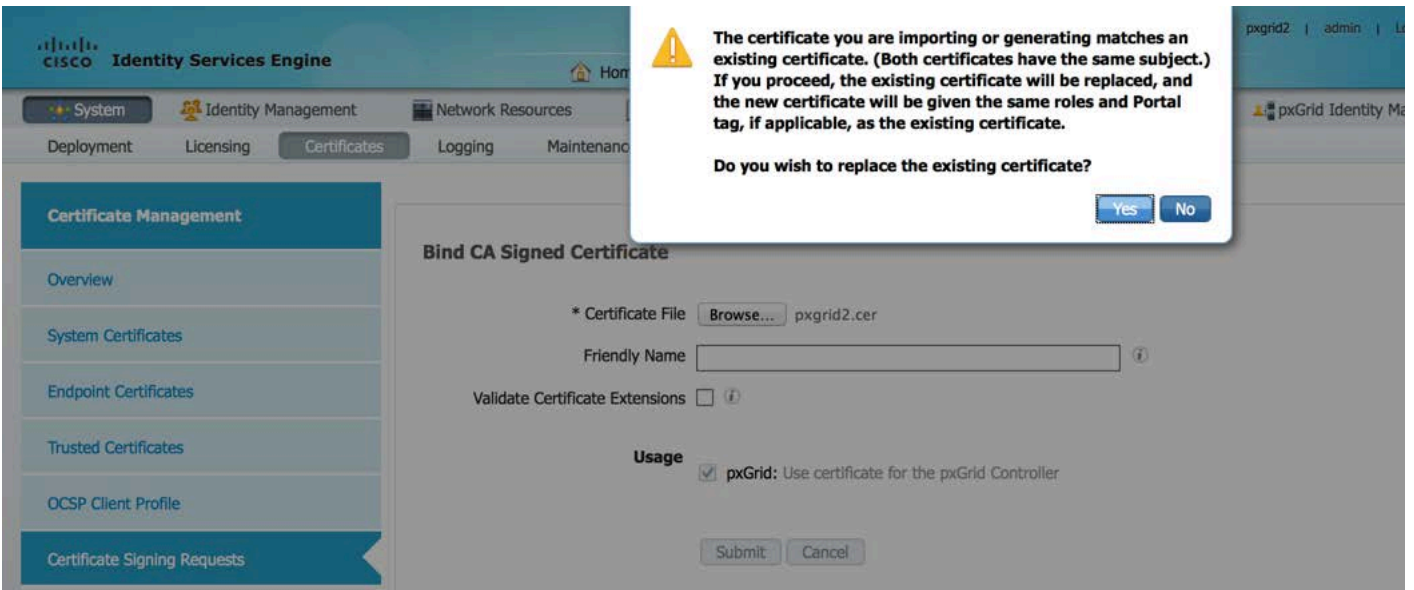
Friendly Name	Certificate Subject	Key Length	Group Tag	Timestamp	Host
<input checked="" type="checkbox"/> admin2#Admin	CN=admin2.lab6.com	2048		Fri, 30 Jan 2015	admin2

步骤 7 分别为每个 ISE 节点导入节点证书，然后提交**步骤 8** 为 pxGrid 节点生成 CSR。
Administration -> System -> Certificates -> Certificate Signing Requests - “pxGrid” 证书用法

步骤 9 提交请求 MS CA “pxGrid” 模板，为 pxGrid 节点的证书请求提供服务。



步骤 10 将 pxGrid 证书与 pxGrid 节点 CSR 请求绑定。
Administration -> System -> Certificates -> Certificate Signing Requests -> 选择 pxGrid 节点并绑定证书



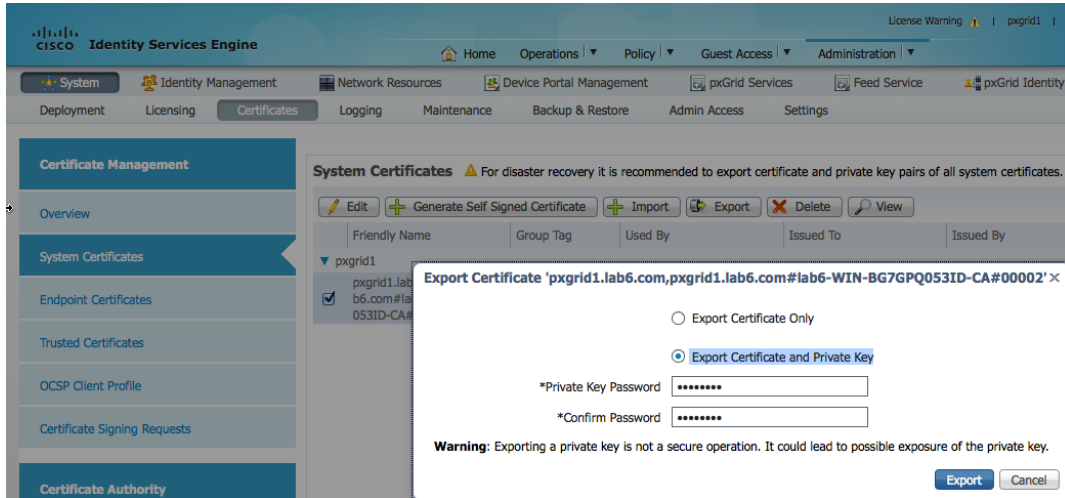
在主要 PAN 节点和 MnT 节点中导出 pxGrid 节点公钥/私钥

必须将 pxGrid 客户端节点的公钥/私钥对复制到主要 PAN 节点和 MnT 节点中。相应步骤如下所述：

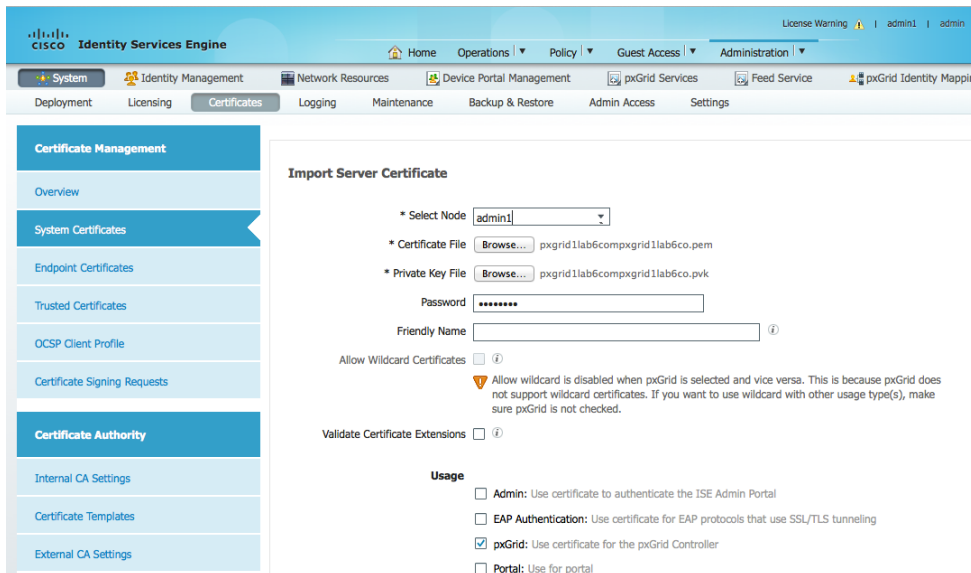
步骤 1 在独立模式的新安装中，从 pxGrid 节点的系统证书库中导出公钥和私钥，然后导入到所需的主要 Admin 节点和 MnT 节点的系统证书库中。

注： 如果存在现有 ISE 1.3 部署并已添加外部 pxGrid 角色，可以从主要 PAN 节点的系统证书库中导出 pxGrid 节点的公钥/私钥对，然后导入到主要 PAN 节点和主要 MnT 节点中

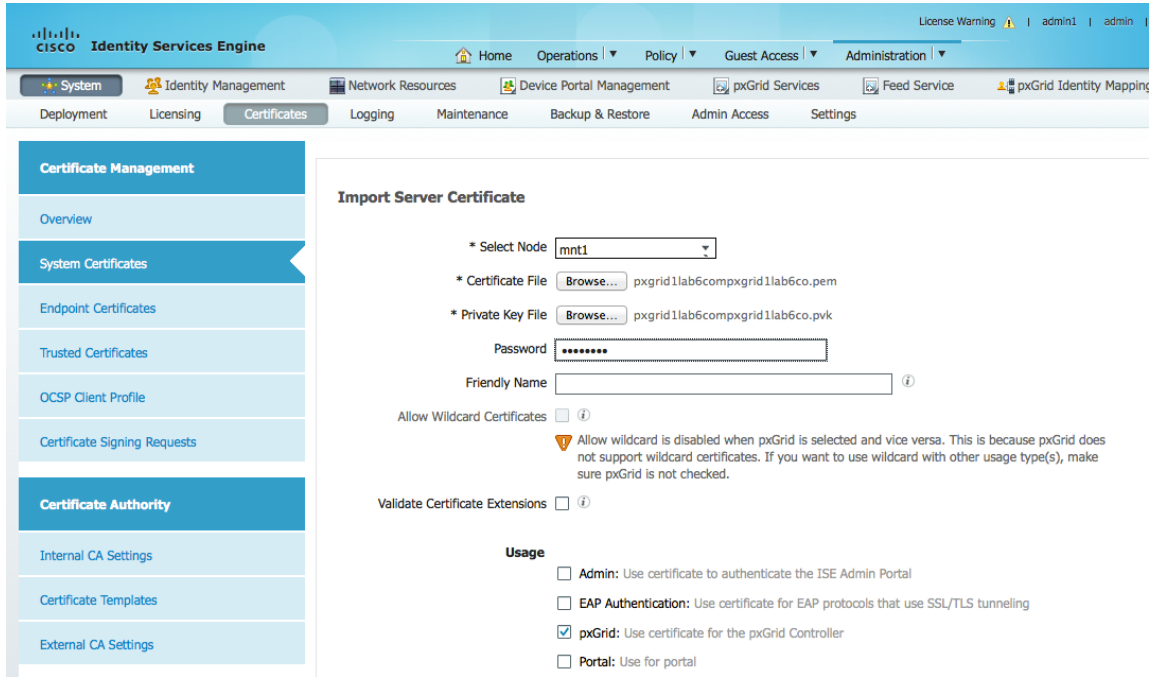
Administration -> System -> Certificates -> System Certificates，选择证书并导出证书和私钥
必须为私钥提供名称（例如 cisco123）。此导出内容会另存为包含 PEM 和 PVK（公钥/私钥对）的压缩文件。



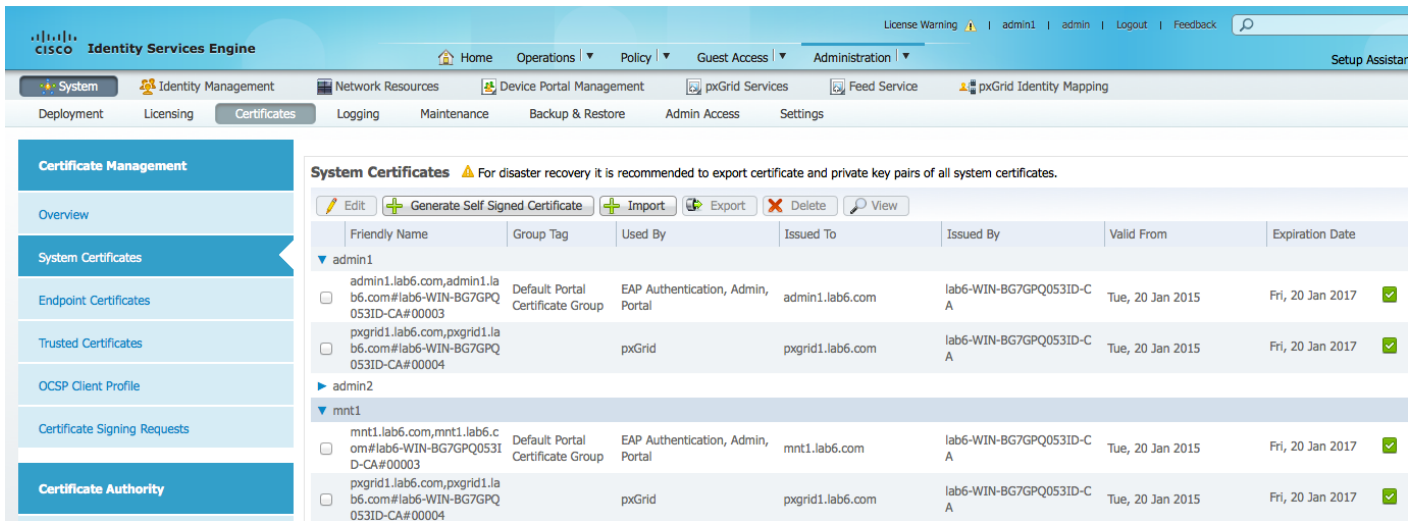
步骤 2 对于所需的主要 Admin 节点，将公钥和私钥都导入到系统证书库中，然后提交。
Administration -> System -> Certificates -> System Certificates，然后导入 pxGrid PEM 证书和 PVK 证书。



步骤 3 对于所需的主要 MnT 节点，将公钥和私钥都导入到系统证书库中，然后提交。
Administration -> System -> Certificates -> System Certificates，然后导入 pxGrid PEM 证书和 PVK 证书。



步骤 4 pxGrid 公钥/私钥将显示于主要 PAN 节点和主要 MnT 节点的系统证书库中。

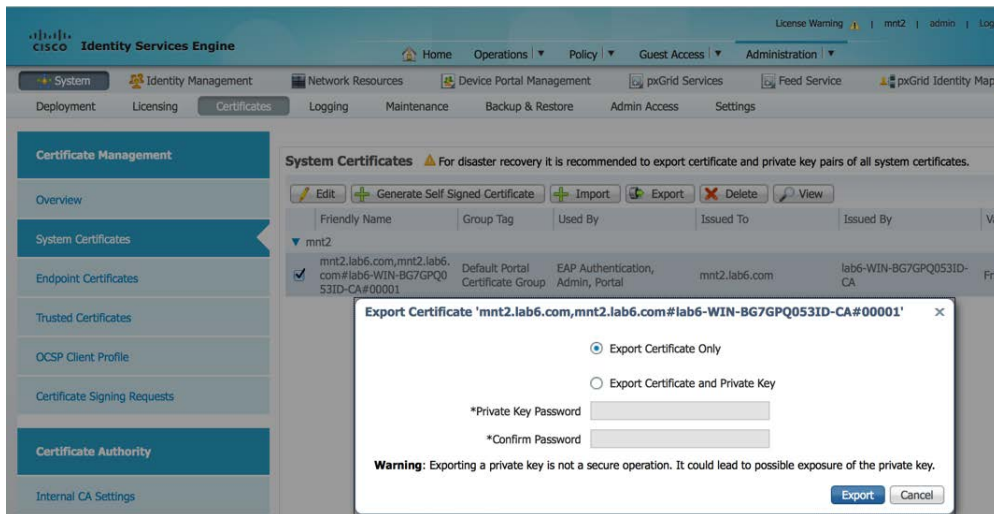


批量会话下载

批量会话下载使用 pxGrid session_download 脚本，从 ISE MnT 节点提供活动会话下载查询。这样即可提供已经过身份验证的 802.1X 会话中有关可用 ISE 情景信息的可用会话属性。将 MnT 节点的公钥 (PEM) 复制到 pxGrid 客户端并转换为 DER，然后导入到 truststoreFilename 密钥库中。此操作将于稍后介绍，而现在则要按照下述步骤导出 MnT 节点证书。

注：在 pxGrid 主用-备用配置中，需要将主要 MnT 节点和辅助 MnT 节点的证书都导入到 pxGrid 客户端中。如果其中任一个证书不存在，则会在注册客户端时出现问题，而且无法连接到 pxGrid 节点。

步骤 1 仅从所需的 MnT 节点导出公共证书密钥。此证书供 pxGrid 客户端用于批量会话下载 Administration -> Certificates -> Certificate Management -> System Certificates，然后选择 MnT 身份证书并导出公共证书

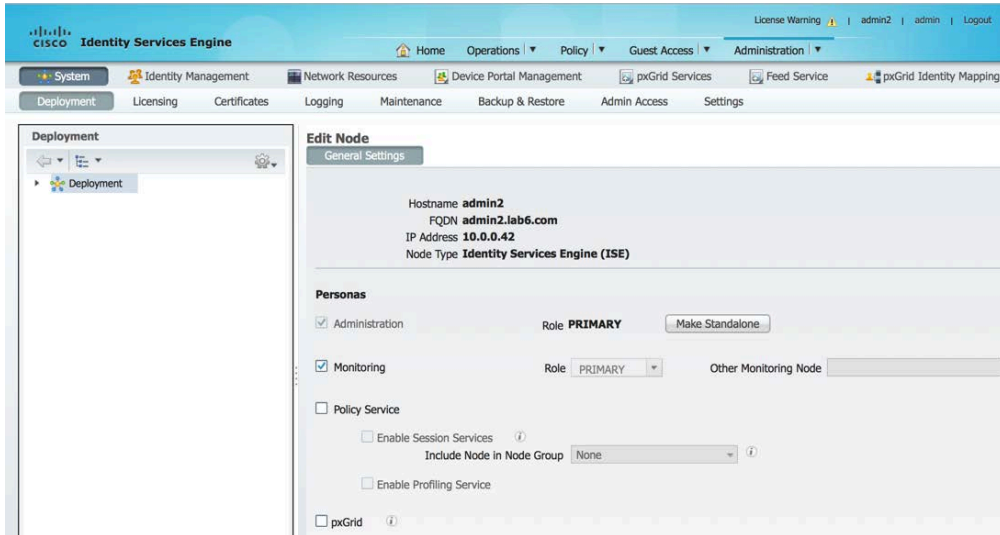


为分布式环境注册 ISE 节点

通过主要 Admin (PAN) 节点注册用于主要 PAN 节点、主要 MnT 节点、PSN 节点和 pxGrid 节点的所需的独立 ISE 节点。

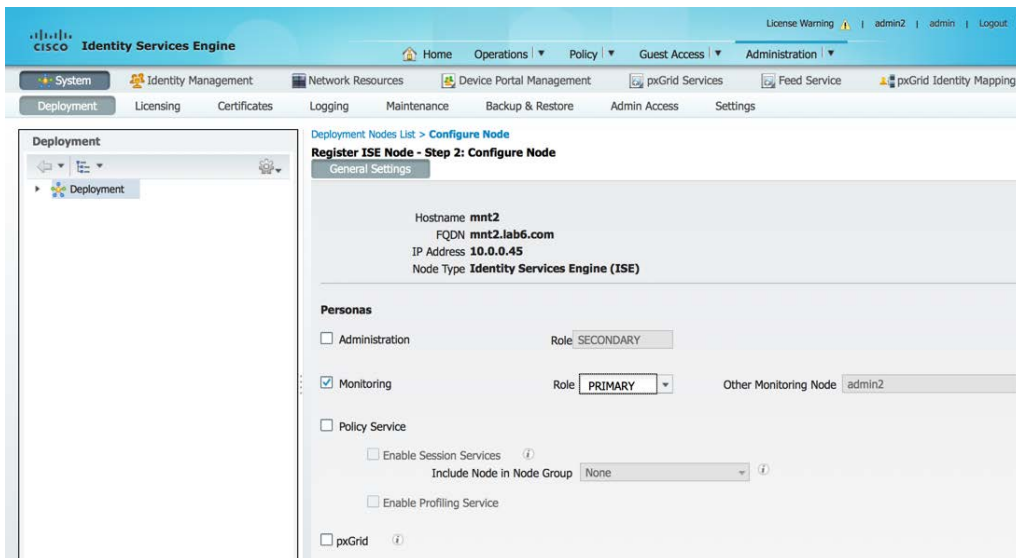
相应步骤定义如下：

步骤 1 将所需的 Admin 节点设置为最初包括主要 Admin 和主要 MnT 角色。

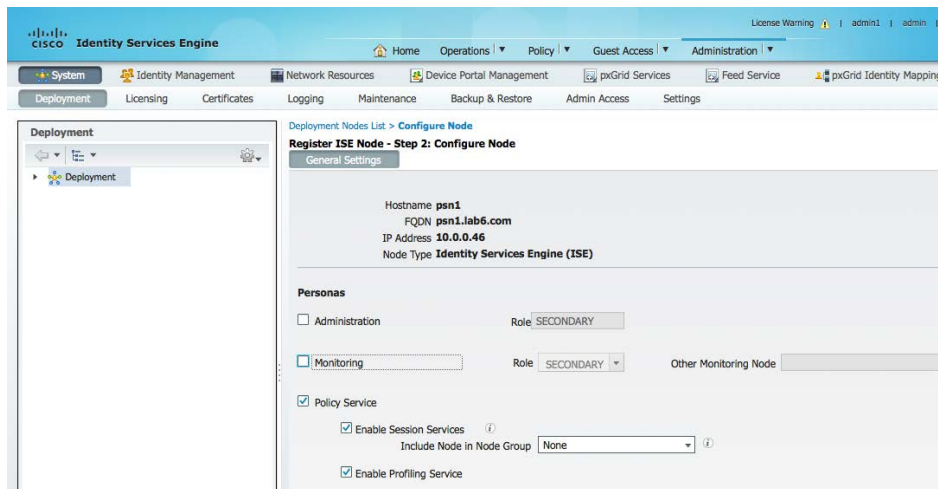


步骤 2 注册要作为主要 MnT 节点的所需的 MnT 节点。

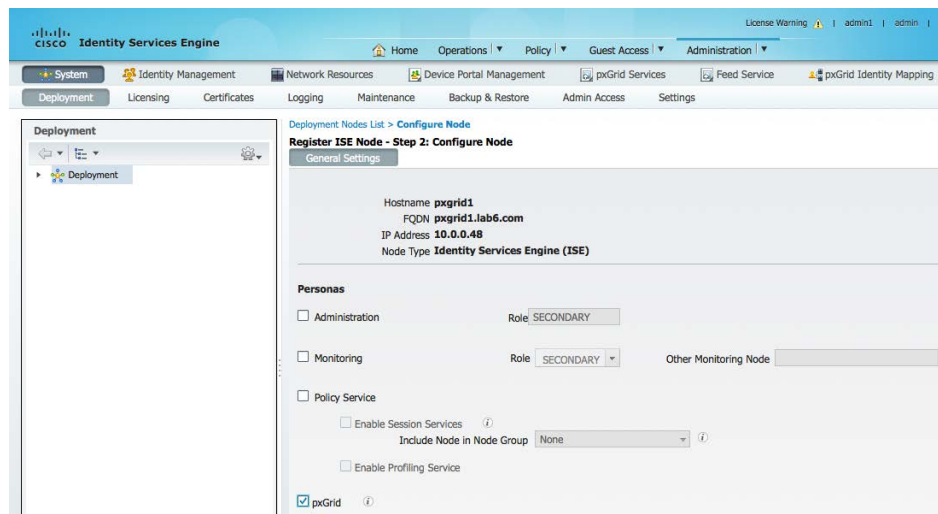
注： 主要 PAN 节点将自动成为辅助 MnT 角色。禁用辅助 MnT 角色。



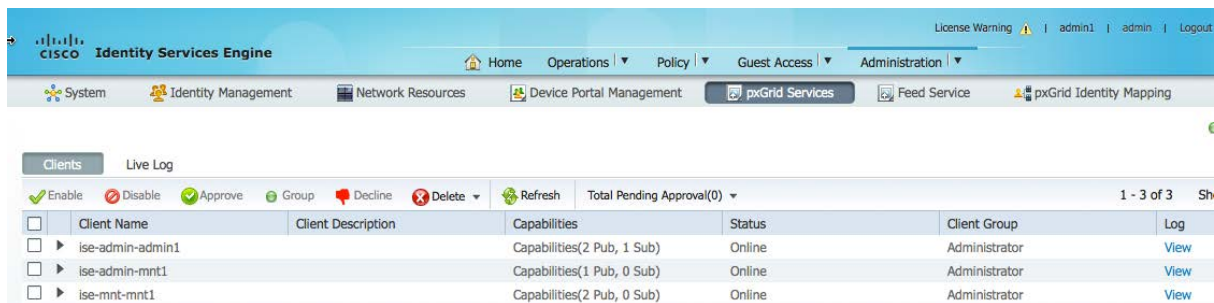
步骤 3 注册 PSN 节点



步骤 4 注册 pxGrid 节点

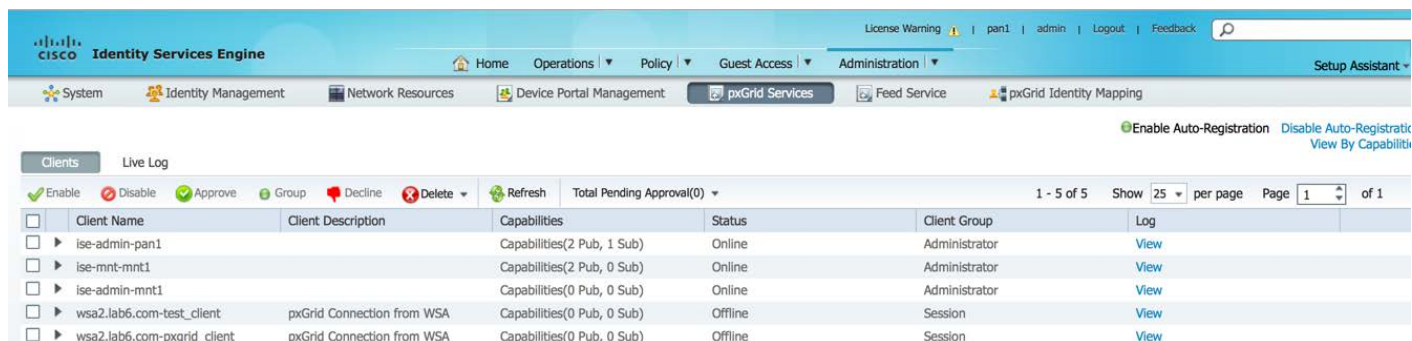


步骤 5 确保 pxGrid 服务已启动并且您有 ISE 发布的功能 Administration -> pxGrid Services, 同时启用 Auto Registration



pxGrid 客户端管理

pxGrid Service 菜单提供客户端管理、客户端注册/删除以及在禁用 Auto-Registration 时对客户端“挂起”请求进行授权的功能。此菜单还可用于查看客户端已注册功能或信息主题的日志历史记录。



Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-pan1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
wsa2.lab6.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View
wsa2.lab6.com-pxgrid_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Enable Auto-Registration - 启用自动注册，在 pxGrid 客户端初始身份验证完成后，pxGrid 客户端将自动注册。

Disable Auto-Registration - 禁用自动注册，pxGrid 客户端将保持“挂起”状态，直到管理员将其移入相应的“session”组或“EPS”组中。

Client Groups - client 组主要注册到“session”组，用于 pxGrid 操作。

Administrator - 为 ISE 预留

Session - 访问会话属性信息

EPS - “session”组的 **superset**，用于 ANC “自适应网络控制”缓解操作

Live Log - 显示客户端注册和主题订用的历史记录

License Warning | pan1 | admin | Logout

CISCO Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services | Feed Service | pxGrid Identity Map

Clients **Live Log**

Clear Logs | Resync | Refresh | 1 - 25 of 2104 | Show

Client Name	Capability Name	Event Type	Timestamp	Other Attributes
ise-admin-pan1@xgrid.cisco.com	GridControllerAdminServiceCapab...	Client subscribed	7:49:49 PM EST, Apr 17 2015	
		Resync database	7:49:49 PM EST, Apr 17 2015	
ise-admin-mnt1@xgrid.cisco.com		Client online	3:13:34 PM EST, Apr 16 2015	
ise-admin-mnt1@xgrid.cisco.com		Client deleted	3:13:33 PM EST, Apr 16 2015	
		Resync database	3:13:29 PM EST, Apr 16 2015	
ise-admin-mnt1@xgrid.cisco.com		Client online	3:09:07 PM EST, Apr 16 2015	
		Resync database	3:09:02 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com	SessionDirectoryCapability-1.0	Publisher added	3:07:34 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com	IdentityGroupCapability-1.0	Publisher added	3:07:33 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com		Client online	3:07:33 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com		Client deleted	3:07:31 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com	SessionDirectoryCapability-1.0	Publisher deleted	3:07:31 PM EST, Apr 16 2015	
ise-mnt-mnt1@xgrid.cisco.com	IdentityGroupCapability-1.0	Publisher deleted	3:07:19 PM EST, Apr 16 2015	
ise-admin-pan1@xgrid.cisco.com	GridControllerAdminServiceCapab...	Client subscribed	2:44:47 PM EST, Apr 16 2015	
		Resync database	2:44:47 PM EST, Apr 16 2015	
wsa2.lab6.com-pxgrid_client@xg...	SessionDirectoryCapability-1.0	Client subscribed	8:17:37 PM EST, Apr 15 2015	
wsa2.lab6.com-pxgrid_client@xg...	TrustSecMetaDataCapability-1.0	Client subscribed	8:17:37 PM EST, Apr 15 2015	

pxGrid 客户端配置

本节介绍如何安装用于 pxGrid 示例脚本测试的 pxGrid java SDK。系统将运行 Register.sh，连接 pxGrid 控制器并与其建立连接。然后将运行 Session_download.sh，从 ISE 下载活动会话记录。系统使用这些脚本进行基本测试，以确保 pxGrid 客户端与 ISE 之间的连接和通信能正常工作。如果要测试所有 shell 脚本（包括以前称为终端保护服务 [EPS] 的自适应网络控制 [ANC] 缓解操作），请参阅：
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 Java sdk 安装

请联系思科客户团队获取 pxGrid java SDK 库

请下载您的 Linux 操作系统适用的 Oracle Java Development Kit:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

要安装 Oracle Java Development Kit，必须卸载系统中现有的旧版本的 Java。

注： 如果使用 MAC 进行测试，请参阅以下网址了解如何卸载 Java: https://www.java.com/en/download/help/mac_uninstall_java.xml
如果您使用的是 Centos 6.5，请参阅附录在 **Centos 6.5 中删除 Java 和安装 JDK 8.0**

解压文件夹。tar -zxf pxgrid-sdk-x.x.x-dist.tar.gz

您将看到以下内容：

- Lib - 包含所有 GCL 库
- Samples - 包含 bin、certs、conf、lib 和 src 目录
- Bin - 包含所有示例脚本
- Certs - 包含所有样本 pxGrid 身份证书和 rootSample 证书
- Src - 包含所有 Java 源文件

要运行 pxGrid 示例脚本，请在“JAVA_HOME=”环境变量中加入 jre 路径。

下面以 MAC 为例加以说明。

要查看 jre 路径的位置，请运行以下命令：

注： 运行 sudo 命令时需要 root 权限

```
sudo find / -name java
Password:
/Applications/pxGridsdk/pxgrid-sdk-1.0.0/samples/src/java
find: /dev/fd/3: Not a directory
find: /dev/fd/4: Not a directory
/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/java
/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/bin/java
/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre/bin/java
```


将路径 “/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre” 添加到 JAVA_HOME

```
export JAVA_HOME=/Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre
```

如果使用的 Linux 版本不同（例如使用 Centos 64），请确保路径中包含 “keytool”

Append the “./jdk1.7._51/bin” to PATH

```
export
PATH=/usr/lib64/qt3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/jeppich/bin:/usr
/java/jdk1.7.0_51/bin
```

pxGrid 客户端 SDK Java 密钥库简介

Java 密钥库包含诸如 CA 根证书、主机身份证书或 pxGrid 客户端证书、自签名证书等证书的公钥/私钥对。Java 密钥库本身为 PKCS #12 格式 (.JKS)。

证书本身为 PEM 或 CER 格式，会被转换为 DER 并导入到 Java 密钥库中。

在本文档中，我们将使用 CA 签名的 pxGrid 客户端证书和 CA 签名的 ISE 证书。

pxGrid 有两个密钥库：包含 pxGrid 客户端身份证书的 keystoreFilename 以及代表 CA 根证书和 MnT 节点证书的 truststoreFilename。

此外，将证书导入到密钥库中时，这些密钥库值还包含关联的密码 keystorePassword 和 truststorePassword。

keystoreFilename、keystorePassword、truststoreFilename 和 truststorePassword 在 pxGrid SDK 脚本中用于 SASL 身份验证和 pxGrid 角色连接。

在下面的说明示例中，pxGrid 客户端注册并连接到 pxGrid 控制器。

```
./register.sh -keystoreFilename pxGridClient.jks -keystorePassword cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -group Session -description test -username macbook-pro -hostname 10.0.0.48

----- properties -----
version=1.0.0
hostnames=10.0.0.48
username=macbook-pro
descriptipon=test
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
-----
registering...
connecting...
account enabled
connected.
done registering.
connection closed
```

在下面的说明示例中，pxGrid 客户端从 MnT 节点下载活动会话记录

```
./session_download.sh -keystoreFilename pxGridClient.jks -keystoreFilename cisco123 -truststoreFilename
root3.jks -truststorePassword cisco123 -username macbook-pro -hostname 10.0.0.48

----- properties -----
version=1.0.0
hostnames=10.0.0.48
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
```

pxGrid 客户端证书配置

以下程序表示下列过程的步骤：为 pxGrid 客户端生成密钥、创建 CSR 请求、导入证书并将其转换为 DER 添加到密钥库。

注：该 pxGrid 客户端配置适用于具有 CA 签名的 pxGrid 客户端和 CA 签名的 pxGrid 节点证书的情况。有关其他证书部署的注意事项，请参阅参考资料。

具体过程如下所述：

- 为 pxGrid 客户端生成私钥
- 根据私钥生成 CSR（证书签名请求）。质询密钥是必须的，它将在稍后用于密钥库管理
- CA 机构使用此前定义的有效 pxGrid 模板为 CSR 请求签名
- 根据公钥/私钥对和根证书创建 PKCS#12 文件。此文件将用于创建密钥库 keystoreFilename (JKS) 和 truststoreFilename (JKS)
- 创建 keystoreFilename (JKS)
- 创建 truststoreFilename (JKS)
- 从用于活动会话记录或批量下载会话的 ISE MnT 主要节点和 ISE MnT 辅助节点导入 ISE 身份证书。

- 将 ISE 身份证书 PEM 文件转换为 DER 格式，连同 CA 根证书一起添加到 truststorefileName 密钥库中。
- 将 pxGrid 客户端证书导入到 keystoreFilename (JKS) 中
- 将 CA 根证书导入到 tuststoreFilename (JKS) 中
- 将两个文件都复制到 pxGrid 的 “../samples/bin/..” 文件夹中并运行脚本

步骤 1 生成私钥

为 pxGrid 客户端生成私钥（例如 mac.key）。

注：此 .key 名称可以是任意名称，此处以 mac.key 为例

```
openssl genrsa -out mac.key 4096

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

步骤 1 生成 CSR 请求

生成向 CA 机构请求证书的 CSR 请求（例如 mac.csr）。提供质询密码（例如 cisco123）

注：csr 可以是任意名称，为保持一致，此处仍以 mac.csr 为例；同样，质询密码也可以是任意名称

```
openssl req -new -key mac.key -out mac.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
在本文档各处使用相同的密码可便于维护，并减少错误
```

步骤 2 CA 机构为 PxGrid CS 请求签名。

CA 机构必须使用 pxGrid 模板（同时包含用于客户端身份验证和服务器身份验证的 EKU）提供用户证书。

注：由于选择的是 Windows 2003 的 CA 模板，所以它会显示于下拉列表中。复制的用户模板同时包含用于客户端身份验证和服务器身份验证的 EKU。

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):

```

iOCAQEAXjh+u8GMpwxadhin6yxCwKYl8YhOY5jrURxf
wCs4log7P4tQ6ajlGik3chergzdBkQMhYVzhvZhgq
Prz3cMgOCyAscTxhn8NlfsvLZYk5ayPpmuah3lL3
Hm+6thRTVhrKOG61ejxFd+0lzQxEn19YMov7sRSWFU1
jlf+Z+ptK87AYGzPYVWr/kl86b8TG1hSuMMF+AgIco
0Q23iwmr46gYabvhP6nmku4lQ8g==
-----
UEST-----

```

Certificate Template:

pxGrid

Additional Attributes:

Attributes:

Submit >

步骤 3 创建 PKCS12 文件

根据 pxGrid 客户端证书（例如 mac.cer）中的私钥创建 pxGrid 客户端 pkcs12 文件 (mac.p12)。此文件将用于密钥库管理，可以是扩展名为 .p12 的随机文件名。包括 CA 根文件（例如 root2a）。

```
openssl pkcs12 -export -out mac.p12 -inkey mac.key -in mac.cer -chain -CAfile root2a.cer
```

Enter Export Password: cisco123

Verifying - Enter Export Password: cisco123

步骤 4 为 pxGrid 客户端创建 keystoreFilename

创建 pxGrid 客户端身份密钥库（例如 mac.jks）。这是 pxGrid 客户端身份密钥库，可以是扩展名为 .jks 的随机文件名。这将在 pxGrid 脚本示例中充当 keystoreFilename 和关联的 keystorePassword。

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

Enter destination keystore password: cisco123

Re-enter new password: cisco123

Enter source keystore password:

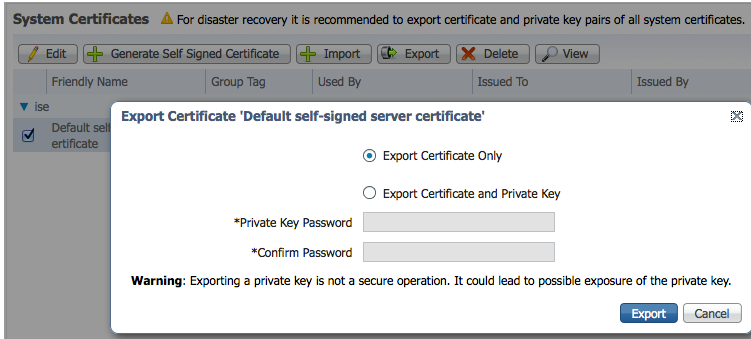
Entry for alias 1 successfully imported.

Import command completed: 1 entries successfully imported, 0 entries failed or cancelled

步骤 5 从 ISE MnT 主要节点和 ISE MnT 辅助节点导出公共 ISE 身份证书

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。在本例中，该文件被重命名为 mnt1.pem。

注：如果已进行 pxGrid 主用-备用配置，则 pxGrid 客户端同时需要 ISE MnT 主要节点和 ISE Mnt 辅助节点的证书



步骤 6 将 ISE MnT 节点身份证书从 PEM 格式转换为 DER 格式

```
openssl x509 -outform der -in mnt1.pem -out mnt1.der
```

步骤 7 将 ISE MnT DER 文件添加到 truststoreFilename 中

将 ISE 身份证书添加到信任密钥库（例如 caroot1.jks）中。这是受信任的密钥库，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 truststoreFilename 和 truststorePassword。

```
keytool -import -alias isemnt -keystore caroot1.jks -file mnt1.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: 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  00...*.H.....
0020: 00 80 30 07 06 05 2B 0E  03 02 07 30 0A 06 08 2A  00...+...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  00...+.....0...+
0020: 01 05 05 07 03 04 30 0C  06 0A 2B 06 01 04 01 82  00...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  00...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF  40 02 01 64 02 01 03  00...#...@...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                               ....
]
]

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

```

步骤 8 将 pxGrid 客户端证书导入到 keystoreFilename 中

将 pxGrid 客户端证书导入到身份密钥库中。

```

Johns-MacBook-Pro:pxGridsdk jeppich$ keytool -import -alias pxGridMAC -keystore mac.jks -file
mac.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”，这不会有任何问题。我选择了“yes”，因此我们可以验证后来是否添加了证书。

步骤 9 将 CA 根证书添加到 truststoreFilename 中

将 CA 根证书添加到受信任的密钥库中。CA 根证书也需要是受信任的。

```
keytool -import -alias ca_root1 -keystore caroot1.jks -file root2a.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 10 将身份密钥库 (mac.jks) 和信任密钥库 (caroot1.jks) 复制到 pxGrid “../samples/bin/..” 文件夹中。

pxGrid 客户端主用-备用配置示例

对于 pxGrid 主用-备用配置，需要将主要 MnT 节点和辅助 MnT 节点公共证书 (PEM) 都导出到 pxGrid 客户端中并转换为 DER 格式。需要将这两个证书都连同 CA 根证书 (root2a.cer) 一起添加到 truststoreFilename 密钥库中。


```

Johns-Macbook-Pro:mntnodes jeppich$ openssl x509 -outform der -in mnt1.pem -out mnt1.der
Johns-Macbook-Pro:mntnodes jeppich$ keytool -import -alias lab1 -keystore caroot1.jks -file mnt1.der
Enter keystore password:
Re-enter new password:
Owner: CN=mnt1.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61326a18000000000031
Valid from: Tue Jan 20 20:08:40 EST 2015 until: Fri Jan 20 20:18:40 EST 2017
Certificate fingerprints:
    MD5:  D7:EC:5C:10:37:8D:6A:64:4C:51:BE:0B:7E:46:A4:36
    SHA1: 6A:CF:48:0D:55:34:41:AA:D8:68:2C:06:86:6E:85:1A:80:7A:8E:BE
    SHA256:
66:7C:74:C3:D8:50:D0:09:A2:AA:60:5C:9D:97:09:D9:75:30:DD:3D:4B:56:47:77:91:47:84:DF:46:57:53:6F
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:
    [URName: 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: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt1.lab6.com
]

#11: 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 keystore
Johns-Macbook-Pro:mntnodes jeppich$ openssl x509 -outform der -in mnt2.pem -out mnt2.der
Johns-Macbook-Pro:mntnodes jeppich$ keytool -import -alias lab1 -keystore caroot1.jks -file mnt2.der
Enter keystore password:
keytool error: java.lang.Exception: Certificate not imported, alias <lab1> already exists
Johns-Macbook-Pro:mntnodes jeppich$ keytool -import -alias lab2 -keystore caroot1.jks -file mnt2.der
Enter keystore password:
Owner: CN=mnt2.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 613244ec000000000044
Valid from: Wed Mar 04 18:11:54 EST 2015 until: Fri Mar 03 18:11:54 EST 2017
Certificate fingerprints:
    MD5:  1E:96:5E:35:A1:3E:FA:CD:16:32:A7:01:2C:5A:E6:12
        SHA1: 8F:0D:8A:58:DD:80:82:D3:56:F1:CE:26:E4:A3:C3:3F:F8:F6:D1:28
        SHA256:
3A:70:F0:E6:43:93:E8:10:11:C5:FE:61:24:66:A2:C8:2A:FA:AC:04:38:4A:B5:B6:20:2C:E6:3C:21:D5:45:C3
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 12 00 57 00 65 00 62   00 53 00 65 00 72 00 76   ...W.e.b.S.e.r.v
0010: 00 65 00 72               .e.r

```

```
#2: 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
  ]
]

#3: 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,
]
]

#4: 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]
  ]]

#5: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
]

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

#7: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt2.lab6.com
]

#8: 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 keystore
Johns-Macbook-Pro:mntnodes jeppich$ keytool -list -v -keystore caroot1.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: lab2
Creation date: Mar 4, 2015
Entry type: trustedCertEntry

Owner: CN=mnt2.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 613244ec000000000044
Valid from: Wed Mar 04 18:11:54 EST 2015 until: Fri Mar 03 18:11:54 EST 2017
```

```

Certificate fingerprints:
    MD5:  1E:96:5E:35:A1:3E:FA:CD:16:32:A7:01:2C:5A:E6:12
    SHA1: 8F:0D:8A:58:DD:80:82:D3:56:F1:CE:26:E4:A3:C3:3F:F8:F6:D1:28
    SHA256:
3A:70:F0:E6:43:93:E8:10:11:C5:FE:61:24:66:A2:C8:2A:FA:AC:04:38:4A:B5:B6:20:2C:E6:3C:21:D5:45:C3
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 12 00 57 00 65 00 62  00 53 00 65 00 72 00 76  ...W.e.b.S.e.r.v
0010: 00 65 00 72                                     .e.r

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

#3: 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,
  ]
]

#4: 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]
  ]]

#5: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
]

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

#7: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt2.lab6.com
]

#8: 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: lab1
Creation date: Mar 4, 2015
Entry type: trustedCertEntry
```

```
Owner: CN=mtl.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61326a18000000000031
Valid from: Tue Jan 20 20:08:40 EST 2015 until: Fri Jan 20 20:18:40 EST 2017
```

```
Certificate fingerprints:
    MD5: D7:EC:5C:10:37:8D:6A:64:4C:51:BE:0B:7E:46:A4:36
    SHA1: 6A:CF:48:0D:55:34:41:AA:D8:68:2C:06:86:6E:85:1A:80:7A:8E:BE
    SHA256:
66:7C:74:C3:D8:50:D0:09:A2:AA:60:5C:9D:97:09:D9:75:30:DD:3D:4B:56:47:77:91:47:84:DF:46:57:53:6F
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: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt1.lab6.com
]

#11: 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:mntnodes jeppich$ openssl x509 -outform der -in root2a.cer -out root2a.der
Johns-Macbook-Pro:mntnodes jeppich$ keytool -import -alias lab3 -keystore caroot1.jks -file root2a.der
Enter keystore password:
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
```


在 ISE 分布式环境中测试 xGrid 客户端

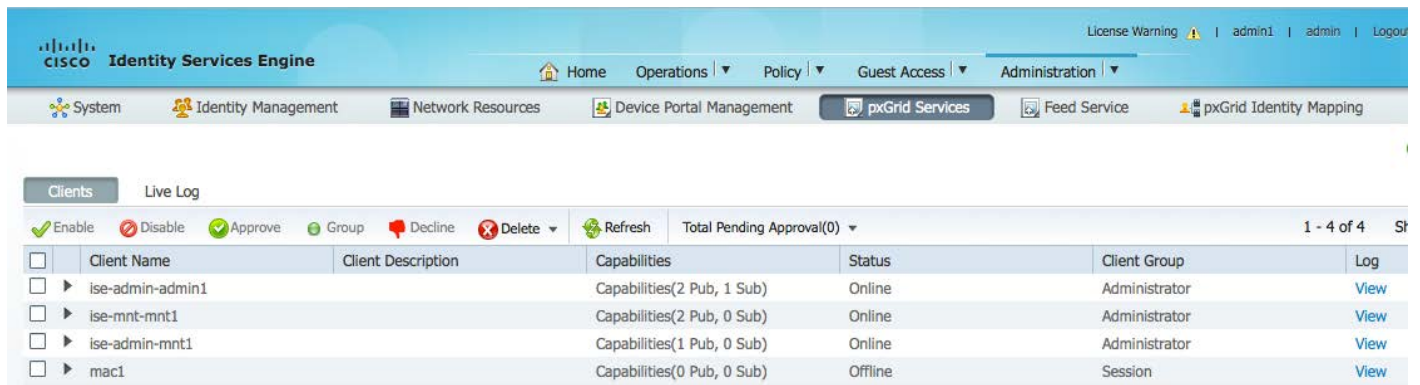
系统将运行 pxGrid 脚本 `register.sh` 和 `session_download.sh` 来确保 pxGrid 客户端连接和 pxGrid 注册。会话下载可确保 ISE MNT 证书和 pxGrid 客户端没有问题。

步骤 1 注册 pxGrid 客户端

```
Johns-Macbook-Pro:bin jeppich$ ./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 -username mac1 -group Session
----- properties -----
version=1.0.0
hostnames=10.0.0.48
username=mac1
descriptipon=null
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
-----
registering...
connecting...
connected.
done registering.
connection closed
Johns-Macbook-Pro:bin jeppich$
```

验证 pxGrid 客户端是否已注册到 pxGrid 控制器

Administration -> pxGrid Services



Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
mac1		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

步骤 2 运行会话下载

```
Johns-Macbook-Pro:bin jeppich$ ./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 -username mac1
----- properties -----
version=1.0.0
hostnames=10.0.0.48
username=mac1
keystoreFilename=mac.jks
keystorePassword=cisco123
```

```
truststoreFilename=caroot1.jks
truststorePassword=cisco123
filter=null
start=null
end=null
-----
connecting...
connected.
starting at Thu Mar 05 21:45:49 EST 2015...

session (ip=10.0.0.17, Audit Session Id=0A0000020000000D02D814C0, User Name=jeplich, 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:29:77:D6:85, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint
Profile=VMWare-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/23, RADIUSAVPairs=[ Acct-Session-
Id=00000004], Posture Status=null, Posture Timestamp=, Session Last Update Time=Thu Mar 05 21:33:02 EST
2015 )
session (ip=null, Audit Session Id=0A0000020000000C0003672C, User Name=68:EF:BD:F6:76:56, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=68:EF:BD:F6:76:56, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000005], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Thu Mar 05 21:33:44 EST 2015 )... ending at: Thu
Mar 05 21:45:49 EST 2015

-----
downloaded 2 sessions in 35 milliseconds
-----

connection closed
```

查看密钥库条目

通过查看密钥库条目，您可以查看 keystoreFilename 和 truststoreFilename 密钥库的受信任证书条目。

步骤 1 验证 truststoreFilename 密钥库 caroot1.jks

```
Johns-Macbook-Pro:bin jeplich$ keytool -list -v -keystore caroot1.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: lab3
Creation date: Mar 4, 2015
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: lab2
Creation date: Mar 4, 2015
Entry type: trustedCertEntry

Owner: CN=mt2.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 613244ec000000000044
Valid from: Wed Mar 04 18:11:54 EST 2015 until: Fri Mar 03 18:11:54 EST 2017
Certificate fingerprints:
    MD5:  1E:96:5E:35:A1:3E:FA:CD:16:32:A7:01:2C:5A:E6:12
    SHA1: 8F:0D:8A:58:DD:80:82:D3:56:F1:CE:26:E4:A3:C3:3F:F8:F6:D1:28
    SHA256:
3A:70:F0:E6:43:93:E8:10:11:C5:FE:61:24:66:A2:C8:2A:FA:AC:04:38:4A:B5:B6:20:2C:E6:3C:21:D5:45:C3
Signature algorithm name: SHA256withRSA
Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false
0000: 1E 12 00 57 00 65 00 62   00 53 00 65 00 72 00 76   ...W.e.b.S.e.r.v
0010: 00 65 00 72          .e.r

#2: 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
  ]
]

#3: 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,
]
]

#4: ObjectId: 2.5.29.31 Criticality=false
CRLDistributionPoints [
  [DistributionPoint:
    [URName: 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]
]]

#5: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
]

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

#7: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt2.lab6.com
]

#8: 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: lab1
Creation date: Mar 4, 2015
Entry type: trustedCertEntry

Owner: CN=mnt1.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61326a18000000000031
Valid from: Tue Jan 20 20:08:40 EST 2015 until: Fri Jan 20 20:18:40 EST 2017
Certificate fingerprints:
  MD5: D7:EC:5C:10:37:8D:6A:64:4C:51:BE:0B:7E:46:A4:36
  SHA1: 6A:CF:48:0D:55:34:41:AA:D8:68:2C:06:86:6E:85:1A:80:7A:8E:BE
  SHA256:
66:7C:74:C3:D8:50:D0:09:A2:AA:60:5C:9D:97:09:D9:75:30:DD:3D:4B:56:47:77:91:47:84:DF:46:57:53:6F
  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: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt1.lab6.com
]

#11: 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 keystoreFilename 密钥库 mac.jks

```
Johns-Macbook-Pro:bin jeppich$ keytool -list -v -keystore mac.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: 1
Creation date: Jan 28, 2015
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: 6118d613000000000034
Valid from: Wed Jan 28 14:35:54 EST 2015 until: Sat Jan 28 14:45:54 EST 2017
Certificate fingerprints:
    MD5:  93:E4:D9:1B:00:5B:48:75:C1:9F:36:BC:E7:5C:27:73
    SHA1: 33:79:37:44:81:EA:68:B8:EC:A3:26:75:18:70:AA:11:E4:58:B2:AF
    SHA256:
DA:6C:BA:E3:E8:76:DD:8A:30:BA:EE:0B:46:3B:78:BF:F9:CE:B4:68:2C:5D:CE:8A:9D:FB:66:A8:1F:97:BE:4A
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  00...*.H.....
0020: 00 80 30 07 06 05 2B 0E  03 02 07 30 0A 06 08 2A  00...+...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  00...+.....0...+
0020: 01 05 05 07 03 04 30 0C  06 0A 2B 06 01 04 01 82  00...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  00...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF  40 02 01 64 02 01 03  00...#...@..d...

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

```

[
  accessMethod: caIssuers
  accessLocation: URName: 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:
    [URName: 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: 81 52 81 84 98 22 43 85   5E 95 06 14 D2 5A A8 70   .R..."C.^....Z.p
    0010: 15 06 CF DB                               ....
  ]
]

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,
]
]

*****
*****

Alias name: macstore
Creation date: Jan 28, 2015
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: 6118d613000000000034
Valid from: Wed Jan 28 14:35:54 EST 2015 until: Sat Jan 28 14:45:54 EST 2017
Certificate fingerprints:
  MD5: 93:E4:D9:1B:00:5B:48:75:C1:9F:36:BC:B7:5C:27:73
  SHA1: 33:79:37:44:81:EA:68:B8:EC:A3:26:75:18:70:AA:11:E4:58:B2:AF
  SHA256:
DA:6C:BA:E3:E8:76:DD:8A:30:BA:EE:0B:46:3B:78:BF:F9:CE:B4:68:2C:5D:CE:8A:9D:FB:66:A8:1F:97:BE:4A
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: 81 52 81 84 98 22 43 85   5E 95 06 14 D2 5A A8 70   .R..."C.^....Z.p
0010: 15 06 CF DB                               ....
]
]

*****
*****

Johns-Macbook-Pro:bin jeppich$

```

采用 pxGrid 主用-备用配置的 ISE 分布式部署简介

本节介绍 pxGrid 主用-备用配置。在 ISE 分布式部署中，只能有 (2) 个 pxGrid 节点。一个处理控制 pxGrid 服务的 pxGrid 客户端连接，另一个用于故障切换。每次只有一个 pxGrid 节点处于活动状态。

采用 pxGrid 主用-备用配置的 ISE 分布式部署包括主要 Admin 节点、辅助 Admin 节点、主要 MnT 节点，辅助 MnT 节点、两个 PSN 节点和两个不同的 pxGrid 角色。

我们将添加辅助 Admin 节点、辅助 MnT 节点和辅助 pxGrid 节点，构成 pxGrid 主用-备用配置。

将公钥/私钥从第一个或主要 pxGrid 角色导出到主要 Admin 节点和主要 MnT 节点的系统证书库中。

注：在初始 ISE 分布式部署过程中已经完成此配置。

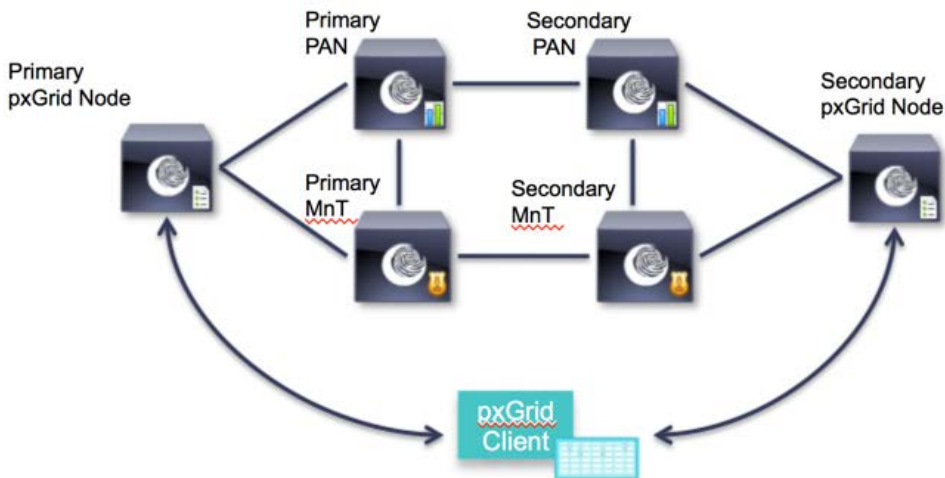
将公钥/私钥从第二个或辅助 pxGrid 角色导出到辅助 Admin 节点和辅助 MnT 节点的系统证书库中。

将主要和辅助 MnT 节点身份证书导出到 pxGrid 客户端中，用于批量活动会话下载。如果缺少其中任一证书，pxGrid 客户端都无法注册。

注册的客户端帐户、订用和主题等为主用-主用配置，通过 PAN 节点在 pxGrid 服务器之间同步。主要和辅助 pxGrid 节点为主用-备用配置。

pxGrid 客户端连接到主要 PxGrid 节点。如果主要 pxGrid 节点断开，客户端会连接到辅助 pxGrid 节点，所有注册的客户端和事务都会转移到该节点。本文档将对此加以说明。

pxGrid Active-Standby Configuration



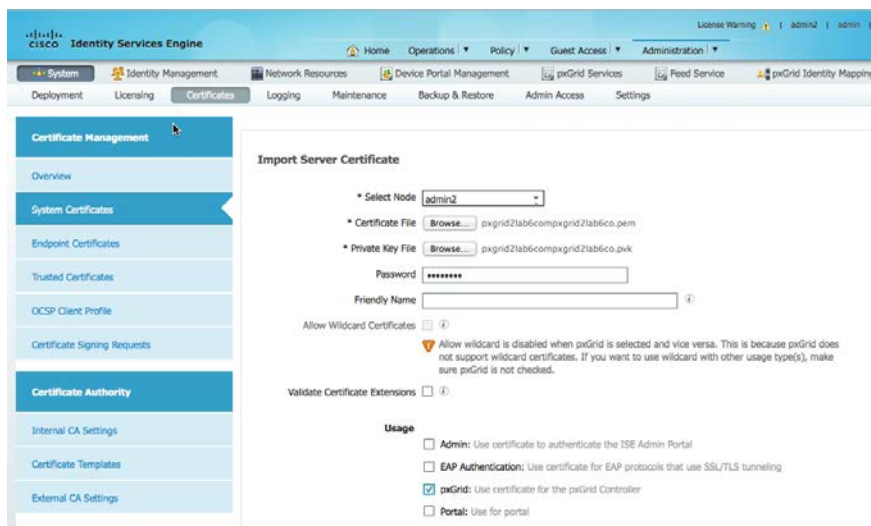
为分布式环境 pxGrid 主用-备用配置注册 ISE 节点

此处注册的是辅助节点。

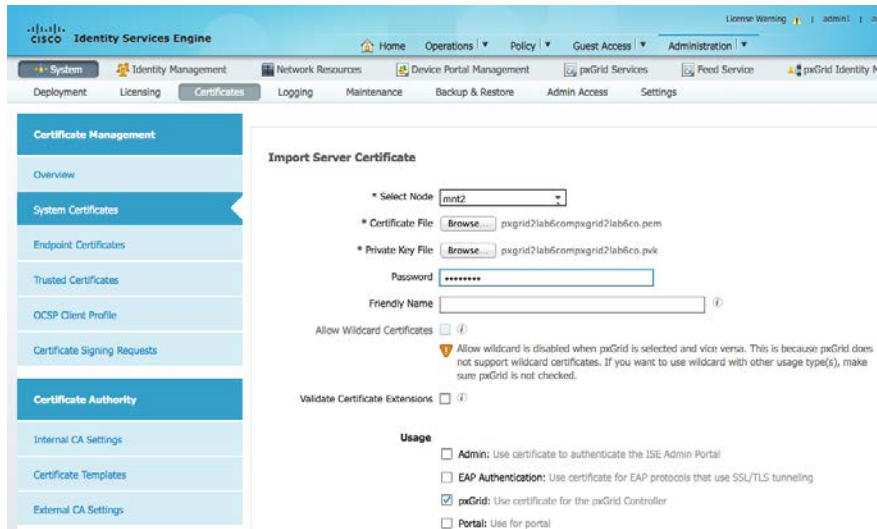
步骤 1 将辅助 pxGrid 节点的公钥/私钥对导入到辅助 PAN 节点中。
Administration -> System -> Certificate -> Certificate Management -> System Certificates, 然后导入辅助 pxGrid 节点的公钥/私钥

注: 可以在所有节点处于独立模式时完成此操作, 也可以直接从主要 PAN 节点完成此操作。

此处假定已经从辅助 pxGrid 节点导出公钥/私钥对。



步骤 2 将辅助 pxGrid 节点的公钥/私钥对导入到辅助 PAN 节点中。
Administration -> System -> Certificate -> Certificate Management -> System Certificates, 然后导入辅助 pxGrid 节点的公钥/私钥



步骤 3 公钥/私钥对应该已经成功导入到 ISE 辅助 PAN 节点和 ISE 辅助 MnT 节点中。
Administration -> System -> Certificates -> Certificate Management -> System Certificates

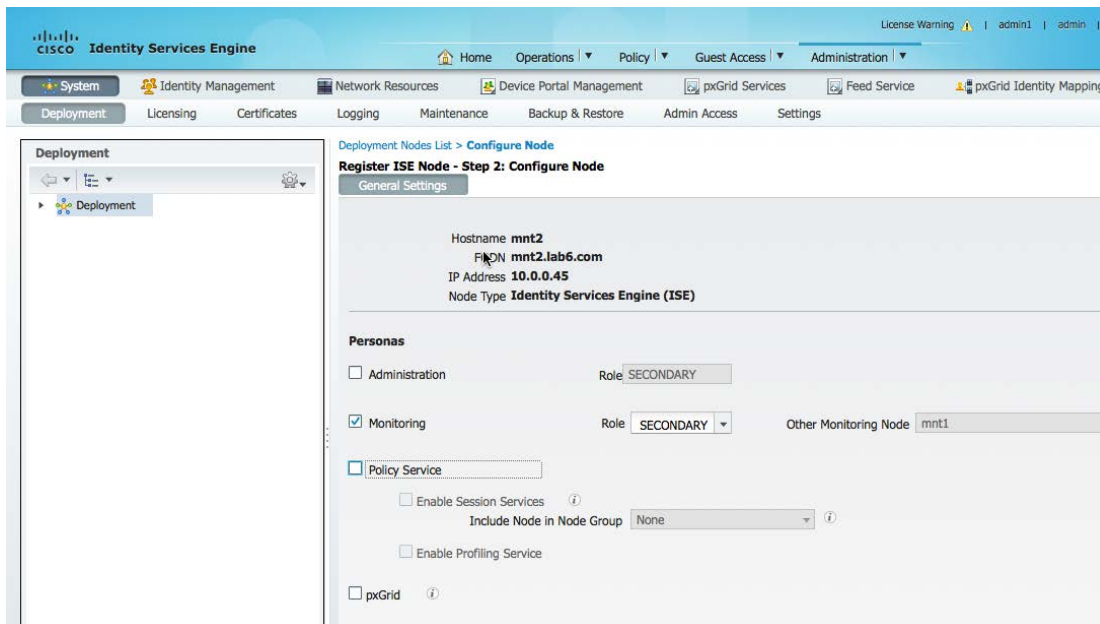
The screenshot shows the 'System Certificates' page in the Cisco ISE Administration console. The page title is 'System Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.' Below the title are buttons for 'Edit', 'Generate Self Signed Certificate', 'Import', 'Export', 'Delete', and 'View'. A table lists certificates for two nodes: 'admin2' and 'mnt2'. Each node has two certificates: one for 'EAP Authentication, Admin, Portal' and one for 'pxGrid'. The table columns are: Friendly Name, Group Tag, Used By, Issued To, Issued By, Valid From, and Expiration Date. All certificates have a green checkmark in the rightmost column, indicating they are valid.

Friendly Name	Group Tag	Used By	Issued To	Issued By	Valid From	Expiration Date	
▼ admin2							
admin2.lab6.com,admin2.lab6.com#lab6-WIN-BG7GPQ0531D-CA#00001	Default Portal Certificate Group	EAP Authentication, Admin, Portal	admin2.lab6.com	lab6-WIN-BG7GPQ0531D-CA	Wed, 4 Mar 2015	Fri, 3 Mar 2017	✓
pxgrid2.lab6.com,pxgrid2.lab6.com#lab6-WIN-BG7GPQ0531D-CA#00002		pxGrid	pxgrid2.lab6.com	lab6-WIN-BG7GPQ0531D-CA	Wed, 4 Mar 2015	Sat, 4 Mar 2017	✓
▼ mnt2							
mnt2.lab6.com,mnt2.lab6.com#lab6-WIN-BG7GPQ0531D-CA#00001	Default Portal Certificate Group	EAP Authentication, Admin, Portal	mnt2.lab6.com	lab6-WIN-BG7GPQ0531D-CA	Wed, 4 Mar 2015	Fri, 3 Mar 2017	✓
pxgrid2.lab6.com,pxgrid2.lab6.com#lab6-WIN-BG7GPQ0531D-CA#00002		pxGrid	pxgrid2.lab6.com	lab6-WIN-BG7GPQ0531D-CA	Wed, 4 Mar 2015	Sat, 4 Mar 2017	✓

步骤 4 通过主要 Admin 节点注册辅助 Admin 节点
Administration -> System -> Deployment, 将 ISE 节点注册为辅助 Admin 节点

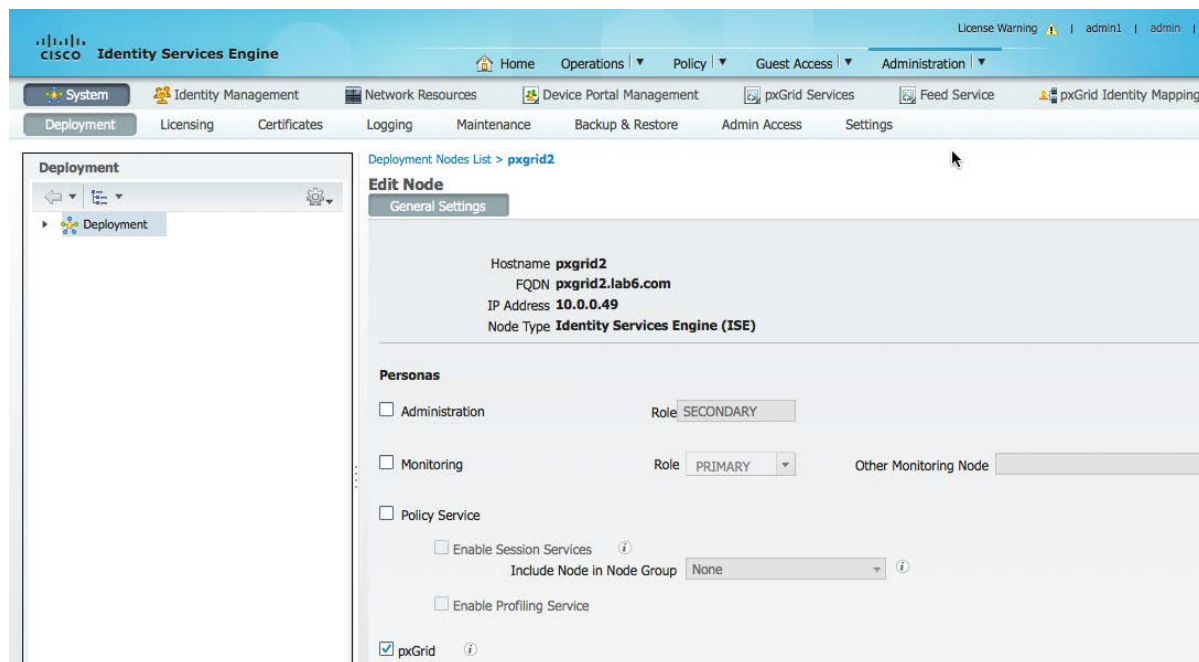
The screenshot shows the 'Register ISE Node - Step 2: Configure Node' page in the Cisco ISE Administration console. The page title is 'Register ISE Node - Step 2: Configure Node' with a sub-tab 'General Settings'. The page displays configuration details for a node named 'admin2'. The Hostname is 'admin2', FQDN is 'admin2.lab6.com', and IP Address is '10.0.0.42'. The Node Type is 'Identity Services Engine (ISE)'. Under the 'Personas' section, 'Administration' is checked with a role of 'SECONDARY'. 'Monitoring' is unchecked with a role of 'SECONDARY' and an 'Other Monitoring Node' field. 'Policy Service' is unchecked, with options for 'Enable Session Services' (unchecked), 'Include Node in Node Group' (set to 'None'), and 'Enable Profiling Service' (unchecked). 'pxGrid' is also unchecked.

步骤 5 通过主要 Admin 节点注册辅助监控节点
Administration -> System -> Deployment, 将 ISE 节点注册为辅助监控节点

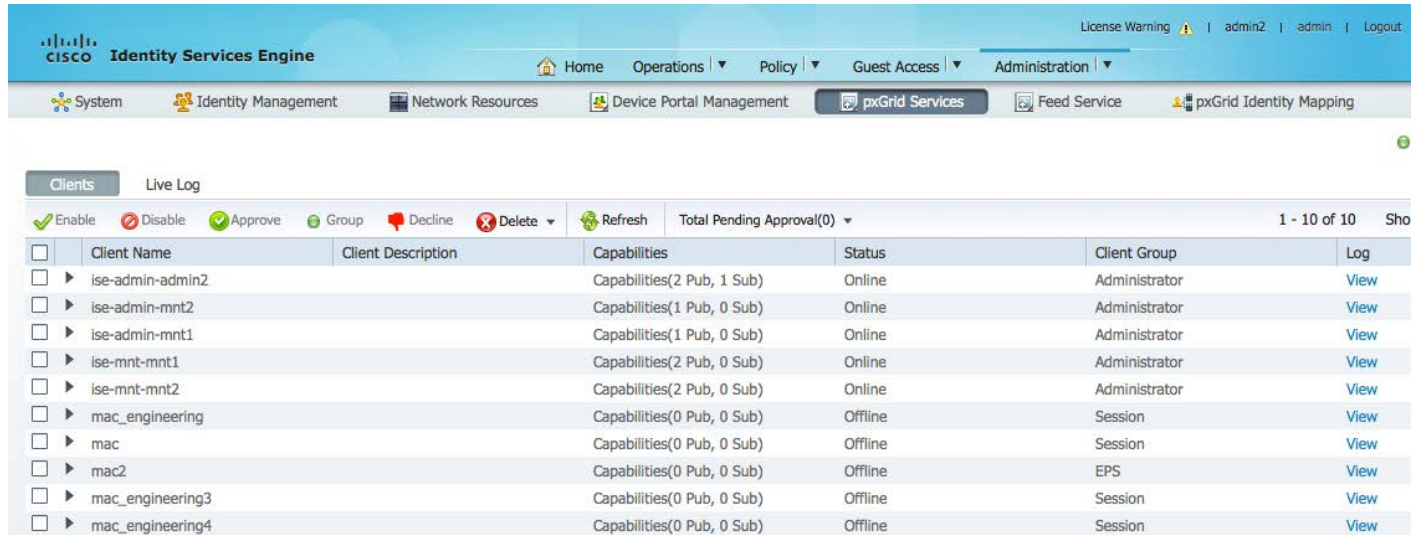


注：确保辅助 Mnt 节点已加入域，检查外部身份服务，如果辅助 Mnt 节点尚未加入域，则不会连接到 pxGrid 节点。

步骤 6 添加辅助 pxGrid 节点
Administration -> System -> Deployment, 将 ISE 节点注册为辅助 pxGrid 节点



步骤 7 确保 pxGrid 服务已启动并且您能看到 ISE 发布的节点：
Administration -> pxGrid Services



License Warning | admin2 | admin | Logout

Home Operations Policy Guest Access Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service pxGrid Identity Mapping

Clients Live Log

Enable Disable Approve Group Decline Delete Refresh Total Pending Approval(0) 1 - 10 of 10 Sho

<input type="checkbox"/>	Client Name	Client Description	Capabilities	Status	Client Group	Log
<input type="checkbox"/>	ise-admin-admin2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
<input type="checkbox"/>	ise-admin-mnt2		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/>	ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/>	ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/>	ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
<input type="checkbox"/>	mac_engineering		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
<input type="checkbox"/>	mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
<input type="checkbox"/>	mac2		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View
<input type="checkbox"/>	mac_engineering3		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
<input type="checkbox"/>	mac_engineering4		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

在 ISE 分布式环境 pxGrid 主用-备用配置中测试 pxGrid 客户端

本节通过添加辅助 PAN 节点、辅助 MnT 节点和辅助 pxGrid 节点来说明 pxGrid 主用-备用配置。此外，我们还将通过以下方式测试该配置：

基本操作：

- 将 pxGrid 客户端注册到主要 pxGrid 节点

注：在 pxGrid 主用-备用配置中，只有主要 pxGrid 节点可处于活动状态，而辅助 pxGrid 节点则处于“not running”状态，正如在 pxGrid 辅助节点上发出“sh application status ise”命令时所示

- 从 MnT 主要节点下载活动会话记录
- 在 ISE 中查看注册的 pxGrid 客户端状态
- 查看部署节点状态以显示 pxGrid 节点状态

测试 pxGrid 节点能否故障切换为辅助 pxGrid 节点

- 在主要 pxGrid 节点上发出“application stop ise”命令，模拟 pxGrid 节点断开的情况
- 在辅助 pxGrid 节点上发出“application start ise”命令，启动辅助 pxGrid 节点
- 从 MnT 主要节点下载活动会话以便对其进行比较，这些会话应该相同
- 将 pxGrid 客户端注册到辅助 pxGrid 节点
- 在 ISE 中查看注册的 pxGrid 客户端
- 查看部署节点状态以显示 pxGrid 节点状态

恢复 pxGrid 主要节点

- 在辅助 pxGrid 节点上发出“application stop ise”命令
- 在主要 pxGrid 节点上发出“application start ise”命令
- 从 MnT 主要节点下载活动会话以便对其进行比较，这些会话应该相同
- 将 pxGrid 客户端注册到主要 pxGrid 节点
- 在 ISE 中查看注册的 pxGrid 客户端
- 查看部署节点状态以显示 pxGrid 节点状态

测试 pxGrid 主用-备用配置

基本操作

此处我们在 pxGrid 主用-备用配置中，将 pxGrid 客户端注册到第一个 pxGrid 节点或主要 pxGrid 节点。

基本操作：

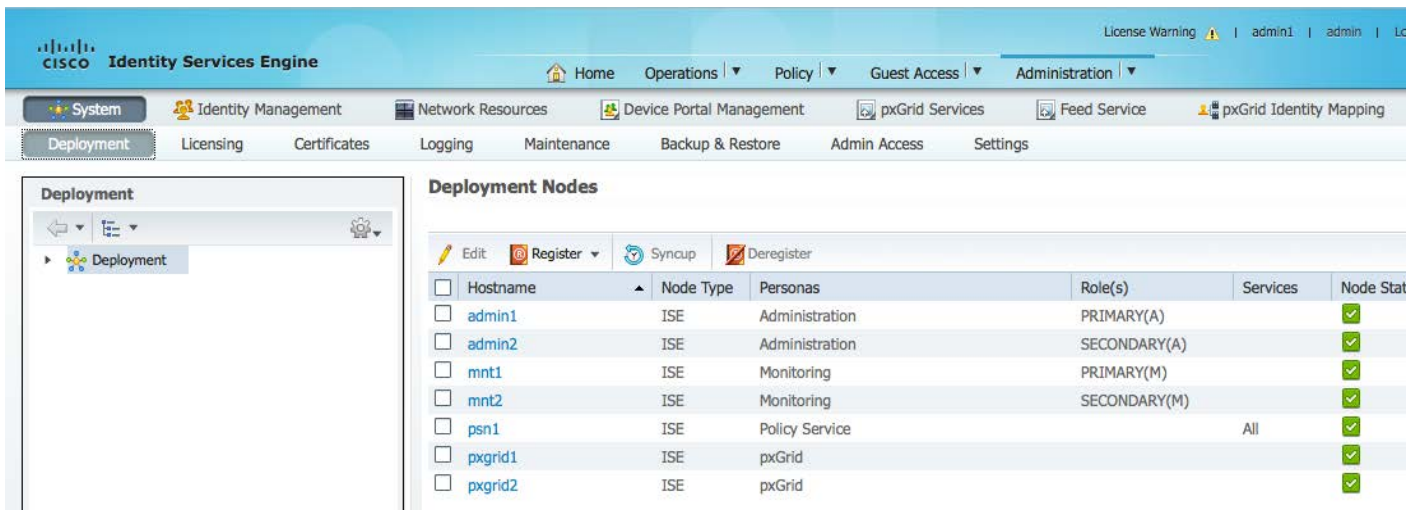
- 将 pxGrid 客户端注册到主要 pxGrid 节点

注：在 pxGrid 主用-备用配置中，只有主要 pxGrid 节点可处于活动状态，而辅助 pxGrid 节点则处于“not running”状态，正如在 pxGrid 辅助节点上发出“sh application status ise”命令时所示

- 从 MnT 主要节点下载活动会话记录
- 在 ISE 中查看注册的 pxGrid 客户端状态
- 查看部署节点状态以显示 pxGrid 节点状态

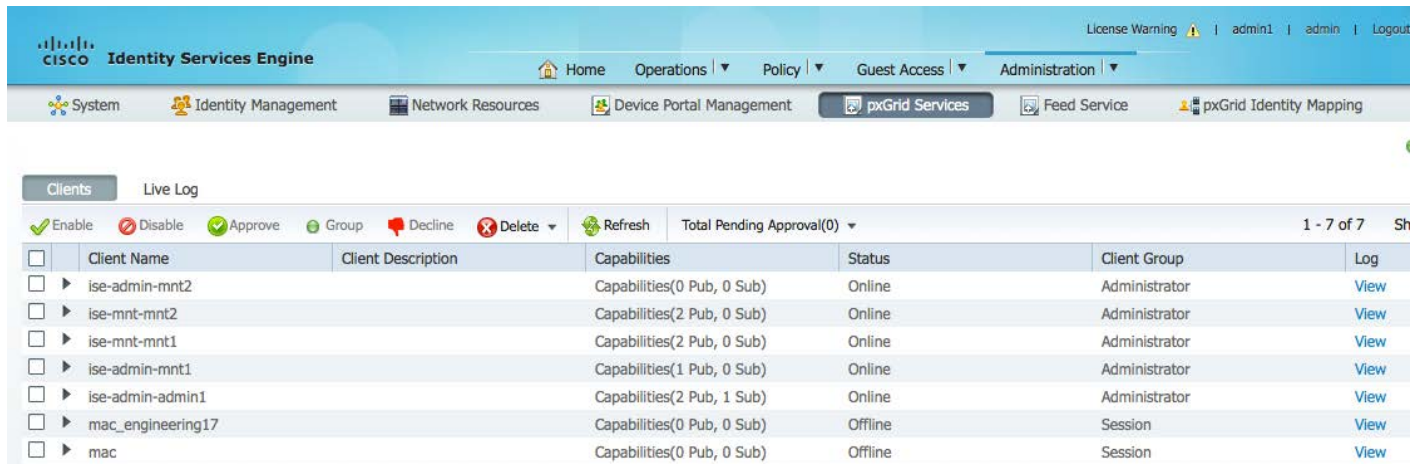
下图说明所有节点都处于活动状态

步骤 1 验证所有节点是否都处于活动状态
Administration -> System -> Deployment, 您应该看到所有节点



Hostname	Node Type	Personas	Role(s)	Services	Node Stat
admin1	ISE	Administration	PRIMARY(A)		✓
admin2	ISE	Administration	SECONDARY(A)		✓
mnt1	ISE	Monitoring	PRIMARY(M)		✓
mnt2	ISE	Monitoring	SECONDARY(M)		✓
psn1	ISE	Policy Service		All	✓
pxgrid1	ISE	pxGrid			✓
pxgrid2	ISE	pxGrid			✓

- 步骤 2** 验证 pxGrid 服务是否已启动，ISE 主要 PAN 节点、ISE 辅助 PAN 节点、ISE 主要 MnT 节点和 ISE 辅助 MnT 节点是不是注册的客户端。
Administration -> pxGrid Services



Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

- 步骤 3** 使用 pxGrid register 脚本和 session_download shell 脚本注册 pxGrid 客户端并下载活动会话记录。记下 pxGrid 节点的主 IP 地址和备用 IP 地址的 IP 地址用作 hostname。

注：在生产环境中，您可能通过 GUI 指定辅助 pxGrid 节点。

```
Johns-Macbook-Pro:bin jeppich$ ./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username
mac_engineering15 -group Session
----- properties -----
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac_engineering15
descriptipon=null
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
-----
registering...
connecting...
connected.
done registering.
connection closed
Johns-Macbook-Pro:bin jeppich$ ./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username
mac_engineering15
----- properties -----
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac_engineering15
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
filter=null
start=null
```

```

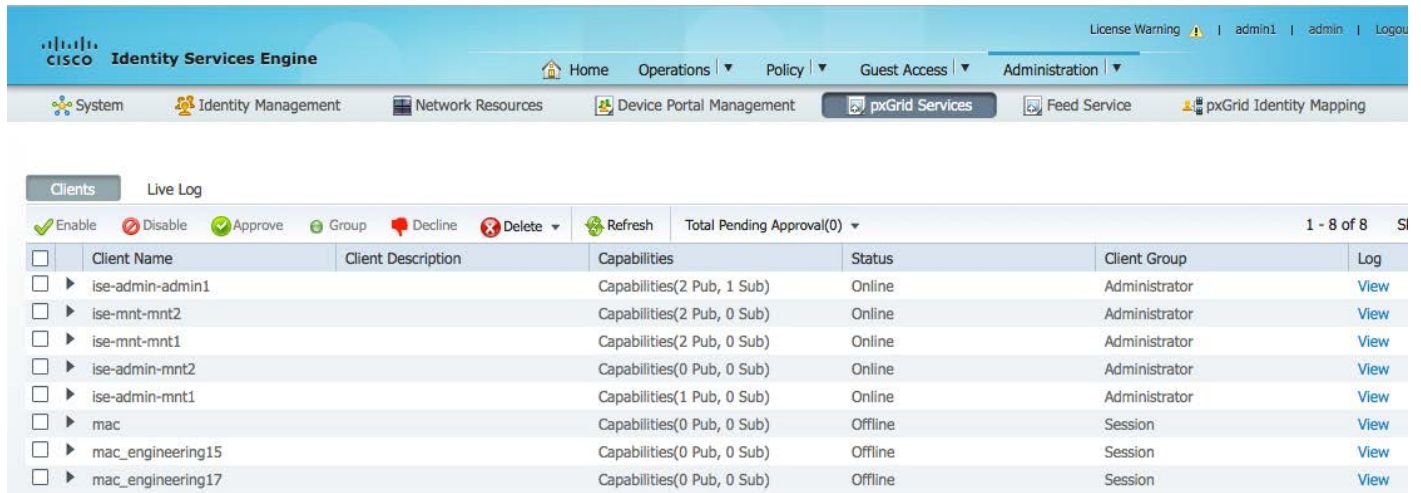
end=null
-----
connecting...
connected.
starting at Thu Mar 05 00:54:43 EST 2015...

session (ip=10.0.0.17, Audit Session Id=0A0000020000000E027B9538, User Name=jeplich, 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:29:77:D6:85, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint
Profile=VMware-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/23, RADIUSAVPairs=[ Acct-Session-
Id=00000006], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 20:06:47 EST
2015 )
session (ip=10.0.0.51, Audit Session Id=0A0000020000000C00035232, User Name=68:EF:BD:F6:76:56, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=68:EF:BD:F6:76:56, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000004], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 21:18:38 EST 2015 )... ending at: Thu
Mar 05 00:54:43 EST 2015

-----
downloaded 2 sessions in 12 milliseconds
-----

```

步骤 4 您应该看到注册的客户端 mac_engineering15 Administration -> pxGrid Services



The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The 'Administration' menu is expanded to show 'pxGrid Services'. Below the navigation, there are tabs for 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'pxGrid Identity Mapping'. The 'pxGrid Services' tab is active, displaying a 'Clients' section with a 'Live Log' button. The table below shows a list of clients with columns for 'Client Name', 'Client Description', 'Capabilities', 'Status', 'Client Group', and 'Log'. The client 'mac_engineering15' is listed as 'Offline'.

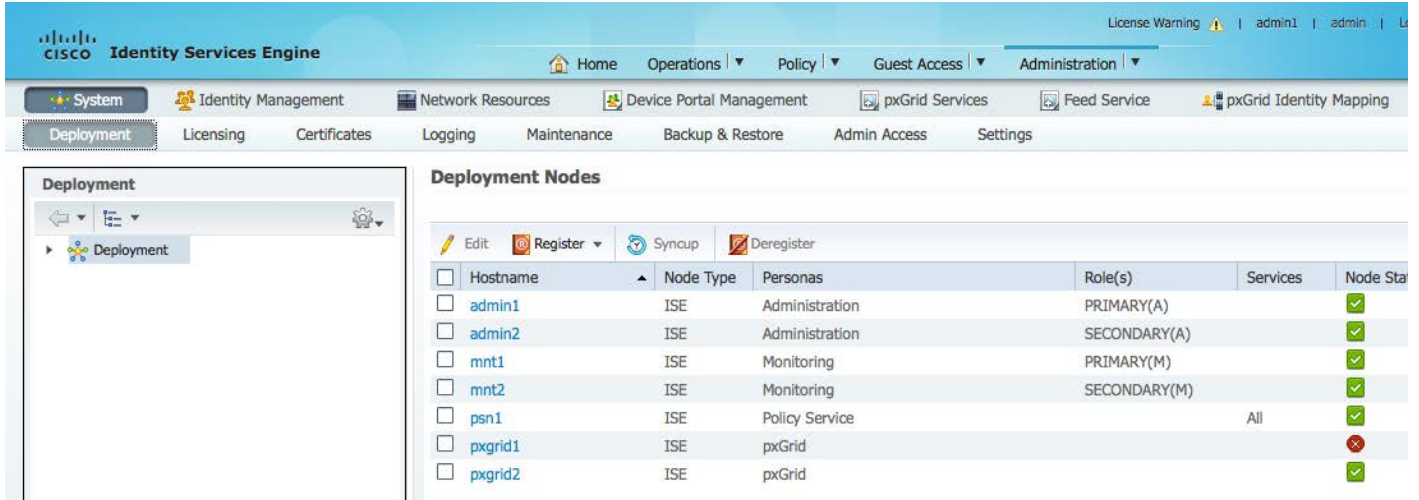
Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

测试故障切换

测试 pxGrid 节点能否故障切换为辅助 pxGrid 节点

- 在主要 pxGrid 节点上发出 “application stop ise” 命令，模拟 pxGrid 节点断开的情况
- 在辅助 pxGrid 节点上发出 “application start ise” 命令，启动辅助 pxGrid 节点
- 从 MnT 主要节点下载活动会话以便对其进行比较，这些会话应该相同
- 将 pxGrid 客户端注册到辅助 pxGrid 节点
- 在 ISE 中查看注册的 pxGrid 客户端
- 查看部署节点状态以显示 pxGrid 节点状态
- 在主要 pxGrid 节点上发出 “application stop ise” 命令，模拟 pxGrid 节点断开的情况
- 在辅助 pxGrid 节点上发出 “application start ise” 命令，启动辅助 pxGrid 节点
- 从 MnT 主要节点下载活动会话以便对其进行比较，这些会话应该相同

步骤 1 验证主要 pxGrid 节点或 pxGrid 1 是否断开。
Administration -> System -> Deployment



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation path is Administration > System > Deployment. The 'Deployment Nodes' table is displayed, showing the status of various nodes. The 'pxgrid1' node is highlighted in red, indicating it is in a failed state, while other nodes like 'admin1', 'admin2', 'mnt1', 'mnt2', 'psn1', and 'pxgrid2' are in a healthy state (green checkmarks).

Hostname	Node Type	Personas	Role(s)	Services	Node Sta
admin1	ISE	Administration	PRIMARY(A)		✓
admin2	ISE	Administration	SECONDARY(A)		✓
mnt1	ISE	Monitoring	PRIMARY(M)		✓
mnt2	ISE	Monitoring	SECONDARY(M)		✓
psn1	ISE	Policy Service		All	✓
pxgrid1	ISE	pxGrid			✗
pxgrid2	ISE	pxGrid			✓

步骤 2 运行注册和会话下载命令，验证是否连接到辅助 pxGrid 节点。

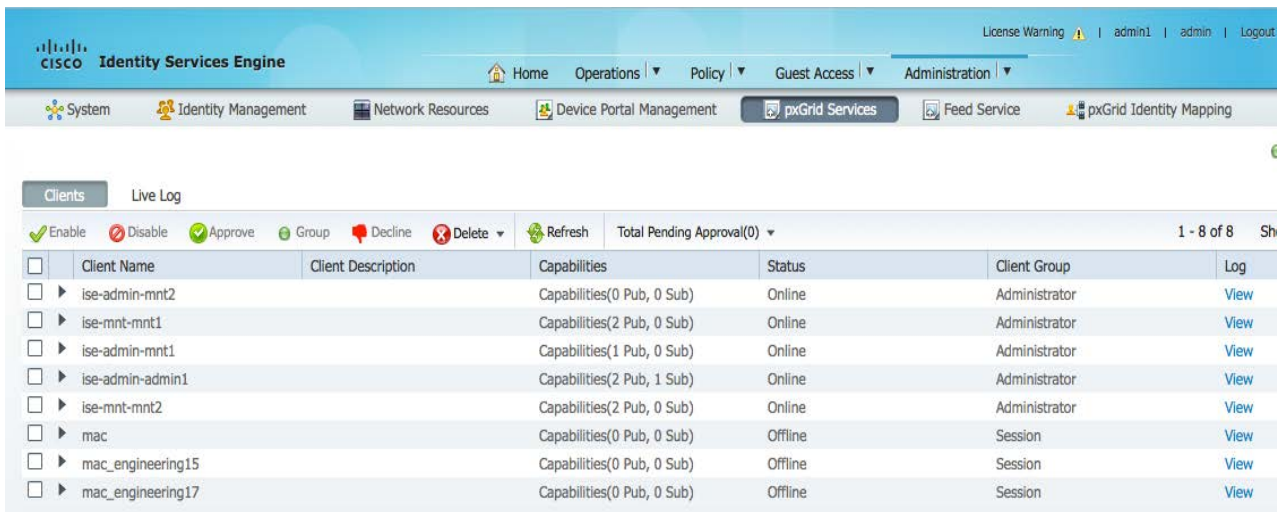
```
Johns-Macbook-Pro:bin jeppich$ ./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.49 -username mac_engineering15
----- properties -----
version=1.0.0
hostnames=10.0.0.49
username=mac_engineering15
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
filter=null
start=null
end=null
-----
connecting...
connected.
starting at Thu Mar 05 01:32:40 EST 2015...

session (ip=10.0.0.17, Audit Session Id=0A0000020000000E027B9538, User Name=jeppich, 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:29:77:D6:85, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint Profile=VMWare-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/23, RADIUSAVPairs=[ Acct-Session-Id=00000006], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 20:06:47 EST 2015 )
session (ip=10.0.0.51, Audit Session Id=0A0000020000000C00035232, User Name=68:EF:BD:F6:76:56, AD User DNS Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station id=68:EF:BD:F6:76:56, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint Profile=Cisco-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000004], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 21:18:38 EST 2015 )... ending at: Thu Mar 05 01:32:40 EST 2015

-----
downloaded 2 sessions in 12 milliseconds
-----

connection closed
Johns-Macbook-Pro:bin jeppich$
```

步骤 3 验证 pxGrid 服务是否已启动，您能否看到 ISE 发布的节点。
Administration -> pxGrid Services

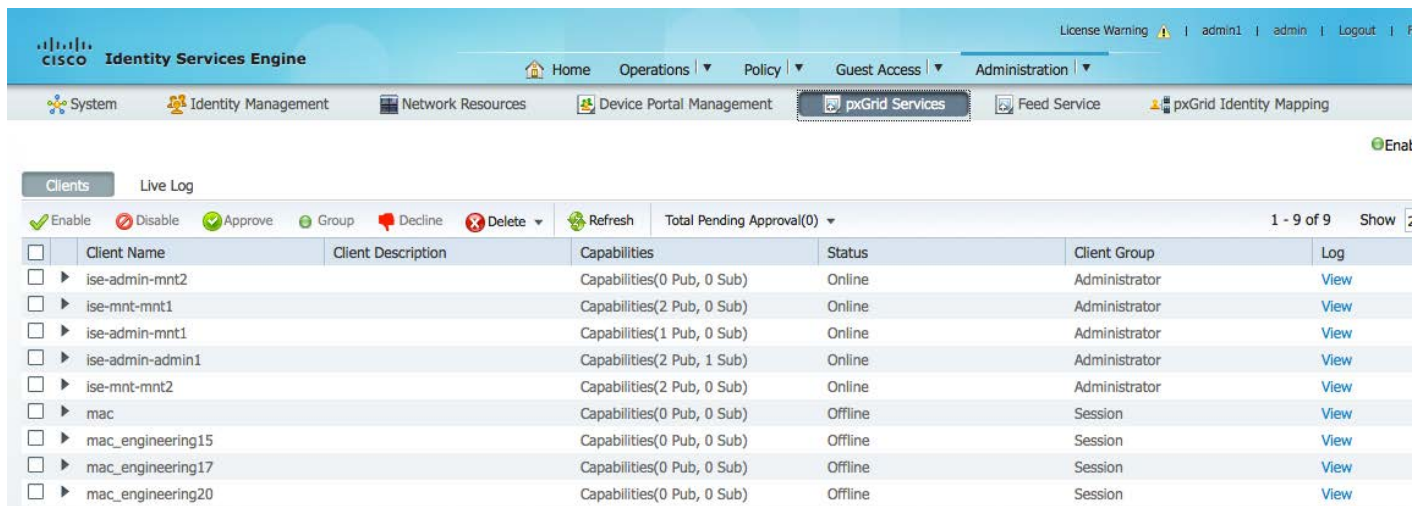


Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

步骤 4 在主要 pxGrid 节点断开的情况下，使用 pxGrid register 脚本和 session_download shell 脚本注册 pxGrid 客户端并下载活动会话记录。

```
Johns-Macbook-Pro:bin jeppich$ ./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.49 -username mac_engineering20 -
group Session
----- properties -----
version=1.0.0
hostnames=10.0.0.49
username=mac_engineering20
descriptipon=null
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
-----
registering...
connecting...
connected.
done registering.
connection closed
Johns-Macbook-Pro:bin jeppich$
```

步骤 5 验证您能否看到注册的 pxGrid 客户端 mac_engineering20
Administration -> pxGrid Services



Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering20		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

恢复主要节点

恢复 pxGrid 主要节点

- 在辅助 pxGrid 节点上发出 “application stop ise” 命令
- 在主要 pxGrid 节点上发出 “application start ise” 命令
- 从 MnT 主要节点下载活动会话以便对其进行比较，这些会话应该相同
- 将 pxGrid 客户端注册到主要 pxGrid 节点
- 在 ISE 中查看注册的 pxGrid 客户端
- 查看部署节点状态以显示 pxGrid 节点状态

步骤 1 验证主要 pxGrid 节点是否已恢复
Administration -> System -> Deployment, 您应该看到所有节点

The screenshot shows the ISE Administration console. The 'Deployment' tab is selected, and the 'Deployment Nodes' table is visible. The table lists various nodes with their roles and statuses.

Hostname	Node Type	Personas	Role(s)	Services	Node Status
admin1	ISE	Administration	PRIMARY(A)		✓
admin2	ISE	Administration	SECONDARY(A)		✓
mnt1	ISE	Monitoring	PRIMARY(M)		✓
mnt2	ISE	Monitoring	SECONDARY(M)		✓
psn1	ISE	Policy Service		All	✓
pxgrid1	ISE	pxGrid			✓
pxgrid2	ISE	pxGrid			✗

步骤 2 验证 pxGrid 服务是否正在运行，您能否看到 ISE 发布的节点
Administration -> pxGrid Services

The screenshot shows the ISE Administration console with the 'pxGrid Services' tab selected. The 'Clients' table is displayed, showing a list of registered clients and their status.

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering20		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

步骤 3 验证是否仍有连接正在运行 session_download 命令下载活动会话

```
Dddd
Johns-Macbook-Pro:bin jeppich$ ./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username
mac_engineering15
----- properties -----
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac_engineering15
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
filter=null
start=null
end=null
-----
connecting...
connected.
starting at Thu Mar 05 01:57:14 EST 2015...

session (ip=10.0.0.17, Audit Session Id=0A0000020000000E027B9538, User Name=jeppich, 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:29:77:D6:85, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint
Profile=VMWare-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/23, RADIUSAVPairs=[ Acct-Session-
Id=00000006], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 20:06:47 EST
2015 )
session (ip=10.0.0.51, Audit Session Id=0A0000020000000C00035232, User Name=68:EF:BD:F6:76:56, AD User DNS
Domain=null, AD Host DNS Domain=null, AD User NetBIOS Name=null, AD Host NETBIOS Name=null, Calling station
id=68:EF:BD:F6:76:56, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint Profile=Cisco-
Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000004], Posture
Status=null, Posture Timestamp=, Session Last Update Time=Wed Mar 04 21:18:38 EST 2015 )... ending at: Thu
Mar 05 01:57:14 EST 2015

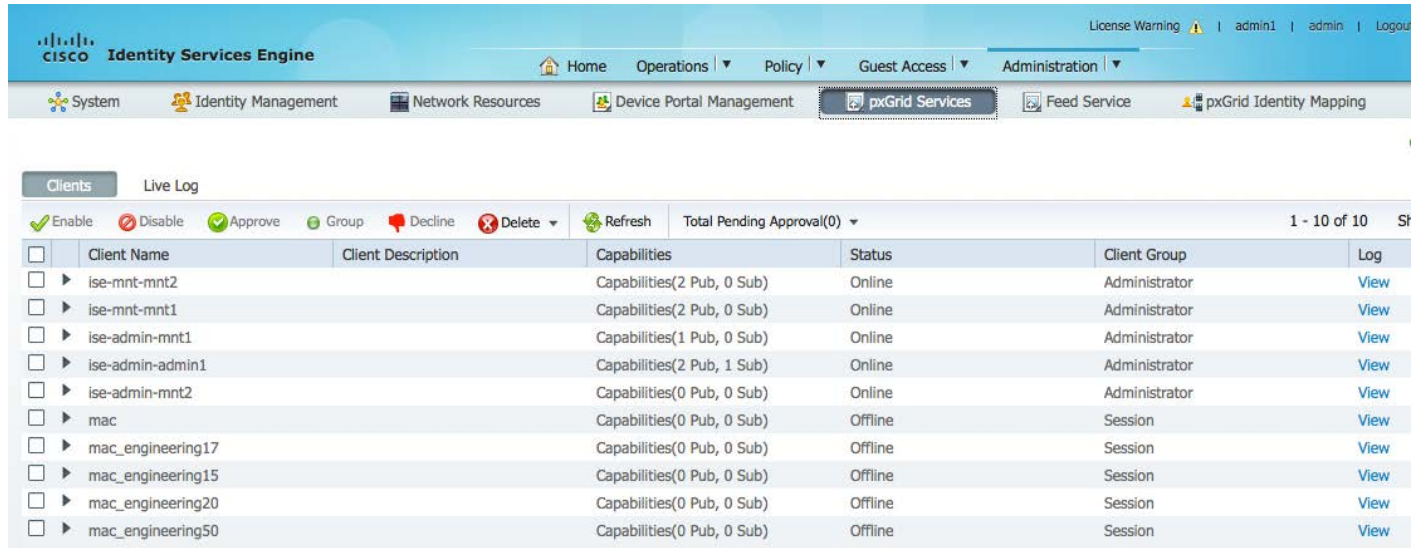
-----
downloaded 2 sessions in 12 milliseconds
-----

connection closed
```

步骤 4 通过注册 pxGrid 客户端来验证是否一切正常。

```
Johns-Macbook-Pro:bin jeppich$ ./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username
mac_engineering50 -group Session
----- properties -----
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac_engineering50
descriptipon=null
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
-----
registering...
connecting...
connected.
done registering.
connection closed
```


步骤 5 在 ISE pxGrid 控制器上查看 pxGrid 客户端 mac_engineering50
Administration -> pxGrid Services



The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes "Home", "Operations", "Policy", "Guest Access", and "Administration". The "Administration" menu is expanded, showing "pxGrid Services" as the selected option. Below the navigation bar, there are tabs for "Clients" and "Live Log". The "Clients" tab is active, displaying a table of clients. The table has columns for "Client Name", "Client Description", "Capabilities", "Status", "Client Group", and "Log". The client "mac_engineering50" is highlighted in yellow. The table also includes action icons for "Enable", "Disable", "Approve", "Group", "Decline", "Delete", and "Refresh". The "Total Pending Approval(0)" is shown as 0. The page number "1 - 10 of 10" is visible in the bottom right corner.

Client Name	Client Description	Capabilities	Status	Client Group	Log
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering20		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering50		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

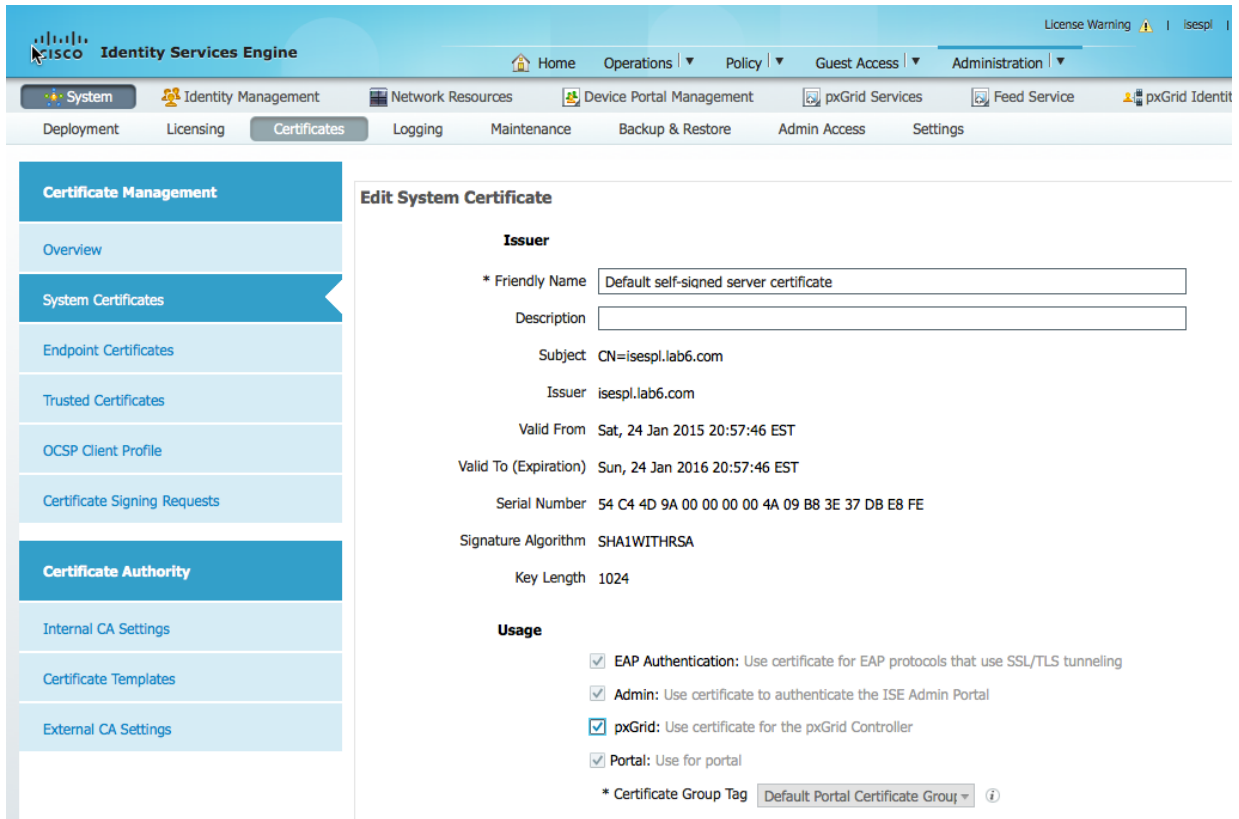
ISE 自签名身份证书

如果外部 CA 机构不可用，或者要在不使用 pxGrid SDK 中的样本证书的情况下测试 pxGrid 和 ISE 实施，则可使用 pxGrid 的 ISE 自签名身份证书。默认情况下，自签名身份证书包含增强型密钥用法 (EKU)，可同时用于服务器身份验证 (1.3.6.1 .5.5.7.3.1) 和客户端身份验证 (1.3.6.1 .5.5.7.3.2)，其位于 ISE 系统证书库中。

pxGrid 客户端可以使用自签名证书，请参阅：“将自签名证书与 pxGrid ISE 节点和 pxGrid 客户端配合使用”

pxGrid 客户端也可以使用 CA 签名的证书，请参阅：“将自签名证书与 pxGrid ISE 节点和 CA 签名的 pxGrid 客户端配合使用”。

- 步骤 1** 在 ISE 自签名身份证书中启用 pxGrid 用法
Administration -> System -> Certificates -> System Certificates -> Edit ISE 自签名证书并选择 pxGrid，然后点击 Save

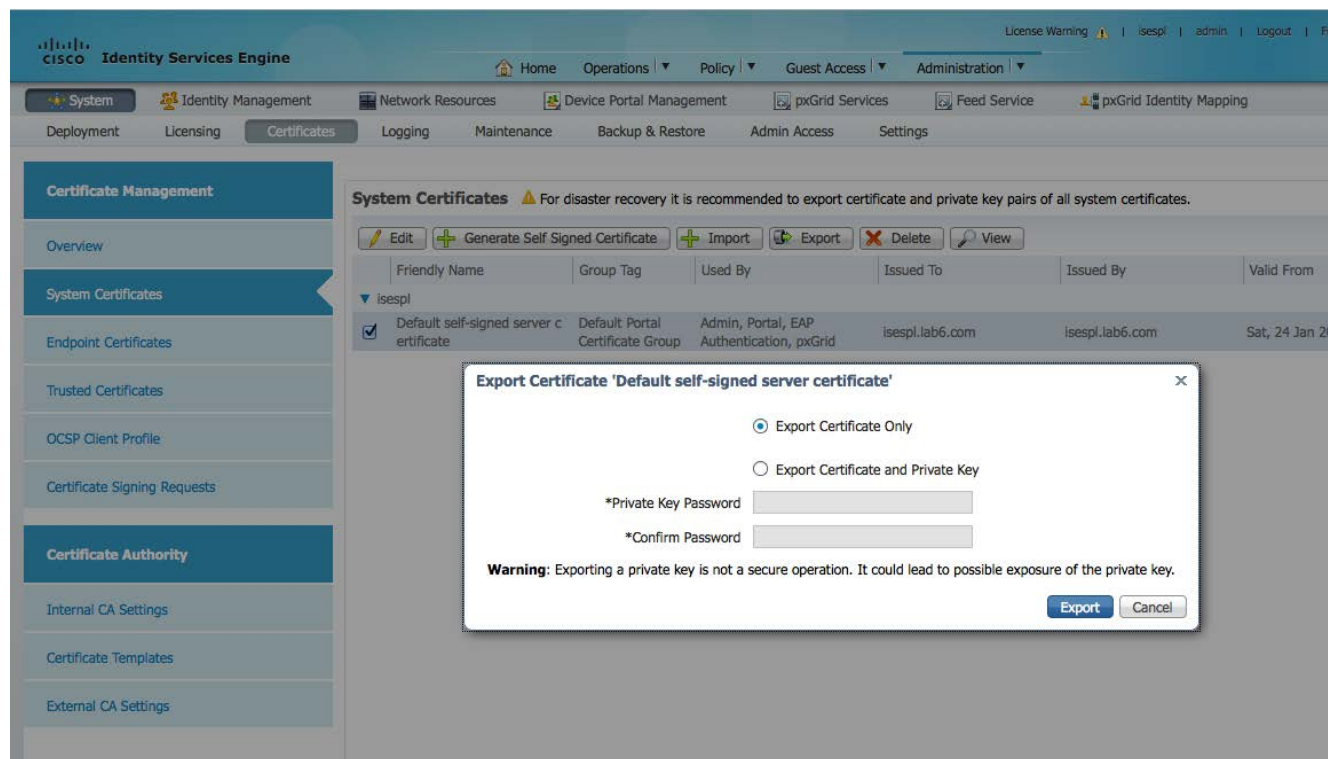


The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The main navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The left sidebar shows 'Certificate Management' with sub-items like 'Overview', 'System Certificates', 'Endpoint Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests', 'Certificate Authority', 'Internal CA Settings', 'Certificate Templates', and 'External CA Settings'. The main content area is titled 'Edit System Certificate' and contains the following information:

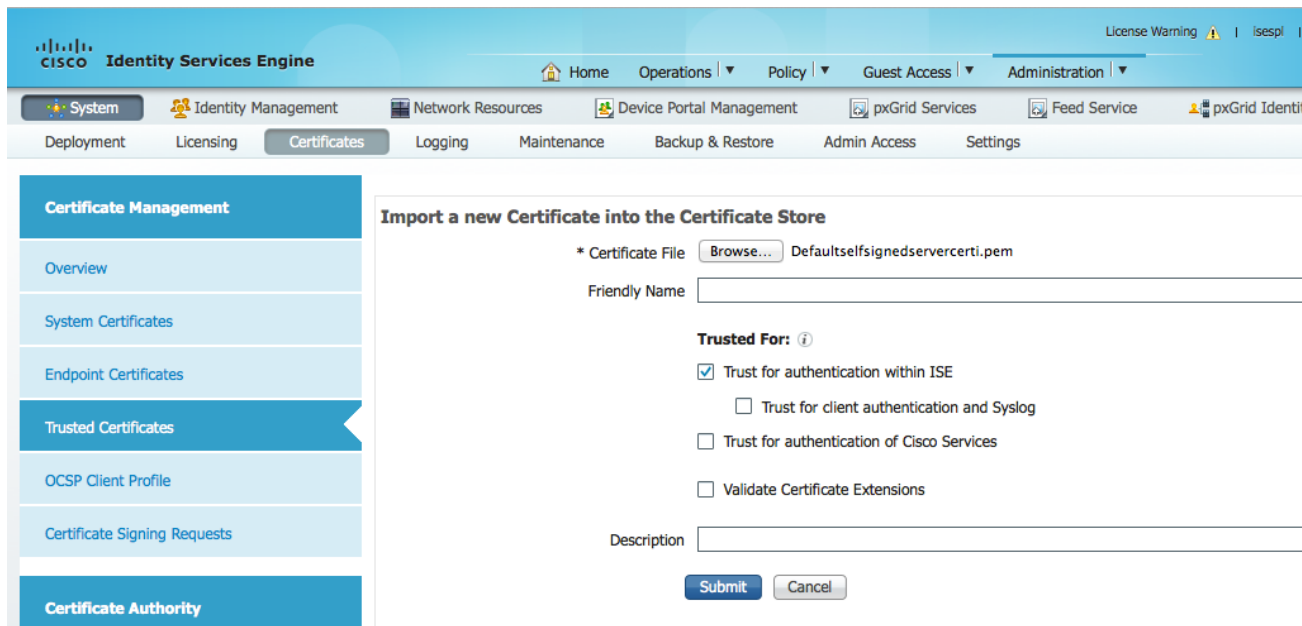
- Issuer**
- * Friendly Name: Default self-signed server certificate
- Description: [Empty field]
- Subject: CN=isespl.lab6.com
- Issuer: isespl.lab6.com
- Valid From: Sat, 24 Jan 2015 20:57:46 EST
- Valid To (Expiration): Sun, 24 Jan 2016 20:57:46 EST
- Serial Number: 54 C4 4D 9A 00 00 00 00 4A 09 B8 3E 37 DB E8 FE
- Signature Algorithm: SHA1WITHRSA
- Key Length: 1024
- Usage**
- EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- Admin: Use certificate to authenticate the ISE Admin Portal
- pxGrid: Use certificate for the pxGrid Controller
- Portal: Use for portal
- * Certificate Group Tag: Default Portal Certificate Group

步骤 2 导出 Trusted Certificates 下的公共 ISE 自签名身份证书。

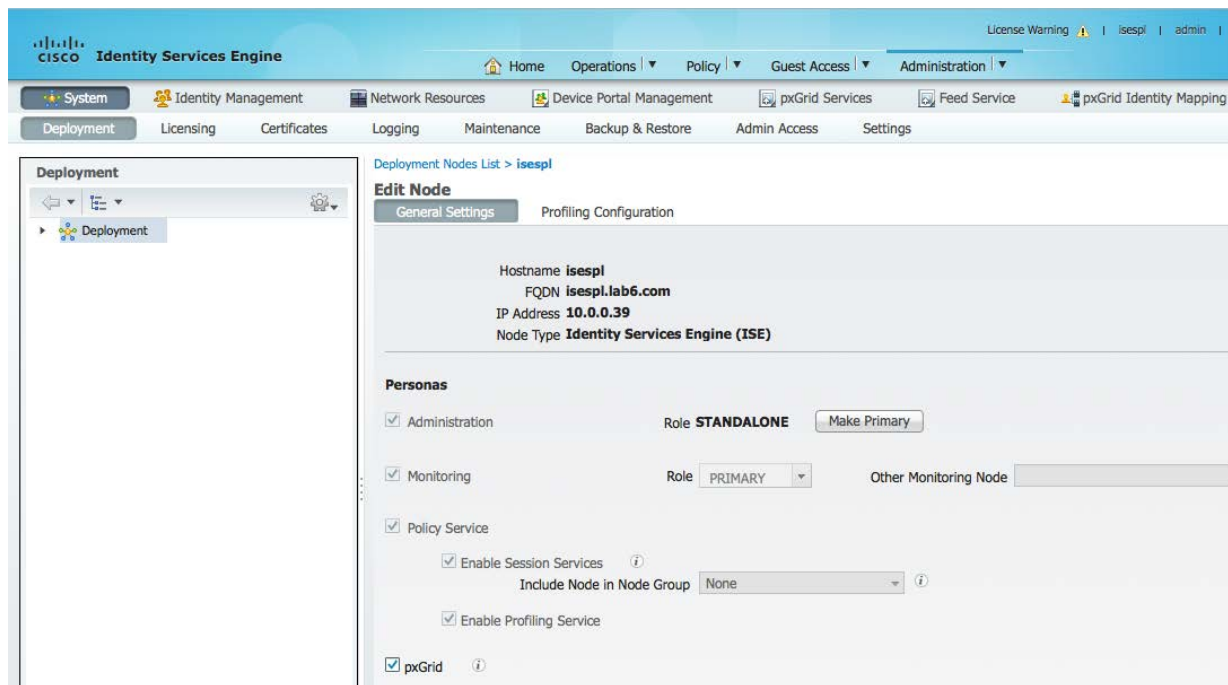
Administration -> System -> Certificates -> Edit 自签名证书，然后选择“Export Certificate Only”

注：此证书将另存为 PEM 文件

- 步骤 3** 将 PEM 文件导入到受信任的证书库中
Administration -> System -> Certificates -> Trusted Certificates -> 选择 PEM certificate 并启用 “Trust for authentication within ISE”，然后提交



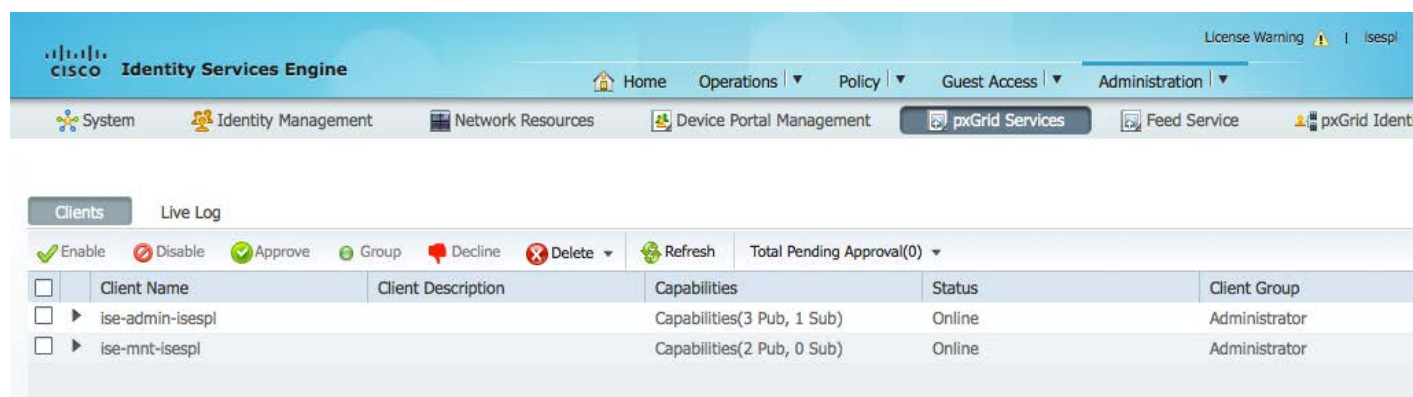
- 步骤 4** 启用 pxGrid 角色
Administration -> System -> Deployment -> Edit 部署节点并启用 pxGrid，然后点击 Save



步骤 5 启动 pxGrid 服务

Administration -> pxGrid Services

注：如果没有看到与 pxGrid 节点的连接，可能需要一些时间才能显示出来。



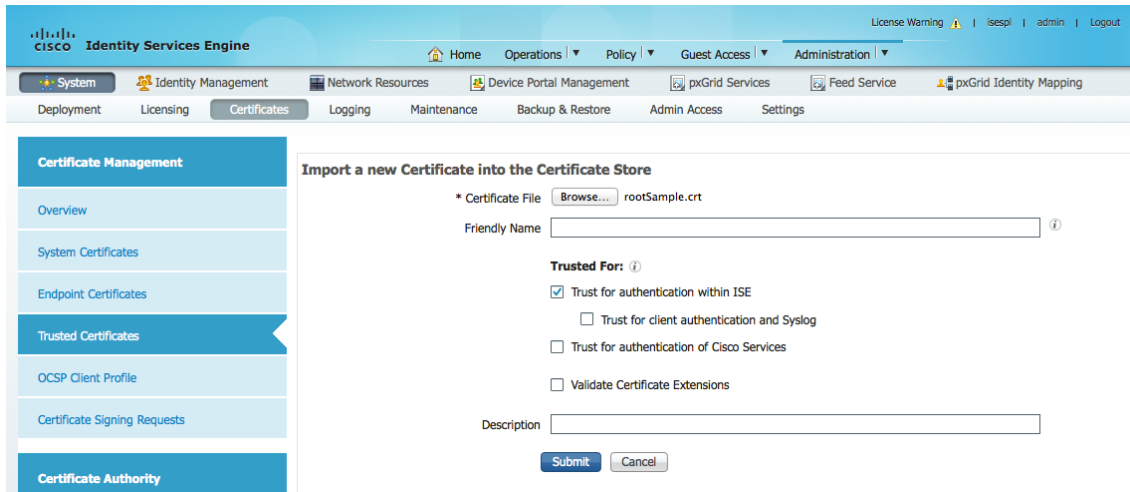
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes "Home", "Operations", "Policy", "Guest Access", and "Administration". The "Administration" menu is expanded to show "pxGrid Services". Below the navigation bar, there are several tabs: "System", "Identity Management", "Network Resources", "Device Portal Management", "pxGrid Services", "Feed Service", and "pxGrid Ident". The "pxGrid Services" tab is active, displaying a "Clients" section with a "Live Log" button. The "Clients" section includes a toolbar with "Enable", "Disable", "Approve", "Group", "Decline", "Delete", and "Refresh" buttons, along with a "Total Pending Approval(0)" dropdown. A table lists the following clients:

<input type="checkbox"/>	Client Name	Client Description	Capabilities	Status	Client Group
<input type="checkbox"/>	ise-admin-isespl		Capabilities(3 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	ise-mnt-isespl		Capabilities(2 Pub, 0 Sub)	Online	Administrator

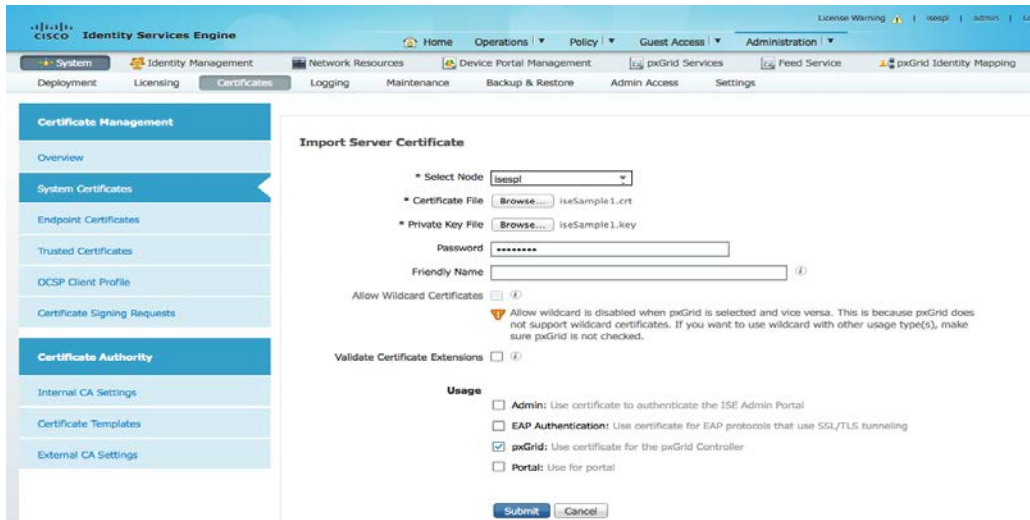
SDK 中的样本证书

本示例中使用的是 pxGrid SDK 中的样本证书，它只能用于 POC，不能在生产环境中使用。此处我们导入 rootSample.crt 作为信任的 CA 证书，并导入 iseSample1.crt 和 iseSample1.key，充当 pxGrid 客户端用于客户端注册的公钥/私钥对。有关 POC 部署、样本证书和 pxGrid 示例 shell 脚本的更多详细信息，请参阅：
http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

步骤 1 将 rootSample.crt 导入到 ISE 的受信任系统证书中
 Administration -> System -> Certificates -> Trusted Certificate -> 导入 rootSample.crt，然后点击 Submit

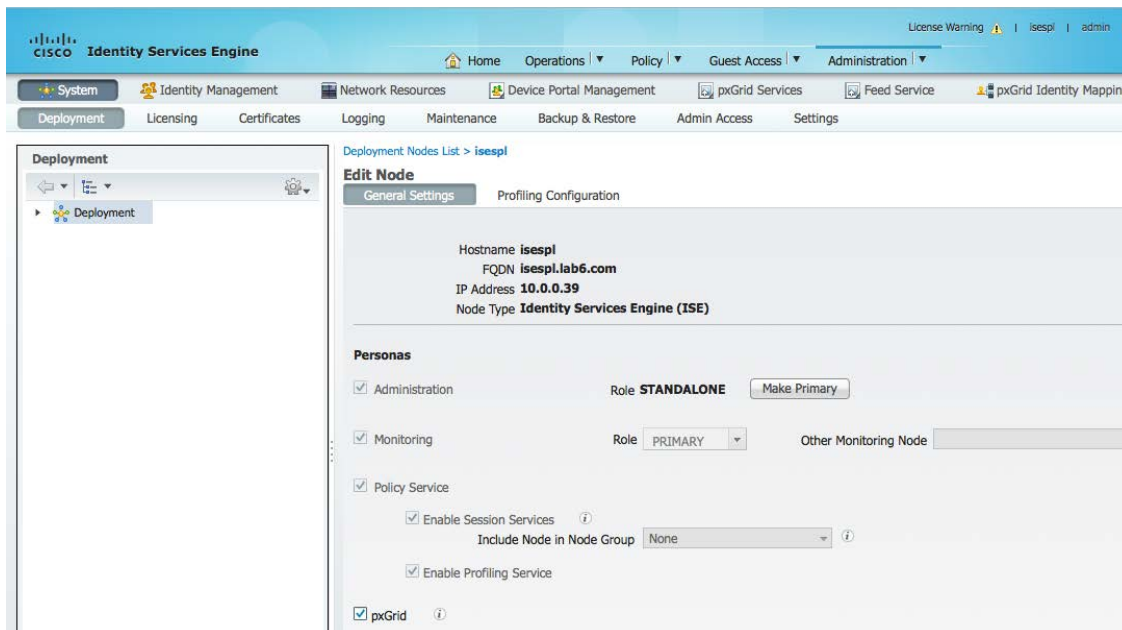


步骤 2 将 iseSample1.crt 和 iseSample1.key 导入到 ISE 的系统证书库中
 Administration -> System -> Certificates -> System Certificates -> Import，使用 **cisco123** 作为密码，然后提交。



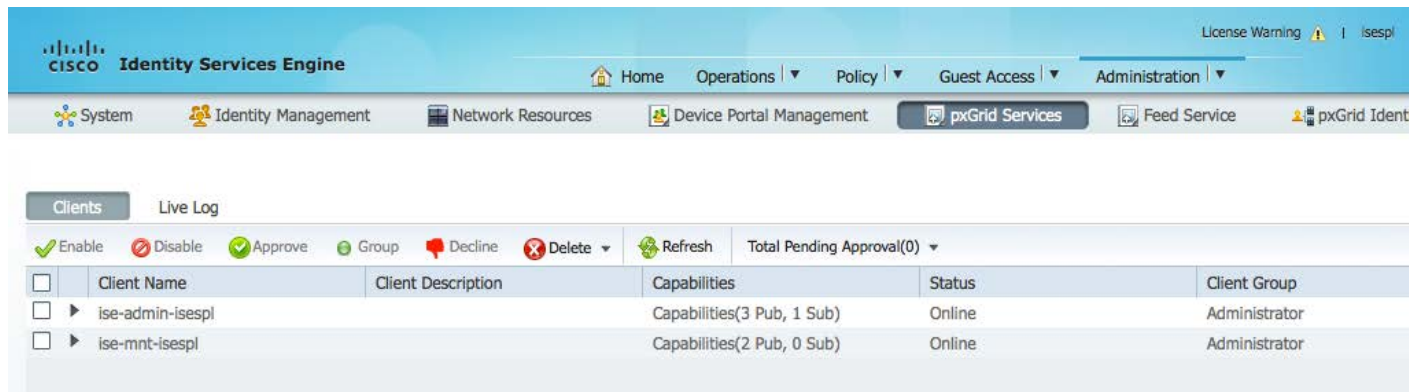
步骤 3 启用 pxGrid 角色

Administration -> System -> Deployment -> Edit 部署节点并启用 pxGrid，然后点击 Save

**步骤 4** 启动 pxGrid 服务

Administration -> pxGrid Services

注：如果没有看到与 pxGrid 节点的连接，可能需要一些时间才能显示出来。



测试 pxGrid 客户端

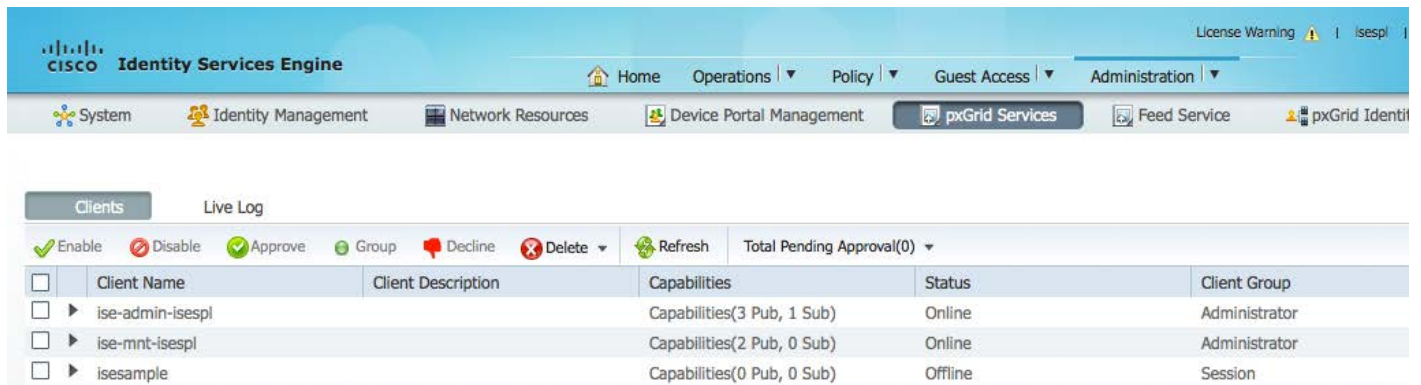
确保从 MnT 节点导出 ISE 自签名身份证书，如果是独立部署，则导出到用于批量会话下载的 pxGrid 客户端（请参阅“批量会话下载”）。

此处我们要检查客户端注册和会话下载

步骤 1 使用 register.sh 脚本并运行以下命令：

```
./register.sh -keystoreFilename iseSample1.jks -keystorePassword cisco123 -truststoreFilename rootSample.jks
--truststorePassword cisco123 -group Session -username iseSample -hostname 10.0.0.39 -group Session
----- properties -----
version=1.0.0
hostnames=10.0.0.39
username=iseSample
descriptipon=null
keystoreFilename=iseSample1.jks
keystorePassword=cisco123
truststoreFilename=rootSample.jks
truststorePassword=cisco123
-----
registering...
connecting...
connected.
done registering.
connection closed
```

验证 pxGrid 客户端 iseSample 是否在 pxGrid Services 下显示为已注册的客户端



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The 'pxGrid Services' tab is selected. Below the navigation bar, there are several tabs: 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'pxGrid Identif'. The 'Clients' tab is active, showing a table of registered clients. The table has columns for 'Client Name', 'Client Description', 'Capabilities', 'Status', and 'Client Group'. The 'ise-sample' client is listed with a status of 'Offline'.

Client Name	Client Description	Capabilities	Status	Client Group
ise-admin-isespl		Capabilities(3 Pub, 1 Sub)	Online	Administrator
ise-mnt-isespl		Capabilities(2 Pub, 0 Sub)	Online	Administrator
isesample		Capabilities(0 Pub, 0 Sub)	Offline	Session

参考资料

操作指南-配置并测试 pxGrid

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

将自签名证书与 pxGrid ISE 节点和 pxGrid 客户端配合使用

将自签名证书与 pxGrid ISE 节点和 CA 签名的 pxGrid 客户端配合使用

将 CA 签名的证书与 pxGrid ISE 节点和 pxGrid 客户端配合使用

附录

故障排除

本节提供有关故障排除的信息。

如果看到以下错误消息，请确保 pxGrid 客户端、pxGrid 节点和 ISE 可通过 DNS 进行解析：

```
jeppich$ ./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -truststoreFilename
caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username mac
----- properties -----
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
filter=null
start=null
end=null
-----
connecting...
connected.
19:27:48.224 [main] WARN o.a.cxf.phase.PhaseInterceptorChain - Interceptor for
{https://mnt1.lab6.com/pxgrid/mnt/sd}WebClient has thrown exception, unwinding now
org.apache.cxf.interceptor.Fault: Could not send Message.
    at
org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSende
rInterceptor.java:64) ~[cxf-api-2.7.3.jar:2.7.3]
    at org.apache.cxf.phase.PhaseInterceptorChain.doIntercept(PhaseInterceptorChain.java:271) ~[cxf-api-
2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.AbstractClient.doRunInterceptorChain(AbstractClient.java:581) [cxf-rt-
frontend-jaxrs-2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:904) [cxf-rt-frontend-
jaxrs-2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:772) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:759) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.WebClient.invoke(WebClient.java:355) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
    at org.apache.cxf.jaxrs.client.WebClient.post(WebClient.java:381) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
    at com.cisco.pxgrid.stub.identity.impl.SessionIteratorImpl.open(SessionIteratorImpl.java:128)
[pxgrid-identity-client-stub-1.0.0.jar:1.0.0]
    at com.cisco.pxgrid.samples.ise.SessionDownload.main(SessionDownload.java:132) [pxgrid-sdk-
1.0.0.jar:1.0.0]
```

在 Centos 6.5 中删除 Java 和安装 JDK 8.0

删除 Java 早期版本

步骤 1 确保 Centos 6.5 是最新的，输入：yum update

注：您可能需要 root 权限，输入：su root yum update

步骤 2 更新完成后，输入以下命令删除任何已安装的其他 JAVA 包：

```
rpm -qa | grep -E '^open[jre|jdk][j][re|dk]'
```

注：由于已经安装了 java-1.6.0-openjdk-1.6.0.0-1.56.1.11.8.el6_3.i686 包，所以我要运行命令将其删除

步骤 3 输入：yum remove java-1.6.0-openjdk

安装 JDK 8.0

步骤 1 切换为 root 用户，输入 su，系统将提示您输入密码。

步骤 2 安装 JDK 8，输入：rpm -Uvh jdk-8u20-linuxx64.rpm

步骤 3 您还需要运行 alternatives 命令：

```
alternatives --install /usr/bin/java java /usr/java/latest/jre/bin/java 200000
alternatives --install /usr/bin/javaws javaws /usr/java/latest/jre/bin/javaws 200000
alternatives --install /usr/lib64/mozilla/plugins/libjavaplugin.so libjavaplugin.so.x86_64
/usr/java/latest/jre/lib/amd64/libnpjp2.so 200000
alternatives --install /usr/bin/javac javac /usr/java/latest/bin/javac 200000
alternatives --install /usr/bin/jar jar /usr/java/latest/bin/jar 200000
java -version
```

检查 Java 版本，输入 java -version，您应该看到：java version "1.8.0_20"