



在 ISE 分布式环境中配置 pxGrid





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	
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	
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	
pxGrid 客户端主用-备用配置示例	
在 ISE 分布式环境中测试 xGrid 客户端	
查看密钥库条目	
采用 pxGrid 主用-备用配置的 ISE 分布式部署简介	
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

cisco.

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-macros-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。

<u>注</u>: 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。

<u>注</u>: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。

ISE Distributed Environment



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

Certificate Templates (WIN-BG7GPC)	Template Display Name 🔺	Minimum Supported CAs	Ver 🔺
	Domain Controller Authentication	Windows Server 2003 Ent	110
	EFS Recovery Agent	Windows 2000	6.1
	R Enrollment Agent	Windows 2000	4.1
	Reproliment Agent (Computer)	Windows 2000	5.1
	Duplicate Template	×	4.1
			6.1
	You can create certificate templates wit	h advanced properties. However,	7.1
	not all Windows CAs support all certifica	te template properties.Select the	8.1
	certificate template.	pported CAS) for the duplicate	7.1
			110
	Windows Server 2003 Enterprise		105
			101
	Windows Server 2008 Enterprise		100
			101
	Learn more about Certificate Template	Versions.	5.1
			4.1
		OK Cancel	6.1
			11.
	Representation Authority	Windows 2000	5.1
	Irust List Signing	Windows 2000	3.1
	I User	Windows 2000	3.1
	🖳 User Signature Only	Windows 2000	4.1
	R Web Server	Windows 2000	4.1
	Workstation Authentication	Windows Server 2003 Ent	101
•			٠ ا

<u>注</u>: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。

🖳 Certificate Templates Console 🚬			- 0 ×
File Action View Help	Properties of New Template		
Certificate Templates (WIN-BG7GPC	Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Server V/r Template display name: Template Server V/r	er Actions	
	pxGrid 6.	.1	ipla 🔺
	4.	.1 More Actions	•
	Minimum Supported CAs: Windows Server 2003 Enterprise 5.	User	
	Template name: 6.	.1 More Actions	• •
	pxGrid 7.	.1	
	8.	.1	
	Validity period: Renewal period: 1	10	
	5 years 52 weeks 10	05	
	10	01	
	Publish certificate in Active Directory	01	
	Do not automatically reenroll if a duplicate certificate exists in Active 5.	.1	
	Directory 4.	.1	
	- For automatic renewal of smart card certificates, use the existing key	1.	
	f a new key cannot be created 5.	.1	
	3.	.1	
	4.	.1	
	4.	.1	
	10	01	
· · ·	OK Cancel Apply Help		

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

File Action View Help	Properties of New Template	×		
🗇 🏟 📅 📓 😖 🔽 🗊	General Request Handling Subject Name	Server		
Certificate Templates (WIN-BG7GPC	Isabalice Hequitements Superseded Templates	Ve	Actions	
	To modify an extension, select it, and then click Edit.	11	Certificate Templa	🔺
	Extensions included in this template:	4.	More Actions	•
	Application Policies	5.	User	
	Basic Constraints Certificate Template Information Issuance Policies		More Actions	•
	Client Authentication Encrypting File System Secure Email Server Authentication	 ▲ ↓ ↓		
4 N	OK Cancel Apply	Help	2	

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。

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

ahah	License Warning 🔥 admin	Logout F
cisco Identity Services Engine	Home Operations Policy Guest Access Administration	
System 🐉 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 11 pxGrid Identity	y Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Certificate Management	Import a new Certificate into the Certificate Store	
Overview	* Certificate File Browse root.cer	
	Friendly Name	Ð
System Certificates	Trusted For: (i)	
Endpoint Certificates	✓ Trust for authentication within ISE	
	Trust for client authentication and Syslog	
Trusted Certificates	Trust for authentication of Cisco Services	
OCSP Client Profile	Validate Certificate Extensions	
Certificate Signing Requests	Description	
Certificate Authority	Submit Cancel	

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

isco Ident	ity Services E	ngine		🙆 Home	Operations 💌	Policy	 Guest Acces 	ss 💌	Administration	
🔶 System	Identity Ma	anagement	Network Resour	ces 🛃 🛙	Device Portal Manag	gement	属 pxGrid Ser	rvices	E Feed Service	💵 📲 pxGr
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Rest	tore	Admin Access	Setti	ngs	
Certificate Ma	nagement									
Overview			Generate	CSR's for these	Nodes:					
Suctem Certifica	toc		Node				CSR Friendly M	Name		
System Certifica	luca		✓ adm	in2			admin2 #Admin			
Endpoint Certific	cates		Subject							
Trusted Certifica	ites		,	ommon Name ((CN) admin2 lab6				1 0	
OCSP Client Pro	file		Orga	nizational Unit (OU)	.com				
Certificate Signii	ng Requests			Organization	(0)					
				City	/ (L)			-		
Certificate Aut	thority			State	(ST)					
Internal CA Sett	ings			Country	/ (C)					
Certificate Temp	olates		C. N				1			
External CA Sett	tinas		Subject Alter	native Name (S	DNS Nam	e	▼ admin2.	lab6.com	1	- #
	lan <mark>T</mark> ala			* Key Ler	ngth 2048	*				
			*	Digest to Sign \	With SHA-256	*				

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-BG7GPQ	53ID-CA
Submit a Certif	ficate Request or Renewal Request	
To submit a sav Request box.	red request to the CA, paste a base-64-enco	ded CMC or PKCS #10 certificate request or PI
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	Iv9Z9LİSOnlaKmRİyt5g7O7fGw+zŴRFİHSg+XYIk9İK ycDLj4KDhrcTL819CFy+UIA4lb2HmcuvMFGAFkXT+rr CCB4RmUjLmiCP+SckXMIYQU9aloxKZSeFDXhbMuSt9 /GrNCWzbWx85jQTwinH=RwoSrUydVwbDhjMlzFn5D2 60yMH0pELvPJYkR1xBbS5tRiXAQM END CERTIFICATE REQUEST	
Certificate Templa	ite:	
	Web Server \$	
Additional Attribu	tes:	
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

cisco Iden	ntity Services Engine			🟠 Home	Operations 🔻	Policy V Guest Ac	cess 🔻	Administration		· /		Setup A
🔹 System	4 Identity Management	Netwo	rk Resources	🛃 D	Device Portal Manage	ement 🗔 pxGrid S	Services	Feed Service	▲ pxGrid Ider	itity Mapping		
Deployment	Licensing Certificates	Loggin	ng Mair	ntenance	Backup & Resto	Admin Access	Settin	gs				
Certificate M	lanagement	Certifica	te Signing	Request	s							
			519 03									
Overview		Generate	Certificate Si	igning Reque	ests (CSR)							
Overview System Certific	cates	Generate A Certifica a request	Certificate Si te Signing Re has been sign	igning Reque equests (CSR ned, click "bin	ests (CSR) ts) must be sent to a ind" to bind the requ	and signed by an externa lest to the signed certific	l authority. C ate issued b	Click "export" to downlo y that authority. Once a	ad one or more CS CSR is bound, it w	Rs so that they may be ill be removed from this	signed by an externa s list.	al author
Overview System Certific Endpoint Certif	cates	Generate A Certifical a request	Certificate Signing Re has been sign	igning Reque equests (CSR ned, click "bin Celete	ests (CSR) ks) must be sent to a ind" to bind the requ Bind Certificate	and signed by an externa lest to the signed certific	l authority. C ate issued b	Click "export" to downlo y that authority. Once a	ad one or more CS a CSR is bound, it w	Rs so that they may be ill be removed from this Show	signed by an externa s list. All	al authori
Overview System Certific Endpoint Certif	cates	Generate A Certifical a request	e Certificate S te Signing Re has been sign Export dly Name	igning Reque equests (CSR ned, click "bin Delete	ests (CSR) ts) must be sent to a ind" to bind the required Bind Certificate	and signed by an externa uest to the signed certific Certificate Subject	l authority. C ate issued by	Click "export" to downlo y that authority. Once a Key Length	a CSR is bound, it w Group Tag	Rs so that they may be iill be removed from this Show A Timestamp	signed by an externa s list. All	al authorif
Overview System Certific Endpoint Certific Trusted Certific	ficates ficates	A Certifica a request l View Friend admin	e Certificate Si te Signing Re has been sign Export dly Name n2#Admin	igning Reque equests (CSR ned, click "bi Delete	ests (CSR) is) must be sent to a ind" to bind the requ Bind Certificate	Certificate Subject	l authority. C ate issued b : :	Click "export" to downly y that authority. Once a Key Length 2048	ad one or more CS a CSR is bound, it w Group Tag	Rs so that they may be ill be removed from this Show Timestamp Fri, 30 Jan 2015	e signed by an externa s list. All	al authori ost dmin2
Overview System Certific Endpoint Certific Trusted Certific OCSP Client Pri	ncates ficates	Generate A Certifical a request I View Frienc Z admir	Certificate Si te Signing Re has been sign Export dly Name n2#Admin	igning Reque equests (CSR ned, click "bin Delete	ests (CSR) (s) must be sent to a ind" to bind the requ Bind Certificate	and signed by an externa exect to the signed certific Certificate Subject CN=admin2.lab6.c	l authority. C ate issued b : :	Click "export" to downky y that authority. Once a Key Length 2048	ad one or more CS a CSR is bound, it w Group Tag	Rs so that they may be ill be removed from this Show 7 Timestamp Fri, 30 Jan 2015	a signed by an external s list. All	al authori ost dmin2

步骤7 分别为每个 ISE 节点导入节点证书, 然后提交

Deployment	Licensing Certificates		
		Logging Maintenance Backup & Restore Admin Access Settings	
Certificate Mana	agement	Blad Of Streed Carbinate	
Overview		Bind CA Signed Certificate	
		* Certificate File Browse admin2.cer	
system Certificate	5	Friendly Name	
Endpoint Certificat	tes	Allow Wildcard Certificates 🔲 🕧	
Frusted Certificate	25	Validate Certificate Extensions 🔲 ④	
OCSP Client Profile	e	Usage Admin: Use certificate to authenticate the ISE Admin Portal	
CSP Client Profile	e Requests	Admin: Use certificate to authenticate the ISE Admin Portal	

步骤 8 为 pxGrid 节点生成 CSR。

Administration -> System -> Certificates -> Certificate Signing Requests - "pxGrid"证书用法

isco Identi	ity services Engine	🟠 Home	Operations Policy	▼ Guest Access ▼	Administration V	
🛃 System	👰 Identity Management	Network Resources	vice Portal Management	pxGrid Services	Feed Service	⊥ ∎ pxGrid
Deployment	Licensing Certificat	es Logging Maintenance	Backup & Restore	Admin Access Set	tings	
Certificate Mar	nagement	Usage				
Overview		Certificate(s) will be used for	or pxGrid	Ţ		
System Certifical	tes	Node(s)				
		Generate CSR's for these No	odes:	CSP Eriendly Name		
Endpoint Certific	ates					
Trusted Certificat	tes	✓ pxgriaz		pxgrid2 #pxGrid		
OCSP Client Prof	file	Subject				
Certificate Signir	na Requests	Common Name (CN) pxgrid2.lab6.com		Ű.	
		Organizational Unit (OL	ມ			
Certificate Aut	hority	Organization (C)			
		City (I	L)			
Internal CA Setti	ings	State (ST	n [
Certificate Temp	lates	Country (C	c)			
External CA Setti	ings		_			
		Subject Alternative Name (SAN	N) DNS Name	 pxgrid2.lab6.co 	m 🚽	+

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。

Microsoft Active	Directory Certificate Services - lab6-WIN-BG7GPQ	53ID-CA
Submit a Certif	ficate Request or Renewal Request	
To submit a sav Request box.	ved request to the CA, paste a base-64-enco	ded CMC or PKCS #10 certificate request or PKCS #7 renewa
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	SRnguZBuWelK9a0GnbjskxGB9ByaucLrc3ctd13mLGM O728rmk12HLsNlxjfrxQeS/HS+7VMF7WoanZitSofV1: 1UNoh05J5FGWG1uvMkNMB0VTnwjD/8gwnzK9ji+44 eztk0iHwHuP0/DUxSXJrcCQPDW7lekvhKRgFo1u9C Anrg7MmXdFrtWzndPBDC3uVow2FgVLWE END CERTIFICATE REQUEST	
Certificate Templa	ate:	
	pxGrid \$	
Additional Attribu	tes:	
Attributes:		
	Submit	

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

alialia cisco Identity Services Engine	🙆 Hon	The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and	hes an pxgrid2 admin subject.) ed, and	
System Aldentity Management	Network Resources	the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.	E pxGrid Identity Ma	
Deployment Licensing Certificates	Logging Maintenanc	Do you wish to replace the existing certificate?		
Certificate Management		Yes No		
Overview	Bind CA Signed Certificat	e		
System Certificates	* Certificate Friendly N	File Browse pxgrid2.cer		
Endpoint Certificates	Validate Certificate Extens	ions [] ①		
Trusted Certificates	Usa	age yxGrid: Use certificate for the pxGrid Controller		
OCSP Client Profile				
Certificate Signing Requests		Submit Cancel		

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。

	ahah	License Warning 👔, pixgridi
	cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
(🔅 System 🛛 🖉 Identity Management	📰 Network Resources 🛃 Device Portal Management 🗔 pxGrid Services 🗔 Feed Service 🍂 pxGrid Identity
	Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
I	Certificate Management	System Certificates 🔺 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.
•	Overview	🖌 Edit 🗍 Generate Self Signed Certificate 🗍 Import 🕼 Export 🗙 Delete 🔎 View
ľ	System Certificates	Friendly Name Group Tag Used By Issued To Issued By
Ì	Endpoint Certificates	pxgrid1.lab Export Certificate 'pxgrid1.lab6.com,pxgrid1.lab6.com#lab6-WIN-BG7GPQ053ID-CA#00002'× b6.com#la
	Trusted Certificates	C Export Certificate Only
	OCSP Client Profile	*Private Key Password
	Certificate Signing Requests	*Confirm Password
I.		Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.
	Certificate Authority	Export Cancel

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。

	alada	License Warning 🔥 admin1 admin
	cisco Identity Services Engine	Home Operations Policy Guest Access Administration
(🔆 System 🛛 👰 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🔤 pxGrid Services 🗔 Feed Service 💵 🚛 pxGrid Identity Mappin
	Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
	Certificate Management	Tmnort Saniar Cartificata
	Overview	Import Server Certificate
j	Durkem Cartiflanten	* Select Node admin1 T
ł	System Ceruncates	* Certificate File Browse pxgrid1lab6compxgrid1lab6co.pem
	Endpoint Certificates	* Private Key File Browse pxgrid1lab6compxgrid1lab6co.pvk
	Trusted Certificates	Password
	OCSP Client Profile	Friendly Name
		Allow Wildcard Certificates 🔲 🕡
l	Certificate Signing Requests	Allow wildcard is disabled when pxGrld is selected and vice versa. This is because pxGrld does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrld is not checked.
	Certificate Authority	Validate Certificate Extensions 🗌 🛈
ĺ	Internal CA Settings	Usage
		Admin: Use certificate to authenticate the ISE Admin Portal
	Certificate Templates	EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
	External CA Settings	✓ pxGrid: Use certificate for the pxGrid Controller
		Portal: Use for portal

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。

Includional Identity Services Engine		
Outer Statestic Menseement	Home Operations I* Policy I* Guest Access I* Administration I*	i Telentitu Meneire
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	I Identity Mappin
Certificate Management		
Overview	Import Server Certificate	
	* Select Node mnt1	
System Certificates	* Certificate File prowse pxgrid1lab6compxgrid1lab6co.pem	
Endpoint Certificates	* Private Key File pxgrid1lab6compxgrid1lab6co.pvk	
Trusted Certificates	Password	
OCSP Client Profile	Friendly Name	
	Allow Wildcard Certificates 📃 (i)	
Certificate Signing Requests	Allow wildcard is disabled when pxGrid is selected and vice versa. This is because px not support wildcard certificates. If you want to use wildcard with other usage type(s sure pxGrid is not checked.	Grid does s), make
Certificate Authority	Validate Certificate Extensions 🗌 🛈	
Internal CA Settings	Usage	
Cortificate Templates	Admin: Use certificate to authenticate the ISE Admin Portal	
	CAP Authentication: Use certificate for the pyGrid Controller	
External CA Settings	Portal: Use for portal	

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。

alialu				License Warr	ning 🛕 admin1 admin	I Logout I Feedback	\$	
cisco Identity Services Engine	🟠 Home	Operations V Policy	▼ Guest Access ▼	Administration V			Setup /	Assistar
System 🕺 Identity Management	🔛 Network Resources 🛛 🛃 De	evice Portal Management	pxGrid Services	Feed Service	2 pxGrid Identity Mappin	g		
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore	Admin Access Se	ettings				
Certificate Management	System Certificates 🔺 For dis	saster recovery it is recomm	nended to export certifica	ate and private key pairs of a	all system certificates.			
Overview	🖊 Edit 🛛 🕂 Generate Self Sign	ed Certificate 🛛 🕂 Impo	rt 😥 Export 🗙	Delete 🔎 View				
	Friendly Name	Group Tag Used I	By Is	ssued To	Issued By	Valid From	Expiration Date	
System Certificates	▼ admin1							
Endpoint Certificates	admin1.lab6.com,admin1.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00003	Default Portal EAP A Certificate Group Portal	uthentication, Admin, a	dmin1.lab6.com	lab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	
Trusted Certificates	pxgrid1.lab6.com,pxgrid1.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00004	pxGrid	р	oxgrid1.lab6.com	lab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	
OCSP Client Profile	admin2							
	▼ mnt1							
Certificate Signing Requests	mnt1.lab6.com,mnt1.lab6.c om#lab6-WIN-BG7GPQ053I D-CA#00003	Default Portal EAP A Certificate Group Portal	uthentication, Admin, m	nnt1.lab6.com	lab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	~
Certificate Authority	pxgrid1.lab6.com,pxgrid1.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00004	pxGrid	р	oxgrid1.lab6.com	lab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	

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。

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

օրեր				License	Warning 👖 mnt2 adm	tin I Logol
cisco Identity Services Engine	🙆 Hom	e Operations 🔻	Policy T Guest Act	ess 🔻 Administratio	n 🛛 🔻	
System All Identity Management	Network Resources	🛃 Device Portal Man	agement 🔤 pxGrid S	Services 🔄 Feed S	Service	entity Mappi
Deployment Licensing Certificates	Logging Maintenance	e Backup & Re	store Admin Access	Settings		
Certificate Management	System Certificates 🔺 F	or disaster recovery	t is recommended to export	certificate and private ke	y pairs of all system certific	ates.
Overview	🖌 Edit 🛛 🕂 Generate Self	Signed Certificate	- Import Export	X Delete Vi	ew	
	Friendly Name	Group Tag	Used By	Issued To	Issued By	Vali
System Certificates	▼ mnt2					
Endpoint Certificates	mnt2.lab6.com,mnt2.lab6 com#lab6-WIN-BG7GPQ0 53ID-CA#00001	 Default Portal Certificate Group 	EAP Authentication, Admin, Portal	mnt2.lab6.com	lab6-WIN-BG7GPQ05 CA	3ID- Fri,
Trusted Certificates	Export Certif	icate 'mnt2.lab6.	com,mnt2.lab6.com#la	b6-WIN-BG7GPQ05	3ID-CA#00001' ×	
OCSP Client Profile			 Export Certifica 	te Only		
Certificate Signing Requests			 Export Certifica 	te and Private Key		
		*Private Key Pa	ssword			
Cartificate Authority		*Confirm Pa	ssword			
Continuate Authority	Warning: Exp	oorting a private key	is not a secure operation. It	could lead to possible ex	posure of the private key.	
Internal CA Settings					Export Cancel	

<u>注</u>: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。

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。

cisco Identity Services Engine	Home Operations Policy Guest Access Administration Administration
🔹 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🖓 Feed Service 💵 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	Edit Node
⟨+ E + @	General Settings
	Provide and the standard of th
	Monitoring Role PRIMARY * Other Monitoring Node
	Policy Service
	Enable Session Services Include Node In Node Group None T Enable Profiling Service
	pxGrid (i)

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。

ahah	License Warning j, j admin j 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 Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	Deployment Nodes List > Configure Node Register TSE Node - Step 2: Configure Node General Settinos
Peptoyment	Hostname mnt2 FQDN mnt2.lab6.com IP Address 10.0.0.45 Node Type Identity Services Engine (ISE) Personas Administration Role SECONDARY Monitoring Role PRIMARY * Other Monitoring Node admin2 Policy Service Enable Session Services () Include Node In Node Group None * () Enable Profiling Service pxGrd ()

步骤 3 注册 PSN 节点

uluulu cisco Identii	ty Services Engine	License Warming ji i admini i admini i admini i admini i admini i
🔅 System	A Identity Management	Pointe Operations Pointy Pointy Courses Rocess Processory Administration Pointy P
Deployment	Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	ŵ.	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings
		Hostname psn1. FQON psn1.lab5.com IP Addres 10.00.46 Node Type Identity Services Engine (ISE)
		Administration Role SECONDARY Monitoring Role SECONDARY Other Monitoring Node
		Policy Service Policy Service Include Node in Node Group None Policy Policy Service Policy Service Policy Service Policy Service Policy Service Policy Service Polic

步骤4 注册 pxGrid 节点

ahaha	License Warning 🚖 admin1 admin
cisco Identity Services Engine	
🚸 System 🦉 Identity Management	📷 Network Resources 🛛 🛃 Device Portal Management 🖓 pxGrid Services 🖓 Feed Service 🕰 pxGrid Identity Mappin
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment ⟨¬ ▼ E= ▼ ∰↓ > ☆ Deployment	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings Hostname pxgrid1 FQDN pxgrid1.lab6.com IP Address 10.0.0.48 Node Type Identity Services Engine (ISE)
	Personas Administration Role SECONDARY Monitorian Pole COCONDARY
	Policy Service Policy Service Include Node in Node Group None v 0 Enable Profiling Service profiling Service profiling Cervice p

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

ob	ախ									License Warn	ling 🛕 admin1 admin	I Logout
CI	sco	Identity Se	ervices Engi	ine		۵	Home Ope	rations V Policy V	Guest Access	Administration		
*	e Sys	stem 🖉	Identity Manag	gement	Network	k Resources	🛃 Device	Portal Management	🛃 pxGrid Services	Feed Service	💵 pxGrid Identity Mappi	ing
												1
C	ionte	Live Los										
L L												
AF	nable	Disable		Group	Decline	Delate =	Refresh	Total Pending Approval	(0) -		1-30	of 3 St
√ E	nable	Disable	Approve	😝 Group	Pecline	🐼 Delete 👻	😵 Refresh	Total Pending Approval	(0) *		1 - 3 c	of 3 Sh
✓E	nable	: Ø Disable Client Name	Approve	Group	Pecline Description	🚷 Delete 👻	Refresh Capabilitie	Total Pending Approval	(0) 👻 Status	Client Gr	1 - 3 c oup	of 3 Sh Log
	nable (Client Name	Approve	Group	Pecline Description	😢 Delete 👻	Refresh Capabilitie Capabilitie	Total Pending Approval es es(2 Pub, 1 Sub)	I(0) Status Online	Client Gr Administ	1 - 3 c oup rator	of 3 Sh Log View
	nable () i	Disable Client Name ise-admin-admir ise-admin-mnt1	Approve	Group Clien	Decline Description	😢 Delete 👻	Refresh Capabilitie Capabilitie Capabilitie	Total Pending Approval es es(2 Pub, 1 Sub) es(1 Pub, 0 Sub)	(0) • Status Online Online	Client Gr Administ Administ	1 - 3 c oup rator rator	of 3 Sh Log View View

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。

altalta cisco Ident	ty Services Engine				License Warning 🔥 pan1 admin	Logout Feedback
		ı	Home Operations Police	cy V Guest Access V	Administration 💌	Setup Assistant ~
💑 System	Analogement Management	Network Resources	🛃 Device Portal Management	t 🛛 🔄 pxGrid Services	Feed Service	ntity Mapping
Clients	re Log					Enable Auto-Registration Disable Auto-Registration View By Capabilitie
🖌 Enable 🛛 🙆 Dis	able 😪 Approve 👩 Group	👎 Decline 🛛 🔞 Delete 👻	Refresh Total Pending App	proval(0) 🔻	1 - 5 0	f 5 Show 25 + per page Page 1 + of 1
Client Nar	e Clien	t Description	Capabilities	Status	Client Group	Log
ise-admin	pan1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-m	nt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-admin	mnt1		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
wsa2.lab6	com-test_client pxGr	id Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	View
wsa2.lab6	com-pxgrid_client pxGr	id 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

安全访问操作指南



սիսիս						License Warning 👔	pan1 admin L	ogout
cisco Id	lentity Servi	ICES EI	ngine	Home Operations	Policy Guest Access	Administration •		
😽 System	🚰 Ider	ntity Ma	nagement 🛛 🔛 Network Resource	es 🛛 🛃 Device Portal M	1anagement 🛛 🕞 pxGrid Services	Feed Service	E pxGrid Identity	Марр
								1
Clients	Live Log							
Clear Logs	Resync	🛞 Re	efresh				1 - 25 of 2104	Sho
Client Name			Capability Name	Event Type	Timestamp	Other Attributes		
ise-admin-pan	1@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-mn	t1@xgrid.cisco.	com		Client online	3:13:34 PM EST, Apr 16 2015			
ise-admin-mnt	t1@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-mn	t1@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.co	m	SessionDirectoryCapability-1.0	Publisher added	3:07:34 PM EST, Apr 16 2015			
ise-mnt-mnt1	@xgrid.cisco.co	m	IdentityGroupCapability-1.0	Publisher added	3:07:33 PM EST, Apr 16 2015			
ise-mnt-mnt1	@xgrid.cisco.co	m		Client online	3:07:33 PM EST, Apr 16 2015			
ise-mnt-mnt1	@xgrid.cisco.co	m		Client deleted	3:07:31 PM EST, Apr 16 2015			
ise-mnt-mnt10	@xgrid.cisco.co	m	SessionDirectoryCapability-1.0	Publisher deleted	3:07:31 PM EST, Apr 16 2015			
ise-mnt-mnt1(@xgrid.cisco.co	m	IdentityGroupCapability-1.0	Publisher deleted	3:07:19 PM EST, Apr 16 2015			
ise-admin-pan	1@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	n-pxgrid_client	@xg	SessionDirectoryCapability-1.0	Client subscribed	8:17:37 PM EST, Apr 15 2015			
wsa2.lab6.com	n-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。

<u>注</u>:如果使用 MAC 进行测试,请参阅以下网址了解如何卸载 Java: <u>https://www.java.com/en/download/help/mac_uninstall_java.xml</u> 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/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:/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 -keystoreFilename 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 kevstorePassword=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=0A000002000000B006E1086, 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: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。

<u>注</u>: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)。质询秘钥是必须的,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。

<u>注</u>: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-BG7GPQ	53ID-CA
Submit a Certi	ficate Request or Renewal Request	
To submit a sav by an external s	red request to the CA, paste a base-64-enco source (such as a Web server) in the Saved	Ided CMC or PKCS #10 certificate request or PKCS #7 real Request box.
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	UMMINUGCC3UCLON UMMINUSCHC2DHUGHUGYLDLAUGU UCCAQEX/H+B&GMpwaadhin6yxCWKYIBYhOY5jrURxf wcs4)pq7PY4tQ6a/1Clk3chergzdBkQMyX2hx2hqg PT23CMgOCyAsTxhn8HirSuZYK3apPomuaH3IL3 Hm+6thRTVhrKOC61ejxFd-012QXEn19YMov7sRSWFU1 Jf+Z+ptK87AYC2PYVWr/kI86b8TC1hSuMMF+Aglcn QQ23lwmg4ogVabwhP6nmku4UQBg== UEST	
Certificate Templa	ate:	
	pxGrid \$	
Additional Attribu	tes:	
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: 61262d760000000000
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...*.н.....
0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 .....*.H.....
0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A ....+...0...*
0030: 86 48 86 F7 0D 03 07
                                                          .н....
#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
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...
```

安全访问操作指南



#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [Γ 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 1 1 #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.у, 1 #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] 11 #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] []]] 1 #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth clientAuth emailProtection 1.3.6.1.4.1.311.10.3.4 1 #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key_Encipherment 1 #10: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`. 0010: AF D8 07 09 Trust this certificate? [no]: yes Certificate was added to keystroke

步骤 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
```

<u>注</u>: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
1
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
  Key CertSign
  Crl Sign
1
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KevIdentifier [
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.у,
]
1
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。

```
安全访问操作指南
```

cisco.

Johns-Macbook-Pro:mntnodes jeppich\$ openssl x509 -outform der -in mntl.pem -out mntl.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: 61326a180000000031 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*.H..... 0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A 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...+...... 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 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 ...y...-...S...8 86 E6 FC 53 86 82 A1 38 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 1 1 #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KevIdentifier [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 i.v, 1 1

```
安全访问操作指南
```



```
#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]
11
#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
[] ]
1
#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
1
#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
 DigitalSignature
  Key Encipherment
1
#10: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: mnt1.lab6.com
1
#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
                                                          . . . .
1
1
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 <labl> 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: 613244ec0000000044
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
```

安全访问操作指南



#2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [Г 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 1 1 #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 i.v, 1 #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] 11 #5: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth 1 #6: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key Encipherment 1 #7: ObjectId: 2.5.29.17 Criticality=false SubjectAlternativeName [DNSName: mnt2.lab6.com 1 #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 1 1 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: 613244ec00000000044 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 [Γ 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 1 #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, 1 1 #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] 11 #5: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth 1 #6: ObjectId: 2.5.29.15 Criticality=true KevUsage [DigitalSignature Key Encipherment 1 #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] 1

cisco.

****** ****** 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: 61326a180000000031 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
 F7
 0D
 03
 04
 02
 02
*.H......

 0020:
 00
 80
 30
 07
 06
 05
 2B
 0E
 03
 02
 07
 30
 0A
 06
 08
 2A

 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

 0020:
 01
 05
 05
 07
 03
 04
 30
 0C
 06
 0A
 2B
 06
 01
 04
 01
 82
 03 02 30 0A 06 08 2B 06 ..+....0...+. 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 00 01 01 0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 AL 0010: 87 CB EB 79 81 89 9D 2D 86 E6 FC 53 86 82 AL 0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.*+....7.... 86 E6 FC 53 86 82 A1 38 ...y...-...S...8 ^...#...@..d... #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [Г 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 1 1 #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 ... &... Z.6 &... 0010: 6A C8 79 2C i.v, 1 #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] 11

```
#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
[]
   1
#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
 serverAuth
  clientAuth
 emailProtection
 1.3.6.1.4.1.311.10.3.4
1
#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
1
#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
1
1
 *******
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 1 #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 1]

j.у,

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 ciscol23 -
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

ISCO Id	fentity Services Engi	ne		ا 🏠	Home Oper	ations V Policy	▼ Guest Access ▼	Administration V		
🔆 System		ement	Network	Network Resources		A Device Portal Management		Feed Service	≟∰ pxGrid Identity Mappi	ing
Clients	Live Log									
lients Inable	Disable OApprove	😝 Group	👎 Decline	🐼 Delete 👻	Sefresh	Total Pending Approv	al(0) 👻		1 - 4 0	of 4
ients inable Client	Live Log Oisable OApprove t Name	Group	Pecline t Description	🔀 Delete 🔻	Refresh Capabilities	Total Pending Approv	al(0) 👻 Status	Client G	1 - 4 o roup	of 4 Loi
itents inable (Client ise-ac	Live Log Disable Approve t Name dmin-admin1	Group Clien	Pecline t Description	😵 Delete 🔻	 Refresh Capabilities Capabilities 	Total Pending Approv s s(2 Pub, 1 Sub)	al(0) 🔻 Status Online	Client Gr Administ	1 - 4 o roup trator	of 4 Log Vie
itents inable Client ise-ac ise-m	Live Log Disable OApprove t Name dmin-admin1 unt-mnt1	Group	Pecline Description	😢 Delete 👻	Refresh Capabilities Capabilities Capabilities	Total Pending Approv s s(2 Pub, 1 Sub) s(2 Pub, 0 Sub)	al(0) Status Online Online	Client G Administ Administ	1 - 4 o roup trator trator	of 4 Lo Vie Vie
Clients Enable (Clien ise-ad ise-m ise-ad	Live Log Disable Approve t Name dmin-admin1 unt-mnt1 dmin-mnt1	Group	Decline t Description	😧 Delete 👻	Refresh Capabilities Capabilities Capabilities Capabilities	Total Pending Approv s s(2 Pub, 1 Sub) s(2 Pub, 0 Sub) s(1 Pub, 0 Sub)	al(0) Status Online Online Online Online	Client Gr Administ Administ Administ	1 - 4 o roup trator trator trator	of 4 Lo Vie Vie Vie

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=0A0000020000000002D814C0, 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=00000004], Posture Status=null, Posture Timestamp=, Session Last Update Time=Thu Mar 05 21:33:02 EST 2015) session (ip=null, Audit Session Id=0A00000200000000003672C, 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 秘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 jeppich$ 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
```

```
安全访问操作指南
```

1

1

1

CISCO

```
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=mnt2.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 613244ec00000000044
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 [
```

Г

] 1

安全访问操作指南



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, 1 1 #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] 11 #5: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth 1 #6: ObjectId: 2.5.29.15 Criticality=true KevUsage [DigitalSignature Key Encipherment 1 #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 1 1 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: 61326a180000000031 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 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 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....

cisco.

```
#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...+......
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 [
  Γ
   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
1
1
#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.у,
1
1
#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]
11
#7: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
[]
   1
#8: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
  emailProtection
  1.3.6.1.4.1.311.10.3.4
1
#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
1
#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...`.
```

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: 6118d6130000000034
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...*
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.
                             03 02 30 0A 06 08 2B 06
0010: 06 08 2B 06 01 05 05 07
                                                       ..+....0...+.
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82
                                                        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....
                                                       ...y...-...S...8
0010: 87 CB EB 79 81 89 9D 2D
                              86 E6 FC 53 86 82 A1 38
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 [
```

. . . .

```
安全访问操作指南
```



Г accessMethod: calssuers 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 1] #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 i.y, 1 1 #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] 11 #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] [] 1 1 #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth clientAuth emailProtection 1.3.6.1.4.1.311.10.3.4 1 #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key_Encipherment 1 #10: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0010: 15 06 CF DB 1 1 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

```
安全访问操作指南
```

Extensions:

1

1

1

CISCO

#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: 6118d6130000000034 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...*.н..... 0030: 86 48 86 F7 0D 03 07 .н.... #2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false 0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 820...+.... 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 [Γ 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 1 1 #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 i.v, 1 #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] 11 #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] [] 1 #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth clientAuth emailProtection 1.3.6.1.4.1.311.10.3.4 1 #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key Encipherment 1 #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 1 1 ***** 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。

isco Identity Services Engine	Difference Difference	erations T Policy	 Guest Access 	Administration	
💀 System 🦉 Identity Management	Network Resources	e Portal Management	a, pxGrid Serv	ices 🛛 🙀 Feed Service	💵 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance E	Backup & Restore	Admin Access	Settings	
Certificate Management					
Overview	Import Server Certificate				
System Certificates	* Select Node	admin2	•	10 Dam	
Endpoint Certificates	* Private Key File	Browse pxgrid24	ab6compxgrid2lab6	co.pvk	
Trusted Certificates	Password				
OCSP Client Profile	Friendly Name			æ	
Certificate Signing Requests	Allow Wildcard Certificates	 W Allow wildcard is dinot support wildcar sure pxGrid is not of 	sabled when pxGrid rd certificates. If you checked.	is selected and vice versa. Tr want to use wildcard with ot	his is because pxGrid does ther usage type(s), make
Certificate Authority	Validate Certificate Extensions	□ ④			
Internal CA Settings	Usage				
		Admin: Use certific	ate to authenticate I	the ISE Admin Portal	
Certricate templates		EAP Authentication	: Use certificate for	EAP protocols that use SSL/T	LS tunneling

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

isco identit	ty services ti	igine	🟠 Home	Opera	tions V Policy	▼ Guest	Access V	Administration *	
💀 System	Identity Ma	nagement	Network Resources	Device Po	ortal Management	🛃 pxGr	id Services	Feed Service	a pxGrid Identity M
Deployment	Licensing	Certificates	Logging Maintenance	Bac	kup & Restore	Admin Acce	ss Set	tings	
Certificate Man	agement								
Overview.			Import Server Certificat	te					
System Certificati	5	<	* Select	Node m	nt2	:			
Endpoint Certifica	ites		* Private Ke	ey File 🔒	rowse pxgrid2	lab6compxgrid	d2lab6co.pvi	m K	
Trusted Certificate	es		Pas	sword 🗔					
OCSP Client Profil	le		Friendly	Name				æ	
Certificate Signing	g Requests		Allow Wildcard Certif	ficates 🗌	Allow wildcard is on not support wildcard sure pxGrid is not	disabled when and certificates checked.	pxGrid is sele . If you want	ected and vice versa. This to use wildcard with othe	is because pxGrid does er usage type(s), make
Certificate Auth	hority		Validate Certificate Exter	nsions 🗌	æ				
Internal CA Settin	nge		U	isage					
Certificate Temple	ates				EAP Authenticatio	wave to authen	ate for EAP p	rotocols that use SSL/TLS	tunneling
External CA Settir	ngs				pxGrid: Use certif	icate for the p	Grid Control	ller	
Contrast Contrastings					Portal: Use for portal				

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

aludu.			License Warning 🥂 admin1 admin Logout Fe	eedback D
cisco Identity Services Engine	☆ Home Operations ▼	Policy V Guest Access V Administration	n I 🔻	Setup Assista
System 🛛 🦉 Identity Management	Network Resources	gement 🔄 pxGrid Services 🔂 Feed S	ervice 💵 📲 pxGrid Identity Mapping	
Deployment Licensing Certificates	Logging Maintenance Backup & Rest	ore Admin Access Settings		
Certificate Management	System Certificates 🔺 For disaster recovery it	is recommended to export certificate and private ke	y pairs of all system certificates.	
Overview	🖊 Edit 🛛 🕂 Generate Self Signed Certificate	🕂 Import 🛛 🚱 Export 🗎 🗙 Delete 🗋 🔑 Vi	W	
	Friendly Name Group Tag	Used By Issued To	Issued By Valid From	Expiration Date
System Certificates	v admin2			
Endpoint Certificates	admin2.lab6.com,admin2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00001	EAP Authentication, Admin, admin2.lab6.com Portal	lab6-WIN-BG7GPQ053ID-C Wed, 4 Mar 20	015 Fri, 3 Mar 2017 🗹
Trusted Certificates	pxgrid2.lab6.com,pxgrid2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00002	pxGrid pxgrid2.lab6.com	lab6-WIN-BG7GPQ053ID-C Wed, 4 Mar 20	015 Sat, 4 Mar 2017 🥑
Trusted Certificates	 b6.com#lab6-WIN-BG7GPQ 053ID-CA#00001 Certificate Group psgrid2.lab6.com,psgrid2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00002 	Portal admin2.lab6.com pxGrid pxgrid2.lab6.com	A Wed, 4 Mar 21 lab6-WIN-BG7GPQ053ID-C Wed, 4 Mar 21 A	015 Fn, 3 Mar 2017 🗹
	▼ mnt2			
Internal CA Settings	mnt2.lab6.com,mnt2.lab6.c	rtal EAP Authentication, Admin, mat 2 li	lab6-WIN-BG7GPQ053ID-C	Wed 4 Mar 2015 Fri, 3 Mar 2
Certificate Templates	D-CA#00001	Group Portal	A	WCu, Thai 2013 Thi 3 hui 2
External CA Settings	pxgrid2.lab6.com,pxgrid2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00002	pxGrid pxgrid;	.lab6.com lab6-WIN-BG7GPQ053ID-C A	Wed, 4 Mar 2015 Sat, 4 Mar

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

alus a	License Warning 🦺 admin
CISCO Identity Services Engine	Home Operations Policy Guest Access Administration
System 🛛 😤 Identity Management	🖀 Network Resources 🛃 Device Portal Management 🔂 pxGrid Services 🗔 Feed Service 12 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment Image: Comparison of the second secon	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings
	Hostname admin2 FQDN admin2.lab6.com IP Address 10.0.0.42 Node Type Identity Services Engine (ISE)
	Personas Image: Administration Role SECONDARY
	Monitoring Role SECONDARY Other Monitoring Node
	Policy Service Enable Session Services Include Node in Node Group None Enable Profiling Service pxGrid

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

dude		-							License	Warning 🚠 admin1 admin
cisco Identi	ty Services En	gine		🟠 Home	Operations 🔻	Policy V	Guest Acces	as 🔻 Adr	ministration 🔻	
🕂 System	🛂 Identity Man	agement	Network Res	ources 🛃	Device Portal Manage	ment	pxGrid Ser	vices	🛃 Feed Service	£ ∎ pxGrid Identity Mapping
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Restor	e Ad	min Access	Settings		
Deployment	it	ŵ.⊷	Personas Admin Monito Policy	Nodes List > Confi SE Node - Step 3 Settings Hostnam FIQ IP Addree Node Typ s istration oring Service Enable Session Inclu	gure Node 2: Configure Node N mnt2.lab6.com ss 10.0.45 re Identity Services Rol Ro Services	e SECOND/ le SECOND/ p None	SE) NRY DARY +	Other M	Ionitoring Node	mnti
			pxGrid	 Enable Profiling (i) 	Service					

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

cisco Identif	y Services E	ingine		🟠 Home	Operations V Polic	Guest Acce	ess 🔻 Admi	nistration 🛛 🔻	
🕂 System	Note that the second se	anagement	Network Res	ources 🛃 D	evice Portal Management	🔊 pxGrid Se	ervices 6	Feed Service	x pxGrid Identity Mappir
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Restore	Admin Access	Settings		
Deployment		ŵ.	Deployment M Edit Node General	Nodes List > pxgrid: 2 Settings	2			*	
				IP Address Node Type	10.0.0.49 Identity Services Engi	ne (ISE)			
			Personas	istration	Role SE	CONDARY			
			. D Monito	pring	Role	RIMARY 🔻	Other Mo	nitoring Node	
			Policy	Service					
			L	Enable Session S	ervices () Node in Node Group	one	+ (Ì)		
				Enable Profiling	Service				
			✓ pxGrid						

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

alia) cisco	J. Identity Services Engine		h (2)	Home Opera	ations 💌 Policy 🔍	Guest Access	License Warning 🔥 I Administration 🛛 🔻	admin2 (admin (Logout
🐝 S)	vstem 🛛 😤 Identity Managen	nent 🔛 Networ	k Resources	Pevice P	ortal Management	😰 pxGrid Services	Feed Service	rid Identity Mapping
Client	s Live Log							0
🖌 Enab	e ⊘ Disable 😪 Approve (🕤 Group 🛛 👎 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0)	•		1 - 10 of 10 Sho
	Client Name	Client Description		Capabilities		Status	Client Group	Log
	ise-admin-admin2			Capabilities	(2 Pub, 1 Sub)	Online	Administrator	View
	ise-admin-mnt2			Capabilities	(1 Pub, 0 Sub)	Online	Administrator	View
	ise-admin-mnt1			Capabilities	(1 Pub, 0 Sub)	Online	Administrator	View
	ise-mnt-mnt1			Capabilities	(2 Pub, 0 Sub)	Online	Administrator	View
	ise-mnt-mnt2			Capabilities	(2 Pub, 0 Sub)	Online	Administrator	View
	mac_engineering			Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	mac			Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
□ ►	mac2			Capabilities	(0 Pub, 0 Sub)	Offline	EPS	View
	mac_engineering3			Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	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
- <u>注</u>: 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
- <u>注</u>: 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

cisco Identi	ty Services El	ngine		🟠 Hom	e Op	erations •	Policy	 Guest A 	ccess 🔻	Administration		
👾 System	🚰 Identity Ma	nagement	Network Re	esources [🛃 Devic	e Portal Mar	nagement	😡 pxGrid	Services	Feed Service	La pxGrid Identity	Mapping
Deployment	Licensing	Certificates	Logging	Maintenance	e I	Backup & R	estore	Admin Access	Settin	gs		
Deployment			Deploy	ment Nodes								
. E .												
 Meployment 	t		/ Edit	💿 Register 👻	3 S)	/ncup	Deregister					
			Hos	tname		Node Type	Personas			Role(s)	Services	Node S
			🗆 adn	nin1		ISE	Administra	ation		PRIMARY(A)		~
			🗆 adn	nin2		ISE	Administra	ation		SECONDARY(A)		
			mnt mnt	1		ISE	Monitoring	9		PRIMARY(M)		~
			mnt mnt	2		ISE	Monitoring	2		SECONDARY(M)		~
			🗆 psn	1		ISE	Policy Ser	vice			All	S
			🗆 рхд	rid1		ISE	pxGrid					
				rid2		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

ahah				License Warning) 🚹 admin1 admin Logout
cisco Identity Services Engine	🟠 Home 🛛	operations 🔹 Policy 💌	Guest Access	Administration	
🔆 System 🛛 🐉 Identity Management	Network Resources	ce Portal Management	🔊 pxGrid Services	Feed Service	E pxGrid Identity Mapping
					1
Clients Live Log					
🖌 Enable 🖉 Disable 😪 Approve 😝 Group 👎	Decline 🔞 Delete 👻 🍪 Refres	h Total Pending Approval(0) +		1 - 7 of 7 Sh
Client Name Client De	escription Capabi	ities	Status	Client Grou	ip Log
□ ► ise-admin-mnt2	Capabi	ities(0 Pub, 0 Sub)	Online	Administra	tor View
□ ▶ ise-mnt-mnt2	Capabi	ities(2 Pub, 0 Sub)	Online	Administra	tor View
ise-mnt-mnt1	Capabi	ities(2 Pub, 0 Sub)	Online	Administra	tor View
ise-admin-mnt1	Capabi	ities(1 Pub, 0 Sub)	Online	Administra	tor View
ise-admin-admin1	Capabi	ities(2 Pub, 1 Sub)	Online	Administra	tor View
mac_engineering17	Capabi	ities(0 Pub, 0 Sub)	Offline	Session	View
mac •	Capabi	ities(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=0A000002000000E027B9538, 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=0A000002000000000035232, 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

սիսի				License Warning 🔥 adm	in1 admin Logou
cisco Identity Services Engine	🏠 H	Nome Operations T Policy T	Guest Access	Administration V	
🐝 System 🛛 💆 Identity Management	Network Resources	🛃 Device Portal Management	🛃 pxGrid Services	Feed Service	dentity Mapping
Clients Live Log					
Sroup	👎 Decline 🛛 🐼 Delete 👻	Refresh Total Pending Approval	0) 👻		1 - 8 of 8 S
Client Name Clien	nt 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

alulo				License Warr	ning 🛕 admin1 a	admin
cisco Identity Services Engine	🙆 Home	e Operations	Policy 🗸 Guest Acces	ss 🔻 Administration 🔻		
💀 System 🦉 Identity Management	Network Resources	Device Portal Man	agement 🛛 🗔 pxGrid Se	rvices 😡 Feed Service	💵 pxGrid Identity I	Mapping
Deployment Licensing Certificates	Logging Maintenance	Backup & Re	store Admin Access	Settings		
Deployment	Deployment Nodes					
 Seployment 	🥖 Edit 🛛 🔯 Register 👻	Syncup	Deregister			
	Hostname	 Node Type 	Personas	Role(s)	Services	Node St
	admin1	ISE	Administration	PRIMARY(A)		~
	admin2	ISE	Administration	SECONDARY(/	A)	
	mnt1	ISE	Monitoring	PRIMARY(M)		~
	mnt2	ISE	Monitoring	SECONDARY(1	M)	
	psn1	ISE	Policy Service		All	 Image: A set of the
	pxgrid1	ISE	pxGrid			0
	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=0A000002000000000035232, 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

alulu								License Warni	ng 🔥 admin1 admin Logout
cisco Ident	ty Services Engi	ine		۵	Home Ope	rations V Policy V	Guest Access	Administration V	
🔆 System	🚰 Identity Manag	gement	Network	Resources	🛃 Device	Portal Management	😺 pxGrid Services	Feed Service	≟: ∰pxGrid Identity Mapping
									e
Clients	ve Log								
🖌 Enable 🖉 Dis	able 😪 Approve	😝 Group	👎 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0)	•		1 - 8 of 8 Shr
Client Nar	ne	Clien	t Description		Capabilitie	S	Status	Client Gro	up Log
□ ► ise-admin	mnt2				Capabilitie	s(0 Pub, 0 Sub)	Online	Administr	ator View
ise-mnt-m	nt1				Capabilitie	s(2 Pub, 0 Sub)	Online	Administr	ator View
ise-admin	mnt1				Capabilitie	s(1 Pub, 0 Sub)	Online	Administr	ator View
ise-admin	admin1				Capabilitie	s(2 Pub, 1 Sub)	Online	Administr	ator View
□ ► ise-mnt-m	nt2				Capabilitie	s(2 Pub, 0 Sub)	Online	Administr	ator View
🗆 🕨 mac					Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
mac_engi	neering15				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
mac_engi	neering17				Capabilitie	s(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。



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

ahaj	 Jidentity Se	rvices Engli	ne					22 33 12	License Warni	ng 🔥 admin1 admin	Logout F
∳ ∦ S	ystem 🛃 1	Identity Manag	ement	Network	Resources	Home Ope	Portal Management	Guest Access pxGrid Services	Administration	ad a pxGrid Identity Mapping	
							L				⊖ Enat
Client	Live Log										
🖌 Enab	le 🖉 Disable	Approve	😝 Group	👎 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0)	•		1 - 9 of 9	Show 2
	Client Name		Client	Description		Capabilitie	S	Status	Client Gro	oup La	g
	ise-admin-mnt2					Capabilitie	s(0 Pub, 0 Sub)	Online	Administr	rator Vi	ew
	ise-mnt-mnt1					Capabilitie	s(2 Pub, 0 Sub)	Online	Administr	rator Vi	ew
	ise-admin-mnt1					Capabilitie	s(1 Pub, 0 Sub)	Online	Administr	rator Vi	ew
	ise-admin-admin	1				Capabilitie	s(2 Pub, 1 Sub)	Online	Administr	rator Vi	ew
	ise-mnt-mnt2					Capabilitie	s(2 Pub, 0 Sub)	Online	Administr	rator Vi	ew
	mac					Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	Vie	ew
	mac_engineering	15				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	Vi	ew
	mac_engineering	17				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	Vi	ew
	mac_engineering	320				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	Vi	ew



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

Suctom	Identity Management	Natwork Pasauroas	IN Dovice Portal M	anagement DevGrid Service	ac Each Sanica	n BoyCrid Identit	Manajag
Peployment	Licensing Certificates	Logging Maintena	nce Backun &	Restore Admin Access	Settinos		y mapping
eployment	conting out in stor	Deployment Node	s		occango		
- • E •	\. \						
🔆 Deployment		/ Edit @ Register	Syncup Node Ture	Deregister	Polo(s)	Convicos	Nodo Status
		admin1	ISE	Administration	PRIMARY(A)	Services	Node Status
		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			0

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

cisco Identity Services Engine	B Home Operations ▼ Policy ↓	▼ Guest Access ▼	License Warning 🔥 I admin	1 admin Logout Feedback 🔎
🔆 System 🦉 Identity Management 🛛 🔛 Network Resources	🛃 Device Portal Management	pxGrid Services	Feed Service	entity Mapping
Clients Live Loo				Enable Auto-Registration
✓ Enable Ø Disable Ø Approve Group Pecline O Decline	- 😵 Refresh Total Pending Approva	al(0) 👻		1 - 9 of 9 Show 25 + per page Page
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
kevstoreFilename=mac.iks
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=0A000002000000000035232, 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.iks
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

սիս	16							License Warr	ing 🥂 admin1 admin Logou
CISC	o Identity Servi	ices Engine		۵	Home Ope	rations • Policy •	Guest Access	Administration V	
*	System 😽 Ider	ntity Management	Networ	k Resources	🛃 Device	Portal Management	🔊 pxGrid Services	Feed Service	⊥ ∰ pxGrid Identity Mapping
Clier	nts Live Log								
V Ena	ble 🕜 Disable 🔮	Approve 🕤 Gro	up 🎈 Decline	🛞 Delete 👻	🚱 Refresh	Total Pending Approval(0) 🖛		1 - 10 of 10 Sł
	Client Name		Client Description		Capabilitie	15	Status	Client Gr	oup Log
	ise-mnt-mnt2				Capabilitie	s(2 Pub, 0 Sub)	Online	Administ	rator View
	ise-mnt-mnt1				Capabilitie	es(2 Pub, 0 Sub)	Online	Administ	rator View
	ise-admin-mnt1				Capabilitie	s(1 Pub, 0 Sub)	Online	Administ	rator View
	ise-admin-admin1				Capabilitie	s(2 Pub, 1 Sub)	Online	Administ	rator View
	ise-admin-mnt2				Capabilitie	s(0 Pub, 0 Sub)	Online	Administ	rator View
	mac				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering17				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering15				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering20				Capabilitie	s(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering50				Capabilitie	s(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

ahah		License Warning 🔔 isespi
Kisco Identity Services Engine	🟠 Home	Operations V Policy V Guest Access V Administration V
🙀 System 🕺 Identity Management	🔛 Network Resources 🛛 🛃	Device Portal Management 🔊 pxGrid Services 🔊 Feed Service 💵 🙀 pxGrid Iden
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore Admin Access Settings
Certificate Management	Edit System Certificate	
Overview	Issuer	
	* Friendly Name	Default self-signed server certificate
System Certificates	Description	
Endpoint Certificates	Subject	CN=isespl.lab6.com
Trusted Certificates	Issuer	isespl.lab6.com
	Valid From	Sat, 24 Jan 2015 20:57:46 EST
OCSP Client Profile	Valid To (Expiration)	Sun, 24 Jan 2016 20:57:46 EST
Certificate Signing Requests	Serial Number	54 C4 4D 9A 00 00 00 00 4A 09 B8 3E 37 DB E8 FE
	Signature Algorithm	SHA1WITHRSA
Certificate Authority	Key Length	1024
Internal CA Settings	Usage	
Certificate Templates		EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
Estamol CA Collinea		Admin: Use certificate to authenticate the ISE Admin Portal
External CA Settings		
		* 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"

<u>建</u>:此证书将另存为 PEM 文件

	🟠 Home	Operations v Poli	cy 🛛 🔻 Guest Access 🗎 🔻	Administration		
💀 System 🏾 👰 Identity Management	Network Resources	Device Portal Managemen	t 😡 pxGrid Services	Feed Service	2 pxGrid Identity M	apping
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore	Admin Access Se	ettings		
Certificate Management	System Certificates A For	disaster recovery it is reco	mmended to export certifica	ite and private key pairs o	f all system certificates.	
Overview	💋 Edit 🛛 🚽 Generate Self Si	gned Certificate 🛛 🕂 In	nport 🕼 Export 🗶	Delete View		
	Friendly Name	Group Tag Use	d By	ssued To	Issued By	Valid From
Endpoint Certificates	 ▼ isespl Default self-signed server c ertificate 	Default Portal Adr Certificate Group Aut	nin, Portal, EAP hentication, pxGrid	espl.lab6.com	isespl.lab6.com	Sat, 24 Jan
Trusted Certificates	Export Cert	ificate 'Default self-si	gned server certificate		×	
OCSP Client Profile			Export Certificate C	Inly		
Certificate Signing Requests			Export Certificate a	nd Private Key		
		*Private Key Passw	ord			
			ord			
Certificate Authority	Warning: E	*Confirm Passw		Id lead to possible every	uro of the private key	
Certificate Authority Internal CA Settings	Warning: E	*Confirm Passw xporting a private key is n	ot a secure operation. It cou	Id lead to possible exposu	Export Cancel	
Certificate Authority Internal CA Settings Certificate Templates	Warning: E	*Confirm Passw xporting a private key is n	ot a secure operation. It cou	Id lead to possible exposu	Export Cancel	

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

սիսիս	License Warning 🔔 isespi
cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
🔅 System 🛛 👰 Identity Management	🎬 Network Resources 🛛 🛃 Device Portal Management 🗔 pxGrid Services 🗔 Feed Service 🎿 🛱 pxGrid Identii
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Quaniau	* Certificate File Browse Defaultselfsignedservercerti.pem
Overview	Friendly Name
System Certificates	
Endnoint Cortificator	Trusted For: 1
Enupoint Certificates	Trust for client authentication and Syslon
Trusted Certificates	Trust for authentication of Cisco Services
OCSP Client Profile	
OCSF Client Frome	Validate Certificate Extensions
Certificate Signing Requests	Description
	Submit Cancel
Certificate Authority	Conce

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

ululu Identity Comisso English	License Warning 🔥 isespi admin
cisco Identity Services Engine	Home Operations Policy Guest Access Administration
🔆 System 🧏 Identity Management	🔛 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🛛 😡 Feed Service 🔍 🔩 pxGrid Identity Mappin
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	Deployment Nodes List > isespl
(- · E · · · · · · · · · · · · · · · · ·	Edit Node
 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018 September 2018<td>General Settings Proming Comiguration</td>	General Settings Proming Comiguration
	Hostname isespi
	FQDN isespi.lab6.com
	IP Address 10.0.0.39
	Node type faentity Services Engine (ISE)
	Personas
	Administration Role STANDALONE Make Primary
	Monitoring Role PRIMARY * Other Monitoring Node
	Policy Service
	✓ Enable Session Services (i)
	Include Node in Node Group None *
	C Enable Profiling Service
	C pixenu V



步骤 5 启动 pxGrid 服务

Administration -> pxGrid Services

		-							License W	aming <u>À</u> isespi
cisco Ide	entity Services Engin	ne		<u>ش</u>	Home Oper	ations 🔻	Policy •	Guest Access	Administration 🗸	
🔆 System	🛃 Identity Manage	ement	Network	Resources	🛃 Device I	Portal Manag	ement	pxGrid Services	Feed Service	💵 📲 pxGrid Iden
Clients		G Gmun	Decline	O Dolato -	Refrech	Total Pendi	ng Approval(0)			
Clients	Live Log Disable Opprove	Group	Decline	🚫 Delete 👻	Refresh Capabilities	Total Pendi	ng Approval(0)) ★ Status	Client G	roup
Clients	Live Log Disable OApprove Name min-isespl	Group Client	Pecline Description	😵 Delete 💌	Refresh Capabilities Capabilities	Total Pendi 5 5(3 Pub, 1 Su	ng Approval(0) ib)	Status Online	Client G Adminis	roup

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

ւլիսվի cisco Identity Services Engine	License Warning 🧎 Isespi admin Logo.
🔅 System 🛛 👰 Identity Management	🖀 Network Resources 🛃 Device Portal Management 😡 pxGrid Services 🔊 Feed Service 🕰 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
Overview	* Certificate File Browse rootSample.crt Friendly Name
System Certificates	Trusted For: (i)
Endpoint Certificates	✓ Trust for authentication within ISE
Tourised Contification	Trust for client authentication and Syslog
Irusteu Ceruncates	Trust for authentication of Cisco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

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。

🚯 System 🥂 Identity Management	🖬 Network Resources 😸 Device Portal Management 🖂 pxGrid Services 🔄 Feed Service 💶 gxGrid Identity Mappin
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	
Overview	Import Server Certificate
Austern Certificates	* Select Node isespi *
Constant Resolution and Constant Constant	* Certificate File Browse iseSample1.crt
Indpoint Certificates	* Private Key File Browse iseSample1.key
husted Certificates	Password
YCEP Client Profile	Friendly Name
ASP Gient Profile	Allow Wildcard Certificates 🔲 🕐
Certificate Signing Requests	W Allow wildcard is disabited when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.
Certificate Authority	Validate Certificate Extensions 🔲 🛞
nternal CA Settings	Usage
and the second se	Admin: Use certificate to authenticate the ISE Admin Portal
centrate rempates	EAP Authentication: Use certificate for EAP protocols that use SSL/ILS tunneling
External CA Settings	 Decentor - case contractor for the becaute contractions

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

ahaha		License Wa	rming 🦺 isespi admin
cisco Identi	ty Services Engine	Home Operations Policy Guest Access Administration Administration	
🙀 System	Identity Management	🔛 Network Resources 🛛 🛃 Device Portal Management 🖓 pxGrid Services 🖓 Feed Service	2. pxGrid Identity Mapping
Deployment	Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Deployment	t	Deployment Nodes List > isespl Edit Node General Settings Profiling Configuration Hostname isespl FQDN isespl.lab6.com IP Address 10.0.39 Node Type Identity Services Engine (ISE) Personas Administration Role STANDALONE Make Primary Monitoring Role PRIMARY V Other Monitoring Node Policy Service Policy Service Enable Session Services T Include Node in Node Group None v (1) Enable Profiling Service	

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。

CISCO 10	intry services Engl	ne		🟠 Home Ope	erations Policy	Guest Access	Administration V	
🐝 System	Identity Manag	lement	Network Resource	es 🛃 Device	Portal Management	pxGrid Services	Feed Service	<mark>≗¦</mark> ∎ pxGrid Ider
Clients	Live Log Disable	😝 Group	👎 Decline 🛛 🛞 Dele	te 🔹 🍪 Refresh	Total Pending Approva	al(0) 👻		
Clients	Live Log Disable OApprove	Group	Decline 😥 Dele	te 👻 🍪 Refresh Capabilitie	Total Pending Approva	al(0) + Status	Client G	roup
Clients	Live Log Disable Approve Name nin-isespl	Group	Pecline Solution	e 👻 🍪 Refresh Capabiliti Capabiliti	Total Pending Approve ses	al(0) + Status Online	Client Gi Administ	roup

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:

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

cisco Iden	tity Services Engi	ne		企	Home Ope	rations V Policy V	Guest Access	Administration V	
🔆 System	🛃 Identity Manag	gement	Network	< Resources	🛃 Device	Portal Management	pxGrid Services	Feed Service	<mark>≗</mark> l≝ pxGrid Ident
Clients	Live Log Disable OApprove	😝 Group	🗬 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0) +		
Clients	Live Log Disable Opprove	Group	Pecline Description	🐼 Delete 👻	Refresh Capabilitie	Total Pending Approval(0) ★ Status	Client Gr	oup
Clients Client Client Na Client Na Lise-admi	Live Log Disable Opprove Inne n-isespl	Group Clien	Decline Description	🐼 Delete 👻	Refresh Capabilitie Capabilitie	Total Pending Approval(0 s s(3 Pub, 1 Sub)	Status Online	Client Gr Administ	oup
Clients Clients Client Na Client Na ise-admi ise-mnt-	Live Log Disable Organization In-isespl Seespl	Group Clien	Decline t Description	😧 Delete 👻	Refresh Capabilitie Capabilitie Capabilitie	Total Pending Approval(0 s s(3 Pub, 1 Sub) s(2 Pub, 0 Sub)	Status Online Online	Client Gr Administ Administ	oup rator rator



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 kevstoreFilename=mac.iks 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-rtfrontend-jaxrs-2.7.3.jar:2.7.3] at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:904) [cxf-rt-frontendjaxrs-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

<u>注</u>: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"