



ISE 분산 환경에서 pxGrid 구성

초안



목차

이 문서 정보	4
소개	5
pxGrid 페르소나로 ISE 분산 구축 소개	6
pxGrid 페르소나 컨피그레이션	8
Microsoft CA 2008 R2 Enterprise pxGrid 템플릿 구성	8
pxGrid 액티브-스탠바이 없이 pxGrid 노드 컨피그레이션	10
CA 서명 노드 인증서 생성	10
주 PAN 및 MnT 노드로 pxGrid 노드 퍼블릭/프라이빗 키 내보내기	15
벌크 세션 다운로드	17
분산된 환경의 ISE 노드 등록	18
pxGrid 클라이언트 관리	20
pxGrid 클라이언트 컨피그레이션	22
pxGrid Java SDK 설치	22
pxGrid 클라이언트 SDK Java Keystore 소개	23
pxGrid 클라이언트 인증서 컨피그레이션	24
pxGrid 클라이언트 액티브-스탠바이 예	30
ISE 분산 환경에서 pxGrid 클라이언트 테스트	32
키 저장소 항목 보기	
pxGrid 액티브-스탠바이로 ISE 분산 배포 소개	46
분산 환경 pxGrid 액티브-스탠바이에 ISE 노드 등록	47
ISE 분산 환경 pxGrid 액티브-스탠바이 모드에서 pxGrid 클라이언트 테스트	51
pxGrid 액티브-스탠바이 테스트	52
기본 작업	52
장애 조치 테스트	55
주 노드로 돌아가기	58
ISE 자체 서명 ID 인증서	61
SDK의 샘플 인증서	65
pxGrid 클라이언트 테스트	68
참조	69
부록	70
문제 해결	70

cisco.

Centos 6.5에서 Java 제거 및 JDK 8.0 설치	71
이전 버전의 Java 삭제	71
JDK 8.0 설치	71

이 문서 정보

이 문서는 제품용 Cisco ISE(Identity Services) 1.3 환경에서 pxGrid를 구축하는 Cisco 엔지니어, 파트너, 고객을 대상으로 합니다. 본 문서를 읽는 사용자는 ISE와 pxGrid에 대해 잘 알고 있어야 합니다.

이 문서에서는 ISE 노드 및 pxGrid 클라이언트용 외부 CA 서명 인증서 배포를 중점적으로 다룹니다.

자체 서명 ISE ID 인증서 및 pxGrid 샘플 인증서를 비롯하여, 인증서 배포 시 고려할 그 밖의 사항은 Deploying Certificates with Cisco pxGrid 문서 시리즈에 자세히 설명되어 있습니다.

- CA(Certificate Authority, 인증 기관) 서명 pxGrid ISE 노드 및 CA 서명 pxGrid 클라이언트
- CA 서명 pxGrid 클라이언트 및 자체 서명 ISE pxGrid 노드 인증서
- ISE pxGrid 노드 및 pxGrid 클라이언트가 포함된 자체 서명 인증서

테스트 환경에서 pxGrid를 구성할 경우 다음 자료를 참조하십시오.

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

이 문서는 분산된 ISE 환경에서의 외부 ISE pxGrid 노드 컨피그레이션 및 pxGrid 액티브-스탠바이 컨피그레이션에 대해 다룹니다. 이러한 컨피그레이션 테스트를 위한 pxGrid 클라이언트는 OSX 10.8.5 및 pxGrid Java SDK용 Oracle Java Development Kit(jdk-8u-20-macros-x64.dmg)를 실행 중인 MacBook Pro입니다. 기타 버전의 Linux를 실행 중인 경우 <u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-</u> <u>Configure_and_Test_Integration_with_Cisco_pxGrid.pdf</u> 를 참조하십시오.

또한 이 문서에서는 POC 배포에서 사용된 자체 서명 인증서 및 샘플 인증서로 pxGrid ISE 노드를 구성하는 방법에 대해서도 간략하게 살펴봅니다. 그러나 자세한 내용은 관련 문서를 참조하십시오.

Microsoft Enterprise 2008 CA R2 Enterprise Server가 CA(Certificate Authority)에 사용되었으며 pxGrid 클라이언트 인증서, pxGrid 노드 인증서 및 ISE 노드 인증서 모두 서명되었습니다.

소개

Cisco pxGrid(Platform Exchange Grid)를 사용하면 보안 모니터링 및 네트워크 탐지 시스템, 네트워크 플랫폼, 자산 및 컨피그레이션 관리, ID/액세스 관리 플랫폼 및 거의 모든 기타 IT 운영 플랫폼을 비롯하여 IT 인프라의 각 요소에 걸쳐 멀티벤더 및 교차 플랫폼 네트워크 시스템 협업을 구현할 수 있습니다. 비즈니스 또는 운영 요구 사항이 발생할 경우, 에코시스템 파트너는 pxGrid를 사용하면 pxGrid를 사용하는 Cisco 플랫폼 및 pxGrid를 사용하는 기타 에코시스템을 활용한 방법의 게시/구독을 통해 상황에 맞는 정보를 교환할 수 있습니다.

pxGrid에는 기본적으로 3가지 구성 요소가 있으며 이는 각각 게시자, pxGrid 클라이언트 그리고 pxGrid 컨트롤러인 Cisco ISE(Identity Services Engine) pxGrid 노드입니다.

- 정보 항목의 pxGrid 게시자, pxGrid 클라이언트는 Cisco ISE(Identity Services Engine) 버전 1.3을 구독합니다. ISE도 호출되므로 ISE는 이러한 정보 또는 기능의 유일한 게시자입니다.
- pxGrid 클라이언트는 Cisco Security 플랫폼, pxGrid 에코시스템 파트너 또는 게시된 정보를 구독하는 pxGrid SDK를 실행 중인 Linux나 MAC 호스트에서 지원 가능합니다.
- pxGrid 컨트롤러 Cisco ISE(Identity Services Engine) pxGrid 노드는 클라이언트 등록/관리 및 항목/서브스크립션 프로세스를 제어합니다.

ISE는 다음과 같은 정보 항목을 게시합니다.

- SessionDirectory 인증된 802.1X 세션의 세션 속성
- EndpointProtectionService ANC(Adaptive Network Control) 격리/격리 해제 완화 작업
- TrustsecMetadataCapability SGT(Security Group Tag) 정보
- EndpointProfileMetadata ISE 정책 정보
- IdentityGroup 그룹 및 프로파일링 정보

pxGrid 클라이언트는 이러한 항목을 구독하고 ISE 상황 정보를 가져옵니다.

ISE는 모든 노드에 별도의 페르소나[주 PAN(Policy Admin node, 정책 관리 노드, 주 MnT(Monitoring, 모니터링) 노드, PSN(Policy Service Node, 정책 서비스 노드)]가 있는 분산된 환경에 구축됩니다. pxGrid 노드는 개별 페르소나로도 구축되며, CA 서명 환경에서 사용자 지정된 pxGrid 템플릿이 필요합니다. 이 문서에서는 ISE pxGrid 노드 및 ISE pxGrid 클라이언트 모두에 CA 서명 인증서를 사용하여 이러한 ISE 분산 환경에서 pxGrid를 구성하는 절차적인 단계를 다룹니다.

이 문서는 pxGrid 액티브-스탠바이 컨피그레이션에 대해서도 살펴봅니다.

OSX 10.8.5를 실행 중인 MAC은 이 문서에서 pxGrid 클라이언트 역할을 수행합니다.

Microsoft Enterprise CA 2008 R2 Server는 지정된 CA 서버입니다. 참고로, pxGrid용 사용자 지정 템플릿은 클라이언트와 서버 인증에 모두 EKU(Enhanced KeyUsage)가 수반됩니다. EKU는 인증서의 용도를 정의하며, 이는 ISO 정의 OID(Object Identifier)에 의해 정의됩니다. 이 사용 사례의 경우 하나는 클라이언트 인증(1.3.6.1.5.5.7.3.2)에 사용되고 다른 하나는 서버 인증(1.3.6.1.5.5.7.3.1)에 사용됩니다.

pxGrid 페르소나로 ISE 분산 구축 소개

Windows 2008 R2 Enterprise CA Server는 CA 인증기관으로 사용되었습니다. CA 루트 인증서는 각 ISE 노드의 신뢰할 수 있는 시스템 인증서 저장소로 가져왔습니다. CSR 노드 요청은 pxGrid 노드를 제외한 ISE 노드에 정의된 웹 서버 템플릿 및 관리자 "사용" 인증서를 사용하는 CA에 의해 지원됩니다.

pxGrid 노드는 클라이언트와 서버 인증 시 모두 EKU가 포함된 맞춤형 템플릿을 사용합니다.

<u>참고:</u> pxGrid 템플릿은 Windows 2003 형식을 사용하는 사용자 템플릿의 복제본이 될 수 있으며, 클라이언트 인증 및 서버 인증이 모두 추가된 경우를 위한 EKU가 포함된 사용자 템플릿의 복제본이 될 수 있습니다.

pxGrid 작업을 올바르게 완료하려면 pxGrid 노드의 퍼블릭/프라이빗 키 쌍을 각각의 주 PAN(관리자) 및 주 MnT(모니터링) 모드의 시스템 인증서 저장소에 복사해야 합니다.

<u>참고</u>: 액티브-스탠바이 pxGrid 구성의 경우, 첫 번째 pxGrid 노드(주 pxGrid 노드)의 퍼블릭/프라이빗 키 쌍은 주 PAN 및 주 MnT 노드로 내보내기 됩니다. 두 번째 pxGrid 노드(보조 pxGrid 노드)의 퍼블릭/프라이빗 키 쌍은 보조 PAN 또는 보조 MnT 노드로 내보내기 됩니다.

아래 다이어그램에는 다양한 ISE 노드의 인증서 생성과 관련된 일반적인 ISE 분산 환경이 나와 있습니다. 모든 ISE 노드의 CSR 요청 생성을 위한 관리자 "사용" 인증서는 pxGrid 노드를 제외한 것입니다. CA 서버는 "웹 서버" 템플릿을 사용하여 이러한 요청을 지원하게 됩니다. pxGrid 노드 CSR 요청의 pxGrid "사용" 인증서는 맞춤형 pxGrid 템플릿에서 지원됩니다.

pxGrid In Distributed ISE Deployment



아래 다이어그램에는 분산된 ISE 환경에서의 pxGrid 노드 컨피그레이션이 나와 있습니다. pxGrid 노드는 모든 프로덕션 환경에서 외부에 있습니다. pxGrid 노드의 퍼블릭/프라이빗 키는 pxGrid 컨트롤러를 활성화하기 전에 주 PAN 및 주 MnT 모두에 사용되는 시스템 인증서 저장소에 복사됩니다.

ISE Distributed Environment



pxGrid 페르소나 컨피그레이션

Microsoft CA 2008 R2 Enterprise pxGrid 템플릿 구성

이 섹션에서는 pxGrid 인증서 템플릿 컨피그레이션에 대해 다룹니다. pxGrid 템플릿에는 클라이언트 인증 및 서버 인증을 위한 EKU가 모두 포함되어야 합니다.

pxGrid 템플릿은 다음 단계에 따라 생성됩니다.

1단계 Administrative Tools -> Certificate Authority -> CA 서버 옆의 "+" 드롭다운 선택->마우스 오른쪽 버튼으로 Certificate Templates -> Manage 클릭

2단계 마우스 오른쪽 버튼으로 Duplicate User template 클릭-> Windows 2003 Enterprise -> OK 클릭



<u>참고</u>: Windows Server 2003 Enterprise를 선택하면 템플릿 CA 창의 드롭다운 메뉴에 표시됩니다.

Certificate Template:

pxGrid

÷

3단계 인증서 템플릿의 이름을 입력한 다음, "Publish certificate in Active Directory" 선택란을 취소하고 유효 기간 및 갱신 기간을 입력합니다.

🚇 Certificate Templates Console 🔔		
File Action View Help	Properties of New Template	
Certificate Templates (WIN-BG7GPC	Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Server Template display name:	Ver Actions
	pxGrid	6.1
	Minimum Supported CAs: Windows Server 2003 Enterprise Template name:	4.1 More Actions 5.1 User 6.1 More Actions
	pxGrid	7.1
	Validity period: 5 years 5 5 years 5 5 weeks 1	8.1 7.1 110 105 101 100 101 5.1
	Directory For automatic renewal of smart card certificates, use the existing key f a new key cannot be created	4.1 6.1 11. 5.1 3.1 3.1 4.1 4.1
	OK Cancel Apply Help	

4단계 Extensions -> Add -> Server Authentication -> OK -> Apply 클릭

Certificate Templates Console			-04
File Action View Help	Properties of New Template		
	General Request Handling Subject Name Server Issuance Requirements Superseded Templates Extensions Security		
Certificate Templates (WIN-BG7GP)		Ver 🔺	Actions
	To modify an extension, select it, and then click Edit.	110	Certificate Templa 🔺
	Extensions included in this template:	4.1	More Actions
	Application Policies	5.1	User 🔺
	Basic Constraints	4.1	More Actions
	Certificate Template Information	7.1	Hore Acourts
	Issuance Policies	8.1	
	Ney Usage	7.1	
		110	
		105	
	Edit	101	
	Description of Application Policies:	101	
	Client Authentication	5.1	
	Encrypting File System	4.1	
	Secure Email	6.1	
		11.	
		3.1	
		3.1	
		4.1	
		4.1	
		101	
<u>۱</u>	OK Cancel Apply Help		
-			

pxGrid 액티브-스탠바이 없이 pxGrid 노드 컨피그레이션

이 섹션에서는 ISE 노드를 정의하고, CSR 요청을 생성하며, CA 인증기관에서 인증서를 가져오는 단계를 설명합니다. 이러한 프로세스는 모든 ISE 분산 구축의 일반적인 방식입니다. 이러한 작업은 주 관리자 노드에서 노드를 결합하기 전에 독립형 방식으로 이루어집니다.

pxGrid 노드는 최초 CSR 요청에 ISE pxGrid 사용 인증서를 사용하며, 이 노드는 이전에 정의된 대로 MS CA "pxGrid" 템플릿에 의해 지원됩니다. 반환된 인증서는 최초 pxGrid CSR 요청에 바인딩됩니다.

퍼블릭/프라이빗 키 쌍을 pxGrid 노드에서 내보낸 다음 주 PAN 및 주 MnT 노드로 가져옵니다.

<u>참고</u>: pxGrid 액티브-스탠바이 컨피그레이션의 경우, 두 번째 또는 보조 pxGrid 노드의 퍼블릭/프라이빗 키 쌍은 보조 PAN 및 보조 MnT 노드로 가져오기 됩니다.

Microsoft CA 루트 인증서는 각 ISE 노드의 신뢰할 수 있는 시스템 인증서 저장소로 다운로드 및 가져오기 되며 "ISE 내에서 인증 신뢰"를 위해 활성화됩니다.

CA 서명 노드 인증서 생성

다음 단계에서는 CA 루트 인증서를 다운로드하고, ISE 노드 CSR 요청을 생성하며, 인증서를 CSR 요청에 바인딩하는 절차를 간략하게 알아봅니다.

참고: CA 루트 인증서 및 기타 지원되는 인증서 요청은 기본 64 형식으로 다운로드해야 합니다.

1단계 CA 루트를 기본 64 형식으로 다운로드합니다.

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 **2단계** 신뢰할 수 있는 인증서 저장소로 가져옵니다. Administration -> System -> Certificates -> Trusted Certificates

راندان cisco Identity Services Engine	
🔆 System 🦉 Identity Management	📓 Network Resources 🔠 Device Portal Management 🔂 pxGrid Services 😡 Feed Service 1 📲 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 root.cer
System Certificates	
Endpoint Certificates	✓ Trust for authentication within ISE
Trusted Certificates	Trust for client authentication and Syslog Trust for authentication of Clsco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

3단계 원하는 관리자, MnT, 노드, 독립형 환경에 사용할 CSR을 생성합니다.

Administration-System -> Certificates -> Certificate Signing Requests-"admin" 인증서 사용

սիսիս			License Warning A admin2 ad
cisco Identity Services Engine	🟠 Home O	perations V Policy V Guest Access	▼ Administration ▼
👾 System 🦉 Identity Managemen	t 🔛 Network Resources 🛃 Devic	e Portal Management 🛛 🔂 pxGrid Servic	es 🛛 🔂 Feed Service 🛛 💵 🔤 pxGrid I
Deployment Licensing Certific	Logging Maintenance	Backup & Restore Admin Access	Settings
Certificate Management	Node(s)	_	
Overview	Generate CSR's for these Nod	es:	
System Certificates	Node	CSR Friendly Nar	ne
Endpoint Cortificator	✓ admin2	admin2 #Admin	
Trusted Certificates	Subject		
OCSP Client Profile	Common Name (CN)	admin2.lab6.com	
	Organizational Unit (OU)		
Certificate Signing Requests	Organization (O)		
	City (L)		
Certificate Authority	State (ST)		
Internal CA Settings	Country (C)		
Certificate Templates	Subject Alternative Name (CAN)	DNC Name	
External CA Settings	Subject Alternative Name (SAN)		b.com
	* Key Length	2048	
	* Digest to Sign With	SHA-256	

4단계 MS CA "Web Server" 템플릿을 사용하여 관리자, MnT, PSN 노드에 대한 인증서 요청을 지원합니다.

Microsoft Active	Directory Certificate Services - Iab6-WIN-BG7GPQ	53ID-CA
Submit a Certi	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):	Iv9Z9LİSOnlaKmRİyf5g7O7fGw+zŴRFİH5g+XYik9İK ycDLJ4KDhrcTL819CFy+UIA4lb2HmcuvMFGAFkXT+m CCB4RmUjLmiCP+5cKxMtYqU9aloxKZSeFpXnbMuSt9 /GrNWzbWx85jqTwim+RwosrUyd/wvbDhjMlzFn5D2 60yMH0pELvPJYkR1xBbS5tRIXAQM END CERTIFICATE REQUEST	
Certificate Templa	ite:	
	Web Server \$	
Additional Attribu	tes:	
Attributes:		
	Submit >	

5단계 기본 64 인코딩 형식으로 다운로드합니다.



6단계 각 ISE 노드에 대한 CSR 요청에 인증서를 각각 따로 바인딩합니다 (예: 관리자, MnT, PSN). Administration-System -> Certificates -> Certificate Signing Requests -> 인증서를 선택하고 Bind 메뉴 선택

altalia cisco Identity Services Engine	Home Operations	▼ Policy ▼ Guest Access ▼	License Warning A admin2 a	dmin Logout Feedback 🔎	Setup Assi:
💀 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal N	Management 🛛 🔂 pxGrid Services	Feed Service	dentity Mapping	
Deployment Licensing Certificates	Logging Maintenance Backup 8	Restore Admin Access Setting	gs		
Certificate Management Overview	Certificate Signing Requests Generate Certificate Signing Requests (CSR)				
System Certificates	A Certificate Signing Requests (CSRs) must be se a request has been signed, click "bind" to bind th	ent to and signed by an external authority. C ne request to the signed certificate issued by	lick "export" to download one or more y that authority. Once a CSR is bound,	CSRs so that they may be signed by an it will be removed from this list.	external authority.
Endpoint Certificates	Niew 🔂 Export 🗙 Delete Bind Cer	tificate		Show All	*
Trusted Certificates	 Friendly Name admin2#Admin 	Certificate Subject CN=admin2.lab6.com	Key Length Group Tag 2048	Timestamp Fri, 30 Jan 2015	 Host admin2
OCSP Client Profile					
Certificate Signing Requests					

7단계 각 ISE 노드에 대한 노드 인증서를 각각 따로 가져온 다음 제출합니다.

🕂 System	🚰 Identity Management	Network Resources	evice Portal Management	pxGrid Service	es 😡 Feed Service	1 pxGrid
Deployment	Licensing Certifica	es Logging Maintenance	Backup & Restore	Admin Access	Settings	
Certificate Ma	nagement					
Overview		Bind CA Signed Certificate				
System Certifica	tes	* Certificate I	File Browse admin2.c	er		
		Friendly Na	me		۲	
Endpoint Certific	cates	Allow Wildcard Certifica	tes 🗌 🛈			
Trusted Certifica	ites	Validate Certificate Extensio	ns 🗌 🛞			
OCSP Client Pro	file	Usa	ge	ate to authenticate the	e ISE Admin Portal	

8단계 pxGrid 노드에 대한 CSR을 생성합니다. Administration -> System -> Certificates -> Certificate Signing Requests-"pxGrid" 인증서 사용

System	Network Resources	Portal Management		Feed Service	u≣ pyGrir
Deployment Licensing Certificates	Logging Maintenance Bac	ckup & Restore A	dmin Access Setti	ngs	L prone
Certificate Management	Usage				
Overview	Certificate(s) will be used for p	xGrid	¥		
System Certificates	Node(s) Generate CSR's for these Nodes:				
Endpoint Certificates	Node		CSR Friendly Name		
Trusted Certificates	✓ pxgrid2	I	pxgrid2 #pxGrid		
OCSP Client Profile	Subject				
Certificate Signing Requests	Common Name (CN)	xgrid2.lab6.com		()	
	Organizational Unit (OU)				
Certificate Authority	Organization (O)				
Internal CA Settings	City (L)				
Certificate Templates	Country (C)				
Edampi CA Sattinga					

9단계 MS CA "pxGrid" 템플릿 요청을 제출하여 pxGrid 노드에 대한 인증서 요청을 지원합니다.

Microsoft Active	Directory Certificate Services – lab6-WIN-BG7GPQ053ID-CA
Submit a Certif	icate Request or Renewal Request
To submit a sav Request box.	ed request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewa
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	SRnquZBuWeIK9a0GnbjskxGB9ByaucLfc3ctd13mLGM O72Brmk12HLsNlxjfrxQeS/HS+7VMF7WoanZitSofV1: 1UNoh05J5FGWG1uvMkNMB0VTnwjD/BgwnzK9JI+44 eztkoliHwHIUP/DUSX5JzfbCQPDW7IekvhKRgFo1u9C Anrg7MmXdFrtWzndPBDC3uVow2FgVLWE END CERTIFICATE REQUEST
Certificate Templa	te:
	pxGrid ÷
Additional Attribu	tes:
Attributes:	
	Submit >

10단계 pxGrid 인증서를 pxGrid 노드 CSR 요청에 바인딩합니다.

Administration-System -> Certificates -> Certificate Signing Requests -> pxGrid 노드 및 bind certificate 선택

oludu cisco Identit	ty Services Engine	A Hom		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	pxgrid2 admin L
•••• System	Anagement Management	Network Resources		the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.	2 pxGrid Identity M
Deployment	Licensing Certificate	Logging Maintenanc		Do you wish to replace the existing certificate?	
Certificate Man	agement	Rind C& Signad Cartific	ato	Yes]
Overview		Bind CA Signed Certific	ate		
System Certificate	25	* Certifica	ate File / Name	Browse pxgrid2.cer	
Endpoint Certifica	ites	Validate Certificate Exte	ensions		
Trusted Certificate	25		Usage	pxGrid: Use certificate for the pxGrid Controller	
OCSP Client Profil	e				
Certificate Signing	g Requests			Submit Cancel	

주 PAN 및 MnT 노드로 pxGrid 노드 퍼블릭/프라이빗 키 내보내기

pxGrid 클라이언트 노드의 퍼블릭/프라이빗 키 쌍은 주 PAN 및 MnT 노드에 복사해야 합니다. 이 단계는 아래에 설명되어 있습니다.

1단계 pxGrid 노드의 시스템 인증서 저장소에서 퍼블릭 및 프라이빗 키를 내보낸 다음, 독립형 모드의 새 설치 환경에서 원하는 주 관리자 노드 및 MnT 노드를 위한 시스템 저장소로 가져옵니다.

참고: 기존 ISE 1.3 구축이 있고 외부 pxGrid 페르소나를 추가할 경우, 주 PAN의 시스템 인증서 저장소에서 pxGrid 노드에 대한 퍼블릭/프라이빗 키 쌍을 내보낸 다음 주 PAN 및 주 MnT로 가져올 수 있습니다.

Administration -> System -> Certificates -> System Certificates를 차례로 누른 다음 인증서를 선택하고 인증서 및 프라이빗 키를 내보냅니다.

프라이빗 키의 이름을 제공해야 합니다(예: cisco123). 이는 PEM 및 PVK(퍼블릭/프라이빗 키 쌍)를 모두 포함하는 압축된 파일로 저장됩니다.

	ahah	License Warning 🔥 pxgrid1
	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
	Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
I	Certificate Management	System Certificates A 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
	System Certificates	Friendly Name Group Tag Used By Issued To Issued By
ł		pxgrid1.lab pxgrid1.lab Export Certificate 'pxgrid1.lab6.com,pxgrid1.lab6.com#lab6-WIN-BG7GPQ053ID-CA#00002'×
	Endpoint Certificates	b6.com#la 053ID-CA# Export Certificate Only
	Trusted Certificates	Export Certificate and Private Key
	OCSP Client Profile	*Private Key Password
	Certificate Signing Requests	*Confirm Password
	Certificate Authority	Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key. Export Cancel

2단계 원하는 주 관리자 노드에서 프라이빗 및 퍼블릭 키를 모두 시스템 인증서 저장소로 가져온 다음 제출합니다.

Administration -> System -> Certificates -> System Certificates를 차례로 누른 다음 pxGrid PEM 및 PVK 인증서를 모두 가져옵니다.

ahah	License Warning 🔥 admin1 admin
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 Mappin
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Tennet Server Certificate
Overview	Anjoir Server Certificate
Sustan Castificator	* Select Node admin1 T
System Cerunicates	* Certificate File Browse pxgrid1lab6compxgrid1lab6co.pem
Endpoint Certificates	* Private Key File Browse pxgrid1lab6compxgrid1lab6co.pvk
Trusted Certificates	Password ••••••
OCSP Client Profile	Friendly Name
	Allow Wildcard Certificates 📃 🛈
Certificate Signing Requests	Allow wildcard is disabled 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 🔲 🛈
Internal CA Settings	Usage
	Admin: Use certificate to authenticate the ISE Admin Portal
Ceruncate rempiates	EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
External CA Settings	pxGrid: Use certificate for the pxGrid Controller
	rotati use lui portati

3단계 원하는 주 MnT 노드에서 퍼블릭 및 프라이빗 키를 모두 시스템 인증서 저장소로 가져온 다음 제출합니다.

Administration -> System -> Certificates -> System Certificates를 차례로 누른 다음 pxGrid PEM 및 PVK 인증서를 모두 가져옵니다.

ahah				License Wa	rning <u>)</u> admin1 admin
cisco Identity Services Engine	🟠 Home Op	perations Policy	▼ Guest Access ▼	Administration 🔻	
System Management	🔛 Network Resources 🛛 🛃 Device	e Portal Management	🔊 pxGrid Services	Feed Service	💵 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore	Admin Access Set	tings	
Certificate Management	Import Server Certificate				
Overview					
System Certificates	* Select Node	mnt1	*		
	* Certificate File	Browse pxgrid1la	b6compxgrid1lab6co.per	n	
Endpoint Certificates	* Private Key File	Browse pxgrid1la	b6compxgrid1lab6co.pvk	C C C C C C C C C C C C C C C C C C C	
Trusted Certificates	Password	•••••			
OCSP Client Profile	Friendly Name			١	
	Allow Wildcard Certificates	i			
Certificate Signing Requests		Allow wildcard is dis not support wildcard sure pxGrid is not c	sabled when pxGrid is sele d certificates. If you want hecked.	ected and vice versa. This to use wildcard with othe	is because pxGrid does er usage type(s), make
Certificate Authority	Validate Certificate Extensions	i			
Internal CA Settings	Usage				
		Admin: Use certific	ate to authenticate the IS	E Admin Portal	
Certificate Templates		EAP Authentication	: Use certificate for EAP p	rotocols that use SSL/TLS	tunneling
External CA Settings		pxGrid: Use certific	ate for the pxGrid Control	ler	
		Portal: Use for port	a		

4단계 주 PAN 및 주 MnT 노드의 시스템 인증서 저장소에 pxGrid 퍼블릭/프라이빗 키가 표시됩니다.

داندان CISCO Identity Services Engine	A Home Or	nerations T Policy T	Guest Arress	License Warnin	ng 🔥 admin1 admin	Logout Feedback 🔎	Satur Ac	reictor
System All Identity Management	Network Resources	ce Portal Management	pxGrid Services	Feed Service	≗∰ pxGrid Identity Mapping	g	Setup As	Sistai
Deployment Licensing Certificates	Logging Maintenance	Backup & Restore Ad	dmin Access Settin	ngs				
Certificate Management	System Certificates A For disast	ter recovery it is recommen	ded to export certificate a	and private key pairs of all	l system certificates.			
Overview	/ Edit Generate Self Signed	Certificate	Export X Del	lete 🔎 View				
	Friendly Name Gro	oup Tag Used By	Issue	ed To 1	Issued By	Valid From	Expiration Date	
System Certificates	▼ admin1							
Endpoint Certificates	admin1.lab6.com,admin1.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00003	fault Portal EAP Authe rtificate Group Portal	entication, Admin, admi	in1.lab6.com	ab6-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	pxgri	rid1.lab6.com	ab6-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	fault Portal EAP Authe rtificate Group Portal	entication, Admin, mnt1	1.lab6.com	ab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	<u>~</u>
Certificate Authority	pxgrid1.lab6.com,pxgrid1.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00004	pxGrid	pxgri	rid1.lab6.com	ab6-WIN-BG7GPQ053ID-C A	Tue, 20 Jan 2015	Fri, 20 Jan 2017	

벌크 세션 다운로드

벌크 세션 다운로드는 pxGrid session_download 스크립트를 사용하여 ISE MnT 노드의 액티브 세션 다운로드 쿼리를 제공합니다. 이렇게 하면 사용 가능한 ISE 상황별 정보에 대한 인증된 802.1X 인증 세션의 사용 가능한 세션 속성이 제공됩니다. MnT 노드의 PEM(Public Key, 퍼블릭 키)은 pxGrid 클라이언트로 복사된 다음, DER로 변환되고 truststoreFilename 키 저장소로 가져오기 됩니다. 나중에 이 내용에 대해서도 다루겠지만, 지금은 아래 설명된 대로 MnT 노드 인증서를 내보내는 방법을 살펴보겠습니다.

<u>참고</u>: pxGrid 액티브 스탠바이 컨피그레이션의 경우, 주 MnT 노드 및 보조 MnT 노드 인증서는 pxGrid 클라이언트로 가져와야 합니다. 이러한 인증서 중 하나가 없을 경우, 클라이언트 등록 시 문제가 발생하며 pxGrid 노드에 연결되지 않습니다.

1단계 원하는 MnT 노드에서 퍼블릭 인증서 키만 내보냅니다. 이는 벌크 세션 다운로드를 위한 pxGrid 클라이언트에서 사용합니다.

Administration -> Certificates -> Certificate Management -> System Certificates를 차례로 누른 다음 MnT ID 인증서를 선택하고 퍼블릭 인증서를 내보냅니다.

cisco Identity Services Engine	👔 Hom	e Operations 🔻	Policy 🔻 Guest Ac	License cess V Administratio	Warning <u>A</u> mnt2 admin	I Logol
System 🦉 Identity Management	Network Resources	Device Portal Man	agement 🛛 🗔 pxGrid S	Services 🔂 Feed S	Service	itity Mappi
Deployment Licensing Certificates	Logging Maintenance	Backup & Re	store Admin Access	Settings		
Certificate Management	System Certificates 🔺 Fo	or disaster recovery i	t is recommended to export	certificate and private ke	ey pairs of all system certificat	es.
Overview	📝 Edit 🛛 🕂 Generate Self	Signed Certificate	Fimport Export	Delete 🔎 Vi	ew	
System Certificates	Friendly Name	Group Tag	Used By	Issued To	Issued By	Vali
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-BG7GPQ053 CA	ID- Fri,
Trusted Certificates	Export Certifi	cate 'mnt2.lab6.o	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			
Certificate Authority	Warning: Exp	orting a private key	is not a secure operation. It	could lead to possible ex	posure of the private key.	
Internal CA Settings	Harning. Co	and g a private hey			Export Cancel	

분산된 환경의 ISE 노드 등록

주 PAN, 주 MnT, PSN, pxGrid에 대한 원하는 독립형 ISE 노드는 주 관리자(PAN) 노드를 통해 등록됩니다. 이러한 단계는 아래와 같이 정의됩니다.

1단계 주 관리 및 주 MnT 페르소나를 처음에 포함하도록 원하는 관리 노드를 설정합니다.



2단계 주 MnT가 될 원하는 MnT 노드를 등록합니다.

<u>참고</u>: 주 PAN은 자동으로 보조 MnT 페르소나가 됩니다. 보조 MnT 페르소나를 비활성화합니다.



3단계 PSN 노드를 등록합니다.

ultulu	License Warning 🔥 admin
cisco identity services Engine	Administration ▼ 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 ISE Node - Step 2: Configure Node
 oge Deployment 	venerar setungs
	Hostname psn1 FQDN psn1.lab6.com IP Address 10.00.046 Node Twe Identity Services Engine (ISE)
	Personas
	Administration Role SECONDARY
	Monitoring Role SECONDARY * Other Monitoring Node
	✓ Policy Service
	Enable Session Services Include Node in Node Group None I
	C Enable Profiling Service

4단계 pxGrid 노드를 등록합니다.

ahaha		License Warning 🧎 admin1 adm	min
cisco Identi	ty Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼	
🙀 System	🚰 Identity Management	🞬 Network Resources 🛃 Device Portal Management 🗔 pxGrid Services 🗔 Feed Service 🕰 pxGrid Identity Ma	apping
Deployment	Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings	
Deployment	ê.	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings Hostname pxgrid1 FQON pxgrid1.lab6.com IP Address 10.0.0.48 Node Type Identity Services Engine (ISE) Personas Administration Role SECONDARY Other Monitoring Node Policy Service Enable Session Services Include Node in Node Group None Include Node in Node Group None	
		V pxGrid 0	

5단계 pxGrid 서비스가 시작되었고 게시된 ISE 기능을 보유하고 있는지 확인합니다. Administration -> pxGrid Services를 누르고 Auto Registration도 활성화합니다.

,	սիսի										License Wa	rning 🔔 admin1	I admin I L	Logout
	cisco	Identi	y Services Eng	gine		۵	Home Oper	rations 🔻	Policy V	Guest Access	Administration 🛛 🔻			
	🔆 Sy	stem	A Identity Mana	agement	Networl	k Resources	🛃 Device	Portal Manag	ement	🔊 pxGrid Services	Feed Service	💵 pxGrid Ide	ntity Mapping	
														6
'n	Client	s Liv	e Loa											
	2 Enabl	e 🔗 Disa	ble Approve	Group	Decline	🕜 Delete 🔻	Refresh	Total Pendi	ng Approval(0) 🔻			1 - 3 of 3	Sh
		Client Nam	2	Clier	t Description	0	Capabilitie	s	5 11 1	Status	Client	Group	Log	J
C	•	ise-admin-a	dmin1				Capabilitie	s(2 Pub, 1 Su	ıb)	Online	Admini	strator	Vie	w
C	•	ise-admin-r	nnt1				Capabilitie	s(1 Pub, 0 Su	ub)	Online	Admini	strator	Vie	w
C		ise-mnt-mr	t1				Capabilities	s(2 Pub, 0 Su	ub)	Online	Admini	strator	Vie	w

pxGrid 클라이언트 관리

pxGrid Serivce 메뉴에서는 클라이언트 관리, 클라이언트 등록/삭제, Auto-Registration이 비활성화된 경우 클라이언트의 "보류" 요청 권한을 제공합니다. 또한 이 메뉴에서는 클라이언트의 등록된 기능 또는 정보 항목에 대한 로그 기록 뷰를 제공합니다.

ahaha						License Warning 🔒 pa	in1 admin Logout Feedback	Q
cisco Identity Ser	vices Engine	企	Home Opera	tions 🔻 Policy	▼ Guest Access ▼	Administration 🔹		Setup Assistant -
🔆 System 🛛 🕺 Ide	entity Management	Network Resources	🛃 Device P	ortal Management	DxGrid Services	Feed Service	pxGrid Identity Mapping	
Clients Live Log							Enable Auto	D-Registration Disable Auto-Registration View By Capabilitie
Senable 🕜 Disable	Approve 😝 Group	👎 Decline 🛛 🛞 Delete 👻	🛞 Refresh	Total Pending Approv	val(0) *		1 - 5 of 5 Show 25 💌	per page Page 1 🗍 of 1
Client Name	Client	Description	Capabilities		Status	Client Group	Log	
□ ▶ ise-admin-pan1			Capabilities	(2 Pub, 1 Sub)	Online	Administrator	View	
□ ▶ ise-mnt-mnt1			Capabilities	(2 Pub, 0 Sub)	Online	Administrator	View	
□ ▶ ise-admin-mnt1			Capabilities	(0 Pub, 0 Sub)	Online	Administrator	View	
wsa2.lab6.com-tes	t_client pxGrid	d Connection from WSA	Capabilities	(0 Pub, 0 Sub)	Offline	Session	View	
wsa2.lab6.com-pxg	grid_client pxGrid	d Connection from WSA	Capabilities	(0 Pub, 0 Sub)	Offline	Session	View	

Enable Auto-Registration - 자동 등록을 활성화하며, 최초 pxGrid 클라이언트 인증이 완료된 후 pxGrid 클라이언트를 자동으로 등록합니다.

Disable Auto-Registration - 자동 등록을 비활성화하며, 관리자가 pxGrid 클라이언트를 적절한 "세션" 또는 "EPS" 그룹으로 이동하기 전까지 해당 클라이언트는 "보류" 상태로 유지됩니다.

Client Groups - 클라이언트 그룹이 기본적으로 pxGrid 작업의 "세션" 그룹에 등록됩니다.

Administrator - ISE에 대해 예약됩니다.

Session - 세션 속성 정보에 액세스합니다.

EPS - "세션" 그룹의 상위 집합으로, ANC(Adaptive Network Control) 완화에 사용됩니다.

Live Log - 클라이언트 등록 및 항목 설명에 대한 기록이 표시됩니다.

보안 액세스 방법 가이드



ahaha					License Warning 🛕 I	pan1 admin Logout
cisco Identit	y Services Er	ngine	☆ Home Operations ▼	Policy Guest Access	Administration •	
🔆 System	🕂 Identity Ma	nagement 🛛 🔛 Network Resource	es 🛛 🛃 Device Portal Manag	gement 🛛 😡 pxGrid Services	Feed Service	💵 pxGrid Identity Mapp
Clients	e Log					
😢 Clear Logs 🛛 🗑 🖡	Resync 🛛 🛞 Re	fresh				1 - 25 of 2104 Sho
Client Name		Capability Name	Event Type	Timestamp	Other Attributes	
ise-admin-pan1@xgr	rid.cisco.com	GridControllerAdminServiceCapab	Client subscribed	7:49:49 PM EST, Apr 17 2015		
			Resync database	7:49:49 PM EST, Apr 17 2015		
ise-admin-mnt1@xg	rid.cisco.com		Client online	3:13:34 PM EST, Apr 16 2015		
ise-admin-mnt1@xgi	rid.cisco.com		Client deleted	3:13:33 PM EST, Apr 16 2015		
			Resync database	3:13:29 PM EST, Apr 16 2015		
ise-admin-mnt1@xg	rid.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	l.cisco.com	SessionDirectoryCapability-1.0	Publisher added	3:07:34 PM EST, Apr 16 2015		
ise-mnt-mnt1@xgrid	l.cisco.com	IdentityGroupCapability-1.0	Publisher added	3:07:33 PM EST, Apr 16 2015		
ise-mnt-mnt1@xgrid	l.cisco.com		Client online	3:07:33 PM EST, Apr 16 2015		
ise-mnt-mnt1@xgrid	l.cisco.com		Client deleted	3:07:31 PM EST, Apr 16 2015		
ise-mnt-mnt1@xgrid	l.cisco.com	SessionDirectoryCapability-1.0	Publisher deleted	3:07:31 PM EST, Apr 16 2015		
ise-mnt-mnt1@xgrid	l.cisco.com	IdentityGroupCapability-1.0	Publisher deleted	3:07:19 PM EST, Apr 16 2015		
ise-admin-pan1@xgr	rid.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-pxgri	id_client@xg	SessionDirectoryCapability-1.0	Client subscribed	8:17:37 PM EST, Apr 15 2015		
wsa2.lab6.com-pxgri	id_client@xg	TrustSecMetaDataCapability-1.0	Client subscribed	8:17:37 PM EST, Apr 15 2015		

pxGrid 클라이언트 컨피그레이션

이 섹션에서는 pxGrid 샘플 스크립트 테스트를 위한 pxGrid Java SDK 설치에 대해 다룹니다. Register.sh는 연결을 수행하고 pxGrid 컨트롤러와의 연결을 설정하기 위해 실행됩니다. Session_download.sh는 ISE에서 액티브 세션 레코드를 다운로드하기 위해 실행됩니다. 이러한 스크립트는 작동 중인 pxGrid 클라이언트와 ISE 간의 연결 및 커뮤니케이션을 확인하기 위한 기본 테스트에 사용됩니다. 이전에는 엔드포인트 보호 서비스(EPS)로 알려진 ANC(Adaptive Network Control) 완화 작업을 비롯한 모든 셸 스크립트를 테스트하려는 경우 다음(<u>http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-</u> <u>Configure_and_Test_Integration_with_Cisco_pxGrid.pdf</u>)을 참조하십시오.

pxGrid Java SDK 설치

pxGrid Java SDK 라이브러리를 가져오려면 Cisco 어카운트 팀에 문의하십시오.

해당 Linux 운영 체제에 맞는 Oracle Java Development Kit 다운로드: <u>http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html</u>

Oracle Java Development Kit를 설치하려면 시스템에 있는 이전 버전의 Java를 제거해야 합니다.

<u>참고:</u> 테스트에 MAC을 사용할 경우 Java 제거 시 <u>https://www.java.com/en/download/help/mac_uninstall_java.xml</u> 을 참조하십시오.Centos 6.5를 사용할 경우, 부록의 Centos 6.5에서 Java 제거 및 JDK 8.0 설치를 참조하십시오.

폴더의 tar를 해제합니다. tar -zxf pxgrid-sdk-x.x.x-dist.tar.gz

다음이 표시됩니다.

- Lib 모든 GCL 라이브러리가 포함됩니다.
- Samples bin, certs, conf, lib, src 디렉토리가 포함됩니다.
- Bin 모든 샘플 스크립트가 포함됩니다.
- Certs 모든 샘플 pxGrid ID 및 rootSample 인증서가 포함됩니다.
- Src 모든 Java 소스 파일이 포함됩니다.

pxGrid 샘플 스크립트를 실행하려면 "JAVA_HOME=" 환경 변수에 jre 경로를 포함합니다.

MAC의 예는 아래에 나와 있습니다.

jre 경로의 위치를 보려면 다음을 실행합니다.

<u>참고</u>: sudo를 실행할 경우 루트 권한이 필요합니다.

```
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
```

"Library/Java/JavaVirtualMachines/jdk1.8.0_25.jdk/Contents/Home/jre" 경로를 JAVA_HOME에 추가합니다.

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

Centos 64 같은 다른 버전의 Linux를 사용할 경우, 경로에 "keytool"이 포함되었는지 확인합니다.

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 클라이언트 SDK Java Keystore 소개

Java keystore에는 CA 루트 인증서, 호스트 ID 또는 pxGrid 클라이언트 인증서, 자체 서명 인증서 같은 인증서의 퍼블릭/프라이빗 키 쌍이 포함되어 있습니다. Java Keystore 자체는 PKCS #12 형식(.JKS)입니다.

인증서 자체는 PEM 또는 CER 형식이며, DER로 변환되고 Java Keystore로 가져오기 됩니다.

이 문서에서는 CA 서명 pxGrid 클라이언트 인증서 및 CA 서명 ISE 인증서를 사용합니다.

pxGrid의 경우 pxGrid 클라이언트 ID 인증서가 포함된 keystoreFilename 및 CA 루트 인증서, MnT 노드 인증서를 나타내는 truststoreFilename 키 저장소가 있습니다.

키 저장소에 인증서를 가져올 경우 이러한 키 저장소 값 외에도 관련 비밀번호, keystorePassword 및 truststorePassword가 포함됩니다.

keystoreFilename, keystorePassword, truststoreFilename, truststorePassword는 SASL 인증 및 pxGrid SDK 페르소나에 연결하기 위한 용도로 pxGrid SDK 스크립트에서 사용 중입니다.

아래에 설명된 예에서, pxGrid 클라이언트가 등록되고 pxGrid 컨트롤러에 연결됩니다.

./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

아래에 설명된 예에서, pxGrid는 클라이언트는 MnT 노드에서 액티브 세션 레코드를 다운로드합니다.

./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 클라이언트 인증서 컨피그레이션

다음 절차에서는 pxGrid 클라이언트에 대한 키를 생성하고, CSR 요청을 생성하고, 인증서를 가져와 DER로 변환하여 키 저장소에 추가하는 단계를 설명합니다.

<u>참고</u>: pxGrid 클라이언트 컨피그레이션에서는 CA 서명 pxGrid 클라이언트 및 CA 서명 pxGrid 노드 인증서를 보유하게 됩니다. 인증서 배포에 대한 기타 고려 사항은 참조 자료를 살펴보십시오.

해당 프로세스는 아래에 설명되어 있습니다.

- 프라이빗 키는 pxGrid 클라이언트에 생성됩니다.
- CSR(Certificate Signing Request)은 프라이빗 키에서 생성됩니다. 챌린지 키는 나중에 키 저장소 관리에 사용됩니다.
- CA 인증기관에서는 이전에 정의된 대로 유효한 pxGrid 템플릿으로 CSR 요청을 서명합니다.
- PKCS#12 파일은 퍼블릭/프라이빗 키 쌍 및 루트 인증서에서 생성됩니다. 이는 keystoreFilename(JKS) 및 truststoreFilename(JKS)의 키 저장소 생성에 사용됩니다.
- keystoreFilename(JKS)가 생성됩니다.
- truststoreFilename(JKS)가 생성됩니다.

보안 액세스 방법 가이드

- 액티브 세션 레코드 또는 벌크 다운로드 세션에 사용된 ISE MnT 주 노드 및 ISE MnT 보조 노드에서 ISE ID 인증서를 가져옵니다.
- ISE ID 인증서 PEM 파일을 DER 형식으로 변환하고 CA 루트 인증서와 함께 truststorefileName 키 저장소에 추가합니다.
- pxGrid 클라이언트 인증서를 keystoreFilename(JKS)로 가져옵니다.
- CA 루트 인증서를tuststoreFilename(JKS)로 가져옵니다.
- 두 파일을 모두 pxGrid "../samples/bin/.. " 폴더에 복사하고 스크립트를 실행합니다.

1단계 프라이빗 키 생성

pxGrid 클라이언트의 프라이빗 키(예: mac.key)를 생성합니다.

<u>참고</u>: 이러한 .key 이름은 어떠한 이름이든 가능하나, 여기에서는 mac.key로 명명합니다.

1단계 CSR 요청 생성 CA 인증기관에 대한 CSR 요청(예: mac.csr)을 생성합니다. 챌린지 비밀번호(예: cisco123)를 제공합니다.

<u>참고</u>: .csr은 어떠한 이름이든 가능하나, 여기에서는 통일성을 위해 mac.csr로 명명합니다. 챌린지 비밀번호 또한 어떠한 이름이든 가능합니다.

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 the same password throughout this documnent, easier to maintain, and cut down on errors

2단계 CA 인증기관이 pxGrid CSR 요청에 서명

CA 인증기관은 클라이언트 인증 및 서버 인증을 위한 EKU가 모두 포함된 pxGrid 템플릿을 사용하여 사용자 인증서를 지원해야 합니다.

<u>참고</u>: Windows 2003의 CA 템플릿이 선택되었으므로, 이는 드롭다운 목록에 표시됩니다. 사용자 템플릿은 클라이언트 및 서버 인증을 위한 EKU를 모두 포함하여 이중화되었습니다.



3단계 PKCS12 파일 생성

pxGrid 클라이언트 인증서(예: mac.cer)의 프라이빗 키에서 pxGrid 클라이언트 pkcs12 파일(mac.p12)을 생성합니다. 이는 키 저장소 관리에 사용되며 확장자가 .p12인 임의의 파일 이름일 수 있습니다. CA 루트 파일(예: root2a)을 포함합니다.

openssl pkcsl2 -export -out mac.pl2 -inkey mac.key -in mac.cer -chain -CAfile root2a.cer Enter Export Password: ciscol23 Verifying - Enter Export Password: ciscol23

4단계 pxGrid 클라이언트의 keystoreFilename 생성

pxGrid 클라이언트 ID 키 저장소(예: mac.jks)를 생성합니다. 이는 pxGrid 클라이언트 ID 키 저장소가 됩니다. 이는 확장자가 .jks인 임의의 파일 이름일 수 있습니다. 이는 pxGrid 스크립트 예에서 keystoreFilename 및 관련 keystorePassword 역할을 수행합니다.

```
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
```

5단계 ISE MnT 주 노드 및 ISE MnT 보조 노드에서 퍼블릭 ISE ID 인증서 내보내기

퍼블릭 ISE ID 인증서만 pxGrid 클라이언트로 내보내며, 이는 .pem 형식으로 이루어집니다. 확장자가 .pem인 파일의 이름을 더 읽기 쉽게 변경할 수 있습니다. 이 예에서 파일의 이름은 mnt1.pem로 변경되었습니다.

<u>참고</u>: pxGrid 액티브-스탠바이가 구성된 경우, ISE pxGrid 클라이언트에는 MnT 주 노드 및 ISE MnT 보조 노드가 모두 필요합니다.



6단계 ISE ID MnT 노드의 PEM 형식을 DER 형식으로 변환

openssl x509 -outform der -in mntl.pem -out mntl.der

7단계 ISE MnT DER 파일을 truststoreFilename에 추가

ISE ID 인증서를 신뢰 키 저장소(예: caroot1.jks)에 추가하면 이는 신뢰할 수 있는 키 저장소가 됩니다. 이는 확장자가 .jks인 임의의 파일 이름일 수 있습니다. 이는 pxGrid 스크립트에 사용된 truststoreFilename 및 truststorePassword가 됩니다.

```
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.....
                                                        ..0...*.н.....
0010: 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....
#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...+.
```

cisco.

```
0020: 01 05 05 07 03 04 30 OC
                               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 [
  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 [
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
                                                        . . . .
1
1
Trust this certificate? [no]: yes
Certificate was added to keystroke
```

8단계 pxGrid 클라이언트를 keystoreFilename로 가져오기 pxGrid 클라이언트 인증서를 ID 키 저장소로 가져옵니다.

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

Note: If you receive the following message the certificate was already added to a pre-existing keystore, you can say "no" and still be okay. I selected "yes" so we can verify thay the certificate was added later on.

9단계 CA 루트 인증서를 truststoreFilename에 추가

CA 루트 인증서를 신뢰할 수 있는 키 저장소에 추가합니다. CA 루트 인증서도 신뢰할 수 있어야 합니다.

```
keytool -import -alias ca root1 -keystore caroot1.jks -file root2a.cer
Enter keystore password: cisco123
Owner: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 448a6d6486c91cb14c6888c127d16c4e
Valid from: Thu Nov 13 20:47:06 EST 2014 until: Wed Nov 13 20:57:06 EST 2019
Certificate fingerprints:
        MD5: 41:10:8A:F5:36:76:79:9C:2C:00:03:47:55:F8:CF:7B
        SHA1: 9D:DA:06:AF:06:3F:8F:5E:84:C7:F4:58:50:95:03:22:64:48:96:9F
        SHA256:
DB:28:50:D6:47:CA:C0:6A:E9:7B:87:B4:0E:9C:3A:C1:A2:61:EA:D1:29:8B:45:B4:76:4B:DA:2A:F1:D8:E0:A3
        Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
  Key CertSign
 Crl_Sign
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06
                                                         ...&..7..Z.6&...
0010: 6A C8 79 2C
                                                         j.у,
```

1

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

10단계 ID 키 저장소(mac.jks) 및 신뢰 키 저장소(caroot1.jks)를 pxGrid "../samples/bin/.." 폴더에 복사합니다.

pxGrid 클라이언트 액티브-스탠바이 예

pxGrid 액티브-스탠바이의 경우, 주 MnT 및 보조 MnT 퍼블릭 인증서(PEM)를 모두 pxGrid 클라이언트로 내보낸 다음 이를 모두 DER로 변환해야 합니다. 두 인증서는 모두 CA 루트 인증서(root2a.cer)와 함께 truststoreFilename 키 저장소에 추가해야 합니다.

```
Johns-Macbook-Pro:mntnodes jeppich$ openssl x509 -outform der -in mnt1.pem -out mnt1.der
Johns-Macbook-Pro:mntnodes jeppich$ keytool -import -alias lab1 -keystore caroot1.jks -file mnt1.der
Enter keystore password:
Re-enter new password:
Owner: CN=mnt1.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61326a1800000000031
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...*.н.....
                                 48 86 F7 0D 03 04 02 02 ...0...*.H.....
0010: 00 80 30 0E 06 08 2A 86
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
                                                           .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
0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82
                                                           ..+....0...+.
                                                           . . . . . . 0 . . . + . . . .
                                                           7...
0030: 37 OA 03 04
#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....
                                 86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0010: 87 CB EB 79 81 89 9D 2D
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
```

```
cisco.
```

```
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
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
#2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  Γ
   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
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.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
]
#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 [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 i.v, 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 KeyUsage [DigitalSignature Key Encipherment #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 ****** 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
 0.0...*.H......

 0020:
 00
 80
 30
 07
 06
 05
 2B
 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 . . . + 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...

 ^...#...@..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 #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 ... &... Z.6 &... 0010: 6A C8 79 2C j.у, 1 #6: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [

보안 액세스 방법 가이드



```
[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
#9: ObjectId: 2.5.29.15 Criticality=true
KevUsage [
 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
******************
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
```

보안 액세스 방법 가이드

Certificate was added to keystore

1

cisco.

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
 Key_CertSign
 Crl_Sign
]
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&...
0010: 6A C8 79 2C j.y,
]
Trust this certificate? [no]: yes

ISE 분산 환경에서 pxGrid 클라이언트 테스트

pxGrid 스크립트인 register.sh 및 session download.sh는 pxGrid 클라이언트 연결 및 pxGrid 등록을 확인하기 위해 실행됩니다. 세션 다운로드는 ISE MNT 인증서 및 pxGrid 클라이언트에 문제가 없는지 확인합니다.

1단계 pxGrid 클라이언트 등록

Johns-Macbook-Pro:bin jeppich\$./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 - truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 -username mac1 -group Session
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\$

pxGrid 클라이언트가 pxGrid 컨트롤러에 등록되었는지 확인합니다.

Administration -> pxGrid Services

ahaha				License Warning 🛕	admin1 admin Logou
cisco Identity Services Engine	🔒 Hom	e Operations	▼ Guest Access ▼	Administration 🛛 🔻	
🐝 System 🛛 👰 Identity Management	Network Resources	🛃 Device Portal Management	DxGrid Services	Feed Service	Grid Identity Mapping
Clients Live Log					
🖌 Enable 🖉 Disable 😪 Approve 😝 Group	👎 Decline 🛛 🐼 Delete 👻 🥳	Refresh Total Pending Approva	al(0) 👻		1 - 4 of 4 Sh
Client Name Client	Description	Capabilities	Status	Client Group	Log
ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□ ► ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□ ▶ ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
mac1		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

2단계 세션 다운로드 실행

```
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=0A0000020000000020814C0, 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
```

키 저장소 항목 보기

키 저장소 항목을 확인하여 keystoreFilename 및 truststoreFilename 키 저장소의 신뢰할 수 있는 인증서 항목을 볼 수 있습니다.

1단계 truststoreFilename 키 저장소인 caroot1.jks를 확인합니다.

```
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:CO: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:
```

```
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
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 [
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
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
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.у,
```

] 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
#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
  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: 61326a1800000000031
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 ....+....0....*
0030: 86 48 86 F7 0D 03 07
                                                      . H . . . . .
#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A
                                                      020...+....0.
0010: 06 08 2B 06 01 05 05 07
                              03 02 30 0A 06 08 2B 06 ..+....0...+.
0020: 01 05 05 07 03 04 30 OC
                              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.... ...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 ^...#...@..d... 40 02 01 64 02 01 03 #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [I 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.y, 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: 2.5.29.17 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:bin jeppich\$

2단계 keystoreFilename 키 저장소인 mac.jks를 확인합니다.

```
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
Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.....
0010: 00 80 30 0E 06 08 2A 86
                              48 86 F7 0D 03 04 02 02 ...0...*.H.....
0020: 00 80 30 07 06 05 2B 0E
                              03 02 07 30 0A 06 08 2A
                                                       ..0...+...0...*
0030: 86 48 86 F7 0D 03 07
                                                       .H....
#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+....0.
0010: 06 08 2B 06 01 05 05 07
                             03 02 30 UA 00 00 ___
06 0A 2B 06 01 04 01 82
                              03 02 30 0A 06 08 2B 06 ..+....0...+.
0020: 01 05 05 07 03 04 30 OC
                                                       ....+....
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 55 66 -_
40 02 01 64 02 01 03
                              86 E6 FC 53 86 82 A1 38 ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF
                                                       ^...#...@..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
```

보안 액세스 방법 가이드

```
cisco.
```

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

보안 액세스 방법 가이드



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 j.y, 1 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
 0000:
 30
 32
 30
 0A
 06
 08
 2B
 06
 01
 05
 07
 03
 01
 30
 0A

 0010:
 06
 08
 2B
 06
 01
 05
 07
 03
 01
 30
 0A

 0010:
 06
 08
 2B
 06
 01
 05
 07
 03
 02
 30
 0A
 06
 08
 2B
 06
 020...+....0. ..+....0...+. 0020: 01 05 05 07 03 04 30 0C 06 0A 2B 06 01 04 01 82 7... 0030: 37 0A 03 04 #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 [Ι 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 &...

Cisco Systems © 2015

```
cisco.
```

```
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: 2.5.29.14 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$
```

pxGrid 액티브-스탠바이로 ISE 분산 배포 소개

이 섹션에서는 pxGrid 액티브-스탠바이에 대해 다룹니다. ISE 분산 배포의 경우, 2가지 pxGrid 전용 노드가 가능합니다. 하나는 pxGrid 클라이언트 연결을 처리하여 pxGrid 서비스를 제어하기 위한 것이고, 다른 하나는 장애 조치용입니다. pxGrid 노드는 한 번에 하나씩 액티브 상태가 될 수 있습니다.

pxGrid 액티브-스탠바이가 포함된 ISE 분산 배포는 주 관리 노드, 보조 관리 노드, 주 MnT 노드, 보조 MnT 노드, PSN 두 개, 별도의 pxGrid 페르소나 2개로 구성됩니다.

여기에서는 보조 관리 노드, 보조 MnT 노드, 보조 pxGrid 노드를 추가하여 pxGrid 액티브-스탠바이 컨피그레이션을 생성합니다.

퍼블릭/프라이빗 키를 첫 번째 또는 주 pxGrid 페르소나에서 주 관리 및 주 MnT 노드 시스템 인증서 저장소로 내보냅니다.

참고: 이는 최초 ISE 분산 배포의 한 부분으로 이미 구성되었습니다.

퍼블릭/프라이빗 키를 두 번째 또는 보조 pxGrid 페르소나에서 보조 관리 및 보조 MnT 노드 시스템 인증서 저장소로 내보냅니다.

벌크 액티브 세션 다운로드를 위해 주 및 보조 MnT ID 인증서를 pxGrid 클라이언트로 내보냅니다. 이러한 인증서 중 하나가 없는 경우, pxGrid 클라이언트 레지스터가 표시되지 않을 수 있습니다.

등록된 클라이언트 어카운트, 서브스크립션, 항목 등이 PAN을 통해 pxGrid 서버 간에 액티브-액티브 동기화됩니다. 주 및 보조 pxGrid 노드는 액티브-스탠바이입니다.

pxGrid 클라이언트는 주 PxGrid 노드에 연결됩니다. 주 pxGrid 노드가 중단된 경우, 클라이언트는 보조 pxGrid 노드에 연결되며 모든 등록된 클라이언트 및 트랜잭션은 그대로 유지됩니다. 이에 대한 내용은 본 문서에서 설명합니다.

pxGrid Active-Standby Configuration



분산 환경 pxGrid 액티브-스탠바이에 ISE 노드 등록

지금부터는 보조 노드를 등록합니다.

1단계 보조 pxGrid 노드의 퍼블릭/프라이빗 키 쌍을 보조 PAN으로 가져옵니다. Administration -> System -> Certificate -> Certificate Management -> System Certificates를 차례로 누른 다음 보조 pxGrid 노드의 퍼블릭/프라이빗 키를 가져옵니다.

참고: 이러한 작업은 모든 노드가 독립형일 때 완료할 수 있습니다. 또한 이는 주 PAN에서 직접 수행할 수도 있습니다. 이 과정에서는 보조 pxGrid 노드에서 퍼블릭/프라이빗 키 쌍을 가져온 것으로 가정합니다.

ahah	License Warning jj. 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 Mapping
Deployment Licensing Certificate	s Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	
Overview	Import Server Certificate
	* Select Node admin2
System Certificates	Certificate File Browse pxgrid2lab6compxgrid2lab6co.pem
Endpoint Certificates	* Private Key File Browse pxgrid2lab6compxgrid2lab6co.pvk
Trusted Certificates	Password
OCSP Client Profile	Friendly Name (1)
	Allow Wildcard Certificates 🔲 🛈
Certificate Signing Requests	Allow wildcard is disabled 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 🗌 (i)
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

2단계 보조 pxGrid 노드의 퍼블릭/프라이빗 키 쌍을 보조 PAN으로 가져옵니다. Administration -> System -> Certificate -> Certificate Management -> System Certificates를 차례로 누른 다음 보조 pxGrid 노드의 퍼블릭/프라이빗 키를 가져옵니다.

Isco Identity Services Engine	Home Operations Policy Guest Access Administration Administration
🔅 System 🦉 Identity Management	📰 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🗔 Feed Service 💵 pxGrid Identit
Deployment Licensing Certific	es Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	
Overview	Import Server Certificate
System Certificates	* Select Node mnt2
	Certificate File Browse pxgrid2lab6compxgrid2lab6co.pem
Endpoint Certificates	* Private Key File pxgrid2lab6compxgrid2lab6co.pvk
Trusted Certificates	Password ••••••
OCSP Client Profile	Friendly Name
	Allow Wildcard Certificates 📃 🛞
Certificate Signing Requests	Whow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid do 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 🔲 🕖
Internal CA Settings	Usage
Certificate Templates	Admin: Use certificate to authenocate the ISE Admin Portal
	PAP Authentication: Use certificate for EAP protocols that use SSL/TLS turneling
External CA Settings	pacing, use cerunicate for the pacing controller

3단계 퍼블릭/프라이빗 키 쌍을 ISE 보조 PAN 및 ISE 보조 MnT 노드에 올바르게 가져와야 합니다. Administration -> System -> Certificates -> Certificate Management -> System Certificates

A A A A A A A A A A A A A A A A A A A			License Warning 🔥 ad	min1 admin Logout Feedback 🔎)
cisco raciaty services Englic	Home Operations 🔻	Policy V Guest Access V	Administration V		Setup Assista
💀 System 🏾 👰 Identity Management	Network Resources 🛛 🛃 Device Portal Manag	gement 😡 pxGrid Services	Feed Service	Identity Mapping	
Deployment Licensing Certificates	Logging Maintenance Backup & Rest	ore Admin Access Setting	gs		
Certificate Management	System Certificates A For disaster recovery it i	s recommended to export certificate a	Ind private key pairs of all system cer	tificates.	
Overview	Friendly Name Group Tag	Used By Issue	d To Issued By	Valid From	Expiration Date
System Certificates	▼ admin2				
Endpoint Certificates	admin2.lab6.com,admin2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00001 Default Portal Certificate Group	EAP Authentication, Admin, admir Portal	n2.lab6.com lab6-WIN-BC A	G7GPQ053ID-C Wed, 4 Mar 2015	Fri, 3 Mar 2017 🛛 🗹
Trusted Certificates	pxgrid2.lab6.com,pxgrid2.la b6.com#lab6-WIN-BG7GPQ 053ID-CA#00002	pxGrid pxgrid	d2.lab6.com A	G7GPQ053ID-C Wed, 4 Mar 2015	Sat, 4 Mar 2017 🛛 🗹
	▼ mnt2				
Internal CA Settings	mnt2.lab6.com,mnt2.lab6.c om#lab6-WIN-BG7GPQ053I Certificate	rtal EAP Authentication, Adm Group Portal	in, mnt2.lab6.com	lab6-WIN-BG7GPQ053ID-C Wed, 4 M	ar 2015 Fri, 3 Ma
Certificate Templates	D-CA#00001 pxgrid2.lab6.com,pxgrid2.la b6.com#lab6-WIN-BG7GPQ	pxGrid	pxgrid2.lab6.com	lab6-WIN-BG7GPQ053ID-C A Wed, 4 M	ar 2015 Sat, 4 Ma

4단계 주 관리 노드를 통해 보조 주 관리 노드를 등록합니다.

Administration -> System -> Deployment를 차례로 누른 다음 ISE 노드를 보조 관리 노드로 등록합니다.

Cisco Identity Services Engine Policy Policy Guest Access Administration Image: Circle of Circl	aluða	License Warning 🚠 admin
System	CISCO Identity Services Engine	Home Operations Policy Guest Access Administration Administration
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings Deployment Deployment Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node Register ISE Node - Step 2: Configure Node Image: Straight and the strai	System 21 Identity Management	🞬 Network Resources 🔄 Device Portal Management 🗔 pxGrid Services 🗔 Feed Service 💵 pxGrid Identity Mapping
Deployment Image: Second and the second and th	Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Enable Session Services Include Node in Node Group None Vone Include Profiling Service	Deployment ↓ ↓ E. ↓ @.↓ Deployment	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings Hostname admin2 FQDN admin2.lab6.com JP Address 10.0.042 Node Type Identity Services Engine (ISE) Personas Administration Role SECONDARY Monitoring Role SECONDARY Enable Session Services Include Node in Node Group None Include Node in Node Group None

5단계 주 관리 노드를 통해 보조 모니터링 노드를 등록합니다. Administration -> System -> Deployment를 차례로 누른 다음 ISE 노드를 보조 모니터링 노드로 등록합니다.

ahah	License Warning 👔 admin
CISCO Identity Services Engine	Home Operations Policy Guest Access Administration Administration
System Alentity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🖓 Feed Service 💵 x儲 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment	Deployment Nodes List > Configure Node Register ISE Node - Step 2: Configure Node General Settings Hostname mnt2 FNXN mnt2.lab6.com IP Address 10.0.0.45 Node Type Identity Services Engine (ISE) Personas Administration Role SECONDARY Ø Monitoring Role SECONDARY Other Monitoring Node Include Node in Node Group Include Node in Node Group None Include Node in Node Group Include Node in Node Group Include Node in Node Group Include Node in Node Group

참고: 보조 MnT 노드가 도메인에 결합되지 않은 경우, pxGrid 노드에 연결되지 않으므로 보조 MnT가 도메인에 결합되었는지 확인하고 외부 ID 서비스를 점검합니다.

6단계 보조 pxGrid 노드를 추가합니다.

Administration -> System -> Deployment를 차례로 누른 다음 ISE 노드를 보조 pxGrid 노드로 등록합니다.

ahah								Lie	icense Warning 🔒 admin1 admin
cisco Identi	ty Services Er	ngine		🛕 Home	Operations •	Policy V	Guest Access	 Administration 	
System	🚰 Identity Ma	nagement	Network Re	sources 🛃	Device Portal Mana	gement	😡 pxGrid Servic	es 🛛 🔂 Feed Se	ervice
Deployment	Licensing	Certificates	Logging	Maintenance	Backup & Res	tore A	Admin Access	Settings	
Deployment	t	£23-₹	Deployment Edit Nod Genera	Nodes List > pxgrid e I Settings	d2			k	
			Persona	Hostnam FQD IP Addres Node Typ s nistration xoring	ne pxgrid2 N pxgrid2.lab6.cc 55 10.0.0.49 Ne Identity Servic	om es Engine (Role SECONI Role PRIM.	ISE) DARY	Other Monitoring N	lode
			: Policy v pxGric	Service Enable Session Inclue Enable Profiling	Services I de Node in Node Gr g Service	oup None		v ()	

7단계 pxGrid 서비스가 시작되었고 게시된 ISE 노드가 표시되는지 확인합니다. Administration -> pxGrid Services

البيالي								License Warn	ing 🕂 admin2 admin Logout
CISCO	o Identity Services	Engine		۵	Home Opera	ations V Policy V	Guest Access	Administration 🛛 🔻	
💑 S	ystem 🛛 💆 Identity M	Management	Network	Resources	🛃 Device P	Portal Management	😡 pxGrid Services	Feed Service	≗∰ pxGrid Identity Mapping
									θ
Client	tra Live Log								
4 Enab		0.0	Decline	Obelete	C Defrech	Total Bonding Approval(0)			1 - 10 of 10 - Cho
V Enab	ne 🖉 Disable 💟 Appi	ove 😝 Group	- Decline	💽 Delete 👻		Iotal Pending Approval(0)	•		1 - 10 0F 10 SHO
	Client Name	Client	Description		Capabilities	5	Status	Client Gr	oup Log
	ise-admin-admin2				Capabilities	(2 Pub, 1 Sub)	Online	Administ	rator View
	ise-admin-mnt2				Capabilities	(1 Pub, 0 Sub)	Online	Administ	rator View
	ise-admin-mnt1				Capabilities	(1 Pub, 0 Sub)	Online	Administ	rator View
	ise-mnt-mnt1				Capabilities	(2 Pub, 0 Sub)	Online	Administ	rator View
	ise-mnt-mnt2				Capabilities	(2 Pub, 0 Sub)	Online	Administ	rator 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

ISE 분산 환경 pxGrid 액티브-스탠바이 모드에서 pxGrid 클라이언트 테스트

이 섹션에서는 보조 PAN, 보조 MnT, 보조 pxGrid 노드를 추가하여 pxGrid-스탠바이 컨피그레이션에 대해 설명합니다. 또한 다음을 통해 컨피그레이션을 테스트합니다.

기본 작업:

• pxGrid 클라이언트를 주 pxGrid 노드에 추가

<u>참고</u>: pxGrid 액티브-스탠바이 컨피그레이션의 경우, 주 pxGrid 노드만 액티브 상태가 될 수 있으며, 보조 pxGrid 노드는 pxGrid 보조 노드에 "sh application status ise"로 표시된 것처럼 "실행되지 않습니다".

- MnT 주 노드에서 액티브 세션 레코드 다운로드
- ISE의 등록된 pxGrid 클라이언트 상태 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시

보조 pxGrid 노드에 대한 pxGrid 노드 장애 조치 테스트

- 주 pxGrid 노드의 "application stop ise"로 중단된 pxGrid 노드 시뮬레이션
- 보조 pxGrid 노드의 "application stp ise"로 보조 pxGrid 노드 시작
- MnT 주 노드의 액티브 세션을 다운로드하여 세션 비교. 세션은 서로 동일해야 함
- pxGrid 클라이언트를 보조 pxGrid 노드에 등록
- ISE의 등록된 pxGrid 클라이언트 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시

pxGrid 주 노드로 돌아가기

- 보조 pxGrid 노드의 "application stop ise"
- 주 pxGrid 노드의 "application stop ise"
- MnT 주 노드의 액티브 세션을 다운로드하여 세션 비교. 세션은 서로 동일해야 함
- 주 pxGrid 노드에 pxGrid 클라이언트 등록
- ISE의 등록된 pxGrid 클라이언트 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시

pxGrid 액티브-스탠바이 테스트

기본 작업

이 단계에서는 pxGrid 액티브-스탠바이 컨피그레이션 과정에서 첫 번째 pxGrid 노드 또는 주 pxGrid 노드에 pxGrid 클라이언트를 등록합니다.

기본 작업:

• pxGrid 클라이언트를 주 pxGrid 노드에 추가

<u>참고</u>: pxGrid 액티브-스탠바이 컨피그레이션의 경우, 주 pxGrid 노드만 액티브 상태가 될 수 있으며, 보조 pxGrid 노드는 pxGrid 보조 노드에 "sh application status ise"로 표시된 것처럼 "실행되지 않습니다".

- MnT 주 노드에서 액티브 세션 레코드 다운로드
- ISE의 등록된 pxGrid 클라이언트 상태 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시

아래 그림에는 액티브 상태인 모든 노드가 나와 있습니다.

1단계 모든 노드가 액티브 상태인지 확인합니다.

Administration -> System -> Deployment를 차례로 누르면 모든 노드가 표시됩니다.

ahahi										License Warning	a <u>A</u> I a	admin1	admin Lo
cisco Identit	y Services En	gine		🟠 Hom	e (Operations •	Policy	Guest Acce	ess 🔻 Admin	istration 🛛			
🙀 System	🚰 Identity Man	nagement	Netwo	ork Resources	🛃 Dev	ice Portal Man	agement	😡 pxGrid Se	ervices 😡	Feed Service	2 pxGri	id Identity	Mapping
Deployment	Licensing	Certificates	Loggi	ing Maintenance	1	Backup & Re	store	Admin Access	Settings				
Deployment			Dej	ployment Nodes									
<		₩ -											
Deployment			/	Edit 🔞 Register 👻	3	Syncup	Deregister						
				Hostname		Node Type	Personas			Role(s)	Se	ervices	Node Stat
				admin1		ISE	Administr	ation		PRIMARY(A)			~
				admin2		ISE	Administr	ation		SECONDARY(A)			
				mnt1		ISE	Monitorin	g		PRIMARY(M)			~
				mnt2		ISE	Monitorin	g		SECONDARY(M)			
				psn1		ISE	Policy Ser	vice			AI	1	~
				pxgrid1		ISE	pxGrid						~
				pxgrid2		ISE	pxGrid						~



2단계 pxGrid 서비스가 가동 중이고 ISE 주 PAN, ISE 보조 PAN, ISE 주 MnT, ISE 보조 MnT 노드가 등록된 클라이언트인지 확인합니다.

Administration -> pxGrid Services

abal	1.									License Wa	rning <u>À</u> admin1 a	admin Logout
cisco	o Identity Se	ervices Engin	e		企	Home Oper	ations 🛛 🔻	Policy •	Guest Access	Administration		
🐝 S)	ystem 🏼 💆	Identity Manage	ment	Network	Resources	🛃 Device F	Portal Manage	ement 🛛	Discrimination of the services 💀	Feed Service	💵 📲 pxGrid Identity I	Mapping
Client												
- 2 Enab	la O Disabla		A Group	Decline	O Dalata -	C Dofroch	Total Bandir		\ -		1	-7 of 7 Sh
V LIND		Approve	Gloup	Peciline	Belete +	Refresh	Iotal Period		, •			-7017 31
	Client Name		Client	Description		Capabilities	5		Status	Client G	Group	Log
	ise-admin-mnt2					Capabilities	(0 Pub, 0 Su	b)	Online	Adminis	strator	View
	ise-mnt-mnt2					Capabilities	(2 Pub, 0 Su	b)	Online	Adminis	strator	View
	ise-mnt-mnt1					Capabilities	(2 Pub, 0 Su	b)	Online	Adminis	strator	View
	ise-admin-mnt1					Capabilities	s(1 Pub, 0 Su	b)	Online	Adminis	strator	View
	ise-admin-admin	1				Capabilities	(2 Pub, 1 Su	b)	Online	Adminis	strator	View
	mac_engineering	17				Capabilities	(0 Pub, 0 Su	b)	Offline	Session		View
	mac					Capabilities	(0 Pub, 0 Su	b)	Offline	Session		View
								51				

3단계 pxGrid 클라이언트를 등록하고 pxGrid 레지스터 및 session_download 셸 스크립트를 사용하여 액티브 세션 레코드를 다운로드합니다. pxGrid 노드의 주 및 보조 IP 주소의 IP 주소는 hostname용입니다.

<u>참고</u>: 프로덕션 환경의 경우 보조 pxGrid 노드를 지정하는 GUI가 있을 수 있습니다.

Johns-Macbook-Pro:bin jeppich\$ truststoreFilename caroot1.jks mac_engineering15 -group Sessio properties version=1.0.0 hostnames=10.0.0.48, 10.0.0.49 username=mac_engineering15 descriptipon=nul1 keystoreFilename=mac.jks keystorePassword=cisco123 truststoreFilename=caroot1.jks truststorePassword=cisco123	./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 - -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username n
<pre>registering connecting connected. done registering. connection closed Johns-Macbook-Pro:bin jeppich\$ truststoreFilename caroot1.jks mac_engineering15 properties version=1.0.0 hostnames=10.0.0.48, 10.0.0.49 username=mac_engineering15 keystoreFilename=mac.jks keystoreFilename=mac.jks keystoreFilename=caroot1.jks truststoreFilename=caroot1.jks truststorePassword=cisco123 filter=nul1 start=nul1 end=nul1 </pre>	./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 - -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username

connecting...

starting at Thu Mar 05 00:54:43 EST 2015...

4단계 등록된 클라이언트인 mac_engineering15가 표시됩니다. Administration -> pxGrid Services

ahah				License Warning 🔥 👔 admin	1 admin Logou
cisco Identity Services Eng	gine	🖹 Home Operations 🔻 Policy	▼ Guest Access ▼	Administration 🛛 🔻	
🐝 System 🛛 💆 Identity Mana	agement 🛛 🔛 Network Resources	🛃 Device Portal Management	pxGrid Services	Feed Service	entity Mapping
Clients Live Log	: 😝 Group 👎 Decline 🔗 Delete	✓ Sefresh Total Pending Approv	al(0) 🔻		1 - 8 of 8 5
Client Name	Client Description	Capabilities	Status	Client Group	Log
□ ▶ ise-admin-admin1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
ise-mnt-mnt2		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
ise-mnt-mnt1		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□ ▶ ise-admin-mnt2		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
ise-admin-mnt1		Capabilities(1 Pub, 0 Sub)	Online	Administrator	View
mac		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
mac_engineering15		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□ ► mac engineering17		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

장애 조치 테스트

보조 pxGrid 노드에 대한 pxGrid 노드 장애 조치 테스트

- 주 pxGrid 노드의 "application stop ise"로 중단된 pxGrid 노드 시뮬레이션
- 보조 pxGrid 노드의 "application stp ise"로 보조 pxGrid 노드 시작
- MnT 주 노드의 액티브 세션을 다운로드하여 세션 비교. 세션은 서로 동일해야 함
- pxGrid 클라이언트를 보조 pxGrid 노드에 등록
- ISE의 등록된 pxGrid 클라이언트 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시
- 주 pxGrid 노드의 "application stop ise"로 중단된 pxGrid 노드 시뮬레이션
- 보조 pxGrid 노드의 "application stp ise"로 보조 pxGrid 노드 시작
- MnT 주 노드의 액티브 세션을 다운로드하여 세션 비교. 세션은 서로 동일해야 함

1단계주 pxGrid 노드 또는 pxGrid 1이 중단되었는지 확인합니다.Administration -> System -> Deployment

ahaha										License Warning	g 🚹 admin1	admin Lo
cisco Identit	ty Services En	gine		🏠 Hor	ne (Operations •	Policy	 Guest Acce 	ss 🔻 Ad	dministration		
🤹 System	Identity Mar	agement	Netwo	rk Resources	🛃 Dev	ice Portal Mar	nagement	😡 pxGrid Se	rvices	😡 Feed Service	2 pxGrid Identit	y Mapping
Deployment	Licensing	Certificates	Loggin	ng Maintenan	ce	Backup & R	estore	Admin Access	Settings			
Deployment			Dep	loyment Nodes								
<= • E •		₩ .										
Deployment	t .		1	Edit 🔞 Register 🦷	3	Syncup	Deregister					
				Hostname	-	Node Type	Personas			Role(s)	Services	Node Sta
				admin1		ISE	Administr	ration		PRIMARY(A)		~
				admin2		ISE	Administr	ation		SECONDARY(A)		~
				mnt1		ISE	Monitorin	g		PRIMARY(M)		~
				mnt2		ISE	Monitorin	g		SECONDARY(M)		_
				psn1		ISE	Policy Ser	rvice			All	 Image: A set of the
				pxgrid1		ISE	pxGrid					8
				pxgrid2		ISE	pxGrid					~

2단계 레지스터 및 세션 다운로드 명령을 실행하여 보조 pxGrid 노드에 연결되어 있는지 확인합니다.

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\$

3단계 pxGrid 서비스가 가동 중이고 게시된 ISE 노드가 표시되는지 확인합니다. Administration -> pxGrid Services

aha	h					License Warning 🛕	admin1 admin Logout
cisc	o Identity Services Engine		🛕 Home Op	erations 🔹 Policy 🖛	Guest Access	Administration 🛛 🔻	
**	System 🦉 Identity Managem	ent 🔛 Network	Resources 🛃 Device	e Portal Management	Discrict Services	🕞 Feed Service 🔒	oxGrid Identity Mapping
							€
Clier	ts Live Log						
🖌 Ena	ole 🧭 Disable 😪 Approve 😝	Group 👎 Decline	🐼 Delete 👻 🍕 Refresh	Total Pending Approval(0)	•		1 - 8 of 8 Sh
	Client Name	Client Description	Capabilit	ies	Status	Client Group	Log
	ise-admin-mnt2		Capabilit	ies(0 Pub, 0 Sub)	Online	Administrator	View
	ise-mnt-mnt1		Capabilit	ies(2 Pub, 0 Sub)	Online	Administrator	View
	ise-admin-mnt1		Capabilit	ies(1 Pub, 0 Sub)	Online	Administrator	View
	ise-admin-admin1		Capabilit	ies(2 Pub, 1 Sub)	Online	Administrator	View
	ise-mnt-mnt2		Capabilit	ies(2 Pub, 0 Sub)	Online	Administrator	View
	mac		Capabilit	ies(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering15		Capabilit	ies(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering17		Capabilit	ies(0 Pub, 0 Sub)	Offline	Session	View

4단계 주 pxGrid 노드가 중단된 동안 pxGrid 클라이언트를 등록하고 pxGrid 레지스터 및 session_download 셸 스크립트를 사용하여 액티브 세션 레코드를 다운로드합니다.



5단계 등록된 pxGrid 클라이언트인 mac_engineering20이 표시되는지 확인합니다. Administration -> pxGrid Services

cisco Identity S	Services Engin	ie		<u> (</u>	Home Ope	rations 🛛 🔻	Policy 🗸	Guest Access	Li	cense Warning 🔔	admin1 admin	Logout F
🔆 System	Identity Manage	ment	Network	Resources	🛃 Device	Portal Manag	gement	🔊 pxGrid Services	Feed Se	rvice 💵	oxGrid Identity Mapping	
Clients Live Lo	9g											⊖Enał
🖌 Enable 🛛 🖉 Disable	Approve	😝 Group	🗬 Decline	🛞 Delete 👻	😵 Refresh	Total Pendi	ing Approval(0) 👻			1 - 9 of 9	Show 2
Client Name		Client	Description		Capabilitie	S		Status		Client Group	Lo	bg
ise-admin-mnt	2				Capabilitie	s(0 Pub, 0 Su	ub)	Online		Administrator	V	iew
□ ► ise-mnt-mnt1					Capabilitie	s(2 Pub, 0 Su	ub)	Online		Administrator	Vi	iew
ise-admin-mnt	1				Capabilitie	s(1 Pub, 0 Su	ub)	Online		Administrator	V	iew
ise-admin-adm	in1				Capabilitie	s(2 Pub, 1 Su	ub)	Online		Administrator	V	iew
ise-mnt-mnt2					Capabilitie	s(2 Pub, 0 Su	ub)	Online		Administrator	V	iew
mac					Capabilitie	s(0 Pub, 0 Su	ub)	Offline		Session	V	iew
mac_engineeri	ng15				Capabilitie	s(0 Pub, 0 Su	ub)	Offline		Session	V	iew
mac_engineeri	ng17				Capabilitie	s(0 Pub, 0 Su	ub)	Offline		Session	V	iew
mac_engineeri	ng20				Capabilitie	s(0 Pub, 0 Su	ub)	Offline		Session	V	iew



주 노드로 돌아가기

pxGrid 주 노드로 돌아가기

- 보조 pxGrid 노드의 "application stop ise"
- 주 pxGrid 노드의 "application stop ise"
- MnT 주 노드의 액티브 세션을 다운로드하여 세션 비교. 세션은 서로 동일해야 함
- 주 pxGrid 노드에 pxGrid 클라이언트 등록
- ISE의 등록된 pxGrid 클라이언트 보기
- 배포 노드 상태를 확인하여 pxGrid 노드 상태 표시
- 1단계주 pxGrid 노드가 백업되었는지 확인합니다.Administration -> System -> Deployment를 차례로 누르면 모든 노드가 표시됩니다.

ahaha					License Warnin	g 🔥 admin1	admin Logout Feedba
cisco Identit	y Services Engine	🟠 Home	Operations 🛛 🔻	Policy Guest Acces	Administration		
ystem	🚰 Identity Management	🔛 Network Resources 🛛 🛃 De	vice Portal Man	agement 🛛 🗔 pxGrid Ser	vices 🛛 🖓 Feed Service	💵 pxGrid Identit	y Mapping
Deployment	Licensing Certificates	Logging Maintenance	Backup & Re	estore Admin Access	Settings		
Deployment		Deployment Nodes					
	- -						
Deployment	104 ·	/ Edit 🔞 Register 👻 🥱	Syncup	Deregister			Sh
		Hostname	Node Type	Personas	Role(s)	Services	Node Status
		admin1	ISE	Administration	PRIMARY(A)		
		admin2	ISE	Administration	SECONDARY(A)		
		mnt1	ISE	Monitoring	PRIMARY(M)		
		mnt2	ISE	Monitoring	SECONDARY(M)	1	
		psn1	ISE	Policy Service		All	
		pxgrid1	ISE	pxGrid			
		pxgrid2	ISE	pxGrid			0

2단계 pxGrid 서비스가 실행 중이고 게시된 ISE 노드가 표시되는지 확인합니다. Administration -> pxGrid Services

alah			L	license Warning 🚹 admin1 admin	Logout Feedback
cisco Identity Services Engine	🟠 Home Op	erations V Policy V	Guest Access	ו ד	
💑 System 🛛 👰 Identity Management	Network Resources	e Portal Management	🗊 pxGrid Services 🛛 🔂 Feed Se	ervice	
					Enable Auto-Registration
Clients Live Log					
✓ Enable Ø Disable Ø Approve	👎 Decline 🛛 🛞 Delete 👻 🛞 Refresh	Total Pending Approval(0)	•	1 - 9 of 9	Show 25 - per page Page
Client Name Client I	Description Capabiliti	es	Status	Client Group Lo	9
□ ▶ ise-mnt-mnt2	Capabiliti	es(2 Pub, 0 Sub)	Online	Administrator Vie	2W
□ ▶ ise-mnt-mnt1	Capabiliti	es(2 Pub, 0 Sub)	Online	Administrator Vie	W
□ ▶ ise-admin-mnt1	Capabiliti	es(1 Pub, 0 Sub)	Online	Administrator Vie	w
□ ▶ ise-admin-admin1	Capabiliti	es(2 Pub, 1 Sub)	Online	Administrator Vie	ew .
ise-admin-mnt2	Capabiliti	es(0 Pub, 0 Sub)	Online	Administrator Vie	2W
mac 🕨 mac	Capabiliti	es(0 Pub, 0 Sub)	Offline	Session Vie	2W
□ ► mac_engineering17	Capabiliti	es(0 Pub, 0 Sub)	Offline	Session Vie	w
mac_engineering15	Capabiliti	es(0 Pub, 0 Sub)	Offline	Session Vie	w
□ ► mac_engineering20	Capabiliti	es(0 Pub, 0 Sub)	Offline	Session Vie	2W

보안 액세스 방법 가이드

3단계 session_download를 실행하여 액티브 세션을 다운로드할 수 있도록 계속 연결되어 있는지 확인합니다.

Dddd Johns-Macbook-Pro:bin jeppich\$./session download.sh -keystoreFilename mac.jks -keystorePassword cisco123 truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username mac engineering15 ----- properties -----version=1.0.0 hostnames=10.0.0.48, 10.0.0.49 username=mac_engineering15 keystoreFilename=mac.jks keystorePassword=cisco123 truststoreFilename=caroot1.iks 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

4단계 pxGrid 클라이언트를 등록하여 모두 작동하는지 확인합니다.

```
Johns-Macbook-Pro:bin jeppich$ ./register.sh -keystoreFilename mac.jks -keystorePassword cisco123 -
truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username
mac engineering50 -group Session
----- properties ------
version=1.0.0
hostnames=10.0.0.48, 10.0.0.49
username=mac engineering50
descriptipon=null
keystoreFilename=mac.jks
keystorePassword=cisco123
truststoreFilename=caroot1.jks
truststorePassword=cisco123
 _____
registering...
connecting...
connected.
done registering.
connection closed
```

5단계 ISE pxGrid 컨트롤러에서 pxGrid 클라이언트인 mac_engineering50을 봅니다. Administration -> pxGrid Services

ahah								License Warning 🔒	admin1 admin Logou
cisco	Identity Services Engin	ne		企	Home Opera	ations V Policy V	Guest Access	Administration V	
💑 Sys	item 🛛 💆 Identity Manag	ement	Network	Resources	🛃 Device P	Portal Management	Disconting services	😡 Feed Service 🔒 🚆 p	kGrid Identity Mapping
Clients	Live Log								
🖌 Enable	Oisable OApprove	😝 Group	👎 Decline	🐼 Delete 👻	🛞 Refresh	Total Pending Approval(0)	•		1 - 10 of 10 Sł
	Client Name	Client	Description		Capabilities	1	Status	Client Group	Log
	se-mnt-mnt2				Capabilities	(2 Pub, 0 Sub)	Online	Administrator	View
🗆 🕨 i	se-mnt-mnt1				Capabilities	(2 Pub, 0 Sub)	Online	Administrator	View
	se-admin-mnt1				Capabilities	(1 Pub, 0 Sub)	Online	Administrator	View
🗆 🕨 i	se-admin-admin1				Capabilities	(2 Pub, 1 Sub)	Online	Administrator	View
	se-admin-mnt2				Capabilities	(0 Pub, 0 Sub)	Online	Administrator	View
	mac				Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering17				Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering15				Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering20				Capabilities	(0 Pub, 0 Sub)	Offline	Session	View
	mac_engineering50				Capabilities	(0 Pub, 0 Sub)	Offline	Session	View

ISE 자체 서명 ID 인증서

pxGrid의 ISE 자체 서명 ID 인증서는 외부 CA 인증기관을 사용할 수 없는 경우, 그리고 pxGrid SDK의 샘플 인증서를 사용하지 않고 pxGrid 및 ISE 구현을 테스트 하는 경우 사용할 수 있습니다. 기본적으로 자체 서명 ID 인증서에는 서버 인증(1.3.6.1.5.5.7.3.1) 및 클라이언트 인증(1.3.6.1.5.5.7.3.2)의 EKU(Enhanced Key Usage)가 모두 포함되며, 이는 ISE 시스템 인증서 저장소에 있습니다.

pxGrid 클라이언트는 자체 서명 인증서를 사용할 수 있으며 다음을 참조하십시오. pxGrid ISE 노드 및 pxGrid 노드가 포함된 자체 서명 인증서 사용

pxGrid 클라이언트는 CA 서명 인증서도 사용할 수 있으며 다음을 참조하십시오. pxGrid ISE 노드 및 CA 서명 pxGrid 클라이언트가 포함된 자체 서명 인증서 사용

1단계ISE 자체 서명 ID 인증서에서 pxGrid 사용을 활성화합니다.Administration -> System -> Certificates -> System Certificates를 차례로 누른 다음 ISE 자체 서명인증서를 편집하고 pxGrid를 선택한 후 Save를 누릅니다.

ahah		License Warning 🔥 isespl					
Risco Identity Services Engine	🟠 Home	Operations V Policy V Guest Access V Administration V					
🙀 System 🐉 Identity Management	📰 Network Resources 🛛 🛃 🛛	evice Portal Management 🛛 💭 pxGrid Services 🖓 Feed Service 💵 pxGrid Identi					
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	r 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					
		Admin: Use certificate to authenticate the ISE Admin Portal					
External CA Settings		pxsna: Use cerunicate for the pxGrid Controller					
		Continents use for portal					

보안 액세스 방법 가이드

2단계 Trusted Certificates 아래에서 퍼블릭 ISE ID 자체 서명 인증서를 내보냅니다. Administration -> System -> Certificates를 차례로 누른 다음 자체 서명 인증서를 편집하고 "Export Certificate Only"를 누릅니다.

<u>참고</u>: 이는 PEM 파일로 저장됩니다.

alialu				Licen	se Warning 🛕 isespi ad	min Logout Fe
cisco Identity Services Engine	🛕 Home	Operations 🛛 🔻	Policy Guest Access	▼ Administration ▼		
🔆 System 🍄 Identity Management	Network Resources	Device Portal Manager	ment 😡 pxGrid Service	es 🗔 Feed Service	≗i≣ pxGrid Identity M	apping
Deployment Licensing Certificates	Logging Maintenance	Backup & Restor	re Admin Access	Settings		
Certificate Management	System Certificates A For	disaster recovery it is	recommended to export certifi	cate and private key pairs	s of all system certificates.	
Overview	🖌 Edit 🕂 Generate Self Si	gned Certificate	Import 🕼 Export	Delete View		
	Friendly Name	Group Tag	Used By	Issued To	Issued By	Valid From
System Certificates	▼ isespl					
Endpoint Certificates	Default self-signed server c ertificate	Default Portal Certificate Group	Admin, Portal, EAP Authentication, pxGrid	isespl.lab6.com	isespl.lab6.com	Sat, 24 Jan 20
Trusted Certificates	Export Certi	ficate 'Default sel	f-signed server certificat	e'	×	
OCSP Client Profile			 Export Certificate 	Only		
Certificate Signing Requests		*Private Key Pa	Export Certificate	and Private Key		
		*Confirm Pa	asword			
Certificate Authority	Warning	· Commin Pa	is pet a secure operation. It a	ould load to possible eves	source of the private key	
Internal CA Settings	warning. E	xporting a private key	is not a secure operation. It o	ouid lead to possible expt	Export Cancel	
Certificate Templates	h					
External CA Settings						

3단계 PEM 파일을 신뢰할 수 있는 인증서 저장소로 가져옵니다.

Administration -> System -> Certificates -> Trusted Certificates를 차례로 누른 다음 PEM 인증서를 선택하고 "Trust for authentication within ISE"를 활성화한 다음 제출합니다.

սիսիս	License Warning 🛓 isespl							
cisco Identity Services Engine	Home Operations ▼ Policy ▼ Guest Access ▼ Administration ▼							
🙀 System 🦉 Identity Management	🚆 Network Resources 🛛 🛃 Device Portal Management 🖓 pxGrid Services 🖓 Feed Service 🕰 🖁 pxGrid Identif							
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings							
Certificate Management	Import a new Certificate into the Certificate Store							
Quentiew	* Certificate File Browse Defaultselfsignedservercerti.pem							
Overview	Friendly Name							
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								
Certificate Signing Requests	Description							
	Submit Cancel							
Certificate Authority								

4단계 pxGrid 페르소나를 활성화합니다.

Administration -> System -> Deployment를 차례로 누른 다음 배포 노드를 편집하고 pxGrid를 활성화한 다음 Save를 누릅니다.

ahah	License Warning 🧎 isespl admin
CISCO Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
System 🐉 Identity Management	🖥 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🗔 Feed Service 🔍 🔩 pxGrid Identity Mappi
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Deployment ↓ t= v Markov Deployment	Deployment Nodes List > isespl Edit Node General Settings Profiling Configuration Hostname isespl FQDN isespl.lab6.com IP Address 10.0.0.39 Node Type Identity Services Engine (ISE) Personas Administration Role STANDALONE Make Primary Monitoring Role PRIMARY V Other Monitoring Node Policy Service Phable Session Services

□ ► ise-mnt-isespl



Administrator

5단계 pxGrid 서비스를 시작합니다. Administration -> pxGrid Services

참고: pxGrid 노드에 대한 연결이 표시되지 않을 경우, 잠시 후에 표시될 수 있습니다.	

ahaha									l	license Warning 🛕 isespl
cisco Ide	itity Services Eng	ine		企	Home Oper	ations 🔹	Policy •	Guest Access	Administration	•
🐝 System	餐 Identity Manag	gement	Network	Resources	🛃 Device I	Portal Mana	gement	😡 pxGrid Services	Feed Ser	vice 💵 📲 pxGrid Ident
Clients	Live Log									
Clients	Live Log			-						
Senable 🖉	Disable 🕜 Approve	Group	Decline	🚷 Delete 👻	Sefresh 8	Total Pend	ling Approval(0)) 🔻		
Client N	ame	Clien	t Description		Capabilitie	5		Status		Client Group
ise-adm	in-isespl				Capabilities	(3 Pub, 1 S	ub)	Online		Administrator

Capabilities(2 Pub, 0 Sub)

Online

SDK의 샘플 인증서

이 예에서는 pxGrid SDK의 샘플 인증서를 사용하며, 이는 프로덕션 환경이 아닌 POC에만 사용됩니다. 이 단계에서는 신뢰할 수 있는 CA 인증서의 rootSample.crt를 가져오고, iseSample1.crt 및 iseSample1.key를 가져옵니다. 이는 클라이언트 등록을 위한 pxGrid 클라이언트의 퍼블릭/프라이빗 쌍 역할을 합니다. POC 배포, 샘플 인증서 및 pxGrid 샘플 셸 스크립트에 대한 보다 자세한 내용은 다음 (http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf)을 참조하십시오.

1단계 rootSample.crt를 ISE의 신뢰할 수 있는 시스템 인증서로 가져옵니다. Administration -> System -> Certificates -> Trusted Certificate를 차례로 누른 다음 rootSample.crt를 가져온 다음 Submit을 누릅니다.

ahah	License Warning 🔒 isespi admin Logout
cisco Identity Services Engine	
💀 System 🛛 🥸 Identity Management	🞬 Network Resources 🛛 🛃 Device Portal Management 🛛 🗔 pxGrid Services 🖓 Feed Service 💵 🕹 pxGrid Identity Mapping
Deployment Licensing Certificate	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Import a new Certificate into the Certificate Store
	* Certificate File Browse) rootSample.crt
Overview	Friendly Name
System Certificates	
	Trusted For: (i)
Endpoint Certificates	✓ Trust for authentication within ISE
Tested California	Trust for client authentication and Syslog
Irusted Cerunicates	Trust for authentication of Cisco Services
OCSP Client Profile	Validate Certificate Extensions
Certificate Signing Requests	Description
Certificate Authority	Submit Cancel

2단계 iseSample1.crt 및 iseSample1.key를 ISE의 시스템 인증서로 가져옵니다. Administration -> System -> Certificates -> System Certificates -> Import를 차례로 누른 다음 비밀번호에 cisco123을 사용하고 Submit을 누릅니다.

abab	License Warning 🍌 isespi admin
CISCO Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼
🔅 System 🛛 👰 Identity Management	🎬 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 14 pxGrid Identity Mapping
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management	Impart Sarvar Cartificata
Overview	Inport Server Certificate
System Certificates	* Select Node isespi
	* Certificate File Browse iseSample1.crt
Endpoint Certificates	* Private Key File Browse iseSample1.key
Trusted Certificates	Password
OCSR Client Brafile	Friendly Name
OCSP Client FIONE	Allow Wildcard Certificates 📃 🕧
Certificate Signing Requests	Allow wildcard is disabled 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
Internal CA Settings	Usage
Certificate Templates	Admin: Use certificate to authenticate the ISE Admin Portai FAD Authentication: Use certificate for EAD antegrale that use CSU (7) C type=line
	Der Aufendation, die dertindate for Der protocols diat dae 350 n.E. turmening
External CA Settings	Portal: Use for portal
	Submit Cancel

3단계 pxGrid 페르소나를 활성화합니다.

Administration -> System -> Deployment를 차례로 누른 다음 배포 노드를 편집하고 pxGrid를 활성화한 다음 Save를 누릅니다.

ahah	License Warning 🛕 isespl admin
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	Deployment Nodes List > isespl Edit Node Ceneral Settings Profiling Configuration Hostname isespl FQDN isespl.lab6.com IP Address 10.0.0.39 Node Type Identity Services Engine (ISE) Personas Madministration Monitoring Role STANDALONE Monitoring Role PRIMARY Other Monitoring Node Policy Service Include Node in Node Group Include Node in Node Group None Include Node in Node Group None Image: Service Include Node in Node Group Image: Service Image: Service Image: Service Ima



4단계 pxGrid 서비스를 시작합니다. Administration -> pxGrid Services

참고: pxGrid 노드	E에 대한 연결이 표시되지	않을 경우, 잠시 후에	표시될 수 있습니다.				
alialia cisco Iden	tity Services Engine		Home Operations V	Policy	Guest Access	License W	arning 🔥 isespl
ాహి System	🛃 Identity Management	Network Resources	Device Portal Manag	gement	pxGrid Services	Feed Service	≗ i≝ pxGrid Ident

Clier	ts Live Log								
🖌 Ena	ble 🕜 Disable	Approve	😝 Group	👎 Decline	🐼 Delete 👻	😵 Refresh	Total Pending Approval(0)	*	
	Client Name		Clien	t Description		Capabilities	3	Status	Client Group
	ise-admin-isespl					Capabilities	(3 Pub, 1 Sub)	Online	Administrator
	ise-mnt-isespl					Capabilities	(2 Pub, 0 Sub)	Online	Administrator
•	ise-mnt-isespl					Capabilities	s(2 Pub, 0 Sub)	Online	Administrator

pxGrid 클라이언트 테스트

MnT 노드에서 ISE 자체 서명 ID 인증서를 가져와야 하며, pxGrid 클라이언트에 대한 독립형 배포의 경우 벌크 세션 다운로드를 지원하는지 확인합니다(벌크 세션 다운로드 참조).

이 단계에서는 클라이언트 등록 및 세션 다운로드를 확인합니다.

1단계 register.sh 스크립트를 사용하여 다음을 실행합니다.

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

pxGrid 클라이언트 iseSample이 pxGrid Services 아래에 등록된 클라이언트로 표시되는지 확인합니다.

սիսիս									License War	ning <u>À</u> isespl
cisco Identit	y Services Engi	ine			Home Oper	rations 🔹	Policy •	Guest Access	Administration	
🔆 System 🛛 👰 Identity Management			Network	k Resources	🛃 Device	Portal Manag	ement	🔊 pxGrid Services	Feed Service	💵 📲 pxGrid Identii
Clients	Live Log									
🖌 Enable 🛛 🖉 Disa	ole 🕜 Approve	😝 Group	👎 Decline	🐼 Delete 👻	😵 Refresh	Total Pend	ng Approval(()) 🔻		
Client Name		Client	t Description		Capabilitie	S		Status	Client Gro	pup
ise-admin-is	espl				Capabilitie	s(3 Pub, 1 S	ıb)	Online	Administr	ator
□ ► ise-mnt-ises	pl				Capabilitie	s(2 Pub, 0 S	ıb)	Online	Administr	ator
isesample					Capabilitie	s(0 Pub, 0 S	ub)	Offline	Session	



참조

pxGrid 구성 및 테스트 방법

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 ISE 노드 및 pxGrid 클라이언트가 포함된 자체 서명 인증서 사용

pxGrid ISE 노드 및 CA 서명 pxGrid 클라이언트가 포함된 자체 서명 인증서 사용

pxGrid ISE 노드 및 pxGrid 클라이언트가 포함된 CA 서명 인증서 사용



부록

문제 해결

이 섹션에서는 문제 해결에 대한 정보를 제공합니다.

다음과 같은 오류 메시지가 표시될 경우 pxGrid 클라이언트, pxGrid 노드 및 ISE가 DNS 확인 가능한지 알아봅니다.

<pre>jeppich\$./session_download.sh -keystoreFilename mac.jks -keystorePassword cisco123 -truststoreFilename caroot1.jks -truststorePassword cisco123 -hostname 10.0.0.48 10.0.0.49 -username mac properties version=1.0.0 hostnames=10.0.0.48, 10.0.0.49 username=mac keystoreFilename=mac.jks keystoreFilename=caroot1.jks truststoreFilename=caroot1.jks truststorePassword=cisco123 filter=null start=null</pre>
end=null
<pre>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.</pre>
at
org.apache.cxf.interceptor.MessageSenderInterceptor\$MessageSenderEndingInterceptor.handleMessage(MessageSende rInterceptor.java:64) ~[cxf-api-2.7.3.jar:2.7.3]
at org.apache.cxr.phase.PhaseInterceptorchain.doIntercept(PhaseInterceptorchain.java:2/1) ~[cxr-api- 2.7.3.jar:2.7.3]
at org.apache.cxf.jaxrs.client.AbstractClient.doRunInterceptorChain(AbstractClient.java:581) [cxf-rt-frontend-jaxrs-2.7.3.jar:2.7.3]
at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:904) [cxf-rt-frontend- jaxrs-2.7.3.jar:2.7.3]
at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:772) [cxf-rt-frontend-jaxrs- 2.7.3.jar:2.7.3]
at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:759) [cxf-rt-frontend-jaxrs- 2.7.3.jar:2.7.3] at org.apache.cxf.jaxrs.client WebClient invoke(WebClient java:355) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3] at org.apache.cxf.jaxrs.client.WebClient.post(WebClient.java:381) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
at com.cisco.pxgrid.stub.identity.impl.SessionIteratorImpl.open(SessionIteratorImpl.java:128) [pxgrid-identity-client-stub-1.0.0.jar:1.0.0]
at com.cisco.pxgrid.samples.ise.SessionDownload.main(SessionDownload.java:132) [pxgrid-sdk- 1.0.0.jar:1.0.0]

Centos 6.5에서 Java 제거 및 JDK 8.0 설치

이전 버전의 Java 삭제

1 단계 Centos 6.5가 최신 버전인지 확인하며, yum update를 입력합니다.

<u>참고</u>: 루트 권한이 필요할 수 있으며, su root yum update를 입력합니다.

2 단계 업데이트가 완료되면 다음을 입력하여 기타 모든 설치된 JAVA 패키지를 제거합니다.

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

<u>참고:</u> java-1.6.0-openjdk-1.6.0.0-1.56.1.11.8.el6_3.i686 패키지가 이미 설치되어 있으므로 이를 실행하여 제거했습니다.

3 단계 입력: yum remove java-1.6.0-openjdk

JDK 8.0 설치

1 단계 루트 사용자로 변경한 다음 su를 입력하면 비밀번호를 입력하라는 메시지가 표시됩니다.

2 단계 JDK 8을 설치하고 rpm -Uvh jdk-8u20-linux-x64.rpm을 입력합니다.

3 단계 다음과 같은 대체 명령도 실행해야 합니다.

```
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
```

Java 버전을 선택하고 java -version을 입력하면 java -version "1.8.0_20"이 표시됩니다.