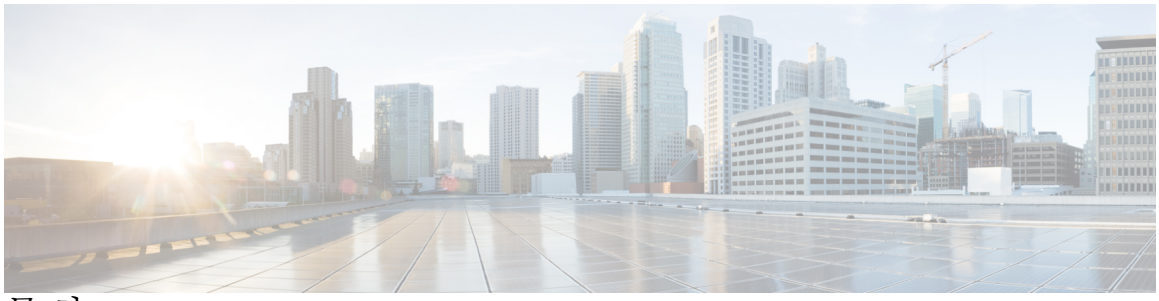
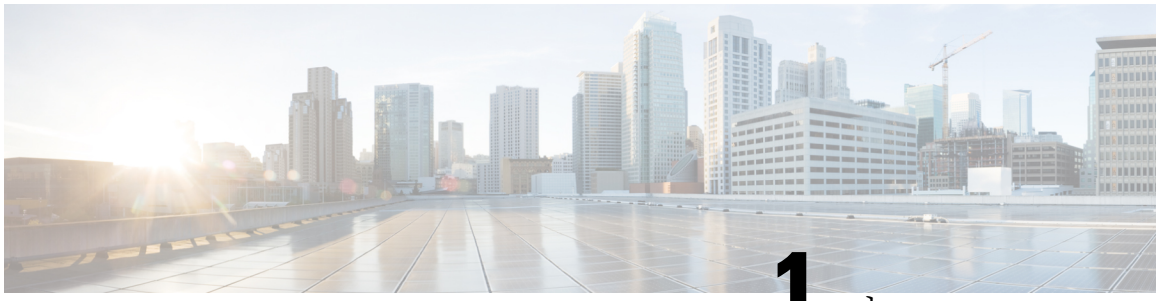
ISE-PIC(Identity Services Engine Passive Identity Connector) 관리자 가이드, 릴리스 3.0

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

소개 ISE-PIC

무단 위협으로부터 네트워크를 보호하려면 사용자 ID를 인증해야 합니다. 이를 위해 보안 제품이 네트워크에서 구현됩니다. 각 보안 제품에는 필요한 인증을 검색하는 고유한 방법이 있으며, 대개 인증된 사용자가 아닌 인증된 IP 주소를 식별합니다. 따라서 이러한 제품은 사용자 로그인 정보를 기반으로 인증을 제공하는 여러 외부 서버 및 방법을 참조하므로 네트워크가 분산됩니다. Cisco ISE(Identity Services Engine) Passive Identity Connector(ISE-PIC)는 중앙 집중식 설치 및 구현을 제공하므로 다양한 소스에서 패시브 인증 데이터를 수집하고 이러한 ID를 보안 제품 가입자와 공유할 수 있습니다.

Cisco ISE-PIC 용어

이 설명서에서는 Cisco ISE-PIC를 다룰 때 다음 용어를 사용합니다.

용어	정의
GUI	그래픽 유저 인터페이스. GUI는 ISE-PIC의 소프트웨어 설치에서 화면 및 탭 중 하나를 가리킵니다.
NIC	Network Interface Card(네트워크 인터페이스 카드).
노드	개별 물리적 또는 가상 Cisco ISE-PIC 어플라이언스.
PAN	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.

용어	정의
파서	시스템 로그 메시지를 수신하고 입력을 ISE-PIC에 관리, 매핑 및 게시할 수 있는 부분으로 나누는 ISE-PIC 백엔드 구성 요소입니다. 파서는 시스템 로그 메시지가 도착할 때마다 각 정보 라인을 통과하여 주요 정보를 찾습니다. 예를 들어 "mac ="를 찾도록 파서가 구성된 경우 파서는 각 구문을 구문 분석하면서 해당 구문을 찾습니다. 구성된 구문을 발견하면 파서가 정의된 정보를 ISE에 전달하도록 설정됩니다.
기본 노드	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.
프로브	프로브는 지정된 소스에서 데이터를 수집하는 메커니즘입니다. 프로브는 메커니즘을 설명하는 일반적인 용어이지만 데이터가 수집되는 방법 또는 수집되는 내용을 구체적으로 설명하지는 않습니다. 예를 들어 AD(Active Directory) 프로브는 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 파서에서 데이터를 수집합니다.
사업자	ISE-PIC가 사용자 ID 정보를 수신, 매핑 및 게시하는 클라이언트 또는 소스입니다.
보조 노드	ISE-PIC 구축의 기본 노드는 PAN(기본 관리 노드)이며 사용 가능한 모든 작업을 수행할 수 있는 노드입니다. ISE-PIC에서 최대 2개의 노드를 설치할 수 있습니다. 두 번째 노드를 설치하는 경우 이를 보조 관리 노드(보조 PAN)라고 합니다.
가입자	사용자 ID 정보를 수신하기 위해 ISE-PIC 서비스를 구독하는 시스템입니다.

ISE-PIC 개요

Passive Identity Connector(ISE-PIC)는 중앙 집중식 원스톱 설치 및 구현을 제공하기 때문에, 사용자는 네트워크를 쉽고 간단하게 구성해 사용자 ID 정보를 받고 Cisco FMC(Firepower Management Center)나 Stealthwatch 같은 다양한 보안 제품 가입자와 공유할 수 있습니다. 수동 식별의 전체 브로커로서 ISE-PIC는 AD DC(Active Directory Domain Controller) 같은 다양한 제공자 소스로부터 사용자 ID를 수집하고, 사용자 로그인 정보를 사용 중인 관련 IP 주소에 매핑한 다음 매핑 정보를 사용자가 구성한 가입자 보안 제품과 공유합니다.

Passive Identity(패시브 ID)란?

AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 802.1X나 Web Authentication(웹 인증) 같은 기술을 활용하고, 사용자 또는 엔드포인트와 직접 통신해 네트워크 액세를 요청한 다음 관련 로그인 자격 증명을 이용해 ID를 확인하고 활성 인증합니다.

패시브 ID 서비스는 사용자를 직접 인증하는 대신 서비스 제공자로 확인된 (Active Directory 같은) 외부 인증 서버에서 사용자 ID와 IP 주소를 수집한 다음 이 정보를 가입자와 공유합니다. ISE-PIC는 먼저 서비스 제공자로부터 (대부분 사용자 로그인 및 암호를 바탕으로) 사용자 ID 정보를 수신한 다음 필요한 확인 작업과 서비스를 수행하여 사용자 ID를 관련 IP 주소와 매치함으로써 인증된 IP 주소를 가입자에게 전달합니다.

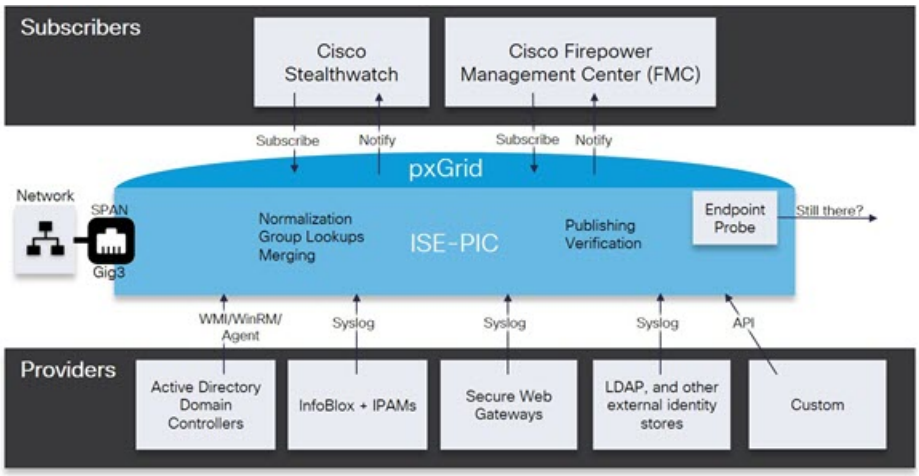
Passive Identity Connector(ISE-PIC) 흐름

ISE-PIC의 흐름은 다음과 같습니다.

1. 서비스 제공자가 사용자 또는 엔드포인트의 인증을 수행합니다.
2. 서비스 제공자가 인증된 사용자 정보를 ISE-PIC에 전송합니다.
3. ISE-PIC는 사용자 정보를 정규화하고 관련 조회와 병합 및 구문 분석을 수행하며 IP 주소에 매핑하고, 매핑한 세부 정보를 pxGrid에 게시합니다.
4. pxGrid 가입자는 매핑된 사용자 세부 정보를 수신합니다.

다음 다이어그램에서는 ISE-PIC에서 제공되는 개괄적인 플로우에 대해 설명합니다.

그림 *1:* 고수준 흐름



Cisco ISE-PIC 아키텍처, 구축 및 노드

Cisco ISE-PIC 아키텍처는 다음 구성 요소를 포함합니다.

- 노드 - Cisco ISE-PIC 구축에서 아래 설명된 대로 최대 2개의 노드를 구성할 수 있습니다.

- 네트워크 리소스
- 엔드포인트

단일 Cisco ISE-PIC 노드가 있는 구축을 독립형 구축이라고 합니다.

두 개의 Cisco ISE-PIC 노드가 있는 구축을 고가용성 구축이라고하며, 여기서 하나의 노드는 기본 어플라이언스(기본 관리 노드 또는 PAN)로 작동합니다. 고가용성 구축은 서비스 가용성을 개선합니다.

PAN이 이 네트워크 모델에 필요한 모든 컨피그레이션 기능을 제공합니다. 보조 Cisco ISE 노드(보조 PAN)는 백업의 역할을 합니다. 보조 노드는 기본 노드를 지원하며 기본 노드와의 연결이 끊길 때마다 기능을 다시 시작합니다.

Cisco ISE-PIC는 기본 Cisco ISE-PIC 노드에 있는 모든 콘텐츠를 보조 Cisco ISE-PIC 노드와 동기화하거나 복제하여 보조 노드가 기본 노드의 상태와 최신 상태를 유지하도록 합니다(따라서 백업으로 사용할 수 있음).

ISE 커뮤니티 리소스

구축 및 확장에 대한 자세한 내용은 ISE 구축 여정을 참조하십시오.

장점 ISE-PIC

ISE-PIC 다음을 제공합니다.

- 다양한 제공자와 상호 작용하는 단일 ID 솔루션입니다.
- 간편한 컨피그레이션, 모니터링 및 문제 해결을 지원하는 친숙한 GUI
- 간단한 설치 및 구성
- 활성 인증을 위해 ISE로 쉽게 업그레이드할 수 있습니다. ISE-PIC에서 전체 ISE 구축으로 업그레이드하고 ISE-PIC 노드를 사용하여 독립형 ISE 구축을 생성할 때 또는 이 노드를 기존 구축에 기본 노드로 추가할 경우 ISE는 업그레이드 이전에 ISE-PIC에서 제공되었던 모든 기능을 계속 제공하고 기존 컨피그레이션이 보존됩니다.

참고 ISE로 업그레이드하려면 평가판을 다운로드하거나 Cisco 담당자에게 문의하여 라이선싱 옵션에 대해 논의하십시오.

기본 노드가 아닌 기존 ISE 구축에 업그레이드된 ISE-PIC를 추가하면 이전 ISE-PIC 컨피그레이션을 덮어 씁니다.

업그레이드 흐름에 대한 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드, 138 페이지를 참조하십시오.

ISE-PIC와 ISE/CDA 비교

ISE-PIC ISE로 쉽고 원활하게 업그레이드하는 기능 등의 다양한 혜택을 제공합니다. Cisco는 ISE-PIC 및 ISE 외에 추가 보안 메커니즘인 CDA도 제공합니다. 이 섹션의 아래 표에서는 세 제품을 비교한 결과를 확인할 수 있습니다.

- ISE-PIC와 ISE의 자세한 비교, 5 페이지
- ISE-PIC와 ISE/CDA의 개략적인 비교, 7 페이지

ISE-PIC와 ISE의 자세한 비교

ISE-PIC 는 패시브 ID만 공유하도록 설계되었고, AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 ISE가 제공하는 권한 부여 또는 인증 서비스는 제공하지 않습니다. 다음 표에서는 두 제품 간의 차이를 자세히 확인할 수 있습니다.

표 *1: ISE-PIC*와 *ISE* 비교

카테고리	기능	ISE-PIC	ISE
Smart Licensing		—	√
인증 및 권한 부여 유형	권한 부여 정책	—	√
	TrustSec	—	√
	WMI를 포함한 Active Directory 수동 인증	√	√

카테고리	기능	**ISE-PIC**	**ISE**
패시브 ID 소스		√	√
	Easy Connect	—	√
	SysLog 소스	√	√
	REST API 소스	√	√
	SPAN	√	√
	Security Group eXchange Protocol (SXP)	—	√
	RADIUS 프록시를 포함한 RADIUS	—	√
	BYOD	—	√
	게스트	—	√
	포스처	—	√
	Device Administration(TACACS+)	—	√
pxGrid	pxGrid 컨트롤러	√ Cisco 가입자 전용	√
	pxGrid 컨트롤러 이중화	√	√
	주제 확장성	—	√
CA(Certificate Authority)	pxGrid 인증서 템플릿	√	√
	엔드포인트 CA	—	√
	보안 전송을 통한 등록(EST)	—	√
	기타 인증서 템플릿	—	√
가시성 및 상황	컨텍스트 디렉토리	—	√
	프로파일링	—	√

카테고리	기능	**ISE-PIC**	**ISE**
리포트		! 참고 ISE-PIC에서는 시스템 상태를 모니터링하고 네트워크 문제를 해결하는 데 사용할 수 있는 보고서를 제공합니다. 하지만 ISE-PIC에서는 ISE와는 달리 기능 하위 집합을 제공하며, 따라서 ISE 보고서 중 일부는 ISE-PIC에서는 사용할 수 없습니다.	√

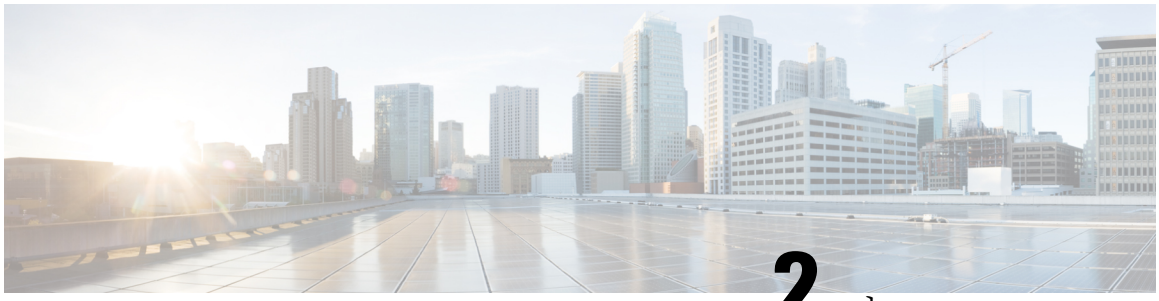
ISE-PIC와 **ISE/CDA**의 개략적인 비교

CDA는 보안 게이트웨이가 네트워크에서 어떤 사용자가 어떤 IP 주소를 사용하는지 확인할 수 있도록 IP 주소를 사용자 이름에 매핑하며, 따라서 이제 이러한 보안 게이트웨이는 사용자(또는 사용자가 속한 그룹)를 기준으로 결정을 내릴 수 있습니다. 그러나 ISE-PIC에서는 사용자 이름, MAC 주소 및 포트 같은 추가 데이터에 액세스하여 사용자 ID를 훨씬 더 정확하게 수집합니다. 다음 표에서는 ISE-PIC, ISE와 CDA의 고수준 비교 결과를 확인할 수 있습니다.

표 ***2: ISE-PIC***와 ***ISE/CDA*** 비교

패시브 인증 세부 정보	전체 **ISE**	**ISE-PIC**	**CDA**
도메인 컨트롤러 숫자	100	100	80
가입자 수	20	20	—
WMI(에이전트 없음)	예	예	예
사용 가능한 Windows 서버 에이전트	예	예	—
DCOM 필수	아니요(SPAN)	아니요(SPAN)	예
Easy Connect	예	—	—

패시브 인증 세부 정보	전체 **ISE**	**ISE-PIC**	**CDA**
SPAN을 이용한 Kerberos 탐지	예	예	—
결합(IP 주소, MAC 주소 및 사용자 이름)	300,000	300,000	64,000



2 장

시작하기 ISE-PIC

관리자 액세스 콘솔

다음 단계에서는 관리 포털에 로그인하는 방법을 설명합니다.

시작하기 전에

Cisco ISE-PIC를 올바르게 설치(또는 업그레이드)하고 구성했는지 확인합니다. Cisco ISE-PIC의 설치, 업그레이드 및 컨피그레이션에 대한 자세한 정보와 지원은 *Identity Services Engine Passive Identity Connector(ISE-PIC)* 설치 및 관리자 가이드를 참조하십시오.

단계 **1** 브라우저의 주소 표시줄에서 Cisco ISE-PIC URL을 입력합니다(예: https://<ise 호스트 이름 또는 IP 주소>/admin/).

단계 **2** 초기 Cisco ISE 설정 중에 지정 및 구성한 사용자 이름과 대/소문자를 구분한 비밀번호를 입력합니다.

단계 **3** **Login(**로그인**)**을 클릭하거나 **Enter** 키를 누릅니다.

로그인이 실패하면 로그인 페이지에서 **Problem logging in?(**로그인하는 데 문제가 있나요**?)** 링크를 클릭하여 지침을 따릅니다.

관리자 로그인 브라우저 지원

Cisco ISE 관리 포털은 다음 HTTPS 사용 가능 브라우저를 지원합니다.

- Mozilla Firefox 61 이하 버전
- Mozilla Firefox ESR 60.9 이하 버전
- Google Chrome 84 이하 버전

ISE 커뮤니티 리소스

Adblock Plus 사용 시 ISE 페이지가 완전히 로드되지 않는 경우

실패한 로그인 시도 이후에 관리자 잠금

관리자 사용자 ID의 암호를 여러 번 잘못 입력하면 지정된 시간 동안 구성에 따라 계정이 일시 중단되거나 잠기게 됩니다. 잠그도록 선택하면 관리 포털이 시스템에서 "잠금" 상태가됩니다. Cisco ISE는 서버 관리자 로그인 보고서에 로그 항목을 추가하고 해당 관리자 ID의 자격 증명을 일시 중단합니다. Cisco Identity Services Engine 설치 가이드의 "관리자 잠금에 따라 비활성화된 암호 재설정" 섹션에 설명된 대로 해당 관리자 ID의 암호를 재설정할 수 있습니다. 관리자 계정을 비활성화하기 전에 허용되는 시도 실패 횟수는 *Cisco Identity Services Engine* 관리자 가이드의 Cisco ISE-PIC에 대한 관리 액세스, 143 페이지 섹션에 설명된 대로 구성할 수 있습니다. 관리자 사용자 계정이 잠기면 Cisco ISE는 해당 정보가 구성된 경우 연결된 관리자에게 이메일을 보냅니다.

Diffie-Hellman 알고리즘을 사용하여 **SSH** 키 교환 보호

Diffie-Hellman-Group14-SHA1 SSH 키 교환만 허용하도록 Cisco ISE-PIC를 구성할 수 있습니다. 이렇게 하려면 Cisco ISE-PIC CLI(Command-Line Interface) 환경 설정 모드에서 다음 명령을 입력해야 합니다.

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

아래에 이 명령의 예제가 나와 있습니다.

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

초기 설정 및 컨피그레이션

Cisco ISE-PIC를 빠르게 사용하려면 다음 흐름을 따르십시오.

1. 라이센스를 설치하고 등록합니다. 자세한 내용은 Cisco ISE-PIC 라이센싱, 11 페이지를 참고하십시오.
2. DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버, 13 페이지를 참고하십시오.
3. NTP 서버의 시계 설정을 동기화합니다.
4. ISE-PIC 설정을 사용하여 초기 서비스 제공자를 구성합니다. 자세한 내용은 다음을 참조하십시오. PassiveID(패시브 ID) 설정 시작하기 , 18 페이지
5. 단일 또는 다중 가입자를 구성합니다. 자세한 내용은 다음을 참조하십시오. Subscribers(가입자), 73 페이지

최초 서비스 제공자와 가입자를 설정하면 추가 서비스 제공자를 쉽게 생성하고(제공자, 33 페이지 참조) ISE-PIC에서 다른 서비스 제공자의 패시브 ID를 관리할 수 있습니다(PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 ISE-PIC, 149 페이지 참조).

Cisco ISE-PIC 라이센싱

Cisco ISE-PIC는 90일 평가 기간과 함께 제공됩니다. 90일 평가 라이센스 만료 후 Cisco ISE-PIC를 계속 사용하려면 라이센스를 얻어 시스템에 등록해야 합니다. ISE-PIC는 평가 라이센스 만료 90, 60, 30일 전에 사용자에게 알림을 보냅니다.

각 영구 라이센스는 단일 ISE-PIC 노드에 업로드되며 , 구축에 노트가 2개 있다면 두 번째 노드에 대한 별도의 라이센스를 받아야 합니다. 설치가 끝나면 UDI별로 별도의 라이센스를 생성한 다음 각 노드에 개별적으로 라이센스를 추가합니다.

라이센싱 설치 및 등록 흐름

1. ISE-PIC 라이센스를 설치하고 등록합니다. ISE-PIC 라이센스 설치 및 등록에 관한 자세한 내용은 라이센스 등록, 12 페이지 항목을 참조하십시오. 라이센스는 다음 시점에 설치할 수 있습니다.
   - ISE-PIC 설치 직후
   - 90일 평가 기간 중 언제든지
2. 먼저 Cisco ISE-PIC 업그레이드 라이선스를 설치한 다음 다음을 수행 하 여 기본 ISE 구축으로 쉽게 업그레이드할 수 있습니다.
   - Base ISE license(기본 ISE 라이센스)를 설치하여 이전 ISE-PIC 노드를 구축을 위한 기본 관리 노드(PAN)로 사용합니다.
   - 업그레이드된 PIC ISE-PIC 노드를 기존 ISE 구축에 추가합니다.
3. 다른 관련 라이센스(Plus, Apex, TACACs+ 등)를 설치하여 기본 ISE 구축을 쉽게 업그레이드하고 스마트 라이센싱으로 업그레이드합니다. ISE 라이센스 설치에 관한 자세한 내용은 *Cisco Identity Services Engine* 관리자 설명서를 참조하십시오.

Cisco ISE 라이센싱 패키지

표 ***3:*** 전체 ***Cisco ISE*** 라이센싱 패키지 옵션

ISE 라이센스 패키지	영구/서브스크립션**(**사용 가능한 기간**)**	포함된 **ISE** 기능	메모
ISE-PIC	영구	패시브 ID 서비스	노드당 라이센스 1개. 각 라이센스는 병렬 세션을 3,000개까지 지원합니다.

ISE-PIC upgrade	영구	이 라이센스는 다음 옵션을 허용합니다. • 추가(최대 300,000개) 병렬 세션을 활성화합니다. • 전체 ISE 인스턴스로 업그레이드	노드당 라이센스 1개. 각 라이센스는 병렬 세션을 300,000개까지 지원합니다. 이 라이센스를 설치하면 업그레이드된 노드가 기존 ISE 구축에 가입할 수 있습니다. 기본 라이센스를 노드에 설치하여 PAN으로 작동하게 할 수도 있습니다.
Base	영구	• 기본 네트워크 액세스: AAA, IEEE-802.1X • 게스트 서비스 • 링크 암호화(MACSec) • TrustSec • ISE 애플리케이션 프로그래밍 인터페이스	
평가	임시(90일)	90일 동안 전체 ISE-PIC 기능을 활성화합니다.	

라이센스 등록

시작하기 전에

ISE-PIC 설치가 끝나면 90일 평가 기간이 진행됩니다. 작업을 원활하게 진행하려면 ISE-PIC 라이센스를 구매, 등록 및 설치해야 합니다. 만료일 전에 라이센서를 등록하고 설치하지 않고 만료일 후에 ISE-PIC에 액세스하면, 모든 ISE-PIC 서비스가 비활성화되고 프로세스를 완료할 수 있는 **Import License(**라이센스 가져오기**)** 영역으로 자동 이동합니다. ISE-PIC 라이센스 관련 문의는 Cisco 파트너/계정 팀에 하십시오.

단계 **1** Cisco 웹사이트(www.cisco.com)의 주문 시스템(CCW - Cisco Commerce Workspace)에서 필요한 라이센스를 주문할 수 있습니다. 구축 내 ISE-PIC 노드별로 라이센스가 하나씩 필요합니다(구축별로 노드 최대 2개).

약 1시간 후에 PAK(Product Authorization Key)가 포함된 확인 이메일이 전송됩니다.

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Licensing(**라이센싱**)**. **Licensing Details(**라이센싱 세부사항**)** 섹션에서 PID(Product Identifier), VID(Version Identifier), SN(Serial Number) 등의 노드 정보를 적어 둡니다.

단계 **3** www.cisco.com/go/licensing으로 이동한 다음 메시지가 표시되면 받은 라이센스의 PAK, 노드 정보 및 회사에 대한 몇 가지 세부사항을 입력합니다.

1일 후에 Cisco에서 라이센스 파일을 전송합니다.

단계 **4** 시스템에서 쉽게 확인할 수 있는 위치에 이 라이센스 파일을 저장합니다.

단계 **5** Cisco ISE-PIC 관리 포털에서 다음을 선택합니다. **Administration(**관리**)** > **Licensing(**라이센싱**)**.

단계 **6** **Licenses(**라이센스**)**섹션에서 **Import License(**라이센스 가져오기**)** 버튼을 클릭합니다.

단계 **7** **Choose File(**파일 선택**)**을 클릭하고 이전에 시스템에 저장한 라이센스 파일을 선택합니다.

단계 **8** **Import(**가져오기**)**를 클릭합니다.

이제 새 라이센스가 시스템에 설치되었습니다.

다음에 수행할 작업

라이센싱 대시보드, **Administration(**관리**)** > **Licensing(**라이센싱**)**을 선택하고 새로 입력한 라이센스가 올바른 세부사항과 함께 표시되는지 확인합니다.

라이센스 제거

시작하기 전에

만료되었거나 불필요한 라이센스를 제거하면 팝업 알림이 표시되지 않으며 라이센싱 대시보드에서 공간이 확보됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Licensing(**라이센싱**)**

단계 **2** **License Files(**라이센스 파일**)** 섹션에서 관련 파일 이름 옆의 확인란을 클릭하고 **Delete License(**라이센스 삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

DNS 서버

DNS 서버를 구성하는 경우 주의해야 할 사항은 다음과 같습니다.

- Cisco ISE에 구성한 DNS 서버는 사용자가 사용하려는 도메인에 대한 정방향 및 역방향 DNS 쿼리를 모두 확인할 수 있어야 합니다.
- DNS 회귀는 지연을 유발하고 심각한 성능 저하를 유발할 수 있으므로, 권한 있는 DNS 서버를 통해 Active Directory 레코드 확인하는 것이 좋습니다.
- 모든 DNS 서버는 추가 사이트 정보 사용 여부와 관계없이 DC, GC 및 KDC에 대한 SRV 쿼리에 응답할 수 있어야 합니다.
- Cisco에서는 성능 향상을 위해서는 서버 IP 주소를 SRV 응답에 추가하는 방법을 권장합니다.

- DNS 서버를 사용하여 공용 인터넷에 쿼리하면 안 됩니다. 이 경우 알 수 없는 이름을 확인해야 할 때 네트워크 관련 정보가 유출될 수 있습니다.

시스템 시간 및 **NTP** 서버 설정 지정

Cisco ISE-PIC에서는 최대 3개의 NTP(Network Time Protocol) 서버를 구성할 수 있습니다. NTP 서버를 사용하면 정확한 시간을 유지하고 서로 다른 표준 시간대 간에 시간을 동기화할 수 있습니다. 또한 Cisco ISE-PIC가 인증된 NTP 서버만 사용해야 하는지 여부를 지정할 수 있으며 이를 위해 인증 키를 하나 이상 입력할 수 있습니다.

모든 Cisco ISE-PIC 노드는 협정 세계시(UTC) 표준 시간대로 설정하는 것이 좋습니다. . 이 절차를 수행하면 구축 내 여러 노드의 보고서 및 로그에서 타임스탬프가 항상 동기화됩니다.

Cisco ISE는 또한 NTP 서버에 대 한 공개 키 인증을 지원 합니다. NTPv4는 대칭 키 암호화를 사용하며, 공개 키 암호화를 기반으로 하는 새로운 Autokey 스키마도 제공합니다. 공개 키 암호화는 일반적으로 대칭 키 암호화 보다 안전하다고 간주됩니다. 보안이 각 서버에서 생성하며 절대로 공개되지 않는 비공개 값을 기반으로 하기 때문입니다. Autokey를 사용하면 모든 키 배포 및 관리 기능에 공개 값만 포함되며, 따라서 키 배포 및 저장이 대폭 간소화됩니다.

Configuration Mode(구성 모드)에서 Cisco ISE CLI의 NTP 서버용 Autokey를 구성할 수 있습니다. 가장 많이 사용하는 IFF(Friend 또는 Foe 식별) 식별 스키마 사용을 권장합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **System Time(**시스템 시간**)**

단계 **2** NTP 서버의 고유한 IP 주소(IPv4/IPv6/FQDN)를 입력합니다.

단계 **3** Cisco ISE가 인증된 NTP 서버만 사용하여 시스템 및 네트워크 시간을 유지하도록 제한하려면 **Only allow authenticated NTP servers(**인증된 **NTP** 서버만 허용**)** 확인란을 선택합니다.

단계 **4** (선택 사항) 개인 키를 이용하여 NTP 서버를 인증하고 싶다면 **NTP Authentication Keys(NTP** 인증 키**)** 탭을 클릭하고, 지정하는 서버에서 인증 키를 통한 인증을 수행해야 하는 경우 다음과 같이 인증 키를 하나 이상 지정합니다.

a) **Add(**추가**)**를 클릭합니다.

b) 필요한 **Key ID(**키 **ID)** 및 **Key Value(**키 값**)**을 입력합니다. 드롭다운 목록에서 **HMAC**를 선택합니다.Key ID(키 ID) 필드에는 1~65,535 사이의 숫자 값을 입력할 수 있으며 Key Value(키 값) 필드에는 영숫자 문자를 15자까지 입력할 수 있습니다.

c) NTP 서버 인증 키 입력을 완료한 후 NTP Server Configuration(NTP 서버 컨피그레이션) 탭으로 돌아옵니다.

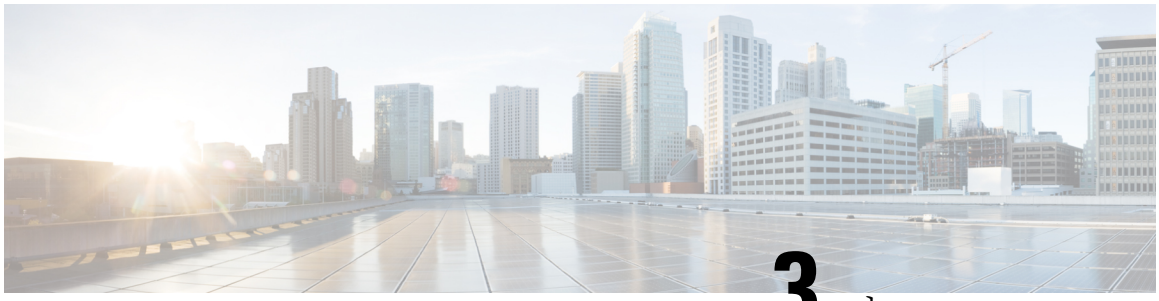
단계 **5** (선택 사항) 공개 키 인증을 사용하여 NTP 서버를 인증하려는 경우 CLI(command-line interface)의 Cisco ISE에서 Autokey를 구성합니다. 자세한 내용은 해당 ISE 릴리스용 Cisco Identity Services Engine CLI 참조 가이드에서 **ntp server** 및 **crypto** 명령을 참조하십시오.

단계 **6** **Save(**저장**)**를 클릭합니다.

ISE-PIC Home(홈) Dashboard(대시보드)

Cisco ISE-PICHome(홈) 대시보드에는 상관관계가 분석되고 통합된 요약 및 통계 데이터가 표시되는데, 이는 효과적인 모니터링 및 문제 해결을 위해서는 필수적이며 실시간으로 업데이트됩니다. dashlet에서는 별도의 설명이 없는 한 지난 24시간 동안의 활동을 표시합니다.

- **Main(**기본**)** 보기에는 선형 메트릭 대시보드, 차트 dashlet 및 목록 dashlet이 있습니다. ISE-PIC에서는 dashlet을 구성할 수 없습니다. 일부 dashlet은 비활성화되어 있으며 ISE의 전체 버전에서만 사용할 수 있습니다. 엔드포인트 데이터를 표시하는 dashlet을 예로 들 수 있습니다. 제공되는 dashlet은 다음과 같습니다.
  - **Passive Identity Metrics(**패시브 **ID** 메트릭**)** - 현재 추적 중인 총 고유 라이브 세션 수, 시스템에 구성된 총 ID 제공자 수, ID 데이터를 능동적으로 전달하는 총 에이전트 수, 현재 구성된 총 가입자 수를 표시합니다.
  - **Provider(**제공자**)** - 제공자는 사용자 ID 정보를 ISE-PIC에 제공합니다. 제공자 소스에서 정보를 수신하는 데 사용할 ISE-PIC 프로브(주어진 소스에서 데이터를 수집하는 메커니즘)를 구성합니다. 예를 들어 AD(Active Directory) 프로브와 에이전트 프로브는 각기 다른 기술을 사용하여 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 파서에서 데이터를 수집합니다.
  - **Subscribers(**가입자**)** - 가입자는 사용자 ID 정보를 검색하기 위해 ISE-PIC에 연결합니다.
  - OS Types (OS 유형)-표시 할 수있는 OS 유형은 Windows뿐입니다. Windows 유형은 Windows 버전별로 표시됩니다. 제공자는 OS 유형을 보고하지 않지만 ISE-PIC는 Active Directory를 쿼리하여 해당 정보를 가져올 수 있습니다. dashlet에는 최대 1,000개의 항목이 표시됩니다. 이보다 많은 엔드 포인트가 있거나 Windows보다 많은 OS 유형을 표시하려는 경우 ISE로 업그레이드 할 수 있습니다.
  - **Alarms(**알람**)** - 사용자 ID 관련 알람입니다.
- **Additional(**추가**)** 보기에는 PIC의 활성 세션 및 PIC 시스템의 시스템 요약이 표시됩니다.



3 장

프로브 및 제공자로서의 Active Directory

Active Directory(AD)는 사용자 이름, IP 주소 및 도메인 이름 같은 사용자 ID 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

AD 프로브인 패시브 ID 서비스는 WMI 기술을 이용해 AD에서 사용자 ID 정보를 수신하지만, 다른 프로브는 다른 기술 과 방법을 이용해 AD를 사용자 ID 제공자로 사용합니다. ISE-PIC에서 제공하는 다른 프로브 및 제공자 유형에 관한 자세한 내용은 제공자, 33 페이지 항목을 참조하십시오.

Active Directory 프로브를 구성하면 (마찬가지로 Active Directory를 소스로 사용하는) 이러한 다른 프로브를 빠르게 구성하고 활성화할 수 있습니다.

- Active Directory 에이전트, 35 페이지

  참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

- SPAN, 45 페이지
- 엔드포인트 프로브, 69 페이지

또한 사용자 정보를 수집할 때 AD 사용자 그룹을 사용할 수 있도록 Active Directory 프로브를 구성합니다. AD 사용자 그룹을 AD, 에이전트, SPAN 및 Syslog 프로브에 사용할 수 있습니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 23 페이지 항목을 참조하십시오.

- Active Directory 작업, 17 페이지
- Active Directory 설정, 28 페이지

Active Directory 작업

패시브 ID 서비스에 대한 Active Directory 프로브를 구성하기 전에 다음을 확인하십시오.

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않습니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았습니다.

- DNS 서버를 올바르게 구성했는지 확인합니다(ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버, 13 페이지를 참고하십시오.
- NTP 서버의 시계 설정을 동기화합니다. 자세한 내용은 시스템 시간 및 NTP 서버 설정 지정, 14 페이지를 참고하십시오.

참고 Cisco ISE-PIC가 Active Directory에 연결되어 있는 경우 작동 문제가 발생하면 **Reports(**보고서**)** 아래의 AD Connector 운영 보고서를 참고해 주십시오. 자세한 내용은 사용 가능한 보고서, 152 페이지의 내용을 참조하십시오.

PassiveID(패시브 ID) 설정 시작하기

ISE-PIC Active Directory를 첫 번째 사용자 ID 제공자로 쉽고 빠르게 구성하여 Active Directory에서 사용자 ID를 수신할 수 있는 마법사를 제공합니다. ISE-PIC용으로 Active Directory를 구성하면, 나중에 다른 제공자 유형도 쉽게 구성할 수 있습니다. Active Directory를 구성한 후에는 가입자(isco FMC(Firepower Management Center) 또는 Stealthwatch 등)를 구성해야 사용자 데이터를 수신할 클라이언트를 정의할 수 있습니다. 가입자에 관한 자세한 내용은 Subscribers(가입자), 73 페이지 항목을 참조하십시오.

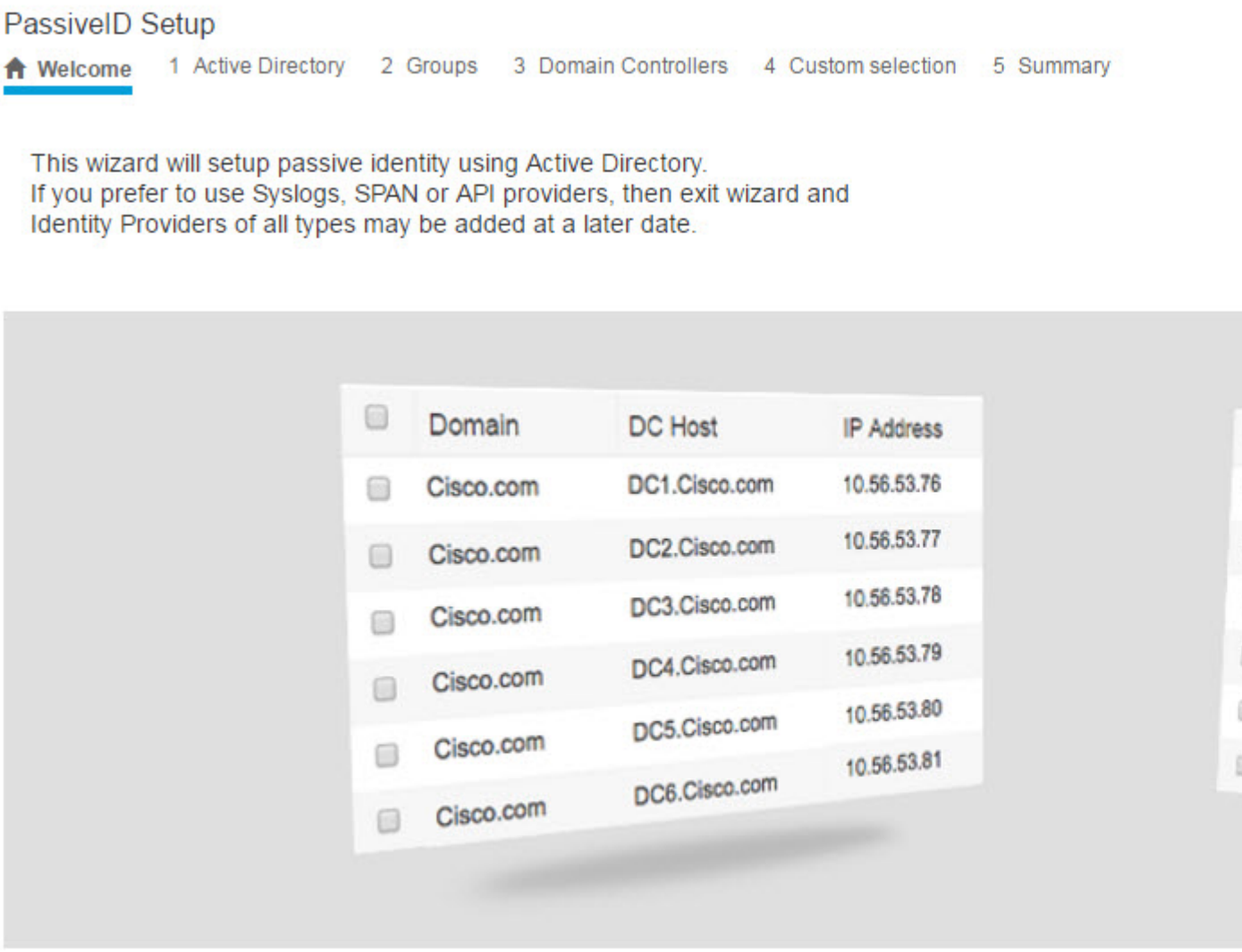
시작하기 전에

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않는지 확인합니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았는지 확인합니다.
- ISE-PIC에 DNS(도메인 이름 서버)의 항목이 있는지 확인합니다. ISE-PIC에서 클라이언트 머신에 대한 역방향 조회를 올바르게 구성했는지 확인합니다. 자세한 내용은 다음을 참조하십시오. DNS 서버, 13 페이지

단계 **1** 다음 메뉴를 선택합니다. **Home(**홈**)** > **Introduction(**소개**)**. Passive Identity Connector Overview(패시브 ID 커넥터 개요) 화면에서 **Passive Identity Wizard(**패시브 **ID** 마법사**)**를 클릭합니다.

PassiveID Setup(패시브 ID 설정)이 열립니다.

그림 ***2: PassiveID Setup(***패시브 ***ID*** 설정***)***



단계 **2** **Next(**다음**)**를 클릭하여 마법사를 시작합니다.

단계 **3** 이 Active Directory 조인 포인트의 고유한 이름을 입력합니다. 이 노드가 연결된 Active Directory 도메인의 도메인 이름을 입력하고 Active Directory 관리자의 사용자 이름과 비밀번호를 입력합니다. Active Directory 설정에 관한 자세한 내용은 다음 항목을 참고하십시오. Active Directory 설정, 28 페이지

관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭하여 Active Directory 그룹을 정의하고 포함 및 모니터링할 사용자 그룹을 확인합니다. Active Directory 사용자 그룹은 이전 단계에서 구성한 Active Directory 조인 포인트에 따라 자동으로 표시됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다. 모니터링할 DC를 선택합니다. Custom(사용자 지정)을 선택했다면 다음 화면에서 모니터링할 특정 DC를 선택합니다. 모두 마쳤으면 **Next(**다음**)**를 클릭합니다.

단계 **6** **Exit(**종료**)**를 클릭하여 마법사를 완료합니다.

다음에 수행할 작업

Active Directory를 초기 제공자로 구성하는 작업이 끝나면, 추가 제공자 유형도 쉽게 구성할 수 있습니다. 자세한 내용은 제공자, 33 페이지를 참고하십시오. 나아가 정의한 제공자가 수집하는 사용자 ID 정보를 수신하도록 지정된 가입자를 구성할 수도 있습니다. 자세한 내용은 Subscribers(가입자), 73 페이지를 참고하십시오.

Active Directory(WMI) 프로브 단계별 설정

패시브 ID 서비스에 대해 Active Directory 및 WMI를 구성하려면 PassiveID(패시브 ID) 설정 시작하기, 18 페이지를 사용하거나 다음과 같이 이 장의 단계를 수행합니다.

1. Active Directory 도메인을 구성합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입, 20 페이지를 참조하십시오.
2. AD 로그인 이벤트를 수신하는 WMI 구성 노드(또는 노드 모음)에 대한 Active Directory 도메인 컨트롤러 목록을 생성합니다. 도메인 컨트롤러 추가, 22 페이지를 참조하십시오.
3. ISE-PIC와 통합할 수 있도록 Active Directory를 구성합니다. 패시브 ID용 WMI 구성, 24 페이지를 참조하십시오.
4. (선택 사항) Active Directory 제공자 관리, 24 페이지.

Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입

시작하기 전에

Cisco ISE-PIC 노드가 NTP 서버, DNS 서버, 도메인 컨트롤러 및 전역 카탈로그 서버가 있는 네트워크와 통신할 수 있는지 확인합니다.

Active Directory에 더해 의 에이전트, 시스템 로그, SPAN 및 엔드포인트 프로브까지 사용하려면 조인 포인트를 생성해야 합니다.

Active Directory와 통합할 때 IPv6을 사용하려면 관련 ISE-PIC 노드에 대해 IPv6 주소를 구성했는지 확인해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Add(**추가**)**를 클릭하고 **Active Directory Join Point Name(Active Directory** 가입 포인트 이름**)** 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다. 자세한 내용은 표 4: Active Directory 조인 포인트 이름 설정 및 도메인 조인 창, 28 페이지의 내용을 참조하십시오.

단계 **3** **Submit(**제출**)**을 클릭합니다.

새로 생성하는 가입 포인트를 도메인에 가입시킬지를 묻는 팝업 메시지가 표시됩니다. 가입 포인트를 도메인에 즉시 가입시키려면 **Yes(**예**)**를 클릭합니다.

No(아니오**)**를 클릭하고 컨피그레이션을 저장하면 Active Directory 도메인 컨피그레이션이 전역적으로 저장되지만 Cisco ISE-PIC 노드가 도메인에 가입되지는 않습니다.

단계 **4** 새로 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**편집**)**. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다. 자세한 내용은 표 5: Active Directory 가입/탈퇴 창, 29 페이지의 내용을 참조하십시오.

단계 **5** 3단계를 진행하는 도중 가입 포인트가 도메인에 가입되지 않은 경우 관련 Cisco ISE-PIC 노드 옆의 확인란을 선택하고 **Join(**가입**)**을 클릭하여 Cisco ISE-PIC 노드를 Active Directory 도메인에 가입시킵니다.

컨피그레이션을 저장한 경우에도 이 작업을 명시적으로 수행해야 합니다. 단일 작업에서 도메인에 여러 Cisco ISE-PIC 노드를 가입시키려면 모든 가입 작업에 사용할 계정의 사용자 이름 및 비밀번호가 같아야 합니다. 각 Cisco ISE-PIC 노드를 가입시키는 데 필요한 사용자 이름 및 비밀번호가 다른 경우에는 각 Cisco ISE-PIC 노드에 대해 가입 작업을 개별적으로 수행해야 합니다.

단계 **6** **Join Domain(**도메인 가입**)** 대화 상자에서 Active Directory 사용자 이름 및 비밀번호를 입력합니다.

관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

가입 작업에 사용되는 사용자는 도메인 자체에 있어야 합니다. 사용자가 다른 도메인이나 하위 도메인에 있는 경우에는 jdoe@acme.com과 같이 UPN 표기법으로 사용자 이름을 표기해야 합니다.

단계 **7** (선택 사항) **Specify Organizational Unit(**조직 단위 지정**)** 확인란을 선택합니다.

CN=Computers,DC=someDomain,DC=someTLD 이외의 특정 조직 단위에 Cisco ISE-PIC 노드 머신 계정을 배치하려는 경우 이 확인란을 선택해야 합니다. Cisco ISE-PIC는 지정된 조직 단위에 머신 계정을 생성하거나, 머신 계정이 이미 있는 경우 이 위치로 이동합니다. 조직 단위를 지정하지 않으면 Cisco ISE-PIC에서는 기본 위치를 사용합니다. 값은 완전한 DN(Distinguished Name) 형식으로 지정해야 합니다. 구문은 Microsoft 지침을 따라야 합니다. /'+,;=<> 줄 바꿈, 공백, 캐리지 리턴 등의 특수 예약 문자는 백슬래시(\)로 이스케이프 처리해야 합니다. 예를 들면 OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 및 Workstations,DC=someDomain,DC=someTLD와 같습니다. 머신 계정이 이미 생성된 경우에는 이 확인란을 선택하지 않아도 됩니다. Active Directory 도메인에 가입한 후 머신 계정의 위치를 변경할 수도 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Active Directory 도메인에 가입시킬 노드를 두 개 이상 선택할 수 있습니다.

가입 작업이 실패하면 오류 메시지가 나타납니다. 각 노드에 대한 오류 메시지를 클릭하면 해당 노드의 상세 로그를 확인할 수 있습니다.

참고 조인이 완료되면 Cisco ISE-PIC는 자신의 AD 그룹과 대응하는 SIDS를 업데이트합니다. Cisco ISE-PIC는 SID 업데이트 프로세스를 자동으로 시작합니다. 이 프로세스를 완료할 수 있는지를 확인해야 합니다.

참고 DNS SRV 레코드가 없으면 Cisco ISE-PIC를 Active Directory 도메인에 가입시키지 못할 수도 있습니다. 가입시키려는 도메인에 대해 도메인 컨트롤러가 해당 SRV 레코드를 보급하지 않기 때문입니다. 문제 해결 정보는 다음 Microsoft Active Directory 설명서를 참조하십시오.

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

참고 ISE에서 최대 200개의 도메인 컨트롤러를 추가할 수 있습니다. 제한을 초과하면 "Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200(<DC FQDN> 생성 오류 - DC 수가 허용된 최대 200개를 초과)" 오류가 표시됩니다.

다음에 수행할 작업

도메인 컨트롤러 추가, 22 페이지

Active Directory 사용자 그룹 구성, 23 페이지

패시브 ID용 WMI 구성, 24 페이지

도메인 컨트롤러 추가

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다.

단계 **3** 참고 Passive Identity(패시브 ID) 서비스용으로 새 DC(Domain Controller)를 추가하려면 해당 DC의 로그인 자격 증명이 필요합니다.

PassiveID(패시브 ID) 탭으로 이동하여 **Add DCs(DC** 추가**)**를 클릭합니다.

단계 **4** 모니터링을 위해 조인트 포인트에 추가할 도메인 컨트롤러 옆의 확인란을 선택하고 **OK (**확인**)**를 클릭합니다. 도메인 컨트롤러는 PassiveID(패시브 ID) 탭의 Domain Controller(도메인 컨트롤러) 목록에 표시됩니다.

단계 **5** 도메인 컨트롤러를 구성합니다.

a) 도메인 컨트롤러에 체크 표시하고 **Edit(**수정**)**를 클릭합니다. **Edit Item(**항목 수정**)** 화면이 나타납니다.

b) 선택 사항으로, 다른 도메인 컨트롤러 필드를 수정합니다. 자세한 내용은 Active Directory 설정, 28 페이지를 참고하십시오.

c) WMI 프로토콜을 선택했다면 **Configure(**구성**)**를 클릭하여 WMI를 자동으로 구성하고 **Test(**테스트**)**를 클릭하여 연결을 테스트합니다. 자동으로 WMI를 구성하는 방법에 관한 자세한 내용은 패시브 ID용 WMI 구성, 24 페이지 항목을 참조하십시오.

DC 페일오버 메커니즘은 페일오버 시 DC가 선택되는 순서를 지정하는 DC 우선 순위 목록을 기반으로 관리됩니다. DC가 오프라인 상태이거나 오류 때문에 연결할 수 없다면 우선 순위 목록에서 우선

순위가 감소합니다. DC가 다시 온라인 상태가 되면 우선 순위 목록에서 우선 순위가 조정(증가)됩니다.

참고 Cisco ISE는 인증 플로우에 대해 읽기 전용 도메인 컨트롤러를 지원하지 않습니다.

Active Directory 사용자 그룹 구성

Active Directory에서 사용자 ID 정보를 수집하는 다른 프로브로 작업할 때 사용할 수 있도록 Active Directory 사용자 그룹을 구성합니다. Cisco ISE는 내부적으로 SID(Security Identifiers)를 사용하여 모호한 그룹 이름 문제를 해결하고 그룹 매핑을 개선합니다. SID를 통해 정확하게 일치하는 그룹을 할당할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**. 그룹을 추가할 조인 포인트를 클릭합니다.

단계 **2** **Groups(**그룹**)** 탭을 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) 다음 메뉴를 선택합니다. **Add(**추가**)** > **Select Groups From Directory(**디렉터리에서 그룹 선택**)** 그런 다음 기존 그룹을 선택합니다.

b) 다음 메뉴를 선택합니다. **Add(**추가**)** > **Add Group(**그룹 추가**)** 그런 다음 수동으로 그룹을 추가합니다. 그룹 이름과 SID를 모두 입력하거나, 그룹 이름만 입력하고 **Fetch SID(SID** 가져오기**)**를 누를 수 있습니다.

사용자 인터페이스 로그인 시 그룹 이름에 큰따옴표(")를 사용하지 마십시오.

단계 **4** 그룹을 수동으로 선택하는 경우 필터를 사용하여 그룹을 검색할 수 있습니다. 예를 들어 필터 기준으로 **admin***를 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭하면 admin으로 시작하는 사용자 그룹을 확인할 수 있습니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다. 그룹은 한 번에 500개만 검색할 수 있습니다.

단계 **5** 권한 부여 정책에서 사용 가능하도록 지정할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 그룹을 수동으로 추가하도록 선택하는 경우 새 그룹의 이름과 SID를 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고 그룹을 삭제하고 원본과 같은 이름으로 새 그룹을 생성하는 경우에는 **Update SID Values(SID** 값 업데이트**)**를 클릭하여 새로 생성한 그룹에 새 SID를 할당해야 합니다. 업그레이드 후 처음으로 가입하고 나면 SID가 자동으로 업데이트됩니다.

패시브 **ID**용 **WMI** 구성

시작하기 전에

AD 도메인 컨피그레이션을 변경하려면 Active Directory 도메인 관리자 자격 증명이 있어야 합니다. **Administration(**관리**) > System(**시스템**) > Deployment(**구축**)**에서 이 노드에 대해 패시브 ID가 활성화되었는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**) > Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다.

단계 **3** Passive ID(패시브 ID) 탭으로 이동하여 관련 도메인 컨트롤러 옆에 있는 확인란을 선택하고 **Config WMI(WMI** 구성**)**를 클릭하여 ISE-PIC가 선택한 도메인 컨트롤러를 자동으로 구성하게 합니다.
Active Directory 및 도메인 컨트롤러를 수동으로 구성하거나 구성 문제를 해결하는 방법은 Active Directory와 Cisco ISE-PIC 통합을 위한 사전 요건, 171 페이지 항목을 참조하십시오.

Active Directory 제공자 관리

Active Directory 조인 포인트를 생성하고 구성했다면, 이러한 작업을 이용해 Active Directory 프로브를 관리해야 합니다.

Test Users for Active Directory(Active Directory 인증을 위해 사용자 테스트**)Groups(**그룹**)**

Test User(사용자 테스트) 도구를 사용하여 Active Directory에서 사용자 그룹을 확인할 수 있습니다. 단일 가입 포인트 또는 범위에 대해 테스트를 실행할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**) > Active Directory**.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 모든 가입 포인트에서 테스트를 실행하려면 **Advanced Tools(**고급 도구**) > Test User for All Join Points((**모든 가입 포인트에 대해 사용자 테스트**)**.

- 특정 가입 포인트에 대해 테스트를 실행하려면 해당 가입 포인트를 선택하고 **Edit(**편집**)**를 클릭합니다. Cisco ISE-PIC 노드를 선택하고 **Test User(**사용자 테스트**)**를 클릭합니다.

단계 **3** Active Directory에서 사용자 또는 호스트의 사용자 이름 및 비밀번호를 입력합니다.

단계 **4** 인증 유형을 선택합니다. Lookup(조회) 옵션을 선택하는 경우에는 3단계에서 비밀번호를 입력하지 않아도 됩니다.

단계 **5** 모든 가입 포인트에 이 테스트를 실행하는 경우 이 테스트를 실행할 Cisco ISE-PIC 노드를 선택합니다.

단계 **6** Active Directory에서 특성을 Retrieve Groups and Attributes(그룹과 특성 가져오기) 확인란을 선택합니다.

단계 **7** **Test(**테스트**)**를 클릭합니다.
테스트 작업의 결과 및 단계가 표시됩니다. 이러한 단계를 통해 실패 사유 및 문제 해결 상황을 파악할 수 있습니다.

Active Directory에서 각 처리 단계를 수행하는 데 걸린 시간(밀리초)을 볼 수도 있습니다. 작업을 수행한 시간이 임계값을 초과하면 Cisco ISE-PIC에서 경고 메시지가 표시됩니다.

노드의 **Active Directory** 가입 보기

Node View(노드 보기**)** 버튼(**Active Directory** 페이지)을 사용하면 지정된 Cisco ISE-PIC 노드에 대한 모든 Active Directory 가입 포인트의 상태나 모든 Cisco ISE-PIC 노드의 모든 가입 포인트를 확인할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Node View(**노드 보기**)**를 클릭합니다.

단계 **3** **ISE Node(ISE** 노드**)** 드롭다운 목록에서 노드를 선택합니다.
테이블에 노드별 Active Directory 상태가 나열됩니다. 구축에 가입 포인트와 Cisco ISE-PIC 노드가 여러 개 있는 경우 이 테이블이 업데이트되는 데 몇 분 정도 걸릴 수 있습니다.

단계 **4** 가입 포인트 **Name(**이름**)** 링크를 클릭하여 해당 Active Directory 가입 포인트로 이동한 후에 다른 특정 작업을 수행합니다.

단계 **5** **Diagnostic Summary(**진단 요약**)** 열에 있는 링크를 클릭하여 **Diagnostic Tools(**진단 도구**)** 페이지로 이동한 후에 특정 문제를 해결합니다. 진단 도구에는 노드당 각 가입 포인트에 대한 최신 진단 결과가 표시됩니다.

Active Directory 문제 진단

Diagnostic Tool(진단 도구)은 모든 Cisco ISE-PIC 노드에서 실행되는 서비스입니다. Active Directory 구축을 자동으로 테스트 및 진단할 수 있으며, 테스트 집합을 실행하여 Cisco ISE-PIC에서 Active Directory를 사용할 때 기능 또는 성능 오류를 발생시킬 수 있는 문제를 탐지할 수 있습니다.

Cisco ISE-PIC는 여러 이유로 Active Directory에 가입하거나 인증하지 못할 수 있습니다. 이 도구를 사용하면 Cisco ISE-PIC를 Active Directory에 연결하기 위한 사전 요구 사항을 올바르게 구성할 수 있습니다. 그리고 네트워킹, 방화벽 컨피그레이션, 클록 동기화, 사용자 인증 등의 문제를 탐지할 수 있습니다. 이 도구는 단계별 설명서 방식으로 작동하며, 필요한 경우 중간에 모든 레이어의 문제를 해결할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Advanced Tools(**고급 도구**)** 드롭다운을 클릭하고 **Diagnostic Tools(**진단 도구**)**를 선택합니다.

단계 **3** 진단을 실행할 Cisco ISE-PIC 노드를 선택합니다.

Cisco ISE-PIC 노드를 선택하지 않으면 모든 노드에서 테스트가 실행됩니다.

단계 **4** 특정 Active Directory 가입 포인트를 선택합니다.

Active Directory 가입 포인트를 선택하지 않으면 모든 가입 포인트에서 테스트가 실행됩니다.

단계 **5** 진단 보고서는 온디맨드 또는 예약 방식으로 실행할 수 있습니다.

- 테스트를 즉시 실행하려면 **Run Tests Now(**지금 테스트 실행**)**를 선택합니다.
- 예약된 간격으로 테스트를 실행하려면 **Run Scheduled Tests(**예약된 테스트 실행**)** 확인란을 선택하여 테스트를 실행할 시작 시간과 간격(시간, 일 또는 주)을 지정합니다. 이 옵션을 활성화하면 모든 진단 테스트가 모든 노드 및 인스턴스에서 실행되며, **Home(**홈**)** 대시보드의 **Alarms(**알람**)** 데슬렛에서 장애가 보고됩니다.

단계 **6** **View Test Details(**테스트 세부사항 보기**)**를 클릭하여 Warning(경고) 또는 Failed(장애) 상태의 테스트에 대한 세부사항을 확인합니다.
이 테이블을 참조하여 특정 테스트를 다시 실행하고, 실행 중인 테스트를 중지하고, 특정 테스트의 보고서를 확인할 수 있습니다.

Active Directory 도메인 탈퇴

이 Active Directory 도메인이나 이 조인 포인트를 사용하여 사용자 ID를 수집하거나, Active Directory 도메인에서 탈퇴할 수 있습니다.

명령줄 인터페이스에서 Cisco ISE-PIC 애플리케이션 컨피그레이션을 재설정하거나 백업 또는 업그레이드 이후 컨피그레이션을 복원하면 Cisco ISE는 탈퇴 작업을 수행하여 Cisco ISE-PIC 노드가 Active Directory 도메인에 이미 가입되어 있는 경우 해당 도메인에서 노드 연결을 끊습니다. 그러나 Cisco ISE-PIC 노드 계정은 Active Directory 도메인에서 제거되지 않습니다. 관리 포털에서 Active Directory 자격 증명을 사용하여 탈퇴 작업을 수행하는 것이 좋습니다. 이렇게 하면 Active Directory 도메인에서 노드 계정도 제거되기 때문입니다. Cisco ISE-PIC 호스트 이름을 변경할 때도 이 방법을 사용하는 것이 좋습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE-PIC 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 테이블이 표시됩니다. 자세한 내용은 표 5: Active Directory 가입/탈퇴 창, 29 페이지의 내용을 참조하십시오.

단계 **3** Cisco ISE-PIC 노드 옆의 확인란을 선택하고 **Leave(**탈퇴**)**를 클릭합니다.

단계 **4** Active Directory 사용자 이름 및 비밀번호를 입력하고 **OK(**확인**)**를 클릭하여 도메인을 탈퇴시킨 후 Cisco ISE-PIC 데이터베이스에서 머신 계정을 제거합니다.

Active Directory 자격 증명을 입력하는 경우 Active Directory 도메인에서 Cisco ISE-PIC 노드가 탈퇴되며 Active Directory 데이터베이스에서 Cisco ISE-PIC 머신 계정이 삭제됩니다.

참고 Active Directory 데이터베이스에서 Cisco ISE-PIC 머신 계정을 삭제하려면 여기서 입력하는 Active Directory 자격 증명에 도메인에서 머신 계정을 제거할 권한이 있어야 합니다.

단계 **5** Active Directory 자격 증명이 없는 경우에는 **No Credentials Available(**사용 가능한 자격 증명 없음**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

Leave domain without credentials(자격 증명을 사용하지 않고 도메인 탈퇴**)** 확인란을 선택하면 기본 Cisco ISE-PIC 노드가 Active Directory 도메인에서 탈퇴됩니다. 이 경우에는 Active Directory 관리자가 가입 시 Active Directory에서 생성된 머신 계정을 수동으로 제거해야 합니다.

Active Directory 컨피그레이션 삭제

특정 Active Directory 구성을 프로브로 사용하지 않으려는 경우 Active Directory 컨피그레이션을 삭제해야 합니다. 다른 Active Directory 도메인에 가입하려는 경우에는 컨피그레이션을 삭제하지 마십시오. 현재 가입되어 있는 도메인은 그대로 두고 새 도메인에 가입할 수 있습니다. 컨피그레이션이 다음에 있는 유일한 컨피그레이션이라면 삭제해선 안 됩니다. ISE-PIC

시작하기 전에

Active Directory 도메인이 남아 있는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Active Directory**.

단계 **2** 구성되어 있는 Active Directory 옆의 확인란을 선택합니다.

단계 **3** 로컬 노드 상태가 가입되지 않음으로 나열되어 있는지 확인합니다.

단계 **4** **Delete(**삭제**)**를 클릭합니다.

Active Directory 데이터베이스에서 컨피그레이션이 제거되었습니다. 나중에 Active Directory를 사용하려는 경우 유효한 Active Directory 컨피그레이션을 다시 제출하면 됩니다.

Active Directory 디버그 로그 활성화

Active Directory 디버그 로그는 기본적으로 기록되지 않습니다. Active Directory 디버그 로그를 활성화하는 경우 ISE-PIC 성능에 영향을 줄 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration** > **Logging(**로깅**)** > **Debug Log Configuration(**디버그 로그 구성**)**.

단계 **2** Active Directory 디버그 정보를 가져올 Cisco ISE-PIC 노드 옆의 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 **3** **Active Directory** 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 **4** Active Directory 옆의 드롭다운 목록에서 **DEBUG**를 선택합니다. 여기에는 오류, 경고 및 자세한 정보 표시 로그가 포함됩니다. 전체 로그를 가져오려면 **TRACE**를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Active Directory 설정

Active Directory(AD)는 사용자 이름과 IP 주소 같은 사용자 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

조인 포인트를 생성하고 수정하여 Active Directory 프로브를 생성하고 관리하려면 **Providers(**제공자**)** > **Active Directory**.

자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입, 20 페이지를 참고하십시오.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** 그런 다음 수정할 조인 포인트를 체크한 다음 **Edit(**수정**)**를 클릭합니다. Join Domain(도메인 가입) 화면에서 **Providers(**제공자**)** > **Active Directory**를 선택한 다음 수정할 조인 포인트를 선택하고 **Join(**조인**)**을 클릭합니다.

표 ***4: Active Directory*** 조인 포인트 이름 설정 및 도메인 조인 창

필드 이름	설명
조인 포인트 이름	구성한 조인 포인트를 빠르고 쉽게 구분할 수 있는 고유한 이름입니다.
Active Directory 도메인	이 노드가 연결된 Active Directory 도메인의 도메인 이름입니다.
도메인 관리자	관리자 권한이 있는 Active Directory 사용자의 사용자 원이름 또는 사용자 계정 이름입니다.
비밀번호	Active Directory에 구성한 도메인 관리자의 암호입니다.
조직 단위 지정	관리자의 조직 단위 정보를 입력합니다.
자격 증명 저장	관리자의 사용자 이름이나 암호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다. 엔드포인트 프로브의 경우에는 **Store credentials(**자격 증명 저장**)**를 반드시 선택해야 합니다.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory**.

표 ***5: Active Directory*** 가입/탈퇴 창

필드 이름	설명
ISE 노드	설치 내 특정 노드의 URL입니다.
ISE 노드 역할	노드가 설치 내 기본 노드인지 보조 노드인지를 나타냅니다.
상태	노드가 Active Directory 도메인에 적극적으로 가입했는지를 나타냅니다.
도메인 컨트롤러	Active Directory에 가입한 노드의 경우 이 열은 Active Directory 도메인에서 노드가 연결된 특정 도메인 컨트롤러를 나타냅니다.
사이트	전체 ISE 설치에만 적용됩니다. 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드, 138 페이지를 참고하십시오.

표 ***6:*** 패시브 ***ID DC(***도메인 컨트롤러***)*** 목록

필드	설명
도메인	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름입니다.
DC 호스트	도메인 컨트롤러가 있는 호스트입니다.
사이트	전체 ISE 설치에만 적용됩니다. 자세한 내용은 전체 ISE 설치로 ISE-PIC 업그레이드, 138 페이지를 참고하십시오.
IP 주소	도메인 컨트롤러의 IP 주소.

필드	설명
모니터링	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이저트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 35 페이지 항목을 참조하십시오.

표 *7:* 패시브 ***ID DC(Domain Controller,*** 도메인 컨트롤러***)*** 편집 화면

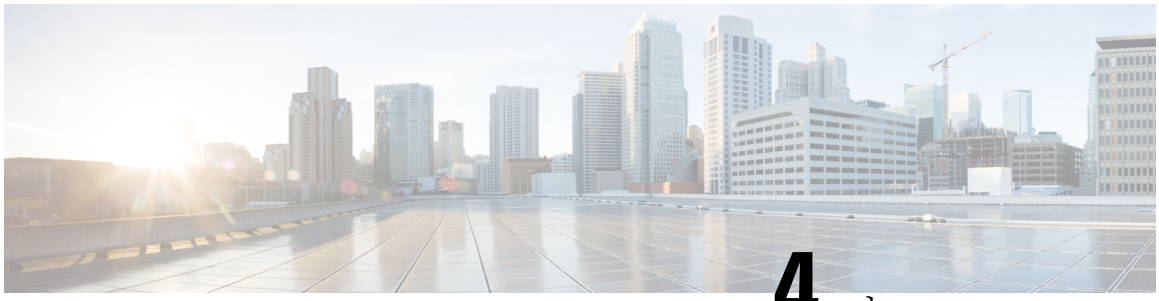
필드 이름	설명
호스트 **FQDN**	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름을 입력합니다.
설명	쉽게 식별할 수 있도록 이 도메인 컨트롤러에 관한 고유한 설명을 입력합니다.
사용자 이름	Active Directory에 액세스하는 데 사용하는 관리자의 사용자 이름입니다.
비밀번호	Active Directory에 액세스하는 데 사용하는 관리자의 암호입니다.
프로토콜	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이저트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 35 페이지 항목을 참조하십시오.

Active Directory 그룹은 Active Directory에서 정의하고 관리하며, 이 탭에서는 이 노드에 가입한 Active Directory의 그룹을 확인할 수 있습니다. Active Directory에 관한 자세한 내용은 https://msdn.microsoft.com/en-us/library/bb742437.aspx 항목을 참조하십시오.

다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** > **Advanced Settings(**고급 설정**)**.

표 ***8: Active Directory*** 고급 설정

필드 이름	설명
기록 간격	이미 수행된 사용자 로그인 정보를 패시브 ID 서비스에서 읽는 시간입니다. 패시브 ID 서비스를 시작하거나 재시작할 때 서비스를 사용할 수 없었던 시간 동안 생성된 이벤트를 확인하려면 이 시간을 설정해야 합니다. 활성 상태인 엔드포인트 프로브는 이 간격의 빈도를 유지합니다.
사용자 세션 에이징 타임	사용자가 로그인할 수 있는 시간입니다. 패시브 ID 서비스는 DC에서 새 사용자 로그인 이벤트를 식별하지만, DC는 사용자가 로그오프할 때는 보고하지 않습니다. 에이징 시간을 설정하면 ISE-PIC는 사용자가 로그인되어 있는 시간 간격을 확인할 수 있습니다.
NTLM 프로토콜 설정	ISE-PIC와 DC 간의 통신 프로토콜로는 NTLMv1 또는 NTLMv2를 선택할 수 있습니다. NTLMv2rk 권장 기본값입니다.



4 장

제공자

ISE-PIC가 서비스에 가입한 고객(가입자)에게 ID 정보를 제공하게 하려면, 먼저 ID 제공자에 연결되는 ISE-PIC 프로브를 구성해야 합니다.

아래 표에는 ISE-PIC에서 사용 가능한 모든 제공자 및 프로브 유형에 대한 세부 사항이 나와 있습니다. Active Directory에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 17 페이지 항목을 참조하십시오.

다음과 같은 제공자 유형을 정의할 수 있습니다.

표 *9:* 제공자 유형

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
AD(Active Directory)	대단히 안전하고 정확하며 가장 자주 사용하는 소스로, 사용자 정보를 수신하는 곳입니다. 프로브로서 AD는 WMI 기술을 이용해, 인증된 사용자 ID를 전달합니다. 프로브로서가 아닌 AD 자체는 다른 프로브가 사용자 데이터를 검색하는 소스 시스템(제공자) 역할을 합니다.	Active Directory 도메인 컨트롤러	WMI	• 사용자 이름 • IP 주소 • 도메인	프로브 및 제공자로서의 Active Directory, 17 페이지
에이전트	Active Directory 도메인 컨트롤러 또는 멤버 서버에 설치된 네이티브 32비트 애플리케이션입니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다.		도메인 컨트롤러 또는 멤버 서버에 설치된 에이전트입니다.	• 사용자 이름 • IP 주소 • 도메인	Active Directory 에이전트, 35 페이지
엔드포인트	다른 구성된 프로브와 함께 백그라운드에서 항상 실행되어 사용자가 여전히 연결되어 있는지를 확인합니다.		WMI	사용자가 계속 연결되어 있는지 여부	엔드포인트 프로브, 69 페이지
SPAN			SPAN(스위치에 설치됨) 및 Kerberos 메시지	• 사용자 이름 • IP 주소 • 도메인	SPAN, 45 페이지

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
	네트워크 트래픽을 수신 대기하기 위해 네트워크 스위치에 상주하며, Active Directory 데이터를 기반으로 사용자 ID 정보를 추출합니다.				
API 제공자	ISE-PIC가 제공하는 RESTful API 서비스를 이용하여, RESTful API 클라이언트와 통신하도록 프로그래밍된 모든 시스템에서 사용자 ID 정보를 수집합니다.	REST API 클라이언트와 통신하도록 프로그래밍된 모든 시스템입니다.	RESTful API. 가입자에게 전송된 JSON 형식의 사용자 ID.	• 사용자 이름 • IP 주소 • 포트 범위 • 도메인	설정 관리, 40 페이지
Syslog	시스템 로그 메시지를 구문 분석하고 MAC 주소를 포함한 사용자 ID를 검색합니다.	• 일반 시스템 로그 메시지 제공자 • DHCP 서버	시스템 로그 메시지	• 사용자 이름 • IP 주소 • MAC 주소 • 도메인	Syslog Providers(시스템 로그 제공자), 47 페이지

- Active Directory 에이전트, 35 페이지
- 설정 관리, 40 페이지
- SPAN, 45 페이지
- Syslog Providers(시스템 로그 제공자), 47 페이지
- 패시브 ID 서비스 필터링, 69 페이지
- 엔드포인트 프로브, 69 페이지

Active Directory 에이전트

ISE-PIC는 네이티브 32비트 애플리케이션인 Domain Controller(DC) 에이전트를 Active Directory(AD) 도메인 컨트롤러(DC) 또는 (컨피그레이션에 따라) 멤버 서버에 설치하여 AD에서 사용자 ID 정보를 검색한 다음, 이러한 ID를 사용자가 구성한 가입자에게 전송합니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다. 에이전트는 별도의 도메

인 또는 AD 도메인에 설치할 수 있으며, 설치한 후에는 1분마다 한 번씩 ISE-PIC 에 상태 업데이트를 제공합니다.

에이전트는 ISE-PIC 가 자동으로 설치 및 구성하며, 사용자가 수동으로 설치할 수도 있습니다. 설치하면 다음과 같은 일이 발생합니다.

- 에이전트와 관련 파일이 **Program Files/Cisco/Cisco ISE PassiveID Agent** 경로에 설치됩니다.
- 에이전트의 로깅 수준을 보여주는 **PICAgent.exe.config**라는 구성 파일이 설치됩니다. 구성 파일에서 로깅 레벨을 수동으로 변경할 수 있습니다.
- CiscoISEPICAgent.log 파일은 모든 로깅 메시지와 함께 저장됩니다.
- nodes.txt 파일에는 에이전트가 통실할 수 있는 구축 내 모든 노드 목록이 있습니다. 에이전트가 목록의 첫 번째 노드에 접촉합니다. 노드에 접촉할 수 없는 경우 에이전트는 목록의 노드 순서에 따라 계속 통신을 시도합니다. 수동 설치의 경우에는 파일을 열고 노드 IP 주소를 입력해야 합니다. (수동 또는 자동으로) 설치가 끝난 후에는 파일을 변경하려면 수동으로 업데이트해야 합니다. 필요하다면 파일을 열고 노드 IP 주소를 추가, 변경 또는 삭제합니다.
- Cisco ISE PassiveID 에이전트 서비스는 Windows Services 대화 상자에서 관리할 수 있는 머신에서 실행됩니다.
- ISE-PIC 는 도메인 컨트롤러를 100개까지 지원하며, 각 에이전트는 도메인 컨트롤러를 10개까지 모니터링할 수 있습니다.

참고 도메인 컨트롤러 100개를 모니터링하려면 에이전트 10개를 구성해야 합니다.

참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

에이전트를 설치할 수 없는 경우에는 패시브 ID 서비스에 Active Directory 프로브를 사용합니다. 자세한 내용은 프로브 및 제공자로서의 Active Directory, 17 페이지를 참조하십시오.

Active Directory 에이전트 자동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE-PIC 에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 자동 설치를 활성화하고 도메인 컨트롤러를 모니터링하도록 에이전트를 구성하는 방법을 설명합니다.

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE-PIC의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 13 페이지 항목을 참조하십시오.
- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 17 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 23 페이지 항목을 참조하십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **Agents(**에이전트**)** 그런 다음 현재 구성된 모든 DC(Domain Controller) 에이전트를 확인하고, 기존 에이전트를 편집 및 삭제하고, 새 에이전트를 구성합니다.

단계 **2** 새 에이전트를 추가하려면 테이블 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 에이전트를 생성하고 이 구성에서 지정한 호스트에 자동으로 설치하려면 **Deploy New Agent(**새 에이전트 구축**)**를 선택합니다.

단계 **4** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 39 페이지를 참고하십시오.

단계 **5** **Deploy(**구축**)**를 클릭합니다.
에이전트는 구성에서 지정한 도메인에 따라 호스트에 자동으로 설치되며 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 테이블에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **6** 다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** 그런 다음 현재 구성된 모든 조인 포인트를 봅니다.

단계 **7** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **8** **Passive ID(**패시브 **ID)** 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **9** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **10** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **11** **Agent(**에이전트**)** 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 암호 자격 증명(있는 경우)을 입력하고 **Save(**저장**)**를 클릭합니다.

Active Directory 에이전트 수동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE-PIC 에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 도메인 컨트롤러를 모니터링하도록 에이전트를 수동으로 설치하고 구성하는 방법을 설명합니다.

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE-PIC의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 13 페이지 항목을 참조하십시오.
- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 17 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 23 페이지 항목을 참조하십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **Agents(**에이전트**)** 그런 다음 현재 구성된 모든 DC(Domain Controller) 에이전트를 확인하고, 기존 에이전트를 편집 및 삭제하고, 새 에이전트를 구성합니다.

단계 **2** **Download Agent(**에이전트 다운로드**)**를 클릭하여 수동 설치를 위한 **`pxagent-installer.zip`** 파일을 다운로드합니다.
파일은 기본 Windows 다운로드 폴더에 다운로드됩니다.

단계 **3** 지정된 호스트 머신에 zip 파일을 배치하고 설치를 실행합니다.

단계 **4** ISE-PIC GUI에서 다시 **Providers(**공급자**)** > **Agents(**에이전트**)**.

단계 **5** 새 에이전트를 구성하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **6** 호스트 머신에 이미 설치한 에이전트를 구성하려면 **Register Existing Agent(**기존 에이전트 등록**)**를 선택합니다.

단계 **7** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 39 페이지를 참고하십시오.

단계 **8** **Save(**저장**)**를 클릭합니다.
에이전트 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 테이블에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **9** 다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Active Directory** 그런 다음 현재 구성된 모든 조인 포인트를 봅니다.

단계 **10** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **11** **Passive ID(**패시브 **ID)** 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **12** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **13** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **14** **Agent(**에이전트**)** 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 암호 자격 증명(있는 경우)을 입력하고 **Save(**저장**)**를 클릭합니다.

에이전트 제거

자동 또는 수동으로 설치된 에이전트는 Windows에서 직접 쉽게(수동으로) 제거할 수 있습니다.

단계 **1** Windows 대화 상자에서 **Programs and Features(**프로그램 및 기능**)**로 이동합니다.
단계 **2** 설치된 프로그램 목록에서 Cisco ISE PassiveID 에이전트를 찾아 선택합니다.
단계 **3** **Uninstall(**제거**)**을 클릭합니다.

Active Directory 에이전트 설정

서로 다른 DC(Domain Controller)에서 사용자 ID 정보를 검색하고 ISE-PIC 가입자에게 해당 정보를 전달하려면 ISE-PIC가 네트워크의 지정된 호스트에 에이전트를 자동으로 설치하도록 허용합니다.

에이전트를 생성하고 관리하려면 다음을 선택합니다. **Providers(**공급자**)** > **Agents(**에이전트**)**. Active Directory 에이전트 자동 설치 및 구축, 36 페이지를 참조하십시오.

표 ***10: Agents(***에이전트***)*** 창

필드 이름	설명
이름	구성한 에이전트 이름입니다.
Host(호스트**)**	에이전트가 설치된 호스트의 FQDN(Fully Qualified Domain Name)입니다.
모니터링	지정된 에이전트가 모니터링 중인 도메인 컨트롤러의 쉼표로 구분된 목록입니다.

표 ***11:*** 에이전트 신규

필드	설명
새 에이전트 구축 또는 기존 에이전트 등록	• Deploy New Agent(새 에이전트 구축): 지정된 호스트에 새 에이전트를 설치합니다. • Register Existing Agent(기존 에이전트 등록): 호스트에 에이전트를 수동으로 설치한 다음 ISE-PIC의 이 화면에서 해당 에이전트를 구성하여 서비스를 활성화합니다.
이름	에이전트를 쉽게 인식할 수 있는 이름을 입력합니다.
설명	에이전트를 쉽게 인식할 수 있는 설명을 입력합니다.
호스트 **FQDN**	이는 에이전트가 설치된(기존 에이전트 등록) 호스트가 설치될(자동 구축) 호스트의 FQDN(Fully Qualified Domain Name)입니다.

필드	설명
사용자 이름	에이전트를 설치할 호스트에 액세스하려면 사용자 이름을 입력합니다. ISE-PIC는 이러한 인증서를 사용하여 에이전트를 설치합니다.
비밀번호	에이전트를 설치할 호스트에 액세스하려면 비밀번호를 입력합니다. ISE-PIC는 이러한 인증서를 사용하여 에이전트를 설치합니다.

설정 관리

Cisco ISE-PIC에서 API Providers(API 제공자) 기능을 이용하면 맞춤형 프로그램이나 터미널 서버(TS)-Agent에서 얻은 사용자 ID 정보를 내장된 ISE-PIC REST API 서비스로 푸시할 수 있습니다. 이렇게 하면 네트워크에서 프로그램 가능 클라이언트를 맞춤화하여 아무 NAC(Network Access Control) 시스템에서 수집한 사용자 ID를 서비스로 전송할 수 있습니다. 또한 Cisco ISE-PIC API 제공자를 이용하면 모든 사용자가 IP 주소는 같지만 고유한 포트에 할당되는 Citrix 서버에서 TS-Agent 같은 네트워크 애플리케이션에 접속할 수 있습니다.

예를 들어 Active Directory(AD) 서버를 대상으로 인증된 사용자의 ID 매핑을 제공하는 Citrix 서버에서 실행하는 에이전트는 REST 요청을 ISE-PIC에 전송하여, 새 사용자가 로그인 또는 로그오프할 때마다 사용자 세션을 추가 또는 삭제할 수 있습니다. ISE-PIC그러면 는 클라이언트에서 전달한, IP 주소와 할당된 포트를 포함한 사용자 ID 정보를 얻은 다음 Cisco FMC(Firepower Management Center) 같은 사전 구성한 가입자에 전송합니다.

ISE-PIC REST API 프레임워크는 HTTPS 프로토콜로 REST 서비스를 구현하며(클라이언트 인증서 검증 필요 없음), 사용자 ID 정보는 JSON(JavaScript Object Notation) 형식으로 제공됩니다. JSON에 관한 자세한 내용은 http://www.json.org/ 항목을 참조하십시오.

ISE-PIC REST API 서비스는 사용자 ID를 구문 분석하고, 이 정보를 포트 범위에 매핑하여 같은 시스템에 동시에 로그인한 사용자를 구분합니다. 포트가 사용자에게 할당될 때마다 API는 ISE-PIC에 메시지를 보냅니다.

REST API 제공자 흐름

클라이언트를 ISE-PIC의 제공자로 선언하고 해당하는 맞춤형 프로그램(클라이언트)이 RESTful 요청을 전송할 수 있도록 ISE-PIC에서 맞춤형 클라이언트로 이어지는 브리지를 구성하면, ISE-PIC REST 서비스는 다음 방식으로 작동하게 됩니다.

1. 클라이언트 인증의 경우 Cisco ISE-PIC는 인증 토큰을 요구합니다. 클라이언트 머신의 맞춤형 프로그램은 연락처를 초기화할 때 인증 토큰 요청을 전송하며, 이후에는 이전 토큰이 만료될 때마다 ISE-PIC가 이를 알립니다. 요청의 응답으로 토큰이 반환되어 클라이언트와 ISE-PIC 서비스 간에 진행 중인 통신을 활성화합니다.
2. 사용자가 네트워크에 로그인하면 클라이언트는 사용자 ID 정보를 검색하고 API Add 명령을 사용하여 ISE-PIC REST 서비스에 정보를 게시합니다.
3. Cisco ISE-PIC가 사용자 ID 정보를 수신하고 매핑합니다.

4. Cisco ISE-PIC가 매핑된 사용자 ID 정보를 가입자에게 전송합니다.
5. 맞춤형 머신은 필요할 때마다 Remove API 호출을 전송하고 전송한 Add 호출의 응답으로 수신한 사용자 ID를 포함하여, 사용자 정보 제거 요청을 전송할 수 있습니다.

ISE-PIC에서 **REST API Providers(REST API** 제공자**)**를 이용한 작업

ISE-PIC에서 REST 서비스를 활성화하려면 다음 단계를 따르십시오.

1. 클라이언트 측을 구성합니다. 자세한 내용은 클라이언트 사용 설명서를 참조하십시오.
2. DNS 서버를 올바르게 구성했는지 확인합니다(ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). ISE-PIC의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 13 페이지 항목을 참조하십시오.
3. 패시브 ID 서비스용 ISE-PIC REST 서비스에 대한 Bridge(브리지)를 구성합니다., 41 페이지를 참조하십시오.

참고 TS-Agent와 함께 작동하도록 API Provider(API 제공자)를 설정하려면, ISE-PIC와 에이전트를 연결하는 브리지를 만들 때 TS-Agent를 추가한 다음 TS-Agent 설명서에서 API 호출 전송 관련 정보를 참조하십시오.

4. 인증 토큰을 생성하고 추가 및 제거 요청을 API 서비스에 전송합니다.

패시브 ID 서비스용 ISE-PIC REST 서비스에 대한 Bridge(브리지)를 구성합니다.

ISE-PIC REST API 서비스가 특정 클라이언트의 정보를 수신하게 하려면, 먼저 Cisco ISE-PIC에서 특정 클라이언를 정의해야 합니다. 서로 다른 IP 주소를 사용하여 여러 REST API 클라이언트를 정의할 수 있습니다.

시작하기 전에

- DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). Cisco ISE-PIC의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 13 페이지 항목을 참고하십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**) > API Providers(API** 공급자**)** 그런 다음 현재 구성된 모든 클라이언트를 확인하고, 기존 클라이언트를 수정 및 삭제하고, 새 클라이언트를 구성합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 API Providers(API 제공자) 표가 표시됩니다.

단계 **2** 새 클라이언트를 추가하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 API 제공자 설정, 42 페이지를 참고하십시오.

단계 **4** **Submit(**제출**)**을 클릭합니다.
클라이언트 구성이 저장되고 화면에 업데이트된 API Providers(API 제공자) 표가 표시됩니다. 이제 클라이언트가 ISE-PIC REST 서비스에 게시물을 보낼 수 있습니다.

다음에 수행할 작업

ISE-PIC REST 서비스에 인증 토큰과 사용자 ID를 게시하도록 사용자 지정 클라이언트를 설정합니다. ISE-PIC REST Service로 API Calls(API 호출) 전송, 42 페이지의 내용을 참조하십시오.

ISE-PIC REST Service로 API Calls(API 호출) 전송

시작하기 전에

패시브 ID 서비스용 ISE-PIC REST 서비스에 대한 Bridge(브리지)를 구성합니다., 41 페이지

단계 **1** 브라우저의 주소 표시줄에서 Cisco ISE URL을 입력합니다(예: *https://<ise* 호스트 이름 또는 *IP* 주소*>/admin/*).

단계 **2** API Providers(API 제공자) 화면에서 지정하고 구성한 사용자 이름과 암호를ISE-PIC GUI에 입력합니다. 자세한 내용은 패시브 ID 서비스용 ISE-PIC REST 서비스에 대한 Bridge(브리지)를 구성합니다., 41 페이지를 참고하십시오.

단계 **3** **Enter** 키를 누릅니다.

단계 **4** 대상 노드의 URL Address(URL 주소) 필드에 API 호출을 입력합니다.

단계 **5** **Send(**전송**)**을 클릭하여 API 호출을 실행합니다.

다음에 수행할 작업

디양한 API 호출과 관련 스키마 및 결과에 관한 자세한 내용과 세부 사항은 API 호출, 43 페이지 항목을 참조하십시오.

API 제공자 설정

ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **API Providers(API** 공급자**)** 그런 다음 패시브 ID 서비스을 위해 새로운 REST API 클라이언트를 구성합니다.

참고 전체 API 정의 및 개체 스키마는 다음과 같이 요청 호출을 통해 검색할 수 있습니다.

- 전체 API 사양(wadl)의 경우 — https://YOUR_ISE:9094/application.wadl
- API 모델 및 개체 스키마의 경우—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

표 *12: API* 제공자 설정

필드	설명
이름	이 클라이언트를 다른 클라이언트와 쉽고 빠르게 구별할 수 있는 고유한 이름을 입력합니다.
설명	이 클라이언트에 관한 명확한 설명을 입력합니다.
상태	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트가 REST 서비스와 상호작용합니다.
호스트/IP	클라이언트 호스트 머신의 IP 주소를 입력합니다. DNS 서버를 올바르게 구성했는지 확인합니다 (ISE-PIC에서의 클라이언트 머신에 대한 역방향 조회 구성 포함).
사용자 이름	REST 서비스에 게시할 때 사용할 고유한 사용자 이름을 생성합니다.
비밀번호	REST 서비스에 게시할 때 사용할 고유한 암호를 생성합니다.

API 호출

Cisco ISE-PIC로 패시브 ID 서비스용 사용자 ID 이벤트를 관리하려면 이러한 API 호출을 사용합니다.

목적: 인증 토큰 생성

- 요청

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  요청에는 BasicAuth 권한 부여 헤더가 포함되어야 합니다. 이전에 ISE-PIC GUI에서 생성한 API 제공자의 자격 증명을 제공합니다. 자세한 내용은 API 제공자 설정, 42 페이지를 참조하십시오.

- 응답 헤더

  헤더에는 X-auth-access-token이 포함됩니다. 추가 REST 요청을 게시할 때 사용하는 토큰입니다.

- 응답 본문

  HTTP 204 No Content

목적: 사용자 추가

- 요청

  POST

https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

POST 요청 헤더에 X-auth-access-token을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  201 Created

- 응답 본문

  {

  "user": "<사용자 이름>",

  "srcPatRange": {

  "userPatStart": <사용자 PAT 시작 값>,

  "userPatEnd": <사용자 PAT 종료 값>,

  "patRangeStart": <PAT 범위 시작 값>

  },

  "srcIpAddress": "<src IP 주소>",

  "agentInfo": "<에이전트 이름>",

  "timestamp": "<ISO_8601 형식, 즉 “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<도메인>"

  }

- 메모
  - 위의 json에서 srcPatRange를 제거하면 단일 IP 사용자 바인딩을 생성할 수 있습니다.
  - 응답 본문에는 생성된 사용자 세션 바인딩에 대한 고유 식별자인 'ID'가 포함됩니다. DELETE 요청을 보낼 때 이 ID를 사용하여 제거 대상 사용자를 표시합니다.
  - 이 응답에는 새로 생성된 사용자 세션 바인딩의 URL인 자체 링크도 포함됩니다.

목적**:** 사용자 제거

- 요청

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  <id>에는 Add(추가) 응답에서 수신한 ID를 입력합니다.

  DELETE 요청 헤더에 X-auth-access-token 토큰을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  200 OK

- 응답 본문

  응답 본문에는 삭제된 사용자 세션 바인딩 관련 세부 사항이 포함됩니다.

SPAN

SPANCisco ISE-PIC에서 직접 작동하도록 Active Directory를 구성하지 않고도 네트워크를 수신 대기하고 사용자 정보를 검색하도록 Cisco ISE-PIC를 빠르고 쉽게 활성화할 수 있는 입니다. SPAN은 네트워크 트래픽을, 특히 Kerberos 메시지를 검사하고 Active Directory에 저장된 사용자 ID 정보를 추출한 다음 정보를 ISE-PIC로 전송합니다. 그러면 ISE-PIC는 정보를 구문 분석하고, ISE-PIC에서 이전에 구성한 가입자에게 사용자 이름, IP 주소와 도메인 이름을 최종 전달합니다.

SPAN이 네트워크를 수신 대기하고 Active Directory 사용자 정보를 추출하려면, ISE-PIC와 Active Directory 모두가 네트워크에서 같은 스위치에 연결되어야 합니다. 이렇게 하면 SPAN은 Active Directory에서 모든 사용자 ID 데이터를 복사하고 미러링할 수 있습니다.

SPAN을 사용하면 사용자 정보를 다음 방법으로 검색합니다.

1. 사용자 엔드포인트에서 네트워크에 로그인합니다.
2. 로그인 및 사용자 데이터가 Kerberos 메시지에 저장됩니다.
3. 사용자가 로그인하고 사용자 데이터가 스위치를 통과하면, SPAN이 네트워크 데이터를 미러링합니다.
4. Cisco ISE-PIC가 네트워크에서 사용자 정보를 수신 대기하고 스위치에서 미러링된 데이터를 검색합니다.
5. Cisco ISE-PIC가 사용자 정보를 구문 분석하고 패시브 ID 매핑을 업데이트합니다.
6. Cisco ISE-PIC가 구문 분석된 사용자 정보를 가입자에게 전달합니다.

SPAN으로 작업

시작하기 전에

ISE-PIC가 네트워크 스위치에서 SPAN 트래픽을 수신하도록 설정하려면 먼저 스위치를 수신 대기할 노드와 노드 인터페이스를 정의해야 합니다. 설치된 서로 다른 ISE-PIC 노드를 SPAN이 수신 대기하도록 구성할 수 있습니다. 각 노드에 대해 하나의 인터페이스만 네트워크를 수신하도록 구성할 수 있으며, 수신하는 데 사용되는 인터페이스는 SPAN 전용이어야 합니다.

또한 다음을 수행해야 합니다.

- 네트워크에 Active Directory가 구성되어 있는지 확인합니다.
- 스위치가 ISE-PIC와 통신할 수 있도록, Active Directory에도 연결된 네트워크의 스위치에서 CLI를 실행합니다.
- AD에서 네트워크를 미러링하도록 스위치를 구성합니다.

- SPAN용 전용 ISE-PIC NIC(네트워크 인터페이스 카드)를 구성합니다. 이 NIC는 SPAN 트래픽에만 사용됩니다.
- SPAN 전용 NIC가 명령줄 인터페이스를 통해 활성화되었는지 확인합니다.
- Kerberos 트래픽만 SPAN 포트로 전송하는 VACL을 생성합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **SPAN** 그런 다음 SPAN을 구성합니다.

단계 **2** 참고 GigabitEthernet0 NIC(네트워크 인터페이스 카드)는 계속 사용 가능한 상태로 유지하고 SPAN 구성 시에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

의미 있는 설명(선택 사항)을 입력하고 **Enabled(**활성화됨**)** 상태를 선택한 다음 네트워크 스위치를 수신하는 데 사용할 노드 및 관련 NIC를 선택합니다. 자세한 내용은 413952, 46 페이지를 참고하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.
SPAN 컨피그레이션이 저장되고 ISE-PIC 가 현재 네트워크 트래픽을 수신 대기하고 있습니다.

413952

구축한 각 노드에서 클라이언트 네트워크에 SPAN을 설치하여, ISE-PIC가 사용자 ID를 수신하도록 빠르고 쉽게 구성합니다.

표 ***13: 413952***

필드	설명
설명	현재 활성화된 노드 및 인터페이스를 구별할 수 있는 고유한 설명을 입력합니다.
상태	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
인터페이스 NIC	ISE-PIC에 설치된 노드 중 하나 또는 둘 다를 선택한 다음, 선택한 각 노드에 대해 네트워크 정보를 수신할 노드 인터페이스를 선택합니다. 참고 GigabitEthernet0 NIC는 사용 가능한 상태로 유지하고 SPAN 구성에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

Syslog Providers(시스템 로그 제공자)

ISE-PIC 에서는 (InfoBlox, Blue Coat, BlueCat, Lucent 등의 제공자가 보낸) 일반 시스템 로그와 DHCP 시스템 로그 메시지를 포함한 시스템 메시지를 전달하는 클라이언트(ID 데이터 제공자)가 보낸 시스템 로그 메시지를 구문 분석하고, MAC 주소를 포함한 사용자 ID 정보를 다시 전송합니다. 그러면 매핑된 사용자 ID 데이터가 가입자에게 전달됩니다.

사용자 ID 데이터를 수신할 시스템 로그 클라이언트를 지정할 수 있습니다(시스템 로그 클라이언트 구성, 48 페이지 참고). 제공자를 구성할 때 관리자는 연결 방법(TCP 또는 UDP)과 구문 분석에 사용할 시스템 로그 템플릿을 지정해야 합니다.

참고 TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, ISE-PIC 는 패킷에서 수신한 IP 주소를 ISE-PIC의 시스템 로그 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 지정하는 것이 좋습니다. 헤더 사용자 지정에 관한 자세한 내용은 시스템 로그 헤더 사용자 지정, 54 페이지 항목을 참조하십시오.

시스템 로그 프로브는 수신한 메시지를 ISE-PIC 구문 분석기로 전송하고, 구문 분석기는 사용자 ID 정보를 매핑한 다음 정보를 ISE-PIC에 게시합니다. 그런 다음 ISE-PIC 가 구분 분석과 매핑이 끝난 사용자 ID 정보를 ISE-PIC 가입자에게 전달합니다.

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE-PIC 는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉터리에 등록된 사용자를 먼저 확인한 다음 IP 주소를 기준으로 사용자를 수신한 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

ISE-PIC 에서 사용자 ID의 시스템 로그 메시지를 구문 분석하려면 다음을 수행하십시오.

- 사용자 ID 데이터를 받을 시스템 로그 클라이언트를 구성합니다. 시스템 로그 클라이언트 구성, 48 페이지의 내용을 참조하십시오.
- 단일 메시지 헤더를 사용자 지정합니다. 시스템 로그 헤더 사용자 지정, 54 페이지의 내용을 참조하십시오.
- 템플릿을 생성하여 메시지 본문을 사용자 지정합니다. 시스템 로그 메시지 본문 사용자 지정, 53 페이지의 내용을 참조하십시오.
- 시스템 로그 클라이언트를 구성할 때 ISE-PIC 에서 사전 정의한 메시지 템플릿을 구문 분석용으로 사용하는 메시지 템플릿으로 사용하거나, 이러한 사전 정의 템플릿에서 사용자 지정한 헤더

나 본문 템플릿을 기반으로 사용합니다. 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지의 내용을 참조하십시오.

시스템 로그 클라이언트 구성

Cisco ISE-PIC가 특정 클라이언트에서 시스템 로그 메시지를 수신하게 하려면, 먼저 Cisco ISE-PIC에서 특정 클라이언를 정의해야 합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **Syslog Providers(**시스템 로그 공급자**)** 그런 다음 현재 구성된 모든 클라이언트를 확인하고, 기존 클라이언트를 수정 및 삭제하고, 새 클라이언트를 구성합니다. 각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 공급자) 표가 표시됩니다.

단계 **2** 새 시스템 로그 클라이언트를 구성하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 모든 필수 필드를 작성하고(자세한 내용은 Syslog 설정, 48 페이지 항목 참조) 필요하다면 메시지 템플릿을 생성하여(자세한 내용은 시스템 로그 메시지 본문 사용자 지정, 53 페이지 항목 참조) 클라이언트를 올바르게 구성합니다.

단계 **4** 제출을 클릭합니다.

Syslog 설정

특정 클라이언트가 보내는 시스템 로그 메시지를 이용해 사용자 IDMAC 주소 포함)를 수신하도록 Cisco ISE-PIC를 구성합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

표 ***14: Syslog Providers(***시스템 로그 제공자***)***

필드 이름	설명
이름	구성한 클라이언트를 빠르고 쉽게 구분할 수 있는 고유한 이름을 입력합니다.
설명	이 시스템 로그 제공자에 대한 유의미한 설명입니다.
상태	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
호스트	호스트 머신의 FQDN을 입력합니다.

필드 이름	설명
연결 유형	UDP 또는 TCP를 입력하여 ISE-PIC가 시스템 로그 메시지를 수신 대기하는 채널을 표시합니다. 참고 TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, Cisco ISE는 패킷에서 수신한 IP 주소를 Cisco ISE의 Syslog(시스템 로그) 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 지정하는 것이 좋습니다. 헤더 사용자 지정에 관한 자세한 내용은 시스템 로그 헤더 사용자 지정, 54 페이지 항목을 참조하십시오.

필드 이름	설명
템플릿	

필드 이름	설명
	템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 본문 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 이 필드에는 시스템 로그 메시지를 인식하고 올바르게 구문 분석하는 데 사용할 (시스템 로그 메시지 본문용) 템플릿을 표시합니다. 사전 정의된 드롭다운 목록에서 선택하거나 **New(**새로 만들기**)**를 클릭하여 맞춤형 템플릿을 생성합니다. 템플릿 생성에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 지정, 53 페이지 항목을 참조하십시오. 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다. 참고 맞춤형 템플릿만 수정하거나 제거할 수 있으며, 드롭다운에 있는 사전 정의된 시스템 템플릿은 수정할 수 없습니다. ISE-PIC는 현재 다음과 같은 사전 정의된 DHCP 제공자 템플릿을 제공합니다. • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP 참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습

필드 이름	설명
	니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다. Cisco ISE는 다음과 같은 사전 정의된 일반 시스템 로그 제공자 템플릿을 제공합니다. • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 템플릿에 관한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지 항목을 참조하십시오.
기본 도메인	도메인이 특정 사용자의 시스템 로그 메시지에서 식별되지 않으면, 모든 사용자에게 도메인이 할당될 수 있도록 이 기본 도메인이 사용자에게 자동으로 할당됩니다. 기본 도메인이나 메시지에서 구문 분석한 도메인을 이용해, 사용자 이름은 username@domain 형식이 되며 사용자 및 사용자 그룹 관련 추가 정보를 얻을 수 있도록 해당 도메인을 포함합니다.

Syslog 메시지 구조 사용자 맞춤화(템플릿)

템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다.

Cisco ISE-PIC에서는 ISE-PIC 구문 분석기에서 사용할 단일 메시지 헤더 및 여러 본문 구조를 사용자 맞춤화할 수 있습니다.

ISE-PIC 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부 정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

메시지 템플릿을 사용자 맞춤화할 때 사전 정의된 옵션 내에서 사용되는 정규식 및 메시지 구조를 참조하여 ISE-PIC 에 미리 정의된 메시지 템플릿을 기반으로 사용자 맞춤화를 수행할 수 있습니다. 사전 정의된 템플릿 정규식, 메시지 구조, 예제 등에 대한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지을 참조하십시오.

다음을 사용자 맞춤화할 수 있습니다.

- 단일 메시지 헤더—시스템 로그 헤더 사용자 지정, 54 페이지
- 복수 메시지 본문—시스템 로그 메시지 본문 사용자 지정, 53 페이지

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 지정 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 지정은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 메시지 본문 사용자 지정

Cisco ISE-PIC를 이용하면 (메시지 본문을 사용자 지정하여) 자체 시스템 로그 메시지 템플릿을 ISE-PIC 구문 분석기로 구문 분석하도록 사용자 지정할 수 있습니다. 템플릿에는 사용자 이름, IP 주소, MAC 주소 및 도메인의 구조를 정의하는 정규식이 포함되어야 합니다.

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 IP 주소를 기준으로 사용자를 수신한 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 지정 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 지정은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 클라이언트 구성 화면에서 시스템 로그 메시지 본문 템플릿을 생성하고 수정합니다.

참고 본인의 사용자 지정 템플릿만 수정할 수 있습니다. 시스템에서 제공하는 사전 정의된 템플릿은 수정할 수 없습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **Syslog Providers(**시스템 로그 공급자**)** 그런 다음 현재 구성된 모든 클라이언트를 확인하고, 기존 클라이언트를 수정 및 삭제하고, 새 클라이언트를 구성합니다. 각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 공급자) 표가 표시됩니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 시스템 로그 클라이언트를 추가 하거나 **Edit(**수정**)**을 클릭하여 이미 구성된 클라이언트를 업데이트합니다. 시스템 로그 클라이언트 구성 및 업데이트에 관한 자세한 내용은 시스템 로그 클라이언트 구성, 48 페이지 항목을 참조하십시오.

단계 **3** **Syslog Providers(**시스템 로그 제공자**)** 창에서 **New(**새로 만들기**)**를 클릭하여 새 메시지 템플릿을 생성합니다. 기존 템플릿을 수정하려면 드롭다운 목록에서 템플릿을 선택하고 **Edit(**수정**))**를 클릭합니다.

단계 **4** 모든 필수 필드를 작성합니다.

올바른 값을 입력하는 자세한 방법은 시스템 로그 맞춤형 템플릿 설정 및 예시, 55 페이지 항목을 참조하십시오.

단계 **5** **Test(**테스트**)**를 클릭하여, 입력된 문자열을 바탕으로 메시지가 올바르게 구문 분석되었는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

시스템 로그 헤더 사용자 지정

시스템 로그 헤더에는 메시지가 생성된 호스트 이름도 포함됩니다. 시스템 로그 메시지를 Cisco ISE-PIC 메시지 구문 분석기가 인식하지 못한다면, 호스트 이름 앞에 오는 구분 기호를 구성하여 메시지 헤더를 사용자 지정해야 Cisco ISE-PIC가 호스트 이름을 인식하고 메시지를 올바르게 구문 분석할 수 있습니다. 이 화면의 필드에 관한 자세한 내용은 시스템 로그 맞춤형 템플릿 설정 및 예시, 55 페이지 항목을 참조하십시오. 사용자 지정 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

참고 헤더 하나만 사용자 지정할 수 있습니다. 헤더를 사용자 지정한 후 **Custom Header(**사용자 지정 헤더**)**를 클릭하고 템플릿을 생성하면 최신 구성만 저장됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**공급자**)** > **Syslog Providers(**시스템 로그 공급자**)** 그런 다음 현재 구성된 모든 클라이언트를 확인하고, 기존 클라이언트를 수정 및 삭제하고, 새 클라이언트를 구성합니다. 각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 공급자) 표가 표시됩니다.

단계 **2** **Custom Header(**사용자 지정 헤더**)**를 클릭하여 Syslog Custom Header(시스템 로그 사용자 지정 헤더)를 엽니다.

단계 **3** **Paste sample syslog(**시스템 로그 예 붙여넣기**)**에 시스템 로그 메시지의 헤더 형식 예를 입력합니다. 예를 들어 다음 메시지 중 하나에서 이 헤더를 복사하여 붙여넣습니다. **`< 181 > Oct 10 15:14:08 Cisco.com`**

단계 **4** **Separator(**구분자**)** 필드에서 단어를 공백과 탭 중 무엇으로 구분할지를 지정합니다.

단계 **5** **Position of hostname in header(**헤더 내 호스트 이름 위치**)**필드에서 호스트 이름 내 헤더 위치를 지정합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.

Hostname(호스트 이름**)** 필드는 처음 3개 필드에 표시된 세부 정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 **Paste sample syslog(**시스템 로그 예 붙여넣기**)**의 헤더 예가 다음과 같다면

<181>Oct 10 15:14:08 Cisco.com

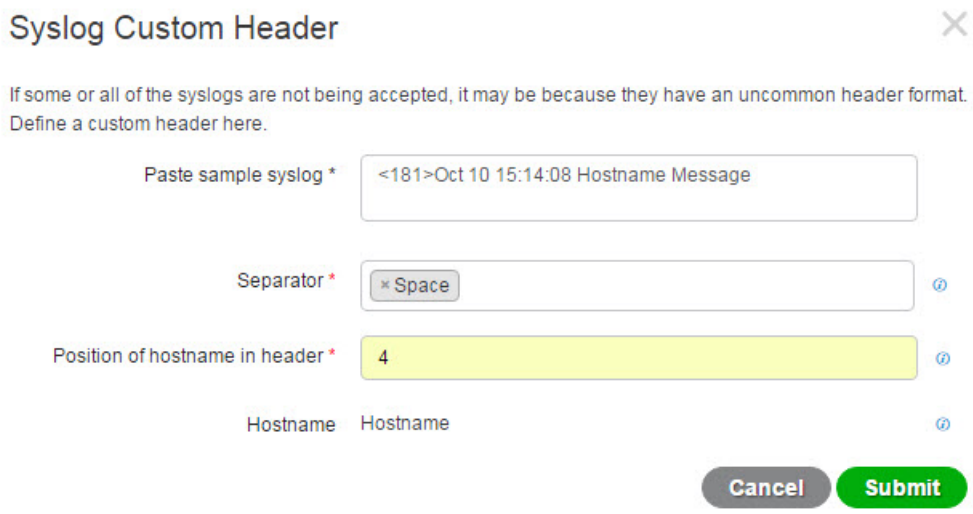
구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다.

Hostname(호스트 이름**)**은 **Paste sample syslog(**시스템 로그 예 붙여넣기**)** 필드에 붙여넣인 헤더 문구의 네 번째 단어인 Cisco.com으로 자동으로 표시됩니다.

호스트 이름이 잘못 표시된다면 **Seperator(**구분자**)** 및 **(Position of hostname in header(**헤더 내 호스트 이름 위치**)** 필드에 입력한 데이터를 확인하십시오.

이 예시는 다음 화면 캡처처럼 표시됩니다.

그림 ***3:*** 시스템 로그 헤더 사용자 지정



단계 **6** **Submit(**제출**)**을 클릭합니다.
사용자 지정 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

시스템 로그 맞춤형 템플릿 설정 및 예시

Cisco ISE-PIC를 이용하면 자체 시스템 로그 메시지 템플릿을 ISE-PIC 구문 분석기로 구문 분석하도록 사용자 지정할 수 있습니다. 맞춤형 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다. ISE-PIC 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부 정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

참고 대부분의 사전 정의된 템플릿은 정규식을 사용합니다. 맞춤형 템플릿은 정규식을 사용해야 합니다.

시스템 로그 헤더 부분

호스트 이름 앞에 오는 구분 기호를 구성하면 시스템 로그 프로브에서 인식하는 단일 헤더를 사용자 지정할 수 있습니다.

다음 표에서는 맞춤형 시스템 로그 헤더에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 17: 맞춤형 템플릿용 정규식, 58 페이지 항목을 참고하십시오.

표 ***15:*** 시스템 로그 맞춤형 헤더

필드	설명
샘플 시스템 로그 붙여넣기	시스템 로그 메시지에 헤더 형식 예를 입력합니다. 예를 들어 이 헤더를 복사하여 붙여넣습니다. **<181>Oct 10 15:14:08** 호스트 이름 메시지
구분자	단어가 공백과 탭 중 무엇으로 구분되는지를 나타냅니다.
헤더 내 호스트 이름 위치	헤더 내 호스트 위치를 표시합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.
호스트 이름	처음 3개 필드에 표시된 세부 정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 샘플 시스템 로그 붙여넣기에 있는 헤더 예가 다음과 같다면 <181>Oct 10 15:14:08 호스트 이름 메시지 구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다. 호스트 이름은 자동으로 Hostname으로 표시됩니다. 호스트 이름이 잘못 표시된다면 구분자 및 헤더 내 호스트 이름 위치 필드에 입력한 데이터를 확인하십시오.

메시지 본문에 대한 시스템 로그 템플릿 부분 및 설명

다음 표에서는 맞춤형 시스템 로그 메시지 템플릿에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 17: 맞춤형 템플릿용 정규식, 58 페이지 항목을 참고하십시오.

표 ***16:*** 시스템 로그 템플릿

부분	필드	설명
	이름	이 템플릿의 용도를 인식하는 데 사용하는 고유한 이름입니다.
매핑 작업	새 매핑	새 사용자를 추가하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 F5 VPN에 로그인한 새 사용자를 나타내려면 이 필드에 'logged on from'을 입력합니다.
	제거된 매핑	사용자를 제거하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 ASA VPN에서 제거해야 하는 사용자를 나타내려면 이 필드에 'session disconnect'를 입력합니다.
사용자 데이터	IP 주소	캡처할 IP 주소를 나타내는 정규식입니다. 예를 들어 Bluecat 메시지의 경우 이 IP 주소 범위 내에서 사용자 ID를 캡처하려면 다음을 입력합니다. (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	사용자 이름	캡처할 사용자 이름 형식을 나타내는 정규식입니다.
	도메인	캡처할 도메인을 나타내는 정규식입니다.
	MAC 주소	캡처할 MAC 주소 형식을 나타내는 정규식입니다.

정규식 예

메시지 구문 분석에는 정규식을 사용합니다. 이 섹션에서는 IP 주소, 사용자 이름 및 매핑 추가 메시지를 구문 분석하는 정규식 예를 확인할 수 있습니다.

예를 들어 정규식을 사용하여 다음 메시지를 구문 분석할 수 있습니다.

<174>192.168.0.1 %ASA-4-722051: 그룹 <DfltGrpPolicy> 사용자 <user1> IP <192.168.0.10> IPv4 ㅈ주소 <192.168.0.6> IPv6 주소 <::> 세션에 할당됨

<174>192.168.0.1 %ASA-6-713228: 그룹 = xyz, 사용자 이름 = user1, IP = 192.168.0.12, 할당된 비공개 IP 주소 192.168.0.8 사용자 제거용

정규식은 다음 표에서처럼 정의됩니다.

표 *17:* 맞춤형 템플릿용 정규식

부분	정규식
IP 주소	주소 <([^\s]+)>|address ([^\s]+)
사용자 이름	사용자 <([^\s]+)>| 사용자 이름 = ([^\s]+)
매핑 메시지 추가	(%ASA-4-722051|%ASA-6-713228)

시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업

시스템 로그 메시지에는 헤더와 메시지 본문을 포함하는 표준 구조가 적용됩니다.

이 섹션에서는 Cisco ISE-PIC에서 제공하는 사전 정의 템플릿을 설명하며, 메시지 출처에 따라 지원되는 헤더용 콘텐츠 세부 정보와 지원되는 본문 구조도 함께 설명합니다.

또한 시스템에서 사전 정의하지 않은 소스에 대한 맞춤형 본문 콘텐츠를 이용해 자체 템플릿을 만들 수도 있습니다. 이 섹션에서는 맞춤형 템플릿에 지원되는 구조에 대해서도 설명합니다. 메시지를 구문 분석할 때 시스템에 사전 정의된 헤더와 함께 사용할 단일 맞춤형 헤더를 구성할 수 있으며, 메시지 본문용으로 여러 맞춤형 템플릿을 구성할 수 있습니다. 헤더 사용자 지정에 관한 자세한 내용은 시스템 로그 헤더 사용자 지정, 54 페이지 항목을 참조하십시오. 본문 사용자 지정에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 지정, 53 페이지 항목을 참조하십시오.

참고 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다.

메시지 헤더

모든 클라이언트 머신의 모든 메시지 유형에 대해, 구문 분석기는 두 가지 헤더 유형(신규 및 제거)을 인식합니다. 두 헤더는 다음과 같습니다.

- <171>호스트 메시지
- <171>Oct 10 15:14:08 호스트 메시지

수신된 헤더는 호스트 이름에 대해 구문 분석됩니다. IP 주소, 호스트 이름 또는 전체 FQDN이 될 수 있습니다.

헤더를 사용자 지정할 수도 있습니다. 헤더를 사용자 지정하는 방법은 시스템 로그 헤더 사용자 지정, 54 페이지 항목을 참조하십시오.

시스템 로그 **ASA VPN** 사전 정의 템플릿

ASA VPN에 대해 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문 메시지	구문 분석 예
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 참고 이 메시지 유형의 구문 분석된 IP 주소는 메시지에 표시된 대로 개인 IP 주소입니다.
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 참고 이 메시지 유형의 구문 분석된 IP 주소는 IPv4 주소입니다.

매핑 제거 본문 메시지

구문 분석기에서 ASA VPN에 대해 지원하는 매핑 제거 메시지는 이 섹션에 설명되어 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[UserA,10.1.1.1]

본문 메시지
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

시스템 로그 Bluecat 사전 정의 템플릿

Bluecat에서 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

이 섹션에서 설명한 대로 Bluecat syslog용 새 매핑에 대해 지원되는 메시지가 나와 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

본문
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

매핑 제거 메시지

Bluecat에 대해 알려진 매핑 메시지 제거가 없습니다.

시스템 로그 F5 VPN 사전 정의 템플릿

F5 VPN에 대해 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 F5 VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[user=UserA,ip=172.16.0.12]

본문
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

매핑 제거 메시지

현재 지원되는 F5 VPN에 대한 제거 메시지가 없습니다.

시스템 로그 Infoblox 사전 정의 템플릿

Infoblox에 대해 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

본문 메시지
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

매핑 제거 메시지

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

- MAC 주소가 포함된 경우:

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC 주소가 포함되지 않은 경우:

  [10.0.10.100]

본문 메시지
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

Syslog Linux DHCPd3 사전 정의 템플릿

Linux DHCPd3에 대해 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 다양한 Linux DHCPd3 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 Linux DHCPd3에 대해 지원하는 매핑 제거 메시지를 설명합니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[00:0c:29:a2:18:34 ,10.0.10.100]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd : DHCPRELEASE of 10.0.10.100 from 00 : 0c : 29 : a2 : 18 : 34 (win10) via eth1

시스템 로그 **MS DHCP** 사전 정의 템플릿

MS DHCP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 MS DHCP 본문 메시지가 있습니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 구분한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,,0x4D53465420352E30,MSFT,5.0

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 MH DHCP에 대해 지원하는 매핑 제거 메시지를 설명합니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 구분한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

syslog SafeConnect NAC 사전 정의 템플릿

SafeConnect NAC에 대해 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 테이블에 나온 대로 구문 분석기가 인식하는 SafeConnect NAC 본문 메시지는 다양합니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

본문 메시지
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

매핑 제거 메시지

현재 지원되는 안전 연결에 대한 제거 메시지가 없습니다.

시스템 로그 Aerohive 사전 정의 템플릿

Aerohive에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Aerohive 본문 메시지가 있습니다.

본문에서 구문 분석된 세부 정보에는 사용자 이름 및 IP 주소가 포함됩니다. 구문 분석에 사용되는 정규식은 다음 예와 같습니다.

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[UserA,10.5.50.52]

본문 메시지
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

매핑 제거 메시지

현재 시스템은 Aerohive에서 매핑 제거 메시지를 지원하지 않습니다.

시스템 로그 **Blue Coat** 사전 정의 템플릿 - 기본 프록시, 프록시 **SG, Squid** 웹 프록시

시스템은 Blue Coat에 대해 다음 메시지 유형을 지원합니다.

- Bluecoat 메인 프록시
- BlueCoat Proxy SG
- BlueCoat Squid 웹 프록시

Bluecat 메시지에서 지원되는 syslog 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Blue Coat 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[UserA,192.168.10.24]

본문 메시지**(**이 예는 **BlueCoat** 프록시 **SG** 메시지에서 가져온 것임**)**
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

다음 표에서는 새 매핑 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4})\s** 사용자 이름 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**
BlueCoat Proxy SG	새 매핑 **(\-\sPROXIED){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4})\s[a-zA-Z0-9_]+\s-** 사용자 이름 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid 웹 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4})\sTCP** 사용자 이름 **\s([a-zA-Z0-9\._]+)\s\-\/**

매핑 제거 메시지

매핑 제거 메시지는 Blue Coat 클라이언트에 대해 지원되지만 현재 사용 가능한 예는 없습니다.

다음 표에서는 매핑 제거 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조 예에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	현재 사용 가능한 예가 없습니다.
BlueCoat Squid 웹 프록시	**(TCP_MISS|TCP_NC_MISS){1}**

시스템 로그 **ISE** 및 **ACS** 사전 정의 템플릿

ISE 또는 ACS 클라이언트를 수신 대기할 때 구문 분석기에서 다음 메시지 유형을 수신합니다.

- Pass authentication(인증 통과) - ISE 또는 ACS에서 사용자를 인증하면 인증이 성공했음을 알리고 사용자 세부 정보를 포함하는 통과 인증 메시지가 발급됩니다. 메시지가 구문 분석되고 사용자 세부 정보 및 세션 ID가 해당 메시지에서 저장됩니다.
- Accounting start and accounting update messages (new mapping)(계정 관리 시작 및 계정 관리 업데이트 메시지(새 매핑)) - ISE 또는 ACS에서 수신한 계정 관리 시작 또는 계정 관리 업데이트 메시지는 Pass Authentication(인증 통과) 메시지에서 저장한 사용자 세부 정보 및 세션 ID로 구문 분석되고 사용자가 매핑됩니다.
- Accounting stop (remove mapping)(계정 관리 중지(매핑 제거)) - ISE 또는 ACS에서 수신하면 사용자 매핑이 시스템에서 삭제됩니다.

ISE 및 ACS에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

인증 통과 메시지

다음 메시지는 인증 통과에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  사용자 이름 및 세션 ID만 구문 분석됩니다.

  [UserA,5]

계정 관리 시작**/**업데이트**(**새 매핑**)** 메시지

다음 메시지는 새 매핑에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부 정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

매핑 제거 메시지

다음 메시지는 매핑 제거에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부 정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

시스템 로그 Lucent QIP 사전 정의 템플릿

Lucent QIP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 58 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 Lucent QIP 본문 메시지는 다양합니다.

이러한 메시지의 정규식 구조는 다음과 같습니다.

DHCP_GrantLease|:DHCP_RenewLease

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[00:0C:29:91:2E:5D,10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

매핑 제거 본문 메시지

이러한 메시지의 정규식 구조는 다음과 같습니다.

Delete Lease:|DHCP Auto Release:

본문은 수신된 후에 다음과 같이 사용자 세부 정보에 대해 구문 분석됩니다.

[10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

패시브 ID 서비스 필터링

이름 또는 IP 주소를 기준으로 특정 사용자를 필터링할 수 있습니다. 예를 들어 엔드포인트를 이용해 일반 관리자를 지원하고자 엔드포인트에 로그인한 IT 서비스 관리자가 있다면, 관리자 활동을 필터링하여 Live Sessions(라이브 세션)에는 표시하지 않고 관련 엔드포인트의 일반 사용자에게만 표시되게 할 수 있습니다. Live Session(라이브 세션)에는 Mapping Filters(매핑 필터)에 의해 필터링되지 않은 패시브 ID 서비스 구성 요소가 표시됩니다. 필터는 필요한 수만큼 추가할 수 있습니다. 필터 사이에는 "OR" 논리 연산자가 적용됩니다. 두 필드를 모두 단일 필터에서 지정하는 경우에는 이러한 필드 사이에 "AND" 논리 연산자가 적용됩니다.

단계 **1** 다음 메뉴를 선택합니다. **Providers(**제공자**)** > **Mapping Filters(**매핑 필터**)**.

단계 **2** **Add(**추가**)**를 클릭하고 필터링할 사용자의 사용자 이름 및/또는 IP 주소를 입력한 후에 **Submit(**제출**)**을 클릭합니다.

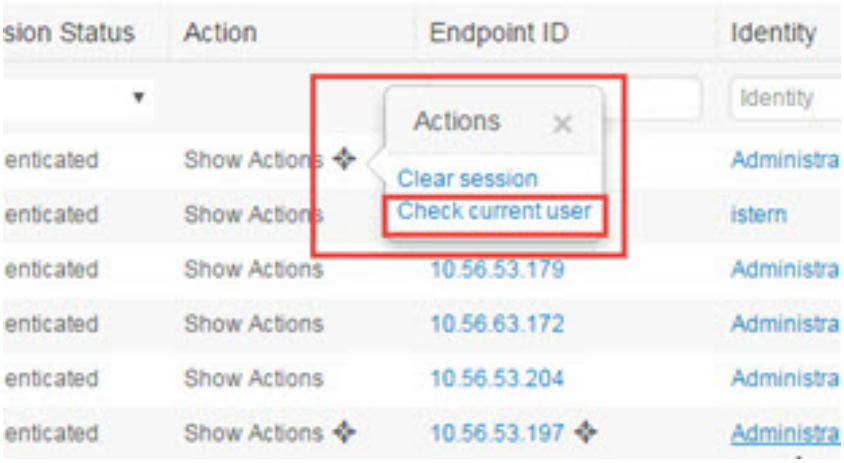
엔드포인트 프로브

사용자가 구성할 수 있는 맞춤형 제공자에 더해, ISE-PIC에서 활성화되고 백그라운드에서 항상 실행되어야 합니다. 엔드포인트 프로브는 각 사용자가 여전히 시스템에 로그인해 있는지를 주기적으로 확인합니다.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 초기 Active Directory 조인 포인트를 구성하고 **Store Credentials(**자격 증명 저장**)**을 선택해야 합니다. 엔드포인트 프로브 구성에 관한 자세한 내용은 엔드포인트 프로브 이용, 71 페이지 항목을 참조하십시오.

엔드포인트 상태를 수동으로 확인하려면 다음 그림에서처럼 **Live Sessions(**라이브 세션**)**로 이동한 다음 **Actions(**작업**)** 열에서 **Show Actions(**작업 표시**)**를 클릭하고 **Check current user(**현재 사용자 확인**)**를 선택합니다.

그림 *4:* 현재 사용자 확인



엔드 포인트 사용자 상태 및 수동으로 검사를 실행하는 방법에 대한 자세한 내용은을 참조하십시오. Live Sessions(라이브 세션), 149 페이지

엔드포인트 프로브가 사용자가 연결되었음을 인식했고 특정 엔드포인트에 대한 세션이 업데이트된 후 4시간이 지났다면, 엔드포인트 프로브는 사용자가 아직도 로그인한 상태인지 확인하고 다음 데이터를 수집합니다.

- MAC 주소
- 운영 체제 버전

확인 결과에 따라 프로브는 다음 작업을 수행합니다.

- 사용자가 여전히 로그인된 상태라면 프로브는 Cisco ISE-PIC를 Active User(활성 사용자)로 업데이트합니다.
- 사용자가 로그아웃했다면 세션 상태는 Terminated(종료됨)으로 업데이트되며, 15분이 지나면 사용자는 Session Directory에서 제거됩니다.
- 예를 들어 사용자에게 연락할 수 없을 때 방화벽에서 연결을 차단하거나 엔드포인트가 종료된다면, 상태는 Unreachable(연결 불가)로 업데이트되고 Subscriber(가입자) 정책에 따라 사용자 세션 처리 방법이 결정됩니다. 엔드포인트는 여전히 Session Directory에 남습니다.

엔드포인트 프로브 이용

시작하기 전에

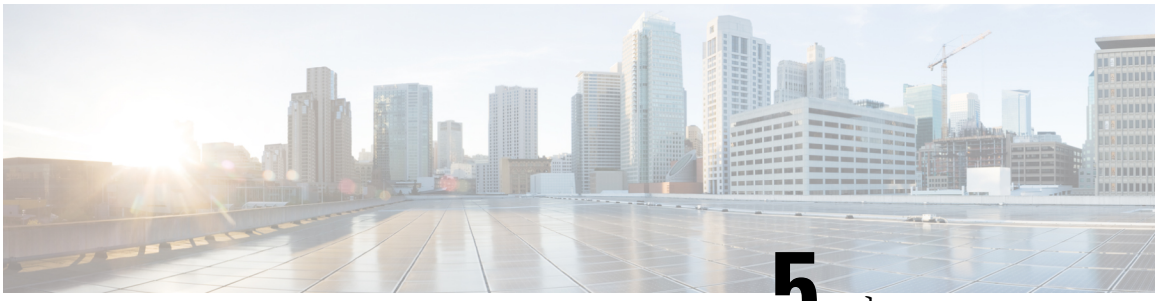
ISE-PIC 설치 시에는 엔드포인트 프로브가 기본적으로 활성화됩니다. 프로브를 활성화 및 비활성화하려면 먼저 다음 항목을 구성해야 합니다.

- 엔드포인트는 포트 445에 네트워크로 연결되어야 합니다.
- ISE-PIC에서 초기 Active Directory 가입 포인트를 구성합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 17 페이지 항목을 참조하십시오.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 Active Directory 프로브를 완전히 구성하지 않은 경우에도 엔드포인트 프로브를 실행할 수 있도록 초기 Active Directory 조인 포인트를 구성해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Providers(**제공자**)** > **Endpoint Probes(**엔드포인트 프로브**)**.

단계 **2** **Enabled(**활성화됨**)** 또는 **Disabled(**비활성화됨**)**를 선택합니다.
화면은 변경되지 않습니다. 그러나 선택한 항목에 따라 프로브는 활성화 또는 비활성화되며, 활성화된 경우 프로브는 백그라운드에서 실행되어 데이터를 수집합니다.



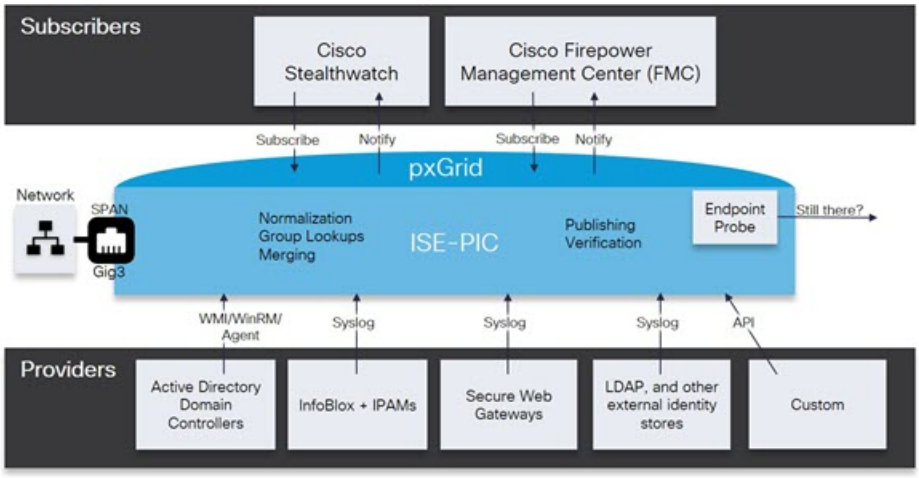
5 장

Subscribers(가입자)

ISE-PIC사용Cisco pxGrid 서비스를 사용하여 다양한 제공자로부터 수집하여 Cisco ISE-PIC 세션 디렉토리가 저장한 인증된 사용자 ID를 Cisco Stealthwatch나 Cisco FMC(Firepower Management Center) 같은 다른 네트워크 시스템으로 전달합니다.

다음 그림에서 pxGrid 노드는 외부 제공자로부터 사용자 ID를 수집합니다. 이러한 ID는 구문 분석, 매핑 및 형식화됩니다. pxGrid는 형식화된 사용자 ID를 가져와서 ISE-PIC 가입자에게 전송합니다.

그림 ***5: ISE-PIC Flow***



Cisco ISE-PIC에 연결된 가입자는 등록해야 pxGrid 서비스를 사용할 수 있습니다. 가입자는 고유한 이름과 인증서 기반 상호 인증을 사용하여 pxGrid에 로그인할 수 있습니다. 유효한 인증서를 전송하면, Cisco pxGrid 가입자는 자동으로 ISE-PIC에 의해 승인됩니다.

가입자는 pxGrid 서버 호스트 이름 또는 IP 주소에 연결할 수 있습니다. Cisco에서는 불필요한 오류를 방지하기 위해, 특히 DNS 쿼리가 올바르게 작동할 수 있도록 호스트 이름 사용을 권장합니다. 기능은 가입자가 게시 및 구독할 수 있도록 pxGrid에 생성되는 정보 토픽 또는 채널입니다. Cisco ISE-PIC에서는 SessionDirectory 및 IdentityGroup만 지원됩니다. 기능 정보는 **Capabilities(**기능**)** 탭의 **Subscribers(**가입자**)**로 이동하여 게시자로부터 게시, 직접 쿼리 또는 대량 다운로드 쿼리를 통해 사용할 수 있습니다.

가입자가 ISE-PIC에서 정보를 수신하게 하려면 다음 작업을 수행해야 합니다.

1. 선택 사항으로, 가입자 측에서 인증서를 생성합니다.
2. ISE-PIC에서 가입자를 위한 pxGrid 인증서 생성, 74 페이지 작업을 수행합니다.
3. 가입자 활성화, 75 페이지에 전달하는 고성능 고속 어플라이언스입니다. 가입자가 ISE-PIC에서 사용자 ID를 수신하게 하려면 이 단계를 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 76 페이지의 내용을 참조하십시오.

- 가입자를 위한 pxGrid 인증서 생성, 74 페이지
- 가입자 활성화, 75 페이지
- Live Logs(라이브 로그)에서 가입자 이벤트 보기, 76 페이지
- 가입자 설정 구성, 76 페이지

가입자를 위한 pxGrid 인증서 생성

시작하기 전에

설치 시 ISE-PIC에서는 기본 ISE-PIC 노드에서 디지털 서명한 pxGrid 서비스용 자체 서명 인증서를 자동으로 생성합니다. 이후에는 pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 궁극적으로는 사용자 ID가 ISE-PIC에서 가입자로 전달됩니다.

단계 **1** **Subscribers(**가입자**)**를 선택하고 **Certificates(**인증서**)** 탭으로 이동합니다.

단계 **2** **I want to(**수행할 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**):** 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다. Common Name(일반 이름) 필드에 pxGrid FQDN을 입력합니다(pxGrid는 접두사로 추가됩니다). (예: www.pxgrid-ise.ise.net) 와일드 카드를 사용할 수도 있습니다. (예: *. ise.net)
- **Generate a single certificate with a certificate signing request(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**: 이 옵션을 선택하면 인증서 서명 요청 세부 정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부 사항을 포함하는 CSV 파일을 업로드할 수 있습니다.
- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: ISE 공용 루트 인증서를 다운로드하여 pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소에 추가합니다. ISE pxGrid 노드는 새로 서명한 pxGrid 클라이언트 인증서만 신뢰하며 반대의 경우도 마찬가지라, 외부 인증 기관을 이용하지 않아도 됩니다.

단계 **3** (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **4** 이 인증서가 기반으로 하는 pxGrid 인증서 템플릿을 보거나 수정합니다. 인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다. PxGrid의 경우 Passive Identity(패시브 ID) 서비스를 사용할 때는 pxGrid 인증서 템플릿만 사용할 수 있으며, 이

템플릿에서는 Subject(주체) 정보만 수정할 수 있습니다. 이 템플릿을 수정하려면 다음을 선택합니다. **Certificates(**인증서**)** > **Certificate Templates(**인증서 템플릿**)Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Templates(**인증서 템플릿**)**.

단계 **5** SAN(대체 주체 이름)을 지정합니다. 여러 SAN을 추가해도 됩니다. 다음 옵션을 사용할 수 있습니다.

- **FQDN**: ISE 노드의 정규화된 도메인 이름을 입력합니다. (예: www.isepic.ise.net) FQDN에 와일드 카드를 사용할 수도 있습니다. (예: *. ise.net)

  pxGrid FQDN을 입력할 수 있는 FQDN용 추가 회선을 추가할 수 있습니다. Common Name(일반 이름) 필드에 사용한 FQDN과 동일해야 합니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 ISE 노드의 IP 주소를 입력합니다. 가입자가 FQDN 대신 IP 주소를 사용한다면 이 정보를 반드시 입력해야 합니다.

참고 Generate Bulk Certificate(대량 인증서 생성) 옵션을 선택했다면 이 필드는 표시되지 않습니다.

단계 **6** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)(PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **7** 인증서 비밀번호를 입력합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

가입자 활성화

가입자가 Cisco ISEISE-PIC에서 사용자 ID를 수신하려면 이 작업을 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 76 페이지의 내용을 참조하십시오.

단계 **1** 다음 메뉴를 선택합니다. **Subscribers(**가입자**)** 그런 다음 **Clients(**클라이언트**)** 탭이 표시되는지 확인합니다.

단계 **2** 가입자 옆의 확인란을 선택하고 **Approve(**승인**)**를 클릭합니다.

단계 **3** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

Live Logs(라이브 로그)에서 가입자 이벤트 보기

Live Logs(라이브 로그) 페이지에는 모든 가입자 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 가입자 및 기능 이름이 포함됩니다.

이벤트 목록을 확인하려면 **Subscribers(**가입자**)** 로 이동하고 **Live Log(**라이브 로그**)** 탭을 선택합니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

가입자 설정 구성

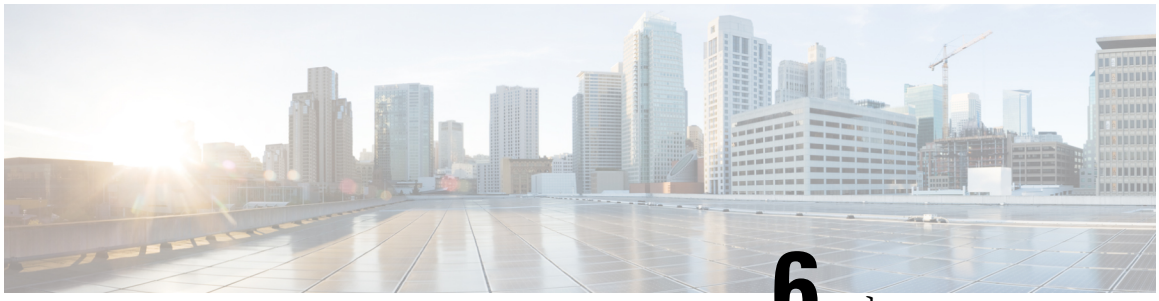
단계 **1** **Subscribers(**가입자**)**를 선택하고 **Settings(**설정**)** 탭을 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- Automatically Approve New Accounts(새 계정 자동 승인)—새 pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- Allow Password Based Account Creation(암호 기반 계정 생성 허용)—pxGrid 클라이언트에 대해 사용자 이름/암호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

  pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. pxGrid 컨트롤러는 클라이언트 등록 중에 pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.



6 장

Cisco에서 인증서 관리 ISE-PIC

인증서는 개인, 서버, 회사 또는 다른 엔터티를 식별하고 엔터티를 공용 키에 연결하는 전자 문서입니다. PKI(Public Key Infrastructure)는 보안 통신을 수행할 수 있도록 하고 디지털 서명을 사용 중인 사용자의 신원을 확인하는 암호화 기술입니다. 인증서는 네트워크에서 보안 액세스를 제공하기 위해 사용됩니다. 인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. 자체 서명된 인증서는 자체 생성자가 서명합니다. CA 서명 디지털 인증서는 업계 표준이며 더 안전한 것으로 간주됩니다. ISE-PIC는 pxGrid 가입자의 pxGrid 인증서에 디지털 서명을 하는 pxGrid의 외부 CA 역할을 할 수 있습니다.

Cisco ISE-PIC는 노드 간 통신 (각 노드가 서로 통신하기 위해 다른 노드에 인증서를 제공함) 및 pxGrid (ISE-PIC 및 pxGrid가 서로에게 인증서를 제공함)와 통신하는 데 인증서를 사용합니다. 이러한 두 가지 목적을 위해 노드 당 하나의 인증서를 생성할 수 있습니다. 인증서는 pxGrid에 대한 Cisco ISE 노드를 식별하고 pxGrid와 Cisco ISE 노드 간 통신을 보호합니다.

설치시 ISE-PIC는 각 ISE-PIC 노드에 대해 자체 서명된 인증서(설치 중에 관리자가 기본 노드에서 자동으로 보조 노드에 대해 생성된 인증서를 수락하라는 메시지가 표시됨) 및 기본 ISE-PIC 노드에서 디지털 서명한 pxGrid 서비스에 대한 인증서를 자동으로 생성합니다. 이후에는 pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 궁극적으로는 사용자 ID가 ISE-PIC에서 가입자로 전달됩니다. ISE-PIC의 인증서 메뉴를 사용하여 인증서를 보고, 추가 ISE-PIC 인증서를 생성하고, 몇 가지 고급 작업을 수행할 수 있습니다.

참고 관리자는 엔터프라이즈 인증서를 사용할 수 있지만, ISE-PIC는 가입자에 대한 pxGrid 인증서 발급에 내부 권한을 사용하도록 기본적으로 설계되었습니다.

Cisco ISE-PIC에서 인증서 매칭

구축에서 Cisco ISE-PIC 노드를 설정할 때 이 두 노드는 서로 통신합니다. 시스템은 각 ISE-PIC 노드의 FQDN이 일치하는지 확인합니다(예: ise1.cisco.com 및 ise2.cisco.com 또는 와일드 카드 인증서를 사용하는 경우 *.cisco.com). 또한 외부 시스템이 ISE-PIC 서버에 인증서를 제공하면 인증을 위해 제공되는 외부 인증서가 ISE-PIC 서버의 인증서와 비교하여 확인됩니다. 두 인증서가 일치하면 인증이 성공합니다.

Cisco ISE-PIC에서는 다음과 같이 일치하는 주체 이름을 확인합니다.

1. Cisco ISE-PIC에서 인증서의 SAN(Subject Alternative Name) 확장을 확인합니다. SAN에 하나 이상의 DNS 이름이 있는 경우 DNS 이름 중 하나를 Cisco ISE 노드의 FQDN과 일치시켜야 합니다. 와일드카드 인증서를 사용하는 경우 와일드카드 도메인 이름을 Cisco ISE 노드 FQDN의 도메인과 일치시켜야 합니다.
2. SAN에 DNS 이름이 없거나 SAN이 완전히 누락된 경우, 인증서의 Subject(주체) 필드에 있는 CN(Common Name) 또는 인증서의 Subject(주체) 필드에 있는 와일드카드 도메인을 노드의 FQDN과 일치시켜야 합니다.
3. 일치 항목이 발견되지 않으면 인증서가 거부됩니다.

와일드카드 인증서

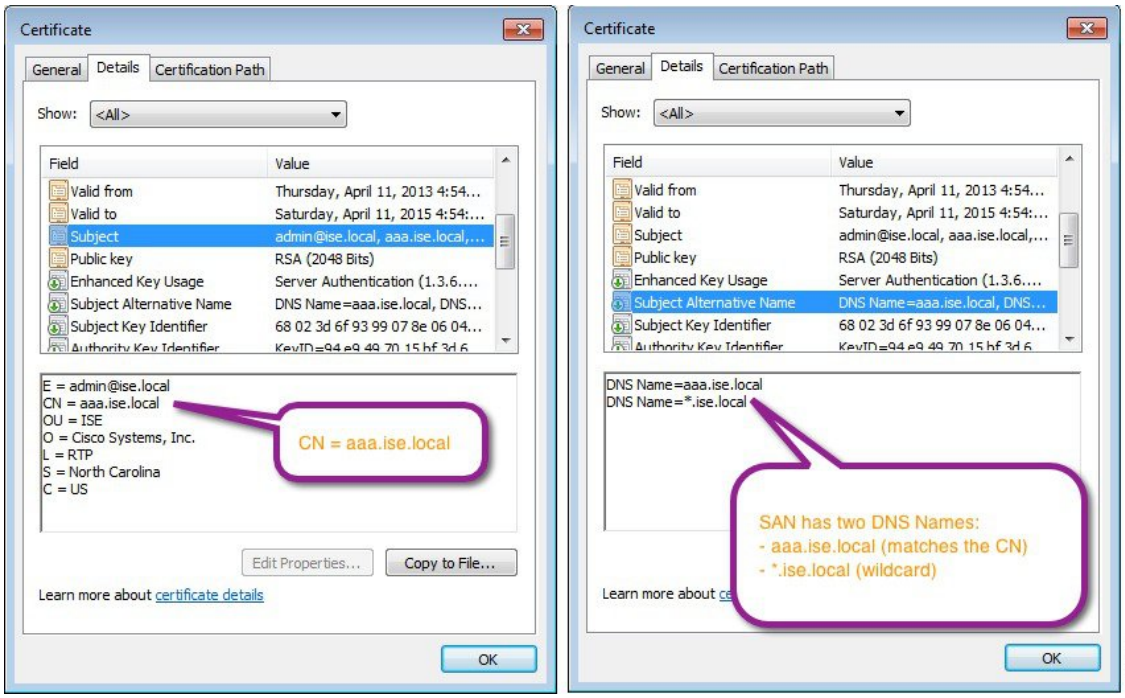
와일드카드 인증서는 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 사용하므로 조직의 여러 호스트 간에 인증서를 공유할 수 있습니다. 예를 들어 인증서 주체의 CN 값은 aaa.ise.local과 같은 일반 호스트 이름이고, SAN 필드에는 동일한 일반 호스트 이름과 함께 DNS.1=aaa.ise.local 및 DNS.2=*.ise.local과 같은 와일드카드 표기법이 포함된다고 가정합니다.

*.ise.local을 사용하도록 와일드카드 인증서를 구성하는 경우 동일한 인증서를 사용하여 DNS 이름이 psn.ise.local과 같이 ".ise.local"로 끝나는 다른 모든 호스트를 보호할 수 있습니다.

와일드카드 인증서는 일반 인증서와 동일한 방법으로 통신을 보호하며 요청은 동일한 검증 방법을 사용하여 처리됩니다.

다음 그림에는 웹 사이트를 보호하는 데 사용되는 와일드카드 인증서의 예가 나와 있습니다.

그림 *6:* 와일드카드 인증서 예



SAN 필드에 별표(*)를 사용하면 단일 인증서를 두 노드와 공유할 수 있으며(두 노드를 설치한 경우) 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE 노드용으로 고유한 서버 인증서를 각각 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

참고 FQDN의 일부 예는 전체 ISE 설치에서 가져온 것이므로 ISE-PIC 설치와 관련된 주소와 다를 수 있습니다.

와일드카드 인증서를 사용하는 경우의 이점

- 비용 절감. 타사 인증 기관이 서명하는 인증서는 비용이 많이 드는데 서버 수가 증가할수록 더욱 그렇습니다. 와일드카드 인증서는 Cisco ISE 구축의 여러 노드에서 사용할 수 있습니다.
- 운영 효율성. 와일드카드 인증서를 사용하면 모든 PSN(Policy Service Node) EAP 및 웹 서비스에서 동일한 인증서를 공유할 수 있습니다. 막대한 비용 절감 효과를 거둘 수 있을 뿐 아니라, 인증서를 한 번 생성하여 모든 PSN에 적용하는 방식으로 인증서 관리 작업도 간소화할 수 있습니다.
- 인증 오류 감소. 와일드카드 인증서는 클라이언트가 프로파일에 신뢰할 수 있는 인증서를 저장하지만 서명 루트를 신뢰할 수 있는 iOS 키 체인을 따르지 않는 Apple iOS 디바이스에서 발생하는 문제를 해결해 줍니다. PSN과 처음 통신하는 iOS 클라이언트는 신뢰할 수 있는 인증 기관이 인증서에 서명한 경우에도 PSN 인증서를 명시적으로 신뢰하지 않습니다. 와일드카드 인증서를

사용하면 인증서가 모든 PSN에서 동일하게 유지되므로 사용자가 인증서를 수락하기만 하면 여러 PSN에 대한 이후의 인증은 오류 또는 메시지 없이 진행됩니다.

- 신청자 컨피그레이션 간소화. 예를 들어 PEAP-MSCHAPv2 및 서버 인증서 신뢰가 활성화되어 있는 Microsoft Windows 신청자에서는 각 서버 인증서를 신뢰하도록 지정해야 합니다. 아니면 클라이언트가 다른 PSN을 사용하여 연결할 때 사용자에게 각 PSN 인증서를 신뢰하는지 묻는 메시지가 표시될 수 있습니다. 와일드카드 인증서를 사용하면 각 PSN의 개별 인증서가 아니라 단일 서버 인증서를 신뢰할 수 있습니다.
- 와일드카드 인증서를 사용하면 메시지 수를 줄이고 원활한 연결을 진행할 수 있으므로 사용자 환경을 개선할 수 있습니다.

와일드카드 인증서를 사용하는 경우의 단점

다음은 와일드카드 인증서와 관련된 몇 가지 보안 고려 사항입니다.

- 감사 기능 손실 및 미거부
- 개인 키의 노출 증가
- 일반적이지 않거나 관리자가 이해할 수 없음

와일드카드 인증서는 SE 노드 기준의 고유 서버 인증서보다 보안성이 낮은 것으로 간주됩니다. 그러나 보안 위험 문제보다 비용 및 다른 작동 요소의 이점이 훨씬 큽니다.

ASA와 같은 보안 디바이스도 와일드카드 인증서를 지원합니다.

와일드카드 인증서를 구축할 때에는 주의해야 합니다. 예를 들어 *.company.local을 사용하여 인증서를 생성하는 경우 공격자가 개인 키를 복구할 수 있으면 공격자는 company.local 도메인의 서버를 스푸핑할 수 있습니다. 그러므로 이러한 종류의 문제를 방지하려면 도메인 공간을 분할하는 것이 좋습니다.

이러한 문제를 해결하고 사용 범위를 제한하려면 조직의 특정 하위 도메인을 보호하도록 와일드카드 인증서를 사용할 수 있습니다. 와일드카드를 지정하려는 공통 이름의 하위 도메인 영역에 별표(*)를 추가합니다.

예를 들어 *.ise.company.local에 대한 와일드카드 인증서를 구성하는 경우 다음과 같이 DNS 이름이 ".ise.company.local"로 끝나는 다른 모든 호스트를 해당 인증서를 사용하여 보호할 수 있습니다.

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

와일드카드 인증서 호환성

와일드카드 인증서는 일반적으로 인증서 주체의 CN(Common Name)으로 나열되는 와일드카드를 사용하여 생성됩니다. Cisco ISE에서는 이러한 생성 유형을 지원합니다. 그러나 모든 엔드포인트 신청자가 인증서 주체의 와일드카드 문자를 지원하는 것은 아닙니다.

테스트를 거친 모든 Microsoft 기본 신청자(Windows Mobile 포함)는 인증서 주체에서 와일드카드 문자를 지원하지 않습니다.

Subject(주체) 필드에서 와일드카드 문자 사용을 허용할 수 있는 Cisco AnyConnect NAM(Network Access Manager) 등의 다른 신청자를 사용할 수 있습니다.

또한 인증서의 주체 대체 이름에 특정 하위 도메인을 포함하여 호환되지 않는 디바이스에서 사용 가능한 DigiCert의 Wildcard Plus와 같은 특수 와일드카드 인증서를 사용할 수도 있습니다.

Microsoft 신청자 제한으로 인해 와일드카드 인증서를 사용할 수 없다고 생각할 수도 있지만, Microsoft 기본 신청자를 포함하여 보안 액세스용으로 테스트된 모든 디바이스에서 사용할 수 있는 와일드카드 인증서를 생성하는 대체 방법이 있습니다.

이러한 인증서를 생성하려면 주체에 와일드카드 문자를 사용하는 대신 SAN(Subject Alterative Name) 필드에 와일드카드 문자를 사용해야 합니다. SAN 필드에서 도메인 이름(DNS 이름) 확인용 확장을 유지 관리할 수 있습니다. 자세한 내용은 RFC 6125 및 2128을 참고해 주십시오.

의ISE-PIC 인증서 계층 구조

ISE-PIC에서 모든 인증서의 인증서 계층 구조 또는 인증서 신뢰 체인을 확인할 수 있습니다. 인증서 계층 구조에는 인증서, 모든 중간 CA(Certificate Authority) 인증서 및 루트 인증서가 포함됩니다. 예를 들어 ISE-PIC에서 시스템 인증서를 보도록 선택하면 기본적으로 해당 시스템 인증서의 세부사항이 표시됩니다. 인증서 계층은 인증서의 상단에 나타납니다. 계층 구조에서 인증서를 클릭하면 해당 세부사항을 볼 수 있습니다. 셀프 서명 인증서에는 계층 구조 또는 신뢰 체인이 없습니다.

인증서 목록 페이지의 Status(상태) 열에는 다음 아이콘 중 하나가 표시됩니다.

- 녹색 아이콘 - 유효한 인증서(유효한 신뢰 체인)를 나타냅니다.
- 빨간색 아이콘 - 오류(예: 신뢰 인증서가 누락되었거나 만료됨)를 나타냅니다.
- 노란색 아이콘 - 인증서가 곧 만료된다고 경고하며 갱신하라는 메시지가 표시됩니다.

시스템 인증서

Cisco ISE-PIC 시스템 인증서는 구축의 다른 노드 및 클라이언트 애플리케이션에 대해 Cisco ISE-PIC 노드를 식별하는 서버 인증서입니다. 시스템 인증서에 액세스하려면 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다. 시스템 인증서는 다음과 같이 사용됩니다.

- Cisco ISE-PIC 구축에서 노드 간 통신에 사용됩니다. Usage(사용) 필드에서 이러한 인증서에 대한 Admin(관리) 옵션을 선택합니다.
- pxGrid 컨트롤러와의 통신에 사용됩니다. Usage(사용) 필드에서 이러한 인증서에 대한 pxGrid 옵션을 선택합니다.

Cisco ISE-PIC 구축의 각 노드에 유효한 시스템 인증서를 설치해야 합니다. 기본적으로 설치 중에 Cisco ISE-PIC 노드에 자체 서명 인증서 2개와 내부 Cisco ISE CA에서 서명 1개가 생성됩니다.

- 관리 및 pxGrid용으로 지정된 자체 서명 서버 인증서(키 크기는 2048이며 1년 동안 유효함)
- SAML IdP와의 통신을 보호하는 데 사용할 수 있는 자체 서명 SAML 서버 인증서(키 크기는 2048이며 1년 동안 유효함)
- pxGrid 클라이언트와의 통신을 보호하는 데 사용할 수 있는 내부 Cisco ISE CA 서명 서버 인증서(키 크기가 4096이고 1년 동안 유효함).

구축을 설정하고 보조 노드를 등록하면 pxGrid 컨트롤러용으로 지정된 인증서가 기본 노드의 CA에서 서명한 인증서로 자동 교체됩니다. 따라서 모든 pxGrid 인증서는 동일한 PKI 신뢰 계층 구조의 일부가 됩니다.

참고 릴리스에 대해 지원되는 키 및 암호 정보를 찾으려면 Cisco Identity Services Engine 네트워크 구성 요소 호환성 설명서의 해당 버전을 확인하십시오.

보안을 향상하기 위해 셀프 서명 인증서는 CA 서명 인증서로 대체하는 것이 좋습니다. CA 서명 인증서를 가져오려면 다음을 수행해야 합니다.

1. 인증서 서명 요청을 생성하고 인증 기관에 CSR 제출, 94 페이지
2. 신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 91 페이지
3. CSR에 CA 서명 인증서 바인딩, 94 페이지

시스템 인증서 보기

시스템 인증서 페이지에는 Cisco ISE-PIC에 추가된 모든 시스템 인증서가 나열됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)** 를 선택합니다.

시스템 인증서 페이지가 표시되고 로컬 인증서에 대해 다음 정보가 제공됩니다.

- 식별 이름 - 인증서의 이름입니다.
- 사용 대상 - 이 인증서가 사용되는 서비스입니다.
- 포털 그룹 태그 - 포털에서 사용하도록 지정된 인증서에만 해당되며, 포털에 사용해야 하는 인증서를 지정합니다.
- 발급 대상 - 인증서 주체의 일반 이름입니다.
- 발급자 - 인증서 발급자의 일반 이름입니다.
- 유효 기간 시작 - 인증서가 생성된 날짜이며 Not Before 인증서 특성이라고도 합니다.
- 만료 날짜 - 인증서의 만료 날짜이며 Not After 인증서 특성이라고도 합니다. 인증서가 만료되는 시기를 나타냅니다. 여기에는 5개 범주가 연결된 아이콘과 함께 표시됩니다.

- 만료 날짜까지 남은 기간이 90일을 초과함(녹색 아이콘)
- 90일 이내에 만료됨(파란색 아이콘)
- 60일 이내에 만료됨(노란색 아이콘)
- 30일 이내에 만료됨(주황색 아이콘)
- 만료됨(빨간색 아이콘)

단계 **2** 인증서를 선택하고 보기 를 선택하여 인증서 세부 사항을 표시합니다.

시스템 인증서 가져오기

관리 포털에서 Cisco ISE-PIC 노드의 시스템 인증서를 가져올 수 있습니다.

참고 기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. PAN(Primary Administration Node)에서 다시 시작이 완료된 후 한 번에 한 노드씩 시스템이 다시 시작됩니다.

시작하기 전에

- 클라이언트 브라우저를 실행 중인 시스템에 시스템 인증서 및 개인 키 파일이 있는지 확인합니다.
- 가져오는 시스템 인증서에 외부 CA가 서명을 한 경우 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)로 가져옵니다.
- 가져오는 시스템 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.
Import Server Certificate(서버 인증서 가져오기) 화면이 열립니다.

단계 **3** 가져올 인증서에 대한 값을 입력합니다.

단계 **4** 제출을 클릭합니다.

셀프 서명 인증서 생성

셀프 서명 인증서를 생성하여 새 로컬 인증서를 추가할 수 있습니다. 내부 테스트 및 평가에 필요한 셀프 서명 인증서만 사용하는 것이 좋습니다. 생산 환경에서 Cisco ISE-PIC를 구축하려는 경우에는 생산 네트워크 전체에서 보다 동일하게 수락될 수 있도록 가능하면 항상 CA 서명 인증서를 사용해야 합니다.

참고 셀프 서명 인증서를 사용 중일 때 Cisco ISE-PIC 노드의 호스트 이름을 변경해야 하는 경우에는 Cisco ISE-PIC 노드의 에 로그인하여 이전 호스트 이름이 지정된 셀프 서명 인증서를 삭제한 다음 새 셀프 서명 인증서를 생성해야 합니다. 이렇게 하지 않으면 Cisco ISE-PIC는 이전 호스트 이름이 지정된 셀프 서명 인증서를 계속 사용합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**.

단계 **2** **Generate Self Signed Certificate(**셀프 서명 인증서 생성**)**를 클릭하고 셀프 서명 인증서 생성 페이지에서 세부사항을 입력합니다.

단계 **3** 셀프 서명 와일드카드 인증서, 즉 주체 이름의 일반 이름 및/또는 주체 대체 이름의 DNS 이름에 별표(*)가 포함된 인증서를 생성하려면 **Allow Wildcard Certificates(**와일드카드 인증서 허용**)** 확인란을 선택합니다. 예를 들어 SAN에 할당되는 DNS 이름이 *.amer.cisco.com일 수 있습니다.

단계 **4** 이 인증서를 사용하려는 서비스를 기준으로 **Usage(**사용**)** 영역의 확인란을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 인증서를 생성합니다.

보조 노드를 다시 시작하려면 CLI에서 다음 명령을 지정된 순서로 입력합니다.

a) **application stop ise**
b) **application start ise**

시스템 인증서 편집

이 페이지를 사용하여 시스템 인증서를 편집하고 셀프 서명 인증서를 갱신할 수 있습니다. 와일드카드 인증서를 편집하면 변경사항이 구축의 모든 노드로 복제됩니다. 와일드카드 인증서를 삭제하면 구축의 모든 노드에서 해당 와일드카드 인증서가 제거됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 셀프 서명 인증서를 갱신하려면 **Renewal Period(**갱신 기간**)** 체크 박스를 선택하고 만료 TTL(Time to Live)를 일, 주, 월 또는 연도 단위로 입력합니다.

단계 **4** **Save**(저장)를 클릭하여 변경 사항을 저장합니다.

Admin(관리**)** 확인란을 선택하면 Cisco ISE-PIC 노드의 애플리케이션 서버가 다시 시작됩니다.

참고 Chrome 65 이상을 사용하여 ISE를 시작하면 URL이 성공적으로 리디렉션되어도 브라우저에서 BYOD 포털 또는 게스트 포털이 시작되지 않을 수 있습니다. 이는 모든 인증서에 주체 대체 이름 필드를 요구하는 Google의 새로운 보안 기능 때문입니다. ISE 릴리스 2.4 이상의 경우 Subject Alternative Name(주체 대체 이름) 필드를 입력해야 합니다.

Chrome 65 이상에서 실행하려면 다음 단계를 수행합니다.

1 Subject Alternative Name(주체 대체 이름) 필드를 입력해 ISE GUI에서 새 자체 서명 인증서를 생성합니다. DNS 및 IP 주소를 모두 입력해야 합니다.

2. 이제 ISE 서비스가 다시 시작됩니다.

3. Chrome 브라우저에서 포털을 리디렉션합니다.

4. 브라우저에서 View Certificate(인증서보기)>Details(세부 사항)>Copy the certificate by selecting base-64 encoded(base-64 인코딩을 선택하여 인증서 복사)를 실행합니다.

5. 신뢰할 수 있는 경로에 인증서를 설치합니다.

6. Chrome 브라우저를 닫고 포털 리디렉션을 시도합니다.

참고 운영 체제 Win RS4 또는 RS5에서 브라우저 Firefox 64 이상에 대해 무선 BYOD 설정을 구성할 때 인증서 예외를 추가하지 못할 수 있습니다. 이 동작은 Firefox 64 이상을 새로 설치하는 경우에 예상되며, 이전 버전에서 Firefox 64 이상으로 업그레이드하는 경우에는 발생하지 않습니다. 이 경우 다음과 같은 단계를 통해 인증서 예외를 추가할 수 있습니다.

1 BYOD 플로우 단일/이중 PEAP 또는 TLS를 구성합니다.

2. Windows ALL 옵션을 사용해 CP 정책을 구성합니다.

3. 엔드 클라이언트 Windows RS4/RS5에서 Dot1.x/MAB SSID를 연결합니다.

4. 게스트/BYOD 포털로의 리디렉션을 위해 FF64 브라우저에 1.1.1.1을 입력합니다.

5. **Add Exception(**예외 추가**)** > **Unable to add certificate(**인증서 추가 불가능**)**을 클릭한 다음 플로우를 진행합니다.

이를 해결하려면 옵션 > 프라이버시 및 설정 > 인증서 보기 > 서버 > 예외 추가로 이동하여 Firefox 64용 인증서를 수동으로 추가해야 합니다.

시스템 인증서 삭제

더 이상 사용하지 않는 시스템 인증서는 삭제할 수 있습니다.

시스템 인증서 저장소에서 한 번에 여러 인증서를 삭제할 수는 있지만, 이 경우 관리 인증에 사용할 수 있는 인증서가 하나 이상 있어야 합니다. 또한 관리 또는 pxGrid 컨트롤러에 사용되는 인증서는 삭제할 수 없습니다. 단, 서비스를 비활성화하는 경우 pxGrid 인증서는 삭제할 수 있습니다.

와일드카드 인증서를 삭제하도록 선택하는 경우에는 구축의 모든 노드에서 인증서가 제거됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)** 를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

시스템 인증서 내보내기

선택한 시스템 인증서 또는 인증서와 연결된 개인 키를 내보낼 수 있습니다. 인증서 및 해당 개인 키를 백업용으로 내보내는 경우 나중에 필요하면 인증서와 키를 다시 가져올 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**)**를 선택합니다. .

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** 인증서만 내보낼지 아니면 인증서 및 연결된 개인 키를 내보낼지를 선택합니다.

팁 인증서와 연결된 개인 키의 값이 노출될 수 있으므로 개인 키는 내보내지 않는 것이 좋습니다. 노드 간 통신용으로 와일드카드 시스템 인증서를 다른 노드로 가져오기 위해 내보내는 등의 경우와 같이 개인 키를 내보내야 하는 경우에는 개인 키용 암호화 비밀번호를 지정합니다. 개인 키의 암호를 해독하려면 이 인증서를 다른 Cisco ISE-PIC 노드로 가져오는 동안 이 비밀번호를 지정해야 합니다.

단계 **4** 개인 키를 내보내도록 선택한 경우 비밀번호를 입력합니다. 비밀번호는 8자 이상이어야 합니다.

단계 **5** **Export(**내보내기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 인증서를 저장합니다.

인증서만 내보내는 경우에는 프라이버시 향상 메일 형식으로 인증서가 저장됩니다. 인증서와 개인 키를 모두 내보내는 경우에는 프라이버시 향상 메일 형식 인증서와 암호화된 개인 키 파일을 포함하는 .zip 파일로 인증서가 내보내집니다.

신뢰할 수 있는 인증서 저장소

신뢰할 수 있는 인증서 저장소에는 신뢰 및 SCEP(Simple Certificate Enrollment Protocol)에 사용되는 X.509 인증서가 포함되어 있습니다.

X.509 인증서는 특정 날짜까지만 유효합니다. 시스템 인증서가 만료되면 해당 인증서를 사용하는 Cisco ISE 기능이 영향을 받게 됩니다. Cisco ISE에서는 만료 날짜까지 남은 기간이 90일 미만이면 시스템 인증서의 보류 중인 만료에 대한 알림을 표시합니다. 이 알림은 다음과 같은 여러 가지 방법으로 표시됩니다.

- 시스템 인증서 페이지에 색상이 지정된 만료 상태 아이콘이 나타납니다.
- Cisco ISE 시스템 진단 보고서에 만료 메시지가 나타납니다.
- 만료 전 90일과 60일, 그리고 마지막 30일 동안에는 매일 만료 경보가 생성됩니다.

만료되는 인증서가 셀프 서명 인증서인 경우에는 인증서를 편집하여 만료 날짜를 연장할 수 있습니다. CA가 서명한 인증서의 경우에는 만료 전에 충분한 여유를 두고 CA로부터 교체 인증서를 받아야 합니다.

Cisco ISE는 다음과 같은 용도로 신뢰할 수 있는 인증서를 사용합니다.

- 인증서 기반 관리자 인증을 사용하여 ISE-PIC에 액세스하는 Cisco ISE 관리자 및 엔드포인트에서 인증을 위해 사용하는 클라이언트 인증서 확인
- 구축에 있는 Cisco ISE-PIC 노드 간의 통신 보호 활성화. 신뢰할 수 있는 인증서 저장소는 구축의 각 노드에 있는 시스템 인증서와의 신뢰 관계를 설정하는 데 필요한 CA 인증서 체인을 포함해야 합니다.
  - 셀프 서명 인증서는 시스템 인증서에 사용되고 각 노드의 셀프 서명 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.
  - CA 서명 인증서가 시스템 인증서로 사용되는 경우 CA 루트 인증서와 함께 신뢰 체인의 중간 인증서는 PAN의 신뢰할 수 있는 인증서 저장소에 위치해야 합니다.

참고

- Cisco ISE로 가져온 X.509 인증서는 PEM(Privacy-Enhanced Mail) 또는 DER(Distinguished Encoding Rule) 형식이어야 합니다. 인증서 체인(시스템 인증서와 여기에 서명하는 신뢰 인증서 시퀀스)이 포함된 파일은 특정 제한 사항에 따라 가져올 수 있습니다.
- 공개 와일드카드 인증서를 게스트 포털에 할당하고 루트 CA 인증서가 포함된 하위 CA를 가져오는 경우 ISE 서비스가 재시작될 때까지 인증서 체인이 전송되지 않습니다.

설치시 신뢰할 수 있는 인증서 저장소가 자동으로 생성된 신뢰할 수 있는 인증서로 채워집니다. 루트 인증서(Cisco 루트 CA)는 Manufacturing (Cisco CA Manufacturing) 인증서에 서명합니다.

신뢰할 수 있는 인증서 명명 제한

CTL의 신뢰할 수 있는 인증서는 이름 제한 확장명을 포함할 수 있습니다. 이 확장명은 인증서 체인 내 후속 인증서의 모든 주체 이름 및 주체 대체 이름 필드 값에 대한 네임스페이스를 정의합니다. Cisco ISE는 루트 인증서에 지정된 제한을 확인하지 않습니다.

지원되는 이름 제한은 다음과 같습니다.

- 디렉토리 이름

  주체/SAN의 디렉토리 이름 접두사를 디렉토리 이름 제한으로 사용해야 합니다. 예를 들면 다음과 같습니다.

  - 올바른 주체 접두사:

    CA 인증서 이름 제한: Permitted: O=Cisco

    클라이언트 인증서 주체: O=Cisco,CN=Salomon

  - 잘못된 주체 접두사:

    CA 인증서 이름 제한: Permitted: O=Cisco

    클라이언트 인증서 주체: CN=Salomon,O=Cisco

- DNS
- 이메일
- URI(URI 제한은 http://, https://, ftp:// 또는 ldap://와 같은 URI 접두사로 시작되어야 함)

지원되지 않는 이름 제한은 다음과 같습니다.

- IP 주소
- 기타 이름

Cisco ISE는 지원되지 않는 제한을 확인할 수 없으므로, 신뢰할 수 있는 인증서에 포함된 제한이 지원되지 않으며 확인 중인 인증서에 적절한 필드가 포함되어 있지 않으면 해당 인증서는 거부됩니다.

신뢰할 수 있는 인증서 내의 이름 제한 정의 예제는 다음과 같습니다.

```
 X509v3 Name Constraints: critical Permitted: othername:<unsupported> email:.abcde.at
email:.abcde.be email:.abcde.bg email:.abcde.by DNS:.dir DirName: DC = dir, DC = emea
DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic DirName: C = BG, ST =
EMEA, L = BG, O = ABCDE Group, OU = Domestic DirName: C = BE, ST = EMEA, L = BN, O = ABCDE
 Group, OU = Domestic DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service
Z100 URI:.dir IP:172.23.0.171/255.255.255.255 Excluded: DNS:.dir URI:.dir
```

위의 정의와 일치하는 허용되는 클라이언트 인증서 주체는 다음과 같습니다.

```
 Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1, CN=cwinwell
```

신뢰할 수 있는 저장소 인증서 보기

신뢰할 수 있는 인증서 페이지에는 Cisco ISE-PIC에 추가된 모든 신뢰할 수 있는 인증서가 나열됩니다.

모든 인증서를 보려면 Choose(선택) **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. 신뢰할 수 있는 인증서 페이지가 표시되고 신뢰할 수 있는 인증서가 모두 나열됩니다.

신뢰할 수 있는 인증서 저장소의 상태 변경

Cisco ISE-PIC가 신뢰를 설정하는 데 인증서를 사용할 수 있도록 인증서의 상태를 활성화해야 합니다. 인증서는 신뢰할 수 있는 인증서 저장소로 가져올 때 자동으로 활성화됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** 활성화하거나 비활성화할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 상태를 변경합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

신뢰할 수 있는 인증서 저장소에 인증서 추가

인증서 저장소 페이지에서 Cisco ISE-PIC에 CA 인증서를 추가할 수 있습니다.

시작하기 전에

- 브라우저를 실행 중인 컴퓨터의 파일 시스템에 인증서 저장소 인증서가 있는지 확인합니다. 인증서는 PEM 또는 DER 형식이어야 합니다.
- 관리자 또는 EAP 인증용으로 인증서를 사용하려는 경우 인증서에 기본 제한이 정의되어 있으며 CA 플래그가 true로 설정되어 있는지 확인합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 필요한 대로 필드 값을 구성합니다.

EAP 인증 또는 인증 기반 관리자 인증용으로 인증서 체인의 하위 CA 인증서를 사용하려는 경우 인증서 체인에서 루트 CA까지의 모든 인증서를 가져오는 동안 **Trust for client authentication and Syslog(**클라이언트 인증 및 **Syslog** 신뢰**)** 확인란이 선택되어 있어야 합니다. Cisco ISE 2.6 패치 1 이상에서 동일한 주체 이름을 가진 CA 인증서를 둘 이상 가져올 수 있습니다. 인증서 기반 관리자 인증의 경우 신뢰할 수 있는 인증서를 추가 할 때 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증 신뢰**)** 확인란을 선택합니다. 저장소에 주체 이름이 동일한 다른 인증서가 있고 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증에 대한 신뢰**)** 확인란이 활성화되어 있으면 신뢰할 수 있는 저장소의 인증서에 대한 **Trust for certificate based admin authentication(**인증서 기반 관리자 인증에 대한 신뢰**)** 옵션을 수정할 수 없습니다.

인증 유형을 비밀번호 기반 인증에서 인증서 기반 인증으로 변경하면 Cisco ISE-PIC는 구축의 각 노드에서 애플리케이션 서버를 재시작합니다. 이때 PAN.

신뢰할 수 있는 인증서 편집

신뢰할 수 있는 인증서 저장소에 추가한 인증서는 설정 편집을 사용하여 추가로 편집할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 편집 가능한 필드를 필요한 대로 수정합니다.

단계 **4** **Save(**저장**)**를 클릭하여 인증서 저장소에 대한 변경사항을 저장합니다.

신뢰할 수 있는 인증서 삭제

더 이상 필요하지 않은 신뢰할 수 있는 인증서는 삭제할 수 있습니다. 그러나 ISE-PIC 내부 CA(Certificate Authority) 인증서는 삭제하면 안 됩니다. ISE-PIC 내부 CA 인증서는 전체 구축에 대해 ISE-PIC 루트 인증서 체인을 교체할 때만 삭제할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **2** 삭제할 인증서 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

경고 메시지가 표시됩니다. ISE-PIC 내부 CA 인증서를 삭제하도록 선택한 경우 다음을 클릭합니다.

- **Delete(**삭제**)** - ISE-PIC 내부 CA 인증서를 삭제합니다. 이 경우 ISE-PIC 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 엔드포인트가 네트워크에 다시 연결할 수 있도록 하려면 같은 ISE-PIC 내부 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
- **Delete & Revoke(**삭제 및 취소**)** - ISE-PIC 내부 CA 인증서를 삭제 및 취소합니다. 이 경우 ISE-PIC 내부 CA가 서명한 모든 엔드포인트 인증서는 무효화되며 엔드포인트가 네트워크에 연결할 수 없게 됩니다. 이 작업은 취소할 수 없으며, 전체 구축에 대해 ISE-PIC 루트 인증서 체인을 교체해야 합니다.

단계 **3** **Yes(**예**)**를 클릭하여 인증서를 삭제합니다.

신뢰할 수 있는 인증서 저장소에서 인증서 내보내기

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

참고 내부 CA에서 인증서를 내보내는 경우 해당 내보내기를 사용하여 백업에서 복원하려는 경우 CLI 명령 `application configure ise`를 사용해야 합니다. 자세한 내용은 Cisco ISE CA 인증서 및 키 내보내기, 107 페이지를 참조하십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **3** 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기

루트 CA 및 중간 CA 인증서를 가져오는 동안 신뢰할 수 있는 CA 인증서를 사용할 서비스를 지정할 수 있습니다.

시작하기 전에

CSR에 서명을 했으며 디지털 서명 CA 인증서를 반환한 인증 기관의 루트 인증서 및 기타 중간 인증서가 있어야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 표시되는 **Import a new Certificate into the Certificate Store(**인증서 저장소에 새 인증서 가져오기**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 CA에서 서명하고 반환한 루트 CA 인증서를 선택합니다.

단계 **4** **Friendly Name**을 입력합니다.

식별 이름을 입력하지 않으면 Cisco ISE-PIC는 *common-name#issuer#nnnnn* 형식의 이름을 이 필드에 자동으로 채웁니다. 여기서 *nnnnn*은 고유한 번호입니다. 인증서를 다시 편집하여 식별 이름을 변경할 수 있습니다.

단계 **5** 이 신뢰할 수 있는 인증서를 사용할 서비스 옆의 확인란을 선택합니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 인증서 설명을 입력합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

해당하는 경우 신뢰할 수 있는 인증서 저장소로 중간 CA 인증서를 가져옵니다.

인증서 체인 가져오기

인증서 저장소에서 수신한 인증서 체인이 들어 있는 단일 파일에서 여러 인증서를 가져올 수 있습니다. 파일의 모든 인증서는 PEM(Privacy-Enhanced Mail) 형식이어야 하며 인증서는 다음 순서로 정렬되어야 합니다.

- 파일의 마지막 인증서는 CA에서 발급된 클라이언트 또는 서버 인증서여야 합니다.
- 이전의 모든 인증서는 루트 CA 인증서이자 발급된 인증서의 서명 체인에 있는 중간 CA 인증서여야 합니다.

2단계 프로세스로 인증서 체인 가져오기:

1. 관리 포털의 신뢰할 수 있는 인증서 저장소로 인증서 체인 파일을 가져옵니다. 이 작업은 마지막 인증서를 제외한 모든 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.
2. CA 서명 인증서 바인딩 작업을 사용하여 인증서 체인 파일을 가져옵니다. 이 작업은 파일에서 마지막 인증서를 로컬 인증서로 가져옵니다.

신뢰할 수 있는 인증서 가져오기 설정

다음 표에서는 Cisco ISE-PIC에 CA(Certificate Authority) 인증서를 추가하는 데 사용할 수 있는 신뢰할 수 있는 인증서 가져오기 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Import**가져오기.

표 ***18:*** 신뢰할 수 있는 인증서 가져오기 설정

필드 이름	설명
Certificate File(인증서 파일**)**	브라우저를 실행 중인 컴퓨터에서 인증서 파일을 선택하려면 **Browse(**찾아보기**)**를 클릭합니다.
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다. 이름을 지정하지 않으면 Cisco ISE-PIC는 <common name> 형식으로 이름을 자동으로 생성합니다.#<issuer>#<nnnnn>, 여기서 <nnnnn>은 고유한 5자리 숫자입니다.
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	다른 ISE-PIC 노드 또는 LDAP 서버의 서버 인증서를 확인하는 데 이 인증서를 사용하려면 확인란을 선택합니다.

필드 이름	설명
Trust for client authentication and Syslog(클라이언트 인증 및 **Syslog** 신뢰**)**	(Trust for authentication within ISE-PIC(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 ISE-PIC에 연결하는 엔드포인트 인증 • Syslog 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Validate Certificate Extensions(인증서 확장명 검증**)**	(Trust for client authentication(클라이언트 인증 신뢰) 및 Enable Validation of Certificate Extensions(인증서 확장명 검증 활성화) 옵션을 둘 다 선택하는 경우에만 해당함) "keyUsage" 확장명이 있고 "keyCertSign" 비트가 설정되어 있으며 CA 플래그가 true로 설정된 기본 제한 확장명이 있는지 확인합니다.
Description(설명**)**	필요에 따라 설명을 입력합니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 86 페이지
인증서 체인 가져오기, 92 페이지
신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 91 페이지

인증서 서명 요청

서명된 인증서를 발급하는 CA(Certificate Authority)의 경우 CSR(Certificate Signing Request)을 생성하고 CA에 제출해야 합니다.

생성한 CSR(Certificate Signing Requests) 목록은 인증서 서명 요청 페이지에서 사용할 수 있습니다. CA(Certificate Authority)에서 서명을 받으려면 CSR을 내보낸 다음 인증서를 CA로 보내야 합니다. CA는 인증서에 서명한 다음 반환합니다.

관리 포털을 통해 중앙에서 인증서를 관리할 수 있습니다. 구축 환경의 모든 노드에 사용할 CSR을 생성하고 내보낼 수 있습니다. 그런 다음 CSR을 CA에 제출하고, CA에서 CA 서명 인증서를 받고, CA에서 반환된 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져온 다음 CA 서명 인증서를 CSR에 바인딩해야 합니다.

인증서 서명 요청을 생성하고 인증 기관에 CSR 제출

CSR(Certificate Signing Request)을 생성하여 구축의 노드용으로 CA에서 서명한 인증서를 가져올 수 있습니다. 구축의 선택한 노드 또는 구축의 모든 노드에 대해 CSR을 생성할 수 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 2 CSR 생성을 위한 값을 입력합니다. 각 필드에 대한 자세한 내용은 인증서 서명 요청 설정을 참조하십시오.

단계 3 **Generate(**생성**)**를 클릭하여 CSR을 생성합니다.

CSR이 생성됩니다.

단계 4 **Export(**내보내기**)**를 클릭하여 메모장에서 CSR을 엽니다.

단계 5 "-----BEGIN CERTIFICATE REQUEST-----"부터 "-----END CERTIFICATE REQUEST-----"까지의 모든 텍스트를 복사합니다.

단계 6 CSR의 내용을 선택한 CA의 인증서 요청에 붙여 넣습니다.

단계 7 서명된 인증서를 다운로드합니다.

일부 CA의 경우 서명된 인증서를 이메일로 전송할 수 있습니다. 서명된 인증서는 zip 파일 형식이며 새로 발급된 인증서와 CA의 공개 서명 인증서가 들어 있습니다. 이러한 인증서를 Cisco ISE-PIC 신뢰할 수 있는 인증서 저장소에 추가해야 합니다. 디지털 서명된 CA 인증서, 루트 CA 인증서 및 기타 중간 CA 인증서(해당하는 경우)가 클라이언트 브라우저를 실행 중인 로컬 시스템에 다운로드됩니다.

CSR에 CA 서명 인증서 바인딩

CA가 디지털 서명된 인증서를 반환하고 나면 해당 인증서를 CSR(Certificate Signing Request)에 바인딩해야 합니다. 관리 포털에서 구축의 모든 노드에 대해 바인딩 작업을 수행할 수 있습니다.

시작하기 전에

- 디지털 서명된 인증서와 CA가 반환한 관련 루트 중간 CA 인증서가 있어야 합니다.
- 관련 루트 및 중간 CA 인증서를 신뢰할 수 있는 인증서 저장소(**Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서)로 가져옵니다. .

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

CSR을 CA 서명 인증서에 바인딩할 노드 옆의 확인란을 선택합니다.

단계 2 **Bind(**바인딩**)**를 클릭합니다.

단계 3 **Browse(**찾아보기**)**를 클릭하여 CA 서명 인증서를 선택합니다.

단계 4 인증서의 식별 이름을 지정합니다.

단계 **5** Cisco **ISE**가 인증서 확장명을 검증하도록 하려면 ISE-PIC 확인란을 선택합니다.

Validation of Certificate Extensions(인증서 확장명 검증**)** 옵션을 활성화하는 경우 가져오는 인증서에 CA 플래그가 true로 설정된 기본 제한 확장명이 포함되어 있으면 키 사용 확장이 있는지 확인하고, keyEncipherment 비트나 keyAgreement 중 하나 또는 두 비트가 모두 설정되어 있는지도 확인합니다.

참고 ISE는 EAP-TLS 클라이언트 인증서가 있어야 디지털 서명 키 사용 확장명을 보유할 수 있습니다.

단계 **6** 사용 영역에서 이 인증서를 사용할 서비스를 확인합니다.

CSR을 생성하는 중에 Usage(사용) 옵션을 활성화한 경우 이 정보는 자동으로 채워집니다. 인증서를 바인딩할 때 사용을 지정하지 않으려면 Usage(사용) 옵션을 선택 취소해 주십시오. 나중에 인증서를 편집하여 사용을 지정할 수 있습니다.

참고 기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다.

기본 PAN에서 관리 역할 인증서의 인증서를 변경하면 다른 모든 노드에서 서비스가 재시작됩니다. PAN(Primary Administration Node)에서 다시 시작이 완료된 후 한 번에 한 노드씩 시스템이 다시 시작됩니다.

단계 **7** **Submit(**제출**)**을 클릭하여 CA 서명 인증서를 바인딩합니다.

Cisco ISE-PIC 노드 간 통신에 이 인증서를 사용하도록 선택한 경우에는 Cisco ISE-PIC 노드의 애플리케이션 서버가 다시 시작됩니다.

이 프로세스를 반복하여 다른 노드에서 CSR을 CA 서명 인증서와 바인딩합니다.

다음에 수행할 작업

신뢰할 수 있는 인증서 저장소로 루트 인증서 가져오기, 91 페이지

인증서 서명 요청 내보내기

이 페이지를 사용하여 인증서 서명 요청을 내보낼 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** 다.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭하여 클라이언트 브라우저를 실행 중인 파일 시스템에 파일을 저장합니다.

인증서 서명 요청 설정

Cisco ISE-PIC에서는 관리 포털에서 단일 요청으로 구축의 노드에 대한 CSR을 생성할 수 있습니다. 또한 선택적으로 구축의 단일 노드 또는 노드에 대한 CSR도 생성할 수 있습니다. 여러 노드에 대한 CSR을 생성하도록 선택하는 경우 ISE는 인증서 주체의 CN= 필드에서 특정 노드의 FQDN(Fully Qualified Domain Name)을 자동으로 대체합니다. 인증서의 SAN(대체 주체 이름) 필드에 항목을 포함

하도록 선택하는 경우 다른 SAN 특성과 함께 ISE-PIC 노드의 FQDN을 입력해야 합니다. 구축의 노드에 대해 CSR을 생성하도록 선택하는 경우 Allow Wildcard Certificates(와일드카드 인증서 허용) 확인란을 선택하고 SAN 필드(DNS 이름)에 와일드카드 FQDN 표기법(예: *.amer.example.com)을 입력합니다. EAP 인증에 인증서를 사용하려는 경우 CN= 필드에 와일드카드 값을 입력하지 마십시오.

와일드카드 인증서를 사용하는 경우에는 각 Cisco ISE-PIC 노드에 대해 고유한 인증서를 더 이상 생성하지 않아도 됩니다. 또한 인증서 경고가 표시되지 않도록 하기 위해 여러 FQDN 값을 SAN 필드에 입력할 필요도 없습니다. SAN 필드에 별표(*)를 사용하면 구축의 노드 에 걸쳐 단일 인증서를 공유할 수 있으며, 인증서 이름 불일치 경고가 표시되지 않습니다. 그러나 와일드카드 인증서를 사용하는 방식은 각 Cisco ISE-PIC 노드용으로 고유한 서버 인증서를 할당하는 방식보다 보안성이 낮은 것으로 간주됩니다.

다음 표에서는 CSR(Certificate Signing Request) 페이지의 필드에 대해 설명합니다. 이 페이지는 CA(Certificate Authority)에 의해 서명될 수 있는 CSR을 생성하는 데 사용할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**.

표 *19:* 인증서 서명 요청 설정

필드	사용 지침
Certificate(s) will be used for(인증서 사용 대상**)**	

필드	사용 지침
	인증서를 사용할 서비스를 선택합니다. **Cisco ISE ID** 인증서 • **Multi-Use(**다용도**)**: 여러 서비스(관리, EAP-TLS 인증, pxGrid)에 사용됩니다. 다용도 인증서는 클라이언트 및 서버 키 사용을 모두 지원합니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **Admin(**관리**)**: 구축의 ISE-PIC 노드 간 통신 및 관리 포털과의 통신을 보호하기 위한 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 웹 서버 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **ISE Messaging Service(ISE** 메시징 서비스**)**: Cisco ISE 메시징을 통한 시스템 로그 기능에서 사용되며, 내장된 UDP 시스템 로그 수집 대상(LogCollector 및 LogCollector2)에 대해 MnT WAN 존속성을 활성화합니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) • **pxGrid**: pxGrid 클라이언트와 서버 간의 통신을 보호하기 위해 클라이언트 및 서버 인증에 사용됩니다. 서명 CA의 인증서 템플릿은 컴퓨터 또는 머신 인증서 템플릿이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) • **SAML**: SAML IdP(Identity Provider)와의 통신을 보호하는 데 사용되는 서버 인증서입니다. SAML에 사용하도록 지정된 인증서는 관리, EAP, 인증 등의 기타 서비스에는 사용할 수 없습니다. • 키 사용: 디지털 서명(서명) • 확장 키 사용: TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) Extended Key

필드	사용 지침

	참고 Usage(확장 키 사용) 속성의 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하지 않는 것이 좋습니다. Extended Key Usage(확장 키 사용) 속성에서 모든 용도 개체 식별자에 대해 2.5.29.37.0 값을 포함하는 인증서를 사용하는 경우 인증서가 유효하지 않은 것으로 간주되고 다음 오류 메시지가 표시됩니다.
	`source=local ; type=fatal ; message="unsupported certificate"`
	Cisco ISE 인증 기관 인증서
	• **ISE Root CA(ISE** 루트 **CA)**: (내부 CA 서비스에만 해당함) 기본 PAN의 루트 CA 및 PSN의 하위 CA를 비롯하여 전체 내부 CA 인증서 체인을 재생성하는 데 사용됩니다.
	• **ISE Intermediate CA(ISE** 중간 **CA)**: (ISE-PIC가 외부 PKI의 중간 CA로 작동하는 경우 내부 CA 서비스에만 해당함) 기본 PAN의 중간 CA 인증서 및 PSN의 하위 CA 인증서를 생성하는 데 사용됩니다. 서명 CA의 인증서 템플릿은 하위 인증 기관이라고도 합니다. 이 템플릿에는 다음과 같은 속성이 있습니다.
	  • 기본 제한: 위험, Certificate Authority
	  • 키 사용: 인증서 서명, 디지털 서명
	  • 확장 키 사용: OCSP 서명(1.3.6.1.5.5.7.3.9)
	• **Renew ISE OCSP Responder Certificates(ISE OCSP** 응답자 인증서 갱신**)**: (내부 CA 서비스에만 해당함) 전체 구축에 대한 ISE-PIC OCSP 응답자 인증서를 갱신하는 데 사용됩니다(및 인증서 서명 요청이 아님). 보안을 위해 ISE-PIC OCSP 응답자 인증서는 6개월에 한 번씩 갱신하는 것이 좋습니다.

Allow Wildcard Certificates(와일드카드 인증서 허용**)**	인증서의 SAN 필드에서 CN 및/또는 DNS 이름에 와일드카드 문자(*)를 사용하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 구축의 모든 노드가 자동으로 선택됩니다. 맨 왼쪽 레이블 위치에 별표(*) 와일드카드 문자를 사용해야 합니다. 와일드카드 인증서를 사용하는 경우에는 보안 향상을 위해 도메인 공간을 분할하는 것이 좋습니다. 예를 들어 *.example.com 대신 *.amer.example.com으로 도메인을 분할할 수 있습니다. 도메인을 분할하지 않으면 심각한 보안 문제가 발생할 수 있습니다.
Generate CSRs for these Nodes(이 노드에 대해 **CSR** 생성**)**	인증서를 생성할 노드 옆에 있는 확인란을 선택합니다. 구축의 선택 노드에 대해 CSR을 생성하려면 Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션의 선택을 취소해야 합니다.

필드	사용 지침
Common Name(공통 이름**) (CN)**	기본적으로 공통 이름은 CSR을 생성하는 ISE-PIC 노드의 FQDN입니다. $FQDN$은 ISE-PIC 노드의 FQDN을 나타냅니다. 구축의 여러 노드에 대해 CSR을 생성하는 경우 CSR의 Common Name(공통 이름) 필드가 해당 ISE 노드의 FQDNdmfh 대체됩니다.
Organizational Unit (OU)(OU(조직 단위**))**	조직 단위의 이름입니다. Engineering 등을 예로 들 수 있습니다.
Organization (O)(O(조직**))**	조직의 이름입니다. Cisco 등을 예로 들 수 있습니다.
City (L)(L(구/군/시**))**	(약어로 표기하지 않음) 구/군/시의 이름입니다. San Jose 등을 예로 들 수 있습니다.
State (ST)(ST(시/도**))**	(약어로 표기하지 않음) 시/도의 이름입니다. California 등을 예로 들 수 있습니다.
Country(국가**) (C)**	국가의 이름입니다. 2자리 ISO 국가 코드를 입력해야 합니다. US 등을 예로 들 수 있습니다.
SAN(Subject Alternative Name)	IP 주소, DNS 이름, URI(Uniform Resource Identifier) 또는 인증서와 연결된 디렉토리 이름 • **DNS** 이름: DNS 이름을 선택하는 경우 ISE-PIC 노드의 정규화된 도메인 이름을 입력합니다. Allow Wildcard Certificates(와일드카드 인증서 허용) 옵션을 활성화한 경우 와일드카드 표기법(별표 및 도메인 이름 앞의 마침표)을 지정합니다. 예: *.amer.example.com • **IP** 주소: 인증서와 연결할 ISE-PIC 노드의 IP 주소입니다. • **Uniform Resource Identifier**: 인증서와 연결할 URI입니다. • 디렉토리 이름: RFC 2253에 따라 정의된 DN(Distinguished Name)의 문자열 표현입니다. 쉼표(,)를 사용하여 DN을 구분합니다. "dnQualifier" RDN의 경우 쉼표를 이스케이프하고 구분 기호로 백슬래시와 쉼표, 즉 "\,"를 사용합니다. 예: CN=AAA,dnQualifier=O=Example\,DC=COM,C=IL
키 유형	공개 키를 생성하는 데 사용할 알고리즘을 RSA 또는 ECDSA로 지정합니다.

필드	사용 지침
Key Length(키 길이**)**	공개 키의 비트 크기를 지정합니다. RSA에는 다음 옵션을 사용할 수 있습니다. • 512 • 1024 • 2048 • 4096 ECDSA에는 다음 옵션을 사용할 수 있습니다. • 256 • 384 참고 RSA 및 ECDSA 공개 키는 동일한 보안 레벨에서 키 길이가 다를 수 있습니다. 공용 CA 서명 인증서를 가져오거나 FIPS 호환 정책 관리 시스템으로 Cisco ISE-PIC를 구축하려면 2048 이상을 선택합니다.
Digest to Sign With(서명에 사용할 다이제스트**)**	SHA-1 또는 SHA-256 해싱 알고리즘 중 하나를 선택합니다.
인증서 정책	인증서가 준수해야 하는 인증서 정책 OID 또는 OID 목록을 입력합니다. 쉼표나 공백을 사용하여 OID를 구분합니다.

Cisco ISE CA 서비스

인증서는 자체 서명되거나 외부 CA(Certificate Authority)에 의해 디지털 서명될 수 있습니다. ISE-PIC는 pxGrid 인증서에 디지털 서명을 하는 pxGrid의 외부 인증서 기관(CA) 역할을 할 수 있습니다. CA 서명 디지털 인증서는 업계 표준으로 보안성이 더 높은 것으로 간주됩니다. ISE-PIC CA는 다음과 같은 기능을 제공합니다.

- Certificate Issuance: 네트워크에 연결되는 엔드포인트에 대한 CSR(Certificate Signing Requests)을 검증하고 서명합니다.
- Key Management: 키와 인증서를.
- Certificate Storage: 사용자 및 디바이스에 발급된 인증서를 저장합니다.
- Support OCSP(Online Certificate Status Protocol): 인증서의 유효성을 확인하도록 OCSP 응답자를 제공합니다.

기본 관리 노드에서 CA 서비스가 비활성화된 경우에도 보조 관리 노드의 CLI에서 실행 중인 것으로 간주됩니다. CA 서비스는 비활성화 된 상태로 표시하는 것이 가장 좋습니다. 이는 알려진 Cisco ISE 문제입니다.

Elliptical Curve Cryptography 인증서 지원

Cisco ISE-PIC CA 서비스는 ECC(Elliptical Curve Cryptography) 알고리즘을 기반으로 하는 인증서를 지원합니다. ECC는 훨씬 작은 키 크기를 사용하는 경우에도 다른 암호화 알고리즘보다 더 우수한 보안 및 성능을 제공합니다.

다음 테이블에서는 ECC 및 RSA의 키 크기와 보안 수준을 비교합니다.

ECC 키 크기**(**비트**)**	**RSA** 키 크기**(**비트**)**
160	1024
224	2048
256	3072
384	7680
521	15360

키 크기가 더 작기 때문에 암호화가 더 빠릅니다.

Cisco ISE-PIC는 다음과 같은 ECC 커브 유형을 지원합니다. 커브 유형 또는 키 크기가 클수록 보안이 우수합니다.

- P-192
- P-256
- P-384
- P-521

ISE-PIC는 인증서의 EC 부분에서 명시적 매개변수를 지원하지 않습니다. 명시적 매개변수를 사용하여 인증서를 가져오려고 하면 Validation of certificate failed: Only named ECParameters(인증서 검증 실패: 명명된 EC 매개변수만 지원됨)라는 오류가 표시됩니다.

인증서 프로비저닝 포털에서 ECC 인증서를 생성할 수 있습니다.

Cisco ISE-PIC Certificate Authority 인증서

CA(인증기관) 인증서 페이지에는 내부 Cisco ISE-PIC CA와 관련된 모든 인증서가 나열됩니다. 이러한 인증서는 이 페이지에 노드별로 나열됩니다. 노드를 펼쳐서 해당 특정 노드의 모든 ISE-PIC CA 인증서를 확인할 수 있습니다. 기본 및 보조 관리 노드에는 루트 CA, 노드 CA, 하위 CA 및 OCSP 응답자 인증서가 있습니다. 구축의 다른 노드에는 엔드포인트 하위 CA 및 OCSP 인증서가 있습니다.

Cisco ISE-PIC CA 서비스를 활성화하면 이러한 인증서가 생성되어 모든 노드에 자동으로 설치됩니다. 또한 전체 ISE-PIC 루트 CA 체인을 교체하면 이러한 인증서가 재생성되어 모든 노드에 자동으로 설치됩니다. 수동 개입이 필요하지 않습니다.

Cisco ISE-PIC CA 인증서는 **Certificate Services** <***Endpoint Sub CA/Node CA/Root CA/OCSP Responder***>-<*node_hostname*>#*certificate_number* 명명 규칙을 따릅니다.

CA 인증서 페이지에서 Cisco ISE-PIC CA 인증서의 편집, 가져오기, 내보내기, 삭제 및 보기가 가능합니다.

Cisco ISE-PIC CA 인증서 편집

Cisco ISE-PIC CA 인증서 저장소에 인증서를 추가한 뒤에는 설정 편집을 사용하여 추가로 편집할 수 있습니다.

단계 **1**

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**.

단계 **3** 편집할 인증서 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 편집 가능한 필드를 필요한 대로 수정합니다. 필드에 대한 설명은 인증서 설정 편집을 참조하십시오.

단계 **5** **Save(**저장**)**를 클릭하여 인증서 저장소에 대한 변경사항을 저장합니다.

Cisco ISE CA 인증서 내보내기

Cisco ISE 루트 CA 및 노드 CA 인증서를 내보내려면 다음을 수행합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Authority Certificates(**인증 기관 인증서**)**.

단계 **2** 내보낼 인증서 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다. 인증서는 한 번에 하나씩만 내보낼 수 있습니다.

단계 **3** 클라이언트 브라우저를 실행 중인 파일 시스템에 프라이버시가 강화된 메일 파일을 저장합니다.

Cisco ISE-PIC CA 인증서 가져오기

가 다른 구축의 Cisco ISE-PIC CA에서 발급한 인증서를 사용하여 네트워크에 인증하려고 하는 경우에는 해당 구축의 Cisco ISE-PIC 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 Cisco ISE-PIC 신뢰할 수 있는 인증서 저장소로 가져와야 합니다.

시작하기 전에

- 엔드포인트 인증서가 서명된 구축에서 ISE-PIC 루트 CA, 노드 CA 및 엔드포인트 하위 CA 인증서를 내보낸 다음 브라우저를 실행 중인 컴퓨터의 파일 시스템에 저장합니다.

단계 **1**

단계 **2** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**.

단계 **3** **Import(**가져오기**)**를 클릭합니다.

단계 **4** 필요한 대로 필드 값을 구성합니다. 자세한 내용은 신뢰할 수 있는 인증서 가져오기 설정을 참조하십시오.

클라이언트 인증서 기반 인증이 활성화되어 있으면 Cisco ISE-PIC는 구축의 각 노드에서 애플리케이션 서버를 다시 시작합니다. 이때 PAN에서 애플리케이션 서버부터 시작한 다음 .

인증서 설정 편집

다음 표에서는 CA(Certificate Authority) 인증서 특성을 편집하는 데 사용할 수 있는 인증서 저장소 인증서 편집 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)** > **Certificate(**인증서**)** > **Edit(**편집**)**.

표 ***20:*** 인증서 저장소 편집 설정

필드 이름	사용 지침
인증서 발급자	
Friendly Name(식별 이름**)**	인증서의 식별 이름을 입력합니다.
상태	Enabled(활성화됨) 또는 Disabled(비활성화됨)를 선택합니다. Disabled(비활성화됨)를 선택하면 ISE가 신뢰를 설정하는 데 인증서를 사용하지 않습니다.
설명	필요에 따라 설명을 입력합니다.
사용	
Trust for authentication within ISE(ISE 내의 인증 신뢰**)**	이 인증서가 다른 ISE 노드 또는 LDAP 서버의 서버 인증서를 확인하도록 하려면 확인란을 선택합니다.

필드 이름	사용 지침
Trust for client authentication and Syslog(클라이언트 인증 및 **Syslog** 신뢰**)**	(Trust for authentication within ISE(ISE 내의 인증 신뢰) 확인란을 선택하는 경우에만 해당함) 다음 용도로 이 인증서를 사용하려는 경우 확인란을 선택합니다. • EAP 프로토콜을 사용하여 ISE에 연결하는 엔드포인트 인증 • Syslog 서버 신뢰
Trust for authentication of Cisco Services(Cisco 서비스의 인증 신뢰**)**	피드 서비스와 같은 외부 Cisco 서비스를 신뢰하는 데 이 인증서를 사용하려는 경우 이 확인란을 선택합니다.
Certificate Status Validation(인증서 상태 검증**)**	ISE는 특정 CA가 발급한 클라이언트 또는 서버 인증서의 취소 상태를 확인하는 두 가지 방법을 지원합니다. 첫 번째 방법은 OCSP(Online Certificate Status Protocol)를 사용하여 인증서를 검증하는 것입니다. 이 경우 CA가 유지 관리하는 OCSP 서비스에 요청을 하게 됩니다. 두 번째 방법은 CA에서 ISE로 다운로드할 수 있는 CRL(Certificate Revocation List)과 대조하여 인증서를 검증하는 것입니다. 이 두 방법은 모두 활성화할 수 있으며 이 경우 OCSP가 먼저 사용됩니다. 상태를 확인할 수 없는 경우에만 CRL이 사용됩니다.
Validate Against OCSP Service(OCSP 서비스와 대조하여 검증**)**	OCSP 서비스와 대조하여 인증서를 검증하려면 확인란을 선택합니다. 먼저 OCSP 서비스를 생성해야 이 확인란을 선택할 수 있습니다.
Reject the request if OCSP returns UNKNOWN status(OCSP에서 **UNKNOWN** 상태를 반환하는 경우 요청 거부**)**	OCSP에서 인증서 상태를 확인할 수 없는 경우 요청을 거부하려면 확인란을 선택합니다. 이 확인란을 선택하면 OCSP 서비스에서 알 수 없는 상태 값을 반환하면 ISE가 현재 평가 중인 클라이언트 또는 서버 인증서를 거부합니다.
Reject the request if OCSP Responder is unreachable(OCSP 응답자에 연결할 수 없는 경우 요청 거부**)**	OCSP 응답자에 연결할 수 없는 경우 ISE가 요청을 거부하도록 하려면 체크 박스를 선택합니다.
Download CRL(CRL 다운로드**)**	Cisco ISE가 CRL을 다운로드하도록 하려면 확인란을 선택합니다.

필드 이름	사용 지침
CRL Distribution URL(CRL 배포 **URL)**	CA에서 CRL를 다운로드할 URL을 입력합니다. 인증 기관 인증서에 URL이 지정되어 있으면 이 필드는 자동으로 채워집니다. URL은 " http", "https" 또는 "ldap"로 시작해야 합니다.
Retrieve CRL(CRL 검색**)**	CRL은 자동으로 다운로드할 수도 있고 정기적으로 다운로드할 수도 있습니다. 이 필드에서 다운로드 간의 시간 간격을 구성합니다.
If download failed, wait(다운로드 실패 시 대기**)**	Cisco ISE가 다시 CRL 다운로드를 시도할 때까지 대기할 시간 간격을 구성합니다.
Bypass CRL Verification if CRL is not Received(CRL이 수신되지 않으면 **CRL** 확인 바이패스**)**	CRL이 수신되기 전에 클라이언트 요청을 수락하려면 이 확인란을 선택합니다. 이 확인란의 선택을 취소하면 선택한 CA가 서명을 한 인증서를 사용하는 모든 클라이언트 요청은 Cisco ISE가 CRL 파일을 받을 때까지 거부됩니다.
Ignore that CRL is not yet valid or expired(CRL 이 아직 유효하지 않거나 만료된 경우 시작일/만료 날짜 무시**)**	Cisco ISE가 시작일과 만료 날짜를 무시하고 아직 활성화되지 않았거나 만료된 CRL을 계속 사용하도록 하고, CRL의 내용에 따라 EAP-TLS 인증을 허용하거나 거부하도록 하려면 이 체크 박스를 선택합니다. Cisco ISE가 CRL 파일에서 Effective Date(유효 날짜) 필드의 시작일과 Next Update(다음 업데이트) 필드의 만료 날짜를 확인하도록 하려면 이 체크 박스의 선택을 취소합니다. CRL이 아직 활성화되지 않았거나 만료된 경우에는 이 CA가 서명을 한 인증서를 사용하는 모든 인증은 거부됩니다.

관련 항목

신뢰할 수 있는 인증서 저장소, 86 페이지
신뢰할 수 있는 인증서 편집, 90 페이지

Cisco ISE-PIC CA 인증서 및 키 백업 및 복원

Cisco ISE-PIC CA 인증서 및 키를 안전하게 백업해야 PAN 장애 발생 시 외부 PKI의 루트 CA 또는 중간 CA로 작동하도록 보조 관리 노드를 승격시키려는 경우 보조 관리 노드에서 다시 복원할 수 있습니다. Cisco ISE-PIC 컨피그레이션 백업에는 CA 인증서 및 키가 포함되지 않습니다. 대신 CLI(Command Line Interface)를 사용하여 CA 인증서 및 키를 리포지토리로 내보냈다가 가져와야 합니다. 제공 **application configure ise** 명령에는 이제 CA 인증서 및 키를 백업하고 복원할 수 있는 export 및 import 옵션이 포함되어 있습니다.

신뢰할 수 있는 인증서 저장소의 다음 인증서가 보조 관리 노드에서 복원됩니다.

- Cisco ISE 루트 CA 인증서
- Cisco ISE 하위 CA 인증서
- Cisco ISE 엔드포인트 RA 인증서
- Cisco ISE OCSP Responder 인증서

다음과 같은 경우에 Cisco ISE CA 인증서 및 키를 백업하고 복원해야 합니다.

- 구축 환경에 보조 관리 노드가 있는 경우
- 전체 Cisco ISE-PIC CA 루트 체인을 바꾸는 경우
- 외부 PKI의 하위 CA 역할을 하도록 Cisco ISE-PIC 루트 CA를 구성하는 경우
- 컨피그레이션 백업에서 데이터를 복원하는 경우. 이 경우에는 먼저 Cisco ISE-PIC CA 루트 체인을 다시 생성한 다음 ISE CA 인증서 및 키를 백업하고 복원해야 합니다.

참고 구축에서 Cisco ISE 내부 CA를 교체할 때마다 ISE 메시징 서비스도 업데이트해야 전체 인증서 체인을 검색할 수 있습니다.

Cisco ISE CA 인증서 및 키 내보내기

PAN에서 CA 인증서 및 키를 내보내야 보조 관리 노드에서 해당 인증서와 키를 가져올 수 있습니다. 이 옵션을 사용하는 경우 PAN이 다운되면 보조 관리 노드가 엔드포인트에 대해 인증서를 발급하고 관리할 수 있으며, 이 경우 보조 관리 노드를 PAN으로 승격합니다.

시작하기 전에

CA 인증서와 키를 저장할 리포지토리를 생성했는지 확인합니다.

단계 **1** 입력 **application configure ise** 명령을 사용하여 CPU 및 메모리 크기를 확인할 수 있습니다.

단계 **2** 입력 7 그런 다음 인증서와 키를 내보냅니다.

단계 **3** 리포지토리 이름을 입력합니다.

단계 **4** 암호화 키를 입력합니다.

내보내진 인증서 목록 및 주체, 발급자, 일련 번호가 포함된 성공 메시지가 나타납니다.

예제:

```
 The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':
Subject:CN=Cisco ISE Self-Signed CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765 Subject:CN=Cisco ISE Endpoint CA of ise-vm1 Issuer:CN=Cisco
 ISE Self-Signed CA of ise-vm1 Serial#:0x7027269d-d80a406d-831d5c26-f5e105fa Subject:CN=Cisco ISE Endpoint
 RA of ise-vm1 Issuer:CN=Cisco ISE Endpoint CA of ise-vm1 Serial#:0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2
 Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
 Serial#:0x6f6d4097-21f74c4d-8832ba95-4c320fb1 ISE CA keys export completed successfully
```

Cisco ISE-PIC CA 인증서 및 키 가져오기

보조 관리 노드를 등록한 후에는 PAN에서 CA 인증서와 키를 내보낸 다음 보조 관리 노드로 가져와야 합니다.

단계 **1** 입력 **application configure ise** 을 Cisco ISE-PIC CLI에서 입력합니다.

단계 **2** 입력 8 그런 다음 CA 인증서와 키를 가져옵니다.

단계 **3** 리포지토리 이름을 입력합니다.

단계 **4** 가져올 파일의 이름을 입력합니다. 파일 이름은 **ise_ca_key_pairs_of_<vm hostname>** 형식이 되어야 합니다.

단계 **5** 파일 암호를 해독할 암호화 키를 입력합니다.

성공 메시지가 나타납니다.

예제:

```
The following 4 CA key pairs were imported: Subject:CN=Cisco ISE Self-Signed CA of ise-vm1 Issuer:CN=Cisco
 ISE Self-Signed CA of ise-vm1 Serial#:0x21ce1000-8008472c-a6bc4fd9-272c8da4 Subject:CN=Cisco ISE Endpoint
 CA of ise-vm1 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1 Serial#:0x05fa86d0-092542b4-8ff68ed4-f1964a56
 Subject:CN=Cisco ISE Endpoint RA of ise-vm1 Issuer:CN=Cisco ISE Endpoint CA of ise-vm1
Serial#:0x77932e02-e8c84b3d-b27e2f1c-e9f246ca Subject:CN=Cisco ISE OCSP Responder Certificate of ise-vm1
 Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1 Serial#:0x5082017f-330e412f-8d63305d-e13fd2a5 Stopping
ISE Certificate Authority Service... ISE Certificate Authority 서비스 시작 중... ISE CA 키 가져오기가 완료되었습니다.
```

기본 PAN 및 PSN에서

구축을 설정할 때 Cisco ISE-PIC는 Cisco ISE CA 서비스용으로 노드. 그러나 노드의 또는 PSN의 도메인 이름이나 호스트 이름을 변경할 때는 기본 PAN에서 루트 CA를, PSN에서 하위 CA를 각각 재생성해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** . .

단계 **2** **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 **3** **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Root CA(ISE 루트 CA)를 선택합니다.

단계 **4** **Replace ISE Root CA Certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

루트 CA 및 하위 CA 인증서가 구축의 모든 노드에 대해 생성됩니다.

다음에 수행할 작업

구축에 보조 PAN이 있는 경우 기본 PAN에서 Cisco ISE-PIC CA 인증서와 키의 백업을 가져온 다음 보조 PAN에서 복원합니다. 그러면 기본 PAN 장애 시 보조 PAN이 루트 CA로 작동할 수 있으며, 이 경우 보조 PAN을 기본 PAN으로 승격합니다.

외부 PKI의 하위 CA로 Cisco ISE-PIC 루트 CA 구성

기본 PAN의 루트 CA가 외부 PKI의 하위 CA로 작동하도록 하려면 ISE-PIC 중간 CA 인증서 서명 요청을 생성하여 외부 CA로 보낸 다음 루트 및 CA 서명 인증서를 받습니다. 그런 다음 루트 CA 인증서는 신뢰할 수 있는 인증서 저장소로 가져오고 CA 서명 인증서는 CSR에 바인딩합니다. 이 경우 외부 CA는 루트 CA이고 노드은 외부 CA의 하위 CA이며 PSN은 노드의 하위 CA입니다.

단계 1 **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다.

단계 2 **Generate Certificate Signing Requests (CSR)(CSR** 생성**)**를 클릭합니다.

단계 3 **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 ISE Intermediate CA(ISE 중간 CA)를 선택합니다.

단계 4 **Generate(**생성**)**를 클릭합니다.

단계 5 CSR을 내보내 외부 CA로 보낸 다음 CA 서명 인증서를 받습니다.

단계 6 외부 CA의 루트 CA 인증서를 신뢰할 수 있는 인증서 저장소로 가져옵니다.

단계 7 CA 서명 인증서를 CSR에 바인딩합니다.

OCSP 서비스

OCSP(Online Certificate Status Protocol)는 x.509 디지털 인증서의 상태를 확인하는 데 사용되는 프로토콜입니다. CRL(Certificate Revocation List) 대신 사용 가능한 이 프로토콜은 CRL 처리로 인해 발생하는 문제를 해결합니다.

Cisco ISE에는 HTTP를 통해 OCSP 서버와 통신하여 인증에서 인증서의 상태를 검증하는 기능이 있습니다. Cisco ISE에 구성되어 있는 모든 CA(Certificate Authority) 인증서에서 참조할 수 있는 재사용 가능한 컨피그레이션 객체에서 OCSP 컨피그레이션을 구성합니다.

CA별로 CRL 및/또는 OCSP 확인을 구성할 수 있습니다. CRL과 OCSP를 모두 선택하면 Cisco ISE는 OCSP를 통해 먼저 확인을 수행합니다. 기본 및 보조 OCSP 서버에서 모두 통신 문제가 탐지되거나 지정된 인증서에 대해 알 수 없는 상태가 반환되면 Cisco ISE는 CRL을 확인하도록 전환됩니다.

Cisco ISE CA Service Online Certificate Status Protocol 응답자

Cisco ISE CA OCSP 응답자는 OCSP 클라이언트와 통신하는 서버입니다. Cisco ISE CA용 OCSP 클라이언트에는 내부 Cisco ISE OCSP 클라이언트 및 ASA(Adaptive Security Appliance)의 OCSP 클라이언트가 있습니다. OCSP 클라이언트는 RFC 2560, 5019에 정의된 OCSP 요청/응답 구조를 사용하여 OCSP 응답자와 통신해야 합니다.

Cisco ISE CA는 OCSP 응답자에 인증서를 발급합니다. OCSP 응답자는 포트 2560에서 모든 들어오는 요청을 수신 대기합니다. 이 포트는 OCSP 트래픽만 허용하도록 구성되어 있습니다.

OCSP 응답자는 RFC 2560, 5019에 정의된 구조를 따르는 요청을 수락합니다. OCSP 요청에서는 Nonce 확장이 지원됩니다. OCSP 응답자는 인증서 상태를 확보하여 OCSP 응답을 생성하고 서명합니다. 최대 기간인 24시간 동안 클라이언트에서 OCSP 응답을 캐시할 수 있지만 OCSP 응답자에서 OCSP 응답은 캐시되지 않습니다. OCSP 클라이언트는 OCSP 응답의 서명을 검증해야 합니다.

PAN의 셀프 서명된 CA 인증서(또는 ISE가 외부 CA의 중간 CA로 작동하는 경우 중간 CA 인증서)는 OCSP 응답자 인증서를 발급합니다. PAN의 이 CA 인증서는 PAN 및 PSN에서 OCSP 인증서를 발급합니다. 이 셀프 서명된 CA 인증서는 전체 구축의 루트 인증서이기도 합니다. 구축 전체의 모든 OCSP 인증서는 이러한 인증서를 사용하여 서명된 응답을 검증하기 위해 ISE의 신뢰할 수 있는 인증서 저장소에 배치됩니다.

OCSP 인증서 상태 값

OCSP 서비스는 지정된 인증서 요청에 대해 다음 값을 반환합니다.

- 정상 - 상태 질의에 대한 긍정적 응답을 나타냅니다. 이는 인증서가 취소되지 않았으며 상태가 다음 시간 간격(Time to Live) 값까지만 정상이라는 것을 의미합니다.
- 취소됨 - 인증서가 취소되었습니다.
- 알 수 없음 - 인증서 상태를 알 수 없습니다. 이 OCSP 응답자의 CA에 의해 인증서가 발급되지 않은 경우 OCSP 서비스에서 이 값을 반환합니다.
- 오류 - OCSP 요청에 대한 응답이 수신되지 않았습니다.

OCSP 고가용성

Cisco ISE는 CA당 최대 2대의 OCSP 서버를 구성할 수 있으며, 이러한 서버를 각각 기본 및 보조 OCSP 서버라고 합니다. 각 OCSP 서버 컨피그레이션에는 다음 매개변수가 포함됩니다.

- URL - OCSP 서버 URL입니다.
- Nonce - 요청에서 전송되는 난수입니다. 이 옵션을 사용하는 경우 재생 공격에서 이전 통신을 사용할 수 없습니다.
- Validate response - Cisco ISE는 OCSP 서버에서 수신되는 응답 서명을 검증합니다.

Cisco ISE는 기본 OCSP 서버와 통신할 때 타임아웃(5초)이 발생하면 보조 OCSP 서버로 전환합니다.

Cisco ISE는 구성 가능한 시간 동안 보조 OCSP 서버를 사용한 후 기본 서버 사용을 다시 시도합니다.

OCSP 실패

3가지 일반 OCSP 실패 시나리오는 다음과 같습니다.

- 실패한 OCSP 캐시 또는 OCSP 클라이언트 측(Cisco ISE) 장애

- 실패한 OCSP 응답자 시나리오. 예를 들어 다음과 같습니다.

  첫 번째 기본 OCSP 응답자가 응답하지 않고 보조 OCSP 응답자가 Cisco ISE OCSP 요청에 응답함

  Cisco ISE OCSP 요청에서 수신되지 않은 응답 또는 오류

  OCSP 응답자가 Cisco ISE OCSP 요청에 대한 응답을 또는 제공하지 않거나 OCSP 응답 상태를 실패한 상태로 반환할 수 있습니다. OCSP 응답 상태 값은 다음과 같습니다.

  - tryLater
  - signRequired
  - unauthorized
  - internalError
  - malformedRequest

    OCSP 요청에는 여러 가지 날짜 및 시간 검사, 서명 유효성 검사 등이 있습니다. 자세한 내용은 *RFC 2560 X.509* 인터넷 공개 키 인프라 *OCSP(Online Certificate Status Protocol)*를 참고하십시오. 여기에서는 오류 상태를 포함한 모든 가능한 상태를 설명합니다.

- 실패한 OCSP 보고서

OCSP 클라이언트 프로파일 추가

OCSP 클라이언트 프로파일 페이지를 사용하여 Cisco ISE에 새 OCSP 클라이언트 프로파일을 추가할 수 있습니다.

시작하기 전에

CA(Certificate Authority)가 비표준 포트(80 또는 443 이외의 포트)에서 OCSP 서비스를 실행 중인 경우 Cisco ISE와 해당 포트의 CA 간에 통신을 허용하도록 스위치에서 ACL을 구성해야 합니다. 예를 들면 다음과 같습니다.

permit tcp <*source ip*> <*destination ip*> **eq** <*OCSP port number*>

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Certificates(**인증서**)** > **OCSP Client Profile(OCSP** 클라이언트 프로파일**)**.

단계 **2** 값을 입력하여 OCSP 클라이언트 프로파일을 추가합니다.

단계 **3** 제출을 클릭합니다.

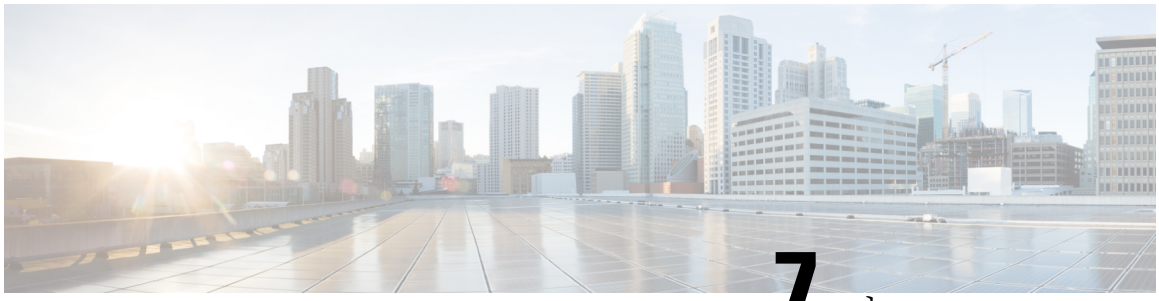
OCSP 통계 카운터

Cisco ISE는 OCSP 카운터를 사용하여 OCSP 서버의 데이터와 상태를 기록하고 모니터링합니다. 5분마다 기록됩니다. Cisco ISE는 syslog 메시지를 모니터링 노드로 보내며, 이 메시지는 로컬 저장소에 보존됩니다. 로컬 저장소에는 지난 5분 동안의 데이터가 포함되어 있습니다. Cisco ISE가 syslog 메시지를 보내고 나면 다음 간격에 대해 카운터가 다시 계산됩니다. 즉, 5분이 지나면 새로운 5분 시간 간격이 다시 시작됩니다.

다음 표에는 OCSP syslog 메시지와 해당 설명이 나와 있습니다.

표 ***21: OCSP syslog*** 메시지

메시지	설명
OCSPPrimaryNotResponsiveCount	응답하지 않는 기본 요청의 수
OCSPSecondaryNotResponsiveCount	응답하지 않는 보조 요청의 수
OCSPPrimaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 인증서의 수
OCSPSecondaryCertsGoodCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '정상' 상태의 수
OCSPPrimaryCertsRevokedCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPSecondaryCertsRevokedCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '취소된' 상태의 수
OCSPPrimaryCertsUnknownCount	기본 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPSecondaryCertsUnknownCount	보조 OCSP 서버를 사용하여 지정된 CA에 대해 반환되는 '알 수 없는' 상태의 수
OCSPPrimaryCertsFoundCount	기본 원본의 캐시에서 발견된 인증서의 수
OCSPSecondaryCertsFoundCount	보조 원본의 캐시에서 발견된 인증서의 수
ClearCacheInvokedCount	간격 이후 일반 캐시가 트리거된 횟수
OCSPCertsCleanedUpCount	간격 이후 정리된 캐시된 엔트리의 수
NumOfCertsFoundInCache	캐시에서 이행된 요청의 수
OCSPCacheCertsCount	OCSP 캐시에서 발견된 인증서의 수



7 장

관리 ISE-PIC

ISE-PIC 노드 관리

보조 노드를 추가하거나 제거하고, 노드간에 데이터를 동기화하고, 보조 노드를 기본 노드로 승격하는 등의 작업을 수행합니다.

Cisco ISE-PIC 구축 설정

Cisco Identity Services Engine 하드웨어 설치 설명서에 설명된 것처럼 모든 노드에 Cisco ISE-PIC를 설치하고 나면 노드가 독립형 상태로 표시됩니다. 그러면 한 노드를 PAN(Primary Administration Node)으로 정의하고 보조 노드를 PAN에 등록해야 합니다.

모든 Cisco ISE-PIC 시스템 및 기능 관련 컨피그레이션은 PAN에서만 수행되어야 합니다. PAN에서 수행한 컨피그레이션 변경 사항은 구축 환경의 보조 노드로 복제됩니다. 보조 노드에서 수행할 수 있는 유일한 작업은 해당 보조 노드를 PAN으로 승격하는 것입니다.

보조 노드를 PAN으로 등록한 후에 보조 노드의 관리 포털에 로그인하는 동안 PAN의 로그인 자격 증명을 사용해야 합니다.

기본 노드에서 보조 ISE-PIC 노드로의 데이터 복제

Cisco ISE 노드를 보조 노드로 등록하는 경우 Cisco ISE-PIC에서는 즉시 기본 노드에서 보조 노드로 연결되는 데이터 복제 채널을 생성하고 복제 프로세스를 시작합니다. 복제는 기본 노드에서 보조 노드로 Cisco ISE-PIC 컨피그레이션 데이터를 공유하는 프로세스입니다. 복제를 통해 구축의 일부에 해당하는 모든 Cisco ISE-PIC 노드에 있는 컨피그레이션 데이터 간에 일관성을 유지할 수 있습니다.

전체 복제는 일반적으로 ISE-PIC 노드를 처음 보조 노드로 등록하는 경우에 발생합니다. 증분 복제는 전체 복제 후에 발생하고, PAN 컨피그레이션 데이터의 추가, 수정 또는 삭제와 같이 새롭게 변경된 내용이 보조 노드에 반영되도록 합니다. 복제 프로세스를 사용하면 구축의 모든 Cisco ISE-PIC 노드

를 동기화할 수 있습니다. Cisco ISE-PIC 관리 포털의 구축 페이지에 있는 노드 상태 열에서 복제 상태를 확인할 수 있습니다. Cisco ISE-PIC 노드를 보조 노드로 등록하거나 PAN과의 수동 동기화를 수행하는 경우 노드 상태에는 요청한 작업이 진행 중임을 의미하는 주황색 아이콘이 표시됩니다. 작업이 완료되면 노드 상태는 보조 노드가 PAN과 동기화됨을 나타내는 녹색으로 바뀝니다.

Cisco ISE-PIC에서 노드 수정의 효과

Cisco ISE-PIC ISE의 노드를 다음과 같이 변경하면 해당 노드가 다시 시작되어 지연이 발생하게 됩니다.

- 노드 등록(독립형에서 보조로)
- 노드 등록 취소(보조에서 독립형으로)
- 기본 노드를 독립형으로 변경(다른 노드가 등록되지 않은 경우, 기본에서 독립형으로)
- 노드 승격(보조에서 기본으로)
- 기본 노드에서 백업을 복원하면 동기화 작업이 트리거되어 기본 노드에서 보조 노드로 데이터 복제

구축에서 2노드를 설정하기 위한 지침

Cisco ISE-PIC를 설정하기 전에 다음 정보를 신중히 읽어보십시오.

- 두 노드에 대해 동일한 NTP(Network Time Protocol) 서버를 선택합니다. 노드 사이의 시간대 문제를 방지하려면 각 노드 설정 시 동일한 NTP 서버 이름을 제공해야 합니다. 이 설정을 사용하면 구축의 다양한 노드에서 제공하는 보고서 및 로그가 항상 타임스탬프와 동기화될 수 있습니다.
- Cisco ISE-PIC 설치 시 Cisco ISE-PIC Admin 비밀번호를 구성합니다. 이전의 Cisco ISE-PIC Admin 기본 로그인 자격 증명(admin/cisco)은 더 이상 유효하지 않습니다. 초기 설정 중에 생성된 사용자 이름 및 비밀번호나 현재 비밀번호(나중에 변경된 경우)를 사용합니다.
- DNS(Domain Name System) 서버를 구성합니다. DNS 서버에서 구축에 포함되는 두 Cisco ISE-PIC 노드의 IP 주소 및 FQDN(Fully Qualified Domain Name)을 입력합니다. 그렇지 않으면, 노드 등록이 실패합니다.
- DNS 서버의 고가용성 구축에 있는 두 Cisco ISE-PIC 노드에 대한 정방향 및 역방향 DNS 조회를 구성합니다. 그렇지 않으면 Cisco ISE-PIC 노드를 등록하고 다시 시작할 때 구축 관련 문제가 발생할 수 있습니다. 두 노드에 대해 역방향 DNS 조회가 구성되지 않은 경우 성능이 저하될 수 있습니다.
- (선택 사항) Cisco ISE-PIC를 PAN에서 제거하려면 보조 Cisco ISE-PIC 노드를 PAN에서 등록 취소합니다.
- PAN 및 보조 노드로 등록하려는 독립형 노드에서 동일한 버전의 Cisco ISE-PIC를 실행하고 있는지 확인합니다.

구축 노드 확인

Deployment Nodes(구축 노드**)** 창에서는 구축에 포함된 모든 ISE-PIC 노드를 확인할 수 있습니다.

단계 **1** 기본 Cisco ISE-PIC 관리 포털에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

구축에 속하는 모든 Cisco ISE 노드가 나열됩니다.

보조 **Cisco ISE-PIC** 노드 등록

보조 노드를 등록하고 나면 보조 노드의 컨피그레이션이 기본 노드의 데이터베이스에 추가되며 보조 노드의 애플리케이션 서버가 재시작됩니다. 재시작이 완료된 후 PAN의 구축 페이지에서 모든 컨피그레이션 변경사항을 확인할 수 있습니다. 그러나 변경사항이 적용되어 구축 페이지에 표시될 때까지는 5분 정도 걸릴 수 있습니다.

단계 **1** PAN에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.
구축에 보조 노드가 등록되지 않은 경우 **Add Secondary Node(**보조 노드 추가**)** 섹션이 페이지 하단에 나타납니다.

단계 **3** **Add Secondary Node(**보조 노드 추가**)** 섹션에서 보조 Cisco ISE 노드의 DNS 확인 가능 호스트 이름을 입력합니다.

Cisco ISE-PIC 노드를 등록하는 동안 호스트 이름을 사용하는 경우에는 *abc.xyz.com*과 같이 등록하려는 독립형 노드의 FQDN(Fully Qualified Domain Name)이 PAN의 DNS 확인 가능 이름이어야 합니다. 그렇지 않으면 노드 등록이 실패합니다. DNS 서버에서 보조 노드의 FQDN 및 IP 주소를 이전에 정의한 상태여야 합니다.

단계 **4** Username(사용자 이름) 및 Password(비밀번호) 필드에 독립형 노드의 UI 기반 관리자 자격 증명을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE-PIC가 보조 노드에 연결하여 호스트 이름, 기본 게이트웨이 등의 몇 가지 기본 정보를 가져온 다음 표시합니다.

구축에 보조 노드가 등록되면 노드가 재시작되며, 구축 페이지에서 보조 노드 정보가 표시되기까지 최대 5분이 걸릴 수 있습니다.

보조 노드가 성공적으로 등록되면 구축 페이지의 **Secondary Node(**보조 노드**)** 섹션에 해당 노드에 대한 세부 사항이 표시됩니다.

보조 노드가 정상적으로 등록되면 노드 등록 성공을 확인하는 경보가 PAN에 수신됩니다. 보조 노드를 PAN에 등록할 수 없는 경우에는 경보가 생성되지 않습니다. 노드가 등록되면 해당 노드에서 애플리케이션 서버가 재시작됩니다. 등록 및 데이터베이스 동기화가 성공한 후 기본 관리 노드의 자격 증명을 입력하여 보조 노드의 사용자 인터페이스에 로그인합니다.

참고 구축의 기존 기본 노드 외에 새 노드를 정상적으로 등록하면 새로 등록된 노드에 해당하는 경보는 표시되지 않습니다. 컨피그레이션 변경됨 경보는 새로 등록된 노드에 해당하는 정보를 반영합니다. 이 정보를 통해 새 노드 등록 성공을 확인할 수 있습니다.

기본 및 보조 **Cisco ISE-PIC** 노드 동기화

기본 PAN을 통해서만 Cisco ISE-PIC의 구성을 변경할 수 있습니다. 컨피그레이션 변경사항은 모든 보조 노드로 복제됩니다. 복제가 정상적으로 수행되지 않는 경우에는 보조 PAN을 기본 PAN과 수동으로 동기화할 수 있습니다.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. .

단계 **3** 기본 PAN과 동기화할 노드 옆의 체크 박스를 선택하고 **Syncup**을 클릭하여 전체 데이터베이스 복제를 강제로 수행합니다.

보조 **PAN**을 기본으로 수동 승격

PAN 자동 장애 조치를 구성하지 않은 상태에서 기본 PAN에 오류가 보조 PAN을 수동으로 승격하여 새 기본 PAN으로 지정해야 합니다.

시작하기 전에

기본 PAN으로 승격하려는 두 번째 Cisco ISE-PIC 노드를 구성했는지 확인해 주십시오.

단계 **1** 보조 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **3** **Promote to Primary(**기본으로 승격**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

원래 기본 PAN이었던 노드가 다시 작동하면 승격된 노드는 자동으로 강등되며 보조 PAN이 됩니다. 이 노드(원래 기본 PAN)에서 수동 동기화를 수행하여 구축으로 다시 가져와야 합니다.

구축에서 노드 제거

구축에서 노드를 제거하려면 노드 등록을 취소해야 합니다. 등록 취소된 노드는 독립형 Cisco ISE-PIC 노드로 설정됩니다.

노트의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. 노드가 독립형 노드가 된 후 노드의 엔드포인트 데이터를 유지하려는 경우 기본 PAN에서 백업을 가져 와서 이 데이터 백업을 복원할 수 있습니다.

기본 PAN의 구축 창에서 이러한 변경사항을 확인할 수 있습니다. 그러나 이러한 변경사항이 적용되어 구축 창에 표시될 때까지는 5분 정도 지연될 수 있습니다.

시작하기 전에

구축에서 노드를 제거하려면 노드 등록을 취소해야 합니다. PAN에서 보조 노드를 등록 취소하면 등록 취소된 노드의 상태가 독립형으로 변경되고 기본 노드와 보조 노드 간 연결이 끊어집니다. 업데이트는 더 이상 등록 취소된 독립형 노드로 전송되지 않습니다.

구축에서 보조 노드를 제거하기 전에 Cisco ISE-PIC 컨피그레이션의 백업을 수행해 주십시오. 필요한 경우 나중에 이 백업을 복원할 수 있습니다.

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **2** 보조 노드 세부 사항 옆에있는 **Deregister(**등록 취소**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** 기본 PAN에서 경보가 수신되는지 확인하여 보조 노드가 정상적으로 등록 취소되었음을 확인합니다. 보조 노드가 기본 PAN에서 등록 취소되지 않으면 경보는 생성되지 않습니다.

Cisco ISE-PIC 노드의 호스트 이름 또는 **IP** 주소 변경

독립형 Cisco ISE-PIC 노드의 호스트 이름, IP 주소 또는 도메인 이름을 변경할 수 있습니다. 노드의 호스트 이름으로 `localhost`를 사용할 수 없습니다.

시작하기 전에

Cisco ISE-PIC 노드가 2노드 구축의 일부분인 경우에는 구축에서 해당 노드를 제거하고 독립형 노드인지를 확인해야 합니다.

단계 **1** ISE-PIC 노드의 호스트 이름 또는 IP 주소는 **hostname**, **ip address,** 또는 **ip domain-name** 명령을 사용하여 변경할 수 있습니다.

단계 **2** Cisco ISE-PIC CLI에서 **application stop ise** 명령을 사용하여 Cisco ISE 애플리케이션 컨피그레이션을 재설정하여 모든 서비스를 재시작합니다.

단계 **3** Cisco ISE-PIC 노드가 2노드 구축의 일부분인 경우에는 기존 PAN에 해당 노드를 등록합니다.

참고 Cisco ISE-PIC 노드를 등록하는 동안 호스트 이름을 사용하는 경우에는 *abc.xyz.com*과 같이 등록하려는 독립형 노드의 FQDN(Fully Qualified Domain Name)이 기본 PAN의 DNS 확인 가능 이름이어야 합니다. 그렇지 않으면 노드 등록이 실패합니다. DNS 서버에서 구축의 일부분인 Cisco ISE-PIC 노드의 IP 주소와 FQDN을 입력해야 합니다.

Cisco ISE-PIC 노드를 보조 노드로 등록하고 나면 기본 PAN이 IP 주소, 호스트 이름 또는 도메인 이름의 변경사항을 구축의 다른 Cisco ISE-PIC 노드로 복제합니다.

Cisco ISE-PIC 어플라이언스 하드웨어 교체

Cisco ISE-PIC 어플라이언스 하드웨어는 문제가 있는 경우에만 교체해야 합니다. 소프트웨어 문제의 경우에는 어플라이언스를 재이미지화하고 Cisco ISE-PIC 소프트웨어를 다시 설치할 수 있습니다.

단계 **1** 새 노드에서 Cisco ISE-PIC 소프트웨어를 재이미지화하거나 다시 설치합니다.

단계 **2** 기본 및 보조 PAN용 UDI가 포함된 라이센스를 얻어 기본 PAN에 설치합니다.

단계 **3** 교체한 기본 PAN에서 백업을 복원합니다.

복원 스크립트는 보조 PAN에서 데이터 동기화를 시도하지만 현재는 보조 PAN이 독립형 노드이므로 동기화가 실패합니다. 데이터는 기본 PAN에서 백업을 가져온 시간으로 설정됩니다.

단계 **4** 새 노드를 보조 노드로 기본 PAN에 등록합니다.

ISE-PIC 설치 관리

패치를 설치하거나, 백업을 실행하거나, 시스템 복원을 구현합니다.

소프트웨어 패치 설치

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)** 선택한 다음 설치를 클릭합니다.

단계 **2** **Browse(**찾아보기**)**를 클릭하여 Cisco.com에서 다운로드한 패치를 선택합니다.

단계 **3** **Install(**설치**)**을 클릭하여 패치를 설치합니다.

패치가 PAN에 설치되고 나면 Cisco ISE-PIC에서 로그아웃되고 다시 로그인하려면 몇 분 정도 기다려야 합니다.

참고 패치 설치가 진행 중일 때

Patch Management(패치 관리) 페이지에서 액세스할 수 있는 기능은 **Show Node Status(**노드 상태 표시**)**뿐입니다.

단계 4 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)** 그런 다음 패치 설치 페이지로 돌아갑니다.

단계 5 보조 노드에 설치한 패치 옆의 라디오 버튼을 클릭하고 **Show Node Status(**노드 상태 표시**)**를 클릭하여 설치가 완료되었는지 확인합니다.

다음에 수행할 작업

보조 노드에 패치를 설치해야 하는 경우에는 노드가 작동 중인지 확인한 다음 이 프로세스를 반복하여 나머지 노드에 패치를 설치합니다.

Cisco ISE-PIC 소프트웨어 패치

Cisco ISE-PIC 소프트웨어 패치는 일반적으로 누적됩니다. Cisco ISE-PIC를 사용하면 CLI 또는 GUI에서 패치 설치 및 롤백을 수행할 수 있습니다.

기본 PAN에서 구축 내 Cisco ISE-PIC 서버에 패치를 설치할 수 있습니다. 기본 PAN에서 패치를 설치하려면 Cisco.com에서 클라이언트 브라우저를 실행하는 시스템에 패치를 다운로드해야 합니다.

GUI에서 패치를 설치하는 경우에는 패치가 먼저 기본 PAN에 자동으로 설치됩니다. 그런 다음 GUI에 나열된 순서대로 구축의 다른 노드에 패치를 설치합니다. 노드가 업데이트되는 순서는 제어할 수 없습니다. 패치 버전을 수동으로 설치, 롤백, 확인할 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Maintenance(**유지 보수**) > Patch Management(**패치 관리**)**.

CLI에서 패치를 설치하는 경우 노드가 업데이트되는 순서를 제어할 수 있습니다. 그러나 기본 PAN에 패치를 먼저 설치하는 것이 좋습니다.

전체 구축을 업그레이드하기 전에 일부 노드에서 패치를 검증하려면 CLI를 사용하여 선택한 노드에 패치를 설치하면 됩니다. 다음 CLI 명령을 사용하여 패치를 설치합니다.

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

자세한 내용은 Cisco Identity Services Engine CLI 참조 설명서의 'EXEC 모드의 Cisco ISE CLI 명령' 장에서 '패치 설치' 섹션을 참조하십시오.

필요한 패치 버전을 직접 설치할 수 있습니다. 예를 들어 현재 Cisco ISE 2.x를 사용 중이고 Cisco ISE 2.x 패치 5를 설치하려는 경우 이전 패치(이 예에서는 ISE 2.x 패치 1~4)를 설치하지 않고 Cisco ISE 2.x 패치 5를 직접 설치할 수 있습니다. 패치 버전을 CLI에서 보려면 다음 CLI 명령을 사용합니다.

```
show version
```

소프트웨어 패치 설치 지침

ISE 노드에 패치를 설치하면 설치가 완료된 후 노드가 재부팅됩니다. 다시 로그인하려면 몇 분 동안 기다려야 할 수 있습니다. 패치 설치를 유지 보수 기간으로 예약하면 일시적인 중단을 방지할 수 있습니다.

네트워크에 구축된 Cisco ISE-PIC 버전에 적용할 수 있는 패치를 설치해야 합니다. Cisco ISE-PIC는 모든 버전 불일치와 패치 파일의 오류를 보고합니다.

참고 Cisco ISE 패치는 ISE-PIC에도 설치할 수 있습니다.

Cisco ISE-PIC에 현재 설치되어 있는 패치보다 낮은 버전의 패치는 설치할 수 없습니다. 마찬가지로, 상위 버전이 현재 Cisco ISE-PIC에 설치되어 있는 경우 하위 버전의 패치 변경 사항을 롤백할 수 없습니다. 예를 들어 Cisco ISE-PIC 서버에 패치 3이 설치된 경우 1 또는 2 패치를 설치하거나 롤백할 수 없습니다.

2노드 구축의 일부인 기본 PAN에서 패치를 설치하는 경우 Cisco ISE-PIC는 기본 노드에 패치를 설치한 다음 보조 노드에 설치합니다. 패치가 기본 PAN에 성공적으로 설치되면 Cisco ISE-PIC가 보조 노드에서 패치 설치를 계속합니다. 기본 PAN에서 패치 설치가 실패하면 보조 노드에서 설치가 진행되지 않습니다.

소프트웨어 패치 롤백

다중 노드 구축에 속한 PAN에서 패치를 롤백하면 Cisco ISE-PIC는 기본 노드에서 패치를 롤백한 다음 구축의 보조 노드에서 패치를 롤백합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)**.

단계 **2** 변경사항을 롤백하려는 패치 버전의 라디오 버튼을 클릭하고 **Rollback(**롤백**)**을 클릭합니다.

참고 패치 롤백이 진행 중일 때 패치 관리 페이지에서 액세스할 수 있는 기능은 **Show Node Status(**노드 상태 표시**)**뿐입니다.

패치가 PAN에서 롤백되고 나면 Cisco ISE에서 로그아웃되며, 몇 분 동안 기다려야 다시 로그인할 수 있습니다.

단계 **3** 로그인한 후 페이지 맨 아래의 **Alarms(**경보**)** 링크를 클릭하면 롤백 작업의 상태를 확인할 수 있습니다.

단계 **4** 패치 롤백의 진행률을 확인하려면 패치 관리 페이지에서 패치를 선택하고 **Show Node Status(**노드 상태 표시**)**를 클릭합니다.

단계 **5** 보조 노드에서 패치의 라디오 버튼을 클릭하고 **Show Node Status(**노드 상태 표시**)**를 클릭하면 구축의 모든 노드에서 패치가 롤백되었는지를 확인할 수 있습니다.

보조 노드에서 패치가 롤백되지 않은 경우에는 해당 노드가 작동 중인지 확인한 다음 이 프로세스를 반복하여 나머지 노드에서 변경사항을 롤백합니다. Cisco ISE-PIC는 해당 버전의 패치가 아직 설치되어 있는 노드에서만 패치를 롤백합니다.

소프트웨어 패치 롤백 지침

구축의 Cisco ISE-PIC 노드에서 패치를 롤백하려면 먼저 PAN에서 변경 사항을 롤백해야 합니다. 작업이 성공한 경우 패치가 보조 노드에서 롤백됩니다. PAN에서 롤백 프로세스가 실패하면 패치가 보조 노드에서 롤백되지 않습니다.

Cisco ISE-PIC가 보조 노드에서 패치를 롤백하는 동안 PAN GUI에서 다른 작업을 계속 수행할 수 있습니다. 롤백 후에는 보조 노드가 다시 시작됩니다.

백업 및 복원

참고 Cisco ISE-PIC는 대부분의 경우 Cisco ISE 백업 및 복원 절차와 동일하게 작동하므로 Cisco ISE라는 용어는 경우에 따라 Cisco ISE-PIC와 관련된 작업 및 기능을 나타내는 의미로 사용됩니다.

Cisco ISE-PIC에서는 기본 또는 독립형 노드의 데이터를 백업할 수 있습니다. 백업은 CLI 또는 사용자 인터페이스에서 수행할 수 있습니다.

Cisco ISE-PIC에서는 다음 데이터 유형을 백업할 수 있습니다.

- 컨피그레이션 데이터 - 애플리케이션별 데이터와 Cisco ADE 운영 체제 컨피그레이션 데이터를 모두 포함합니다.
- 작업 데이터 - 모니터링 및 문제 해결 데이터를 포함합니다.

리포지토리 백업 및 복원

Cisco ISE-PIC에서는 리포지토리를 생성하거나 삭제할 수 있습니다. 다음과 같은 리포지토리 유형을 생성할 수 있습니다.

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

KVM을 사용하여 생성한 가상 CD-ROM의 리포지토리 유형으로 CD-ROM을 생성할 수 있습니다.

참고 리포지토리는 각 디바이스에 대해 로컬입니다.

참고 리포지토리 크기는 소규모 구축(100개 엔드포인트 이하)인 경우 10GB, 중간 규모 구축인 경우 100GB, 대규모 구축인 경우 200GB를 사용하는 것이 좋습니다.

리포지토리 생성

CLI 및 GUI를 사용하여 리포지토리를 생성할 수 있습니다. 다음과 같은 이유로 인해 GUI를 사용하는 것이 좋습니다.

- CLI를 통해 생성하는 리포지토리는 로컬에 저장되며 다른 구축 노드로 복제되지 않습니다. 이러한 리포지토리는 GUI의 리포지토리 페이지에 나열되지 않습니다.
- 기본 PAN에서 생성하는 저장소는 다른 구축 노드로 복제됩니다.

키는 GUI의 기본 PAN에서만 생성되므로 업그레이드 중에 새 기본 관리자의 GUI에서 키를 다시 생성하고 SFTP 서버로 내보내야 합니다. 구축 환경에서 노드를 제거하는 경우 비관리 노드의 GUI에서 키를 생성하고 SFTP 서버로 내보내야 합니다.

RSA 공개 키 인증을 사용하여 Cisco ISE-PIC에서 SFTP 저장소를 구성할 수 있습니다. 관리자가 생성한 비밀번호를 사용하여 데이터베이스 및 로그를 암호화하는 대신 보안 키를 사용하는 RSA 공개 키 인증을 선택할 수 있습니다. RSA 공개 키로 생성된 SFTP 저장소의 경우 GUI를 통해 생성된 저장소는 CLI에서 복제되지 않으며 CLI를 통해 생성된 저장소는 GUI에서 복제되지 않습니다. CLI 및 GUI에서 동일한 저장소를 구성하려면 CLI 및 GUI 모두에서 RSA 공개 키를 생성하고 두 키를 모두 SFTP 서버로 내보냅니다.

시작하기 전에

- RSA 공개 키 인증을 사용하여 SFTP 저장소를 생성하려면 다음 단계를 수행합니다.
  - SFTP 저장소에서 RSA 공개 키 인증을 활성화합니다.
  - **crypto host_key add** 명령을 사용하여 Cisco ISE CLI에서 SFTP 서버의 호스트 키를 입력합니다. 호스트 키 문자열은 저장소 구성 페이지의 **Path(**경로**)** 필드에 입력하는 호스트 이름과 일치해야 합니다.
  - 키 페어를 생성하고 GUI에서 공개 키를 로컬 시스템으로 내보냅니다. Cisco ISE CLI에서 **crypto key generate rsa passphrase** *test123* 명령을 사용하여 키 페어를 생성합니다. 여기서 passphrase는 4자보다 커야 하며 모든 저장소(로컬 디스크 또는 기타 구성된 저장소)로 내보내야 합니다.
  - 내보낸 RSA 공개 키를 PKI 지원 SFTP 서버에 복사하고 "authorized_keys" 파일에 추가합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**를 선택합니다.

단계 **2** 새 리포지토리를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 리포지토리를 설정하는 데 필요한 값을 입력합니다. 필드에 대한 설명은 리포지토리 설정, 123 페이지를 참고하십시오.

단계 **4** 리포지토리를 생성하려면 **Submit(**제출**)**을 클릭합니다.

단계 **5** 왼쪽의 **Operations(**운영**)** 탐색창에서 **Repository(**저장소**)**를 클릭하거나 **Repository(**저장소**)** 창 위쪽의 **Repository List(**저장소 목록**)** 링크를 클릭해 저장소 목록 페이지로 이동하여 저장소가 정상적으로 생성되었는지 확인합니다.

다음에 수행할 작업

- 생성한 저장소가 유효한지 확인합니다. **Repository Listing(**저장소 목록**)** 창에서 확인할 수 있습니다. 해당 저장소를 선택하고 **Validate(**검증**)**를 클릭합니다. 또는 Cisco ISE 명령줄 인터페이스에서 다음 명령을 실행할 수 있습니다.

  show repository *repository_name*

  여기서 *repository_name* 은 생성한 저장소의 이름입니다.

  참고 리포지토리를 생성할 때 입력한 경로가 없으면

  ```
  %Invalid Directory
  ```

  오류가 표시됩니다.

- 온디맨드 백업을 실행하거나 백업을 예약합니다.

리포지토리 설정

다음 표에서는 백업 파일을 저장하기 위한 리포지토리를 생성하는 데 사용할 수 있는 **Repository List(**리포지토리 목록**)** 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**.

표 ***22:*** 리포지토리 설정

필드	사용 지침
Repository(리포지토리)	리포지토리의 이름을 입력합니다. 영숫자 문자를 입력할 수 있으며 최대 길이는 80자입니다.
Protocol(프로토콜)	사용 가능한 프로토콜 중에서 사용하려는 프로토콜 하나를 선택합니다.
호스트	(TFTP, HTTP, HTTPS, FTP, SFTP 및 NFS의 경우 필수) 리포지토리를 생성할 서버의 호스트 이름 또는 IPv4 주소(IPv4 또는 IPv6)를 입력합니다. 참고 IPv6 주소를 사용해 리포지토리를 추가하는 경우 ISE eth0 인터페이스가 IPv6 주소로 구성되어야 합니다.

필드	사용 지침
Path(경로)	리포지토리의 경로를 입력합니다. 경로는 유효해야 하며 리포지토리를 생성할 때 이미 있는 상태여야 합니다. 이 값은 서버의 루트 디렉토리를 나타내는 슬래시 두 개(//) 또는 하나(/)로 시작할 수 있습니다. 그러나 FTP 프로토콜의 경우 슬래시 하나(/)는 루트 디렉토리가 아닌 로컬 디바이스 홈 디렉토리의 FTP를 나타냅니다.

관련 항목

리포지토리 백업 및 복원

리포지토리 생성, 122 페이지

SFTP 리포지토리에서 RSA 공개 키 인증 활성화

SFTP 서버에서 각 노드에는 CLI와 GUI용으로 하나씩, 2개의 RSA 공개 키가 있어야 합니다. SFTP 저장소에서 RSA 공개 키 인증을 활성화하려면 다음 단계를 수행합니다.

단계 **1** */etc/ssh/sshd_config.file*을 편집할 권한이 있는 계정으로 SFTP 서버에 로그인합니다.

참고 *sshd_config* 파일의 위치는 운영 체제 설치에 따라 달라질 수 있습니다.

단계 **2** **vi /etc/ssh/sshd_config** 명령을 입력합니다.

sshd_config 파일의 내용이 나열됩니다.

단계 **3** RSA 공개 키 인증을 활성화하려면 다음 줄에서 "#" 기호를 제거합니다.

- RSAAuthentication: yes(예)
- PubkeyAuthentication: yes(예)

  참고 공개 인증 키가 no인 경우 yes로 변경합니다.

- AuthorizedKeysFile ~/.ssh/authorized_keys

온디맨드 및 예약된 백업

기본 PAN에 대한 온디맨드 백업을 구성할 수 있습니다. 데이터를 즉시 백업하려면 온디맨드 백업을 수행합니다.

Cisco ISE에서는 한 번, 매일, 매주, 매월 실행되도록 예약할 수 있는 시스템 레벨 백업을 예약할 수 있습니다. 백업 작업에는 시간이 오래 걸릴 수 있으므로 중단되지 않도록 백업을 예약할 수 있습니다. 관리 포털에서 백업을 예약할 수 있습니다.

참고 내부 CA를 사용하는 경우 CLI를 사용하여 인증서 및 키를 내보내야 합니다. 관리 포털에서 수행하는 백업은 CA 체인을 백업하지 않습니다.

자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드의 "기본 설정" 장에서 "Cisco ISE CA 인증서 및 키 내보내기" 섹션을 참고하십시오.

온디맨드 백업 수행

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE-PIC를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복원 기능이 내부 CA(인증 기관) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복원을 수행하는 경우 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE-PIC 노드에서 CA 인증서를 내보내고 CLI를 통해 대상 시스템으로 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발행한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  장점**:** 원래 소스 인증서 또는 원래 대상 인증서가 모두 사용되지 않아 안전하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발급된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 온디맨드 백업을 수행하기 전에 Cisco ISE-PIC의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 백업 파일을 저장할 저장소를 생성했는지 확인합니다.
- 로컬 리포지토리를 사용하여 백업해서는 안 됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Backup and Restore(**백업 및 복구**)**.

단계 **2** 백업 유형을 Configuration(구성) 또는 Operational(운영) 중에서 선택합니다.

단계 **3** **Backup Now(**지금 백업**)**를 클릭합니다.

단계 **4** 필요한 값을 입력하여 백업을 수행합니다.

단계 **5** **Backup(**백업**)**을 클릭합니다.

단계 **6** 백업이 정상적으로 완료되었는지 확인합니다.

Cisco ISE-PIC는 백업 파일 이름에 타임스탬프를 추가하여 파일을 지정된 저장소에 저장합니다. Cisco ISE-PIC는 타임스탬프 외에 CFG 태그(구성 백업의 경우) 및 OPS 태그(운영 백업의 경우)도 추가합니다. 백업 파일이 지정된 리포지토리에 있는지 확인합니다.

백업이 실행 중일 때는 노드를 승격하지 마십시오. 이렇게 하면 모든 프로세스가 종료되며 백업을 동시에 실행하는 경우 데이터가 다소 불일치할 수도 있습니다. 백업이 완료될 때까지 기다린 후에 노드를 변경해 주십시오.

참고 백업이 실행 중일 때 높은 CPU 사용률이 관찰되고 높은 로드 평균 알람이 표시될 수 있습니다. 백업이 완료되면 CPU 사용률이 정상으로 돌아옵니다.

백업 예약

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE-PIC를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복원 기능이 내부 CA(인증 기관) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복원을 수행하는 경우 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE-PIC 노드에서 CA 인증서를 내보내고 CLI를 통해 대상 시스템으로 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발행한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  동의**:** 원래 소스 인증서 또는 원래 대상 인증서가 사용되므로 안정하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발행된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 백업을 예약하기 전에 Cisco ISE-PIC의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 리포지토리를 구성했는지 확인합니다.
- 로컬 리포지토리를 사용하여 백업해서는 안 됩니다.

참고 CD-ROM, HTTP, HTTPS 또는 TFTP 리포지토리 유형은 백업 및 복원 작업에서 지원되지 않습니다. 이러한 리포지토리 유형은 읽기 전용이거나 프로토콜이 파일 나열을 지원하지 않기 때문입니다.

CLI를 사용한 복원

CLI와 GUI 둘 다에서 백업을 예약할 수 있지만 GUI를 사용하는 것이 좋습니다. 그러나 보조 모니터링 노드에 대한 운영 백업을 수행하려는 경우 CLI에서만 가능합니다.

백업 기록

백업 기록에서는 예약 백업 및 온디맨드 백업에 대한 기본 정보를 제공합니다. 백업 이름, 백업 파일 크기, 백업이 저장된 저장소 및 백업을 가져온 시점을 나타내는 타임스탬프가 나열됩니다. 이 정보는

운영 감사 보고서와 함께 Backup and Restore(백업 및 복원) 페이지의 History(기록) 테이블에서 사용할 수 있습니다.

실패한 백업의 경우 Cisco ISE-PIC가 경보를 트리거합니다. 백업 기록 페이지에 실패 이유가 제공됩니다. 실패 이유는 운영 감사 보고서에서도 확인할 수 있습니다. 장애 이유가 없거나 명확지 않은 경우 Cisco ISE CLI에서 **backup-logs** 명령을 실행하여 ADE.log에서 자세한 내용을 확인할 수 있습니다.

백업 작업이 진행 중인 경우 **show backup status** CLI 명령을 사용하여 백업 작업의 진행 상황을 확인할 수 있습니다.

백업 기록은 Cisco ADE 운영 체제 컨피그레이션 데이터와 함께 저장됩니다. 이 기록은 애플리케이션이 업그레이드된 후에도 계속 해당 위치에 유지되며 PAN을 재이미지화하는 경우에만 제거됩니다.

백업 실패

백업이 실패하는 경우 다음 사항을 확인해 주십시오.

- NTP 동기화 또는 서비스 장애 문제가 있는지 확인합니다. Cisco ISE의 NTP 서비스가 작동하지 않으면 Cisco ISE에서 NTP 서비스 장애 알람을 생성합니다. Cisco ISE가 구성된 모든 NTP 서버와 동기화할 수 없는 경우 Cisco ISE에서 NTP 동기화 실패 알람을 생성합니다. NTP 서비스가 중지되었거나 동기화 문제가 있는 경우 Cisco ISE 백업이 실패할 수 있습니다. Alarms(알람) dashlet을 확인하고 NTP 동기화 또는 서비스 문제를 해결한 후에 백업 작업을 다시 시도하십시오.
- 다른 백업이 동시에 실행되고 있지 않은지 확인합니다.
- 구성한 리포지토리에 대해 사용 가능한 디스크 공간을 확인합니다.
  - 모니터링 데이터가 할당된 모니터링 데이터베이스 크기의 75%를 사용한 경우 모니터링(운영) 백업이 실패합니다. 예를 들어 노드에 600GB가 할당되어 있고 모니터링 데이터가 스토리지의 450GB 이상을 사용한 경우 모니터링 백업이 실패합니다.
  - 데이터베이스 디스크 사용량이 90%를 초과하면 데이터베이스 크기를 할당된 크기의 75% 이하로 유지하기 위해 제거가 발생합니다.
- 제거가 진행 중인지 확인합니다. 제거가 진행 중일 때에는 백업 및 복원 작업이 수행되지 않습니다.
- 리포지토리가 올바르게 구성되었는지 확인합니다.

Cisco ISE 복원 작업

기본 또는 독립형 노드에서 컨피그레이션 데이터를 복원할 수 있습니다. 기본 PAN에서 데이터를 복원한 후에는 보조 노드를 기본 PAN과 수동으로 동기화해야 합니다.

참고 Cisco ISE-PIC의 새 백업/복원 사용자 인터페이스에서는 백업 파일 이름에 메타데이터를 사용합니다. 그러므로 백업이 완료된 후에 백업 파일 이름을 수동으로 수정해서는 안 됩니다. 백업 파일 이름을 수동으로 수정할 경우 Cisco ISE-PIC 백업/복원 사용자 인터페이스에서 백업 파일을 인식할 수 없습니다. 백업 파일 이름을 수정해야 하는 경우 Cisco ISE CLI를 사용하여 백업을 복원해야 합니다.

데이터 복원 지침

다음은 Cisco ISE-PIC 백업 데이터를 복원할 때 따라야 하는 지침입니다.

- Cisco ISE를 사용하면 ISE 노드 (A)에서 백업을 가져와서 호스트네임이 동일한(IP 주소는 다름) 다른 ISE 노드 (B)에서 복구할 수 있습니다. 그러나 노드 B에서 백업을 복구한 후에는 인증서 및 포털 그룹 태그에 문제가 발생할 수 있으므로 노드 B의 호스트네임을 변경하지 마십시오.
- 특정 표준 시간대에서 기본 PAN의 백업을 가져온 다음 다른 표준 시간대에서 다른 Cisco ISE-PIC 노드에 해당 백업을 복원하려는 경우 복원 프로세스가 실패할 수 있습니다. 백업 파일의 타임스탬프가 백업을 복원하는 Cisco ISE-PIC 노드의 시스템 시간보다 이후이면 이러한 오류가 발생합니다. 백업을 가져오고 1일 후에 동일 백업을 복원하는 경우 백업 파일의 타임스탬프가 시스템 시간 이전에 되어 복원 프로세스가 정상적으로 진행됩니다.
- 백업을 가져온 호스트와 다른 호스트 이름으로 기본 PAN에서 백업을 복원하면 기본 PAN이 독립형 모드로 설정됩니다. 그러면 구축이 손상되고 보조 노드가 작동하지 않게 됩니다. 이 경우 독립형 모드를 기본 노드로 지정하고 보조 노드에서 컨피그레이션을 재설정한 후에 기본 노드에 보조 노드를 등록해야 합니다. Cisco ISE-PIC 노드에서 컨피그레이션을 재설정하려면 Cisco ISE CLI에서 다음 명령을 입력합니다.
  - **application reset-config ise**
- 초기 Cisco ISE-PIC 설치 및 설정 후에는 시스템 표준 시간대를 변경하지 않는 것이 좋습니다.
- 구축의 노드 하나 이상에서 인증서 컨피그레이션을 변경한 경우에는 다른 백업을 가져와 독립형 Cisco ISE-PIC 노드 또는 기본 PAN에서 데이터를 복원해야 합니다. 이렇게 하지 않는 경우 이전 백업을 사용하여 데이터를 복원하려고 하면 노드 간의 통신이 실패할 수 있습니다.
- 기본 PAN에서 컨피그레이션 백업을 복원한 후에는 이전에 내보낸 Cisco ISE CA 인증서 및 키를 가져올 수 있습니다.

  참고 Cisco ISE CA 인증서 및 키를 내보내지 않은 경우 기본 PAN에서 컨피그레이션 백업을 복원한 후에 기본 PAN에서 루트 CA 및 종속 CA를 생성합니다.
- 올바른 FQDN (플래티넘 데이터베이스의 FQDN)을 사용하지 않고 플래티넘 데이터베이스를 복원하려는 경우 CA 인증서를 다시 생성해야 합니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** > **Replace ISE Root CA certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 선택합니다. 그러나 올바른 FQDN을 사용하여 플래티넘 데이터베이스를 복원하는 경우 CA 인증서가 자동으로 다시 생성됩니다.
- Cisco ISE-PIC가 백업 파일을 저장하는 위치인 데이터 리포지토리가 필요합니다. 온디맨드 또는 예약 백업을 실행하려면 리포지토리를 생성해야 합니다.
- 독립형 노드에 오류가 발생하는 경우에는 컨피그레이션 백업을 실행하여 해당 노드를 복원해야 합니다. 기본 PAN에 오류가 발생하는 경우에는 보조 관리 노드를 기본 노드로 승격할 수 있습니다. 기본 PAN이 작동하면 기본 PAN에서 데이터를 복원할 수 있습니다.

참고 Cisco ISE-PIC는 트러블슈팅용으로 로그 및 구성 파일을 수집하는 데 사용할 수 있는 **backup-logs** CLI 명령도 제공합니다.

CLI에서 컨피그레이션 또는 모니터링 백업 복원

Cisco ISE CLI를 통해 컨피그레이션 데이터를 복원하려면 EXEC 모드에서 **restore** 명령을 사용합니다. 컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 다음 명령을 사용합니다.

restore *filename* **repository** *repository-name* **encryption-key hash|plain** *encryption-key name* **include-adeos**

구문 설명

restore	컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 이 명령을 입력합니다.
filename	리포지토리에 있는 백업된 파일의 이름입니다. 최대 120개의 영숫자를 지원합니다. 참고 파일 이름 뒤에 .tar.gpg 확장자를 추가해야 합니다(예: myfile.tar.gpg).
repository	백업이 포함되어 있는 리포지토리를 지정합니다.
repository-name	복원할 백업이 있는 리포지토리의 이름입니다.
encryption-key	(선택 사항) 백업을 복원할 사용자 맞춤화 암호화 키를 지정합니다.
hash	백업을 복원하기 위해 해시된 암호 키입니다. 뒤에 오는 암호화된(해시된) 암호 키를 지정합니다. 최대 40자를 지원합니다.
plain	백업을 복원하기 위한 일반 텍스트 암호 키입니다. 뒤에 오는 암호화되지 않은 일반 텍스트 암호 키를 지정합니다. 최대 15자를 지원합니다.
encryption-key name	암호화 키를 입력합니다.
include-adeos	(선택 사항, 컨피그레이션 백업에만 해당함) 컨피그레이션 백업에서 ADE-OS 컨피그레이션을 복원하려는 경우 이 명령 연산자 매개변수를 입력합니다. 컨피그레이션 백업을 복원할 때 이 매개변수를 포함하지 않으면 Cisco ISE 애플리케이션 컨피그레이션 데이터만 복원됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

EXEC

사용 지침

Cisco ISE-PIC에서 restore 명령을 사용하는 경우 Cisco ISE-PIC 서버가 자동으로 다시 시작됩니다.

데이터를 복원할 때 암호화 키는 선택 사항입니다. 암호화 키를 제공하지 않은 이전 백업을 지원하려는 경우 암호화 키 없이 **restore** 명령을 사용하면 됩니다.

예

```
 ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345 Restore may require a restart of application services. Continue? (yes/no)
[yes] ? yes Initiating restore.  Please wait... ISE application restore is in progress.
This process could take several minutes. Please wait... Stopping ISE Application Server...
 Stopping ISE Monitoring & Troubleshooting Log Processor... Stopping ISE Monitoring &
Troubleshooting Log Collector... Stopping ISE Monitoring & Troubleshooting Alert Process...
 Stopping ISE Monitoring & Troubleshooting Session Database... Stopping ISE Database
processes... Starting ISE Database processes... Starting ISE Monitoring & Troubleshooting
Session Database... Starting ISE Application Server... Starting ISE Monitoring &
Troubleshooting Alert Process... Starting ISE Monitoring & Troubleshooting Log Collector...
 Starting ISE Monitoring & Troubleshooting Log Processor... Note: ISE Processes are
initializing. Use 'show application status ise' CLI to verify all processes are in running
 state. ise/admin#
```

Related Commands

	설명
backup	백업을 수행하고(Cisco ISE-PIC 및 Cisco ADE OS) 리포지토리에 백업을 저장합니다.
backup-logs	시스템 로그를 백업합니다.
repository	백업 컨피그레이션을 위한 리포지토리 하위 모드로 진입합니다.
show repository	특정 리포지토리에 있는 사용 가능한 백업 파일을 표시합니다.
show backup history	시스템 백업 기록을 표시합니다.
show backup status	백업 작업의 상태를 표시합니다.
show restore status	복원 작업의 상태를 표시합니다.

보조 노드에 대한 애플리케이션 복원 후의 동기화 상태 및 복제 상태가 동기화되지 않음인 경우 해당 보조 노드의 인증서를 PAN으로 다시 가져온 다음 수동 동기화를 수행해야 합니다.

GUI에서 컨피그레이션 백업 복원

관리 포털에서 컨피그레이션 백업을 복원할 수 있습니다. GUI에는 현재 릴리스에서 생성한 백업만 나열됩니다. 이 릴리스 이전의 백업을 복원하려면 CLI에서 restore 명령을 사용해 주십시오.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Backup and Restore(**백업 및 복구**)**.

단계 **2** 컨피그레이션 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **3** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **4** **Restore(**복원**)**를 클릭합니다.

다음에 수행할 작업

Cisco ISE CA 서비스를 사용하는 경우 다음을 수행해야 합니다.

1. 전체 Cisco ISE CA 루트 체인을 재생성합니다.
2. PAN에서 Cisco ISE CA 인증서와 키의 백업을 가져온 다음 보조 PAN에서 복원합니다. 그러면 기본 PAN 장애 시 보조 PAN이 루트 CA 또는 외부 PKI의 하위 CA로 작동할 수 있으며, 이 경우 보조 PAN을 기본 PAN으로 승격합니다.

복원 기록

운영 감사 보고서 창에서 모든 복원 작업, 로그 이벤트 및 상태에 대한 정보를 가져올 수 있습니다.

참고 그러나 운영 감사 보고서 창에서는 이전 복원 작업에 해당하는 시작 시간에 대한 정보를 제공하지 않습니다.

문제 해결 정보를 얻으려면 Cisco ISE CLI에서 **backup-logs** 명령을 실행하고 ADE.log 파일을 확인해야 합니다.

복원 작업이 진행 중인 동안에는 모든 Cisco ISE-PIC 서비스가 중지됩니다. 다음 **show restore status** CLI 명령을 사용하여 복구 작업의 진행률을 확인할 수 있습니다.

기본 및 보조 노드 동기화

PAN에서 백업 파일을 복원한 후 기본 노드와 보조 노드의 Cisco ISE-PIC 데이터베이스가 자동으로 동기화되지 않는 경우가 있습니다. 이러한 현상이 발생하는 경우 PAN에서 보조 ISE-PIC 노드로의 전체 복제를 수동으로 강제 수행할 수 있습니다. PAN에서 보조 노드로만 동기화를 강제 수행할 수 있습니다. syncup 작업 중에는 컨피그레이션을 변경할 수 없습니다. Cisco ISE-PIC에서는 동기화가 완료된 후에만 다른 Cisco ISE-PIC 관리 포털 페이지로 이동하여 컨피그레이션을 변경하도록 허용합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **2** 복제 상태가 동기화되지 않은 경우 보조 노드 옆의 확인란을 선택합니다.

단계 **3** **Syncup**을 클릭하고 노드가 PAN과 동기화될 때까지 기다립니다. 이 프로세스가 완료될 때까지 기다려야 Cisco ISE-PIC 관리 포털에 다시 액세스할 수 있습니다.

2노드 구축에서 손실된 노드 복구

이 섹션에서는 2노드 구축에서 손실된 노드를 복구하는 데 사용할 수 있는 문제 해결 정보를 제공합니다. 다음 활용 사례 중 일부에서는 백업 및 복원 기능을, 다른 일부에서는 복제 기능을 사용하여 손실된 데이터를 복구합니다.

2노드 구축에서 기존 **IP** 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

2노드 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 복구 후에 기존 IP 주소와 호스트 이름을 사용하려고 합니다.

예를 들어 N1(기본 정책 관리 노드 또는 기본 PAN) 및 N2(보조 정책 관리 노드 또는 보조 PAN)의 두 개 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다.

가정

구축의 모든 Cisco ISE-PIC 노드가 제거되었습니다. 같은 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 및 N2 노드를 모두 대체해야 합니다. 이제 N1 및 N2 노드에 독립형 컨피그레이션이 사용됩니다.
2. N1 및 N2 노드의 UDI를 사용하여 라이센스를 가져온 다음 N1 노드에 설치합니다.
3. 그런 다음 교체된 N1 노드에서 백업을 복원해야 합니다. 복원 스크립트는 N2에서 데이터 동기화를 시도하지만 이제 N2는 독립형 노드이므로 동기화가 실패합니다. N1의 데이터는 T1 시간으로 재설정됩니다.
4. N1 관리 포털에 로그인하여 N2 노드를 삭제한 다음 다시 등록해야 합니다. N1 및 N2 노드 둘 다의 데이터가 T1 시간의 데이터로 재설정됩니다.

2노드 구축에서 새 IP 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

2노드 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 새 위치에서 새 하드웨어를 재이미지화했으며 새 IP 주소와 호스트 이름이 필요합니다.

예를 들어 N1(기본 정책 관리 노드/PAN) 및 N2(보조 노드)의 두 개 ISE-PIC 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다. Cisco ISE-PIC 노드가 새 위치에서 대체되며, 새 호스트 이름은 N1A(PAN) 및 N2A(보조 노드)입니다. 이 시점에서 N1A 및 N2A는 독립형 노드입니다.

가정

구축의 모든 Cisco ISE-PIC 노드가 제거되었습니다. 다른 위치에서 다른 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 백업을 가져온 다음 N1A에서 복원합니다. 복원 스크립트는 호스트 이름 변경 및 도메인 이름 변경을 식별하여 현재 호스트 이름을 기반으로 구축 컨피그레이션에서 호스트 이름과 도메인 이름을 업데이트합니다.
2. 새 셀프 서명 인증서를 생성해야 합니다.
3. 이전 N2 노드를 삭제합니다.

   새 N2A 노드를 보조 노드로 등록합니다. N1A 노드의 데이터가 N2A 노드로 복제됩니다.

독립형 구축에서 기존 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 N1 데이터베이스의 백업을 만들었습니다. N1 노드는 물리적 장애로 인해 다운되었으며 재이미지화해야 하거나 새 하드웨어를 사용해야 합니다. 같은 IP 주소와 호스트 이름을 사용하여 N1 노드를 다시 작동시켜야 합니다.

가정

이 구축은 독립형이며 새로 사용하거나 재이미지화되는 하드웨어의 IP 주소와 호스트 이름은 같습니다.

해결 단계

재이미지화 후에 N1 노드가 작동하거나 같은 IP 주소 및 호스트 이름을 사용하여 새 Cisco ISE-PIC 노드를 도입한 후에는 이전 N1 노드에서 만든 백업을 복원해야 합니다. 역할은 변경하지 않아도 됩니다.

독립형 구축에서 새 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 만든 N1 데이터베이스의 백업을 사용할 수 있습니다. N1 노드는 물리적 장애로 인해 다운되었으며, 다른 IP 주소와 호스트 이름을 사용하여 다른 위치에서 새 하드웨어로 해당 노드를 교체하려고 합니다.

가정

구축은 독립형이며 교체되는 하드웨어는 IP 주소와 호스트 이름이 다릅니다.

해결 단계

1. N1 노드를 새 하드웨어로 교체합니다. 이 노드는 독립형 상태가 되며 호스트 이름은 N1B입니다.
2. N1B 노드에서 백업을 복원할 수 있습니다. 역할은 변경하지 않아도 됩니다.

컨피그레이션 롤백

문제

실수로 컨피그레이션을 잘못 변경하는 경우가 있을 수 있습니다. 이 경우 변경하기 전에 작성한 백업을 복원하여 원래 컨피그레이션으로 되돌릴 수 있습니다.

가능한 원인

N1(기본 정책 관리 노드 또는 기본 PAN)과 N2(보조 정책 관리 관리 노드)로 구성된 노드 2개와 N1 노드 백업 1개가 지원됩니다. 일부 컨피그레이션을 잘못 변경하여 N1에서 변경 사항을 제거하고자 합니다.

솔루션

잘못된 컨피그레이션 변경이 적용되기 전에 작성된 N1 노드 백업을 가져옵니다. N1 노드에서 이 백업을 복원합니다. 복원 스크립트는 N1의 데이터를 N2와 동기화합니다.

2노드 구축에서 장애 발생 시 기본 노드 복구

시나리오

다중 노드 구축에서 PAN에 장애가 발생했습니다.

예를 들어 N1(PAN) 및 N2(보조 관리 노드)라는 Cisco ISE-PIC 노드가 2개 있는데 하드웨어 문제로 인해 N1에 장애가 발생한다고 가정해 보겠습니다.

가정

2노드 구축의 기본 노드에만 장애가 발생했습니다.

해결 단계

1. N2 관리자 포털에 로그인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 를 선택하고 기본 노드로 N2를 구성합니다.

   N1 노드가 새 하드웨어로 교체되고 재이미지화되며 독립형 상태가 됩니다.

2. N2 관리자 포털에서 새 N1 노드를 보조 노드로 등록합니다.

   이제 N2 노드가 기본 노드가 되고 N1 노드가 보조 노드가 됩니다.

N1 노드를 다시 기본 노드로 지정하려면 N1 관리자 포털에 로그인하여 N1 노드를 기본 노드로 지정합니다. 그러면 N2는 자동으로 보조 서버가 됩니다. 데이터는 손실되지 않습니다.

2노드 구축에서 장애 발생 시 보조 노드 복구

시나리오

다중 노드 구축에서 단일 보조 노드에 장애가 발생했습니다. 복원은 수행하지 않아도 됩니다.

해결 단계

1. 보조 노드를 기본 독립형 상태로 재이미지화합니다.
2. 기본 노드에서 관리 포털에 로그인하고 보조 노드를 삭제합니다.
3. 보조 노드를 다시 등록합니다.

   데이터가 기본 노드에서 보조 노드로 복제됩니다. 복원은 수행하지 않아도 됩니다.

Database Purge(데이터베이스 제거)

제거 프로세스를 사용하면 제거하는 동안 데이터를 유지할 개월 수를 지정하여 데이터베이스의 크기를 관리할 수 있습니다. 기본값은 3개월입니다. 이 값은 제거를 위한 디스크 공간 사용 임계값(디스크 공간의 백분율)을 충족할 때 사용됩니다. 이 옵션에서 각 달은 30일로 구성됩니다. 3개월의 기본값은 90일입니다.

데이터베이스 비우기를 위한 지침

다음은 데이터베이스 디스크 사용량과 관련하여 따라야 하는 지침입니다.

- 데이터베이스 디스크 사용량이 임계값 설정의 80%를 초과하는 경우에는 데이터베이스 크기가 할당된 디스크 크기를 초과했음을 나타내는 중요 경보가 생성됩니다. 디스크 사용량이 90%를 초과하면 또 다른 경보가 생성됩니다.
- 비우기는 데이터베이스의 사용된 디스크 공간 백분율도 기반으로 합니다. 데이터베이스의 사용된 디스크 공간이 임계값(기본값: 80%) 이상이면 비우기 프로세스가 시작됩니다. 이 프로세스에서는 관리 포털에서 구성된 값에 관계없이 모니터링 데이터의 마지막 7일 분량만 삭제합니다. 사용된 디스크 공간이 80% 미만이 될 때까지 루프에서 이 프로세스가 계속 진행됩니다. 비우기를 계속하기 전에 항상 데이터베이스 디스크 공간을 확인합니다.

운영 데이터 제거

Cisco ISE 모니터링 운영 데이터베이스에는 Cisco ISE 보고서로 생성되는 정보가 포함되어 있습니다. 최신 Cisco ISE 릴리스에는 Cisco ISE 관리 CLI 명령 **application configure ise**를 실행한 후 모니터링 운영 데이터를 제거하고 모니터링 데이터베이스를 재설정하는 옵션이 있습니다.

제거 옵션은 데이터를 정리하는 데 사용되며 보존 기간(일)을 지정하라는 메시지를 표시합니다. 재설정 옵션은 데이터베이스를 출고 시 기본값으로 재설정하는 데 사용되며 백업된 모든 데이터를 영구적으로 삭제합니다. 파일이 너무 많은 파일 시스템 공간을 사용하는 경우 데이터베이스를 재설정할 수 있습니다.

참고 재설정 옵션을 사용하면 재시작 전까지 Cisco ISE 서비스를 일시적으로 사용할 수 없게 됩니다.

관련 항목

이전 운영 데이터 비우기, 137 페이지

이전 운영 데이터 비우기

운영 데이터는 일정 기간 동안 서버에 수집되며, 즉시 또는 정기적으로 비울 수 있습니다.

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 제거**)**.

단계 **2** 다음 중 하나를 수행합니다.

- **Data Retention Period(**데이터 보존 기간**)** 영역에서 다음을 수행합니다.

  1. RADIUS 및 TACACS 데이터를 보존할 기간을 일 단위로 지정합니다. 지정한 기간 이전의 모든 데이터는 저장소로 내보내집니다. ISE-PIC에서는 RADIUS 또는 TACACS 기능을 제공하지는 않지만 일부 인프라가 Cisco ISE와 공유되므로 데이터베이스에서 이러한 정보를 주기적으로 제거해야 할 수 있습니다.
  2. **Repository(**저장소**)** 영역에서 **Enable Export Repository(**내보내기 저장소 활성화**)** 체크 박스를 선택하여 데이터를 저장할 저장소를 선택합니다.
  3. **Encryption Key(**암호화 키**)** 텍스트 상자에 필요한 비밀번호를 입력합니다.
  4. **Save(**저장**)**를 클릭합니다.

     참고 구성된 보존 기간이 진단 데이터에 해당하는 기존 보존 임계값보다 작으면 구성된 값이 기존 임계값을 재정의합니다. 예를 들어 보존 기간을 3일로 구성했는데 이 값이 진단 테이블의 기존 임계값(예: 기본값인 5일)보다 작은 경우에는 이 창에서 구성한 값(3일)에 따라 데이터를 제거합니다.

- **Purge Data Now(**지금 데이터 제거**)** 영역에서 다음을 수행합니다.

  1. 모든 데이터를 제거할지 아니면 지정된 기간(일)보다 오래된 데이터를 제거할지 선택합니다. 데이터는 어떤 저장소에도 저장되지 않습니다.

2. **Purge(**제거**)**를 클릭합니다.

전체 ISE 설치로 ISE-PIC 업그레이드

Cisco ISE-PIC는 전체 CISCO ISE GUI를 기반으로 단순하며 직관적인 GUI로 표시됩니다. 그래서 ISE-PIC를 설치하면 ISE로 쉽고 효율적으로 업그레이드할 수 있습니다. ISE-PIC에서 ISE 기본 라이센스로 업그레이드할 때 ISE는 업그레이드하기 전에 ISE-PIC에서 이용할 수 있었던 모든 기능을 계속 제공하며, 업그레이드한 ISE-PIC 노드를 기본 PAN으로 사용한다면 이전에 구성한 설정을 다시 구성하지 않아도 됩니다.

참고 업그레이드한 기존 ISE-PIC 노드를 기본 PAN으로 사용하지 않는다면, 노드에 있는 데이터는 업그레이드할 때 삭제되며 사용자는 새로 추가된 노드에서 기존 전체 ISE 구축의 데이터에 액세스할 수 있습니다.

먼저 노드에 ISE-PIC Upgrade License(업그레이드 라이센스)를 설치한 다음 아래 작업을 수행하면 전체 업그레이드 프로세스를 수행할 수 있습니다.

- 업그레이드한 ISE-PIC 노드를 기존 ISE 구축에 추가합니다.
- 또는 Base 라이센스를 하나 이상 설치합니다.

참고 전체 Cisco ISE 구축으로 업그레이드하면 이전 Cisco ISE-PIC 설치로 롤백할 수 없습니다.

ISE로의 업그레이드가 제공하는 이점에 관한 자세한 내용은 ISE-PIC와 ISE/CDA 비교, 5 페이지 항목을 참고하십시오.

라이선스를 등록하여 ISE로 업그레이드

시작하기 전에

Cisco ISE-PIC 영구 라이선스를 설치했는지 확인합니다. 또한 다음 방법 중 하나로 노드를 업그레이드할 수 있습니다.

- 기존 전체 ISE 구축에 ISE-PIC 노드 추가 - 업그레이드된 ISE-PIC 노드가 기존 구축을 보조 노드로 조인합니다. 이렇게 하려면 Cisco ISE-PIC 업그레이드 라이센스를 사용하여 이 작업의 단계를 5단계까지만 수행합니다. ISE-PIC 노드를 보조 노드로 추가할 경우 기존 ISE 구축의 모든 데이터는 유지되며 새로 조인된(업그레이드된) ISE-PIC 노드에 동기화되지만 원래 ISE-PIC 노드 데이터는 유지되지 않습니다. 이 라이센스는 Cisco 담당자에게 문의하십시오.

- 특정 ISE-PIC 노드를 ISE 구축의 기본 또는 독립형 노드로 업그레이드 - 기존의 모든 데이터를 보존하면서 ISE-PIC 노드를 업그레이드합니다. Cisco ISE-PIC 업그레이드 라이센스 및 Cisco ISE 기본 라이센스에 대해서는 Cisco 담당자에게 문의하십시오.

라이선싱 모델에 대한 자세한 내용은 다음을 참조하십시오. Cisco ISE-PIC 라이센싱, 11 페이지

단계 **1** 보조 노드가 설치되어있는 경우 Cisco ISE-PIC 기본 노드 설치에서 **Administration(**관리**)** > **Deployment(**구축**)** 을 선택하고 보조 노드의 등록을 해제합니다. 그러면 두 노드가 모두 기본 노드가 되며 둘 중 하나를 업그레이드할 수 있습니다.

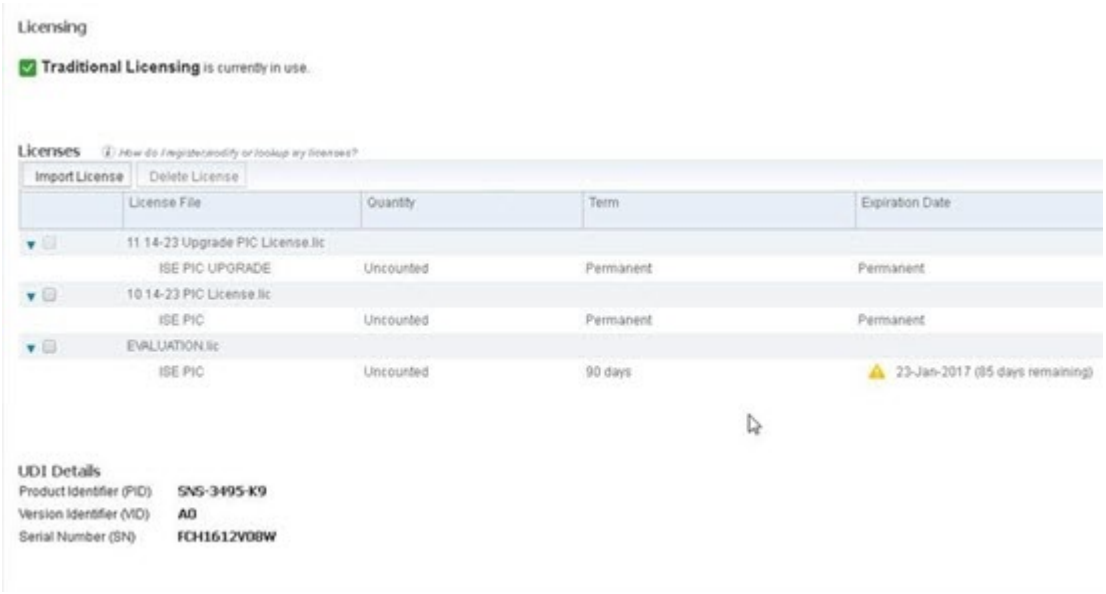
단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Licensing(**라이센싱**)**.

단계 **3** **Import License(**라이센스 가져오기**)**를 클릭합니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭하고 업그레이드 라이센스 파일을 찾아 **OK(**확인**)**를 클릭합니다.

단계 **5** 참고 이 ISE-PIC 노드를 기존 ISE 구축에 추가하는 경우 이 단계를 완료하면 업그레이드를 완료한 것이므로 이제 해당 구축의 기본 노드에서 노드를 등록하여 노드를 추가할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine* 관리 설명서를 참조하십시오.

Import New License File(새 라이선스 파일 가져오기**)** 화면에서 **Import(**가져오기**)**를 클릭합니다.
다음과 같은 업그레이드 라이센스를 포함하여 업그레이드 테이블이 이제 새로 고쳐집니다.



단계 **6** 이 업그레이드된 노드를 전체 ISE 구축의 기본 노드로 만들려면 지금 기본 라이선스를 가져오십시오. **Import License(**라이선스 가져오기**)**를 다시 클릭합니다.

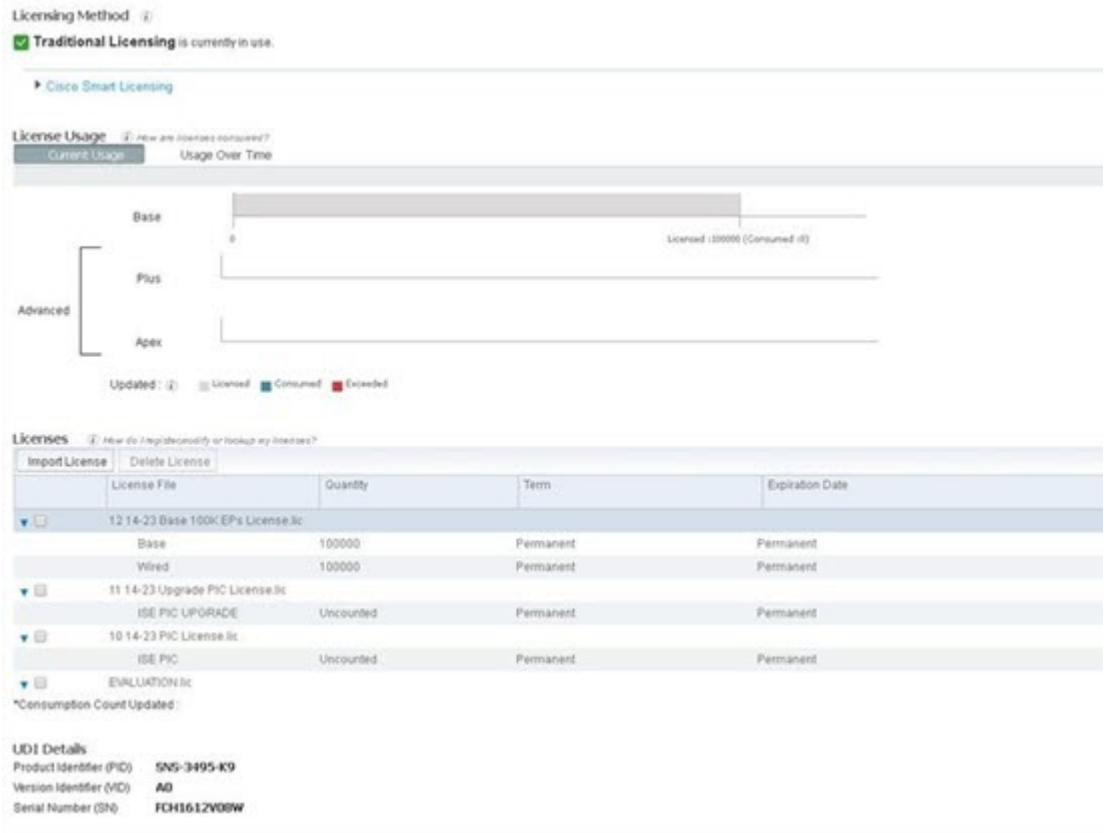
단계 **7** **Choose File(**파일 선택**)**을 클릭하고 Cisco 담당자로부터 받은 전체 ISE 기본 라이센스를 찾은 다음 **OK(**확인**)**를 클릭합니다.

단계 **8** **Import New License File(**새 라이선스 파일 가져오기**)** 화면에서 **Import(**가져오기**)**를 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.
ISE의 기본 노드로의 업그레이드가 시작되고 다음 메시지가 나타납니다. 이 노드는 현재 백그라운드에서 *ISE*로 업그레이드되고 있습니다. 몇 분 정도 기다렸다가 *ISE*에 로그인하십시오.

단계 **10** **OK(**확인**)**를 클릭합니다.

다음과 같은 기본 라이센스를 포함하여 업그레이드 테이블이 이제 새로 고쳐집니다.



몇 분 후에 로그인 화면이 나타납니다. 다시 로그인하여 전체 ISE 기본 라이센스 설치에서 제공하는 모든 메뉴에 액세스합니다.

이제 기본 ISE-PIC 노드를 전체 ISE 설치에서 기본 노드로 업그레이드했으며 이전 보조 노드는 이제 ISE-PIC 독립형 설치에서 기본이자 유일한 노드입니다. 이제 동일한 방식으로 마지막 ISE-PIC 노드를 개별적으로 업그레이드할 수 있습니다.

API 제공자에서 **ISE-PIC**

역할 기반 액세스 제어

Cisco ISE-PIC에서는 특정 시스템 작동 권한을 관리자에게 허용하거나 거부하는 RBAC(Role-based Access Control) 정책을 정의할 수 있습니다. 이러한 RBAC 정책은 개별 관리자 또는 관리자가 속하는 관리 그룹의 ID에 따라 정의됩니다.

보안을 강화하고 관리 포털에 액세스할 수 있는 사용자를 효과적으로 제어하려면 다음을 수행합니다.

- 원격 클라이언트의 IP 주소에 따라 관리 액세스 설정 구성
- 관리 계정을 위한 강력한 비밀번호 정책 정의
- 관리 GUI 세션에 대한 세션 시간 초과 구성

Cisco ISE-PIC 관리자

관리자는 관리 포털을 사용하여 다음을 수행할 수 있습니다.

- 구축 노드 모니터링, 문제 해결을 관리합니다.
- Cisco ISE-PIC 서비스관리자 계정 및 시스템 컨피그레이션 및 작업을 관리합니다.
- 관리자 및 사용자 비밀번호를 변경합니다.

CLI 관리자는 Cisco ISE 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

설치 중에 구성하는 사용자 이름 및 비밀번호는 CLI에 대한 관리 액세스 용도로만 사용됩니다. 이 역할은 CLI 관리자라고도 하는 CLI 관리 사용자로 간주됩니다. 기본적으로 CLI 관리 사용자의 사용자 이름은 admin이고 비밀번호는 설치 과정에서 정의됩니다. 비밀번호는 기본값이 없습니다. 이 CLI 관리 사용자는 기본 관리 사용자이며 이 사용자 계정은 삭제할 수 없습니다. 그러나 이 계정에 대한 비밀번호를 활성화, 비활성화 또는 변경하는 옵션을 포함하여 다른 관리자가 수정할 수 있습니다.

관리자를 만들 수도 있고 기존 사용자를 관리자 역할로 승격시킬 수도 있습니다. 또한 해당 관리 권한을 비활성화하여 관리자를 단순 네트워크 사용자 상태로 강등시킬 수도 있습니다.

관리자는 컨피그레이션에 대한 로컬 권한이 있으며 Cisco ISE-PIC 시스템을 운영하는 사용자입니다.

관리자는 하나 이상의 관리 그룹에 할당됩니다. 이러한 관리자 그룹은 다음 섹션에서 설명하는 것처럼 사용자 편의를 위해 시스템에 미리 정의되어 있습니다.

관련 항목

Cisco ISE-PIC 관리자 그룹, 141 페이지

Cisco ISE-PIC 관리자 그룹

관리자 그룹은 Cisco ISE-PIC의 RBAC(Role-based Access Control) 그룹입니다. 같은 그룹에 속하는 모든 관리자는 공통 ID를 공유하고 동일한 권한을 갖습니다. 특정 관리 그룹의 멤버인 관리자의 ID는 권한 부여 정책에서 조건으로 사용될 수 있습니다. 한 관리자는 여러 관리자 그룹에 속할 수 있습니다.

모든 액세스 수준을 가진 관리자 계정을 사용하여 액세스 권한이 있는 창에서 해당 개체를 수정하거나 삭제할 수 있습니다.

다음 테이블에는 Cisco ISE-PIC에 미리 정의된 관리자 그룹과 함께 해당 그룹의 멤버가 수행할 수 있는 작업이 나열되어 있습니다. 이러한 사전 정의된 그룹만 시스템에서 관리자 사용자를 정의하는 데 사용할 수 있습니다.

표 ***23: Cisco ISE*** 관리자 그룹, 액세스 레벨, 권한 및 제한 사항

관리자 그룹 역할	액세스 레벨	권한	제한 사항
슈퍼 관리자	모든 Cisco ISE-PIC 관리 기능. 기본 관리자 계정은 이 그룹에 속합니다.	모든 Cisco ISE-PIC 리소스에 대한 생성, 읽기, 업데이트, 삭제 및 실행(CRUDX) 권한	
ERS(External RESTful Services) 관리자	GET, POST, DELETE, PUT 등 모든 ERS API 요청에 대한 전체 액세스	• ERS API 요청 생성, 읽기, 업데이트 및 삭제	이 역할은 내부 사용자, ID 그룹 및 엔드포인트를 지원하는 ERS 권한 부여에만 사용됨

CLI 관리자와 웹 기반 관리자의 권한

CLI 관리자는 Cisco ISE-PIC 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE-PIC 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE-PIC 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

새 관리자 생성

Cisco ISE-PIC 관리자에게는 특정 관리 작업을 수행하기 위한 특정 역할이 할당된 계정이 있어야 합니다. 관리자 계정을 생성하고 이러한 관리자가 수행해야 하는 관리 작업을 기준으로 해당 관리자에게 하나 이상의 역할을 할당할 수 있습니다.

Admin Users(관리자 사용자**)** 창을 사용하여 Cisco ISE-PIC 관리자의 특성에 대해 확인/생성/수정/삭제/상태 변경/복제/검색을 수행할 수 있습니다.

참고 관리자 사용자의 도메인이 CLI와 GUI에서 모두 동일할 경우 GUI에 가입하기 전에 Active Directory 액세스를 먼저 구성하는 것이 좋습니다. 그러지 않을 경우, GUI에서 도메인에 다시 가입해야 해당 도메인에 대한 인증 실패를 방지할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)** > **Create an Admin User(**관리자 사용자 생성**)**.

단계 **2** 필드에 값을 입력합니다. **Name(**이름**)** 필드에 입력할 수 있는 문자는 # $ ' ( ) * + -입니다. / @ _입니다.

단계 **3** **Submit(**제출**)**을 클릭하여 Cisco ISE-PIC 내부 데이터베이스에 새 관리자를 생성합니다.

관련 항목

읽기 전용 관리 정책
내부 읽기 전용 관리자 생성
읽기 전용 관리자를 위한 메뉴 액세스 사용자 지정
읽기 전용 관리자 그룹에 외부 그룹 매핑

Cisco ISE-PIC에 대한 관리 액세스

Cisco ISE-PIC 관리자는 자신이 속해 있는 관리 그룹에 따라 다양한 관리 작업을 수행할 수 있습니다. 이러한 관리 작업은 매우 중요합니다. 네트워크에서 Cisco ISE-PIC를 관리할 권한이 있는 사용자에게만 관리 액세스 권한을 부여하십시오.

Cisco ISE-PIC에서는 다음 옵션을 통해 웹 인터페이스에 대한 관리 액세스를 제어할 수 있습니다.

참고 Cisco ISE 서버가 네트워크에 추가되는 경우 웹 인터페이스가 작동하면 실행 중인 상태로 표시됩니다. 그러나 포스처 서비스와 같은 일부 고급 서비스를 사용하려면 시간이 더 오래 걸릴 수 있으므로 모든 서비스가 완전히 작동하는 데 시간이 추가로 소요될 수 있습니다.

관리 액세스 방법

여러 방법으로 Cisco ISE 서버에 연결할 수 있습니다. PAN은 관리자 포털을 실행하며, 관리자 포털에 로그인하려면 관리자 암호가 필요합니다. 다른 ISE 페르소나 서버는 SSH 또는 CLI를 실행하는 콘솔을 통해 액세스할 수 있습니다. 이 섹션에서는 각 연결 유형에 사용 가능한 프로세스 및 암호 옵션에 대해 설명합니다.

- **Admin password(**관리자 암호**)**: 설치하는 동안 생성한 Cisco ISE 관리 사용자는 기본적으로 45일 후에 타임아웃됩니다. 다음에서 암호 수명 주기를 끄는 방식으로 이를 방지할 수 있습니다. **Administration(**관리**)** > **System(**시스템**)** > **Admin Settings(**관리자 설정**)**. **Password Policy(**암호 정책**)** 탭을 클릭하고 **Password Lifetime(**암호 수명 주기**)** 아래에서 **Administrative passwords expire(**관리자 비밀번호 만료**)**를 선택 취소합니다.

  아니면 암호가 만료되고 나서 **application reset-passwd** 명령을 실행하여 CLI에서 관리자 암호를 재설정할 수 있습니다. 콘솔에 연결하여 CLI에 액세스하거나 ISE 이미지 파일을 재부팅하고 부팅 옵션 메뉴에 액세스하여 관리자 암호를 재설정할 수 있습니다.

- **CLI password(CLI** 암호**)**: 설치 중에 CLI 암호를 입력해야 합니다 잘못된 암호로 인해 CLI에 로그인하는 데 문제가 있는 경우 CLI 암호를 재설정할 수 있습니다. 콘솔에 연결하고 **password** CLI 명령을 실행하여 암호를 재설정합니다. 자세한 내용은 *ISE CLI* 참조를 확인하십시오.

-

관리자 액세스 설정

Cisco ISE-PIC를 사용하면 관리자 계정에 대한 일부 규칙을 정의하여 보안을 개선할 수 있습니다. 관리 인터페이스에 대한 액세스를 제한하여 관리자가 강력한 비밀번호를 사용하거나 비밀번호를 정기

적으로 변경하는 등의 작업을 하도록 강제할 수 있습니다. Cisco ISE-PIC의 관리자 계정 설정에서 정의하는 비밀번호 정책은 모든 관리자 계정에 적용됩니다.

Cisco ISE-PIC는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

동시 관리 세션 및 로그인 배너의 최대 수 구성

관리자에게 관리 웹 또는 CLI 인터페이스에 액세스하는 사용자를 알려 주는 동시 관리 GUI 또는 CLI(SSH) 세션 및 로그인 배너의 최대 수를 구성할 수 있습니다. 관리자 로그인 전과 후에 표시되는 로그인 배너를 구성할 수 있습니다. 이러한 로그인 배너는 기본적으로 비활성화됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Access Settings(**액세스 설정**)** > **Session(**세션**)**.

단계 **2** GUI 및 CLI 인터페이스를 통해 허용하려는 동시 관리 세션의 최대 수를 입력합니다. 동시 관리 GUI 세션의 유효한 범위는 1~20입니다. 동시 관리 CLI 세션의 유효한 범위는 1~10입니다.

단계 **3** 관리자 로그인 전에 Cisco ISE-PIC가 메시지를 표시하도록 하려면 **Pre-login banner(**로그인 전 배너**)** 체크 박스를 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **4** 관리자 로그인 후에 Cisco ISE-PIC가 메시지를 표시하도록 하려면 **Post-login banner(**로그인 후 배너**)** 체크 박스를 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

선택한 **IP** 주소에서 **Cisco ISE-PIC**로의 관리 액세스 허용

Cisco ISE-PIC에서는 관리자가 Cisco ISE-PIC 관리 인터페이스에 액세스할 수 있는 IP 주소 목록을 구성할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Access Settings(**액세스 설정**)** > **IP Access(IP** 액세스**)**.

단계 **2** **Allow only listed IP addresses to connect(**목록에 나열된 **IP** 주소만 연결 허용**)**를 선택합니다.

참고 포트 161(SNMP)에 대한 연결은 관리 액세스에 사용됩니다. 그러나 IP 액세스 제한이 구성된 경우, snmpwalk가 수행되는 출처 노드를 관리 액세스용으로 구성하지 않으면 snmpwalk는 실패합니다.

단계 **3** 액세스 제한용 IP 목록 구성 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** IP address(IP 주소) 필드에 IP 주소를 CIDR(Classless Interdomain Routing) 형식으로 입력합니다.

참고 이 IP 주소의 범위는 IPv4~IPv6입니다. 이제 하나의 ISE 노드에 대해 여러 IPv6 주소를 구성할 수 있습니다.

단계 **5** Netmask in CIDR format(CIDR의 네트워크 마스크 형식) 필드에 서브넷 마스크를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다. 위의 과정을 반복하여 이 목록에 IP 주소 범위를 더 추가합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

단계 **8** **Reset(**재설정**)**을 클릭하여 **IP Access(IP** 액세스**)** 페이지를 새로 고칩니다.

관리자 계정의 비밀번호 정책 구성

Cisco ISE-PIC에서는 보안을 강화하기 위해 관리자 계정용 비밀번호 정책을 생성할 수도 있습니다. 여기에서 정의하는 비밀번호 정책은 Cisco ISE-PIC의 모든 관리자 계정에 적용됩니다.

참고

- 내부 관리자 사용자에 대한 이메일 알림은 root@host로 전송됩니다. 이메일 주소를 구성 할 수 없으며 많은 SMTP 서버가 이 이메일을 거부합니다.

  이메일 주소를 변경할 수 있는 개선된 오픈 결함 CSCui5583을 따를 수 있습니다.

- Cisco ISE-PIC는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**.

단계 **2** **Password Policy(**비밀번호 정책**)** 탭을 클릭하고 값을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭하여 관리자 비밀번호 정책을 저장합니다.

참고 로그인 시 외부 ID 저장소를 사용하여 관리자를 인증하는 경우, 관리자 프로파일에 적용되는 비밀번호 정책에 대해 이 설정이 구성되어 있더라도 외부 ID 저장소는 관리자의 사용자 이름과 비밀번호를 계속 검증합니다.

관리자 계정의 계정 비활성화 정책 구성

Cisco ISE-PIC에서는 구성된 연속 기간(일) 동안 관리자 계정이 인증되지 않은 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Account Disable Policy(**계정 비활성화 정책**)**를 선택합니다.

단계 **2** **Disable account after *n* days of inactivity(n**일 동안 비활성 상태였던 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다.

이 옵션을 사용하면 구성된 연속 기간(일) 동안 관리자 계정이 비활성 상태인 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **3** 관리자에 대한 전역 계정 비활성화 정책을 구성하려면 **Save(**저장**)**를 클릭합니다.

관리자에 대한 세션 시간 초과 구성

Cisco ISE-PIC에서는 관리 GUI 세션이 비활성 상태로 계속 연결되어 있을 수 있는 시간을 결정할 수 있습니다. Cisco ISE-PIC가 관리자를 로그아웃 처리할 때까지의 시간을 분 단위로 지정할 수 있습니다. 세션 시간이 초과되고 나면 관리자는 다시 로그인해야 Cisco ISE-PIC 관리 포털에 액세스할 수 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Session Settings(**세션 설정**)** > **Session Timeout(**세션 시간 초과**)**.

단계 2 작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE-PIC가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효한 범위는 6분~100분입니다.

단계 3 **Save(**저장**)**를 클릭합니다.

활성 관리 세션 종료

Cisco ISE-PIC는 필요한 경우 언제든지 세션을 선택하여 종료할 수 있도록 모든 활성 관리 세션을 표시합니다. 동시 관리 GUI 세션의 최대 수는 20개입니다. GUI 세션의 최대 수에 도달하면 슈퍼 관리자 그룹에 속하는 관리자가 로그인하여 일부 세션을 종료할 수 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Session Settings(**세션 설정**)** > **Session Info(**세션 정보**)**.

단계 2 종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관리 포털에서 사용되는 포트

관리 포털은 HTTP 포트 80 및 HTTPS 포트 443을 사용하도록 설정되어 있으며 이러한 설정은 변경할 수 없습니다. 또한 Cisco ISE-PIC에서는 최종 사용자 포털이 동일한 포트를 사용하도록 할당할 수 없습니다. 이 기능으로 인해 관리 포털에 대한 위험이 감소합니다.

알림을 지원하도록 SMTP 서버 구성

알람에 대한 이메일 알림을 보내려면 SMTP(Simple Mail Transfer Protocol) 서버를 구성합니다.

이메일을 전송할 ISE 노드

다음 목록에는 분산 ISE 환경에서 이메일을 전송하는 노드가 나와 있습니다.

이메일 용도	이메일을 전송하는 노드
게스트 만료	기본 PAN
경보	활성 MnT
게스트 및 스폰서 포털의 스폰서 및 게스트 알림	PSN
비밀번호 만료	기본 PAN

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**.

단계 2 **SMTP server(SMTP** 서버**)** 필드에 아웃바운드 SMTP 서버의 호스트 이름을 입력합니다. Cisco ISE-PIC 서버에서 이 SMTP 호스트 서버에 액세스할 수 있어야 합니다. 이 필드의 최대 길이는 60자입니다.

단계 3 **Save(**저장**)**를 클릭합니다.

알람 알림의 수신자는 **Include system alarms in emails(**이메일에 시스템 알람 포함**)** 옵션이 활성화된 모든 내부 관리 사용자가 될 수 있습니다. 경보 알림을 보내기 위한 보낸 사람의 이메일 주소는 ise@<호스트 이름>으로 하드 코드됩니다.

GUI—ERS 설정에서 외부 RESTful 서비스 API 활성화

시작하기 전에

Cisco ISE REST API용으로 개발된 애플리케이션에서 Cisco ISE에 액세스할 수 있도록 Cisco ISE REST API를 활성화해야 합니다. Cisco REST API는 기본적으로 HTTPS 포트 9060을 사용합니다. Cisco ISE REST API가 Cisco ISE 관리자 서버에서 활성화되지 않은 경우, 클라이언트 애플리케이션은 모든 게스트 REST API 요청에 대해 서버에서 시간 초과 오류를 수신합니다.

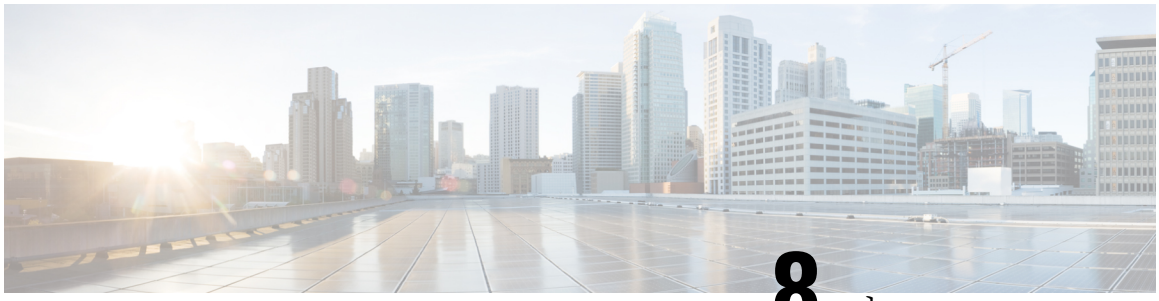
모든 유형의 외부 RESTful 서비스 요청은 기본 ISE 노드에만 유효합니다. 보조 노드에는 읽기-액세스 권한(GET 요청)이 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **ERS Settings(ERS** 설정**)**.

단계 2 **Enable ERS for Read/Write(**읽기/쓰기용 **ERS** 활성화**)**를 선택하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

API 호출 및 ISE-PIC에 대한 자세한 내용은 ISE API 참조 가이드를 참조하십시오.



8 장

PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 ISE-PIC

모니터링 및 문제 해결 서비스는 모든 Cisco ISE-PIC 런타임 서비스에 사용할 수 있는 포괄적인 ID 솔루션으로, 다음과 같은 구성 요소를 사용합니다.

- 모니터링 - 네트워크에 대한 액세스 활동의 상태를 나타내는 의미 있는 데이터를 실시간으로 표시합니다. 이 정보는 쉽게 해석할 수 있으며 작동 조건에 영향을 미칠 수 있습니다.
- 문제 해결 - 네트워크의 액세스 문제를 해결하기 위한 상황별 지침을 제공합니다. 그러면 관리자는 사용자의 문제를 해결하고 시기 적절하게 해결 방법을 제공할 수 있습니다.
- 보고 - 관리자가 트렌드를 분석하고 시스템 성능 및 네트워크 활동을 모니터링하는 데 사용할 수 있는 표준 보고서 카탈로그를 제공합니다. 다양한 방법으로 보고서를 맞춤화하고 나중에 사용하기 위해 저장할 수 있습니다. Identity(ID), Endpoint ID(엔드포인트 ID) 및 ISE Node(ISE 노드) 필드 관련 와일드카드와 여러 값을 사용하여 레코드를 검색할 수 있습니다.

이 섹션에서는 모니터링, 문제 해결 및 보고 도구를 사용하여 ISE-PIC를 관리하는 방법을 확인할 수 있습니다.

Live Sessions(라이브 세션)

다음 표에서는 라이브 세션을 표시하는, **Live Sessions(**라이브 세션**)** 창의 필드를 설명합니다. 메인 메뉴 막대에서 **Live Sessions(**라이브 세션**)**를 선택합니다.

표 *24:* 라이브 세션

필드 이름	설명
Initiated(시작됨**)**	세션이 시작된 타임스탬프를 표시합니다.
업데이트됨	변경으로 인해 세션이 마지막으로 업데이트된 타임스탬프를 표시합니다.
Account Session Time(계정 세션 시간**)**	사용자 세션의 시간 범위를 초 단위로 표시합니다.
Session Status(세션 상태**)**	엔드포인트 디바이스의 현재 상태를 표시합니다.
조치	Actions(작업) 아이콘을 클릭하여 **Actions(**작업**)** 팝업창을 엽니다. 다음을 수행할 수 있습니다. • 세션 지우기 • 현재 사용자의 세션 상태 확인
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
ID	엔드포인트 디바이스의 사용자 이름을 표시합니다.
IP 주소	엔드포인트 디바이스의 IP 주소를 표시합니다.
서버	로그가 생성된 PIC 노드를 나타냅니다.
Auth Method(인증 방법**)**	PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Session Source(세션 소스**)**	RADIUS 세션인지 PassiveID 세션인지를 나타냅니다.
User Domain Name(사용자 도메인 이름**)**	사용자의 등록된 DNS 이름을 표시합니다.
User NetBIOS Name(사용자 **NetBIOS** 이름**)**	사용자의 NetBIOS 이름을 표시합니다.

필드 이름	설명
사업자	엔드포인트 이벤트는 다양한 시스템 로그 소스에서 학습됩니다. 이러한 시스템 로그 소스를 제공자라고 합니다. • WMI(Windows Management Instrumentation)—WMI는 운영 체제, 장치, 애플리케이션 및 서비스 관련 관리 정보에 액세스하기 위한 공통 인터페이스와 개체 모델을 제공하는 Windows 서비스입니다. • Agent(에이전트)-클라이언트나 다른 프로그램을 대신하여 클라이언트에서 실행되는 프로그램입니다. • Syslog(시스템 로그)—클라이언트가 메시지를 전송하는 로깅 서버입니다. • REST—터미널 서버를 통해 인증한 클라이언트입니다. 이 시스템 로그 소스에 대한 TS Agent ID(TS 에이전트 ID), Source Port Start(소스 포트 시작), Source Port End(소스 포트 끝), Source First Port(소스 최초 포트) 값이 표시됩니다. • Span—네트워크 정보는 span 프로브를 이용해 검색합니다. • DHCP—DHCP 이벤트입니다. • 엔드포인트 엔드포인트 세션에서 서로 다른 제공자에서 발생한 두 이벤트를 파악하면, 제공자는 라이브 세션 페이지에 쉼표로 구분된 값으로 표시됩니다.
MAC Address(MAC 주소)	클라이언트의 MAC 주소를 표시합니다.
엔드포인트 확인 시간	엔드포인트 프로브가 엔드포인트를 마지막으로 확인한 시간을 표시합니다.
엔드포인트 확인 결과	엔드포인트 프로브의 결과를 표시합니다. 가능한 값은 다음과 같습니다. • 연결 불가 • 사용자 로그아웃 • 활성 사용자

필드 이름	설명
Source Port Start(소스 포트 시작**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 첫 번째 포트 번호를 표시합니다.
Source Port End(소스 포트 종료**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 마지막 포트 번호를 표시합니다.
Source First Port(소스 첫 번째 포트**)**	(값은 REST 제공자에 대해서만 표시됨) TS(Terminal Server) 에이전트가 할당한 첫 번째 포트를 표시합니다. TS(Terminal Server)는 모뎀이나 네트워크 인터페이스 없이도 여러 엔드포인트가 연결될 수 있고 여러 엔드포인트와 LAN 네트워크 간의 연결을 촉진하는 서버 또는 네트워크 장치를 말합니다. 여러 엔드포인트가 같은 IP 주소를 이용하는 것처럼 보이기 때문에 특정 사용자의 IP 주소를 식별하기가 어렵습니다. 따라서 특정 사용자를 식별하기 위해 각 사용자에 포트 범위를 할당하는 TS 에이전트가 서버에 설치됩니다. 이렇게 하면 IP 주소-포트-사용자 매핑을 만들 수 있습니다.
TS 에이전트 **ID**	(값은 REST 제공자에 대해서만 표시됨) 엔드포인트에 설치된 TS(Terminal Server) 에이전트의 고유 ID를 표시합니다.
AD 사용자가 확인한 **ID**	(값은 AD 사용자에 대해서만 표시됨) 일치하는 잠재적 계정을 표시합니다.
AD 사용자가 확인한 **DN**	(값은 AD 사용자에 대해서만 폿시됨) AD 사용자의 Distinguished Name(고유 이름) 을 표시합니다 (예: CN=chris,CN=Users,DC=R1,DC=com).

사용 가능한 보고서

다음 표에는 미리 구성된 보고서가 범주에 따라 그룹화되어 있습니다. 보고서 기능 및 로깅 범주에 대한 설명도 제공됩니다.

보고서 이름	설명	로깅 범주
IDC 보고서		

보고서 이름	설명	로깅 범주
AD Connector 운영	AD Connector 운영 보고서에서는 ISE-PIC 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 관리 관리 등 AD Connector에서 수행된 작업 로그를 제공합니다. 일부 AD 장애가 발생하면 이 보고서의 세부사항을 검토하여 가능한 원인을 식별할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 AD 커넥터를 선택합니다.
관리자 로그인	관리자 로그인 보고서는 모든 GUI 기반 관리자 로그인 이벤트와 성공한 CLI 로그인 이벤트에 대한 정보를 제공합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
컨피그레이션 변경 감사	컨피그레이션 변경 감사 보고서에서는 지정된 기간 내의 컨피그레이션 변경 사항에 대한 세부사항을 제공합니다. 특정 기능 문제를 해결해야 하는 경우 이 보고서를 통해 최근의 컨피그레이션 변경이 문제에 영향을 미쳤는지 확인할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
현재 활성 세션	현재 활성 세션 보고서를 사용하면 지정된 기간 내에 현재 네트워크에 있는 사용자에 대한 세부사항이 포함된 보고서를 내보낼 수 있습니다. 사용자가 네트워크에 액세스하지 않은 경우에는 세션이 인증 또는 종료되었는지 확인하거나 세션에 다른 문제가 있는지 확인할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 로깅 범주인 Accounting(계정 관리) 및 Radius Accounting(Radius 계정 관리)을 선택합니다.

보고서 이름	설명	로깅 범주
상태 요약	상태 요약 보고서에서는 대시보드와 유사한 세부사항을 제공합니다. 그러나 대시보드에는 지난 24시간 동안의 데이터만 표시되지만 이 보고서에서는 더 자세한 기록 데이터를 검토할 수 있습니다. 이 데이터를 평가하여 데이터의 일관된 패턴을 확인할 수 있습니다. 예를 들어 대부분의 직원이 하루 일과를 시작하는 시점에 CPU 사용량이 증가할 것을 예측할 수 있습니다. 이러한 트렌드의 불일치가 발견되는 경우 잠재적 문제를 식별할 수 있습니다. CPU 사용량 표에는 다양한 ISE-PIC 기능의 CPU 사용량 백분율이 나열됩니다. **show cpu usage** CLI 명령의 출력이 이 표에 나와 있으며, 이러한 값을 구축 내 문제와 연결하여 문제 원인을 식별할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 로깅 범주인 Administrative and Operational Audit(관리 및 운영 감사), System Diagnostics(시스템 진단), System Statistics(시스템 통계)를 선택합니다.
운영 감사	운영 감사 보고서에서는 백업 실행, ISE-PIC 노드 등록 또는 애플리케이션 다시 시작 등 작동 변경에 대한 세부사항을 제공합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.
PassiveID	Passive ID(패시브 ID) 보고서에서는 도메인 컨트롤러에 대한 WMI 연결의 상태를 모니터링하고 그와 관련된 통계(예: 수신된 알림 개수, 초당 사용자 로그인/로그아웃 수 등)를 수집할 수 있습니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Identity Mapping(ID 매핑)을 선택합니다.

보고서 이름	설명	로깅 범주
pxGrid 관리자 감사	pxGrid 관리자 감사 보고서에서는 클라이언트 등록, 클라이언트 등록 취소, 클라이언트 승인, 항목 생성, 항목 삭제, 게시자-구독자 추가 및 게시자-구독자 삭제 등의 pxGrid 관리 작업에 대한 세부사항을 제공합니다. 각 레코드에는 노드에 대한 작업을 수행한 관리자 이름이 있습니다. 관리자 및 메시지 기준에 따라 pxGrid 관리자 감사 보고서를 필터링할 수 있습니다.	—
시스템 진단	시스템 진단 보고서에서는 ISE-PIC 노드의 상태에 대한 세부사항을 제공합니다. ISE-PIC 노드를 등록할 수 없는 경우 이 보고서를 검토하여 문제를 해결할 수 있습니다. 이 보고서를 사용하려면 먼저 여러 진단 로깅 범주를 활성화해야 합니다. 이러한 로그를 수집하면 ISE-PIC 성능에 부정적 영향을 줄 수 있습니다. 그러므로 이러한 범주는 기본적으로 활성화되어 있지 않으므로 데이터를 수집하는 기간 동안만 활성화해야 합니다. 그렇지 않으면, 30분 후에 자동으로 비활성화됩니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Internal Operations Diagnostics(내부 운영 진단), Distributed Management(분산형 관리), Administrator Authentication and Authorization(관리자 인증 및 권한 부여) 기록 범주를 선택합니다.
사용자 변경 비밀번호 감사	사용자 변경 비밀번호 감사 보고서에서는 직원의 비밀번호 변경에 대한 확인을 표시합니다.	다음 메뉴를 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**기록**)** > **Logging Categories(**기록 범주**)** 그런 다음 Administrative and Operational Audit(관리 및 운영 감사)를 선택합니다.

Cisco ISE-PIC 알람

알람은 네트워크의 조건에 대해 알리며 알람 dashlet에 표시됩니다. 세 가지 알람 심각도, 즉 중요, 경고 및 정보가 있습니다. 또한 데이터 제거 이벤트와 같은 시스템 활동에 대한 정보도 제공합니다. 시스템 활동에 대한 알림을 어떤 식으로 받으려는지 구성할 수 있습니다. 아니면 경보를 완전히 비활성화할 수도 있습니다. 특정 경보에 대한 임계값도 구성할 수 있습니다.

대부분의 경보에는 일정이 연결되어 있지 않으며 이벤트가 발생한 직후에 경보가 전송됩니다. 특정한 시점에 보존되는 경보 수는 최신 경보를 기준으로 15,000개입니다.

이벤트가 다시 발생하는 경우 약 1시간 동안 동일한 경보가 표시되지 않습니다. 이벤트가 다시 발생하는 기간 동안에는 트리거에 따라 경보가 다시 표시되려면 약 1시간이 소요될 수 있습니다.

다음 표에는 모든 Cisco ISE-PIC 경보, 설명 및 해당 해결 방법이 나와 있습니다.

표 ***25: Cisco ISE-PIC*** 알람

경보 이름	경보 설명	경보 해결 방법
관리 및 운영 관리 감사		
구축 업그레이드 장애	ISE PIC 노드에서 업그레이드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 장애 이유와 정정 작업을 확인해 주십시오.
업그레이드 번들 다운로드 장애	ISE-PIC 노드에서 업그레이드 번들 다운로드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 장애 이유와 정정 작업을 확인해 주십시오.
CRL에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	CRL 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	OCSP 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CRL에서 취소된 인증서를 발견하여 보안 syslog 연결이 다시 연결됨	CRL 확인 결과 syslog 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. syslog 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 syslog 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 syslog 연결이 다시 연결됨	OCSP 확인 결과 syslog 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. syslog 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 syslog 서버에 설치해 주십시오.
관리자 계정 잠금/비활성화	비밀번호 만료 또는 잘못된 로그인 시도로 인해 관리자 계정이 잠기거나 비활성화되었습니다. 자세한 내용은 관리자 비밀번호 정책을 참고해 주십시오.	관리자 비밀번호는 다른 관리자가 GUI 또는 CLI를 사용하여 재설정할 수 있습니다.
ERS에서 더 이상 사용되지 않는 URL을 식별함	ERS에서 더 이상 사용되지 않는 URL을 식별함	요청 URL이 더 이상 사용되지 않으므로 해당 URL을 사용하지 않는 것이 좋습니다.
ERS에서 오래된 URL을 식별함	ERS에서 오래된 URL을 식별함	요청한 URL이 오래되었으므로 최신 URL을 사용하는 것이 좋습니다. 이 URL는 향후 릴리스에서 제거되지 않습니다.
ERS 요청 content-type 헤더가 오래되었습니다.	ERS 요청 content-type 헤더가 오래되었습니다.	요청 content-type 헤더에 나와 있는 요청 리소스 버전이 오래되었습니다. 이는 리소스 스키마가 수정되었음을 의미합니다. 하나 이상의 특성이 추가되었거나 제거되었을 수 있습니다. 오래된 스키마 문제를 해결하기 위해 ERS Engine은 기본값을 사용합니다.
ERS XML 입력에서 XSS 또는 삽입 공격이 의심됨	ERS XML 입력에서 XSS 또는 삽입 공격이 의심됩니다.	xml 입력을 검토하십시오.

경보 이름	경보 설명	경보 해결 방법
백업 실패	Cisco ISE-PIC 백업 작업이 실패했습니다.	Cisco ISE-PIC와 리포지토리 사이의 네트워크 연결을 확인해 주십시오. 다음 사항을 확인해 주십시오. • 리포지토리에 사용되는 자격 증명이 올바릅니다. • 리포지토리에 충분한 디스크 공간이 있습니다. • 리포지토리 사용자에게 쓰기 권한이 있습니다.
CA 서버 작동 중지됨	CA 서버가 작동 중지되었습니다.	CA 서비스가 CA 서버에서 작동되어 실행 중인지 확인해 주십시오.
CA 서버 작동	CA 서버가 작동합니다.	관리자에게 CA 서버가 작동하고 있음을 알리는 알림입니다.
인증서 만료	이 인증서가 곧 만료됩니다. 인증서가 만료되면 ISE-PIC가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE-PIC를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 취소됨	관리자가 내부 CA에 의해 엔드포인트로 발급된 인증서를 취소했습니다.	처음부터 새 인증서로 프로비저닝될 때까지 ISE-PIC 흐름을 진행해 주십시오.
인증서 프로비저닝 초기화 오류	인증서 프로비저닝 초기화에 실패했습니다.	주체에서 동일한 CN(CommonName) 속성 값을 가진 여러 인증서가 발견된 경우 인증서 체인을 작성할 수 없습니다. 시스템의 모든 인증서를 확인하십시오.

경보 이름	경보 설명	경보 해결 방법
인증서 복제 실패	보조 노드에 대한 인증서 복제에 실패했습니다.	보조 노드의 인증서가 유효하지 않거나 다른 영구적인 오류 조건이 있습니다. 보조 노드에 기존의 충돌하는 인증서가 있는지 확인해 주십시오. 충돌하는 인증서가 있는 경우, 보조 노드에서 기존 인증서를 삭제하고 기본 노드에서 새 인증서를 내보내고 인증서를 삭제한 다음 가져와 복제를 다시 시도하도록 해 주십시오.
인증서 복제 일시적 실패	보조 노드에 대한 인증서 복제가 일시적으로 실패했습니다.	네트워크 중단과 같은 일시적 상태로 인해 인증서가 보조 노드로 복제되지 않았습니다. 복제가 성공할 때까지 재시도됩니다.
인증서 만료됨	이 인증서가 만료되었습니다. Cisco ISE-PIC가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다. 노드 간 통신에도 영향을 미칠 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE-PIC를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 요청 전달 실패	인증서 요청 전달에 실패했습니다.	들어오는 인증 요청이 발신자의 특성과 일치하는지 확인해 주십시오.
컨피그레이션 변경됨	Cisco ISE 컨피그레이션이 업데이트되었습니다. 이 경보는 사용자 및 엔드포인트에서 컨피그레이션이 변경된 경우에는 트리거되지 않습니다.	컨피그레이션 변경이 예상되는지 확인해 주십시오.
CRL 검색 실패	서버에서 CRL을 검색할 수 없습니다. 지정된 CRL을 사용할 수 없는 경우에 발생할 수 있습니다.	다운로드 URL이 올바르고 서비스에 사용할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
DNS 확인 실패	노드에서 DNS 확인에 실패했습니다.	명령 **ip name-server** 로 구성한 DNS 서버에 연결할 수 있는지 확인해 주십시오. 'CNAME <노드의 호스트 이름>에 대한 DNS 확인 장애'라는 경보가 나타나면 각 Cisco ISE 노드에 대해 A 레코드와 함께 CNAME RR을 생성해야 합니다.
펌웨어 업데이트 필요	이 호스트에서 펌웨어를 업데이트해야 합니다.	펌웨어 업데이트를 받으려면 Cisco Technical Assistance Center(TAC)에 문의해 주십시오.
불충분한 가상 머신 리소스	이 호스트에서 CPU, RAM, 디스크 공간 또는 IOPS와 같은 VM(Virtual Machine) 리소스가 충분하지 않습니다.	Cisco ISE 하드웨어 설치 설명서에 명시된 VM 호스트에 대한 최소 요구사항을 확인해 주십시오.
NTP 서비스 실패	이 노드에서 NTP 서비스 작동이 중지되었습니다.	이는 NTP 서버와 Cisco ISE-PIC 노드 사이의 시간 차이가 크기 때문에(1,000초 이상) 발생할 수 있습니다. NTP 서버가 적절히 작동 중인지 확인하고 **ntp server** <서버 이름> CLI 명령을 사용하여 NTP 서비스를 재시작하고 시간 격차 문제를 해결해 주십시오.
NTP 동기화 실패	이 노드에 구성된 모든 NTP 서버에 연결할 수 없습니다.	실행 **show ntp** 명령을 실행해 주십시오. Cisco ISE-PIC에서 NTP 서버에 연결할 수 있는지 확인해 주십시오. NTP 인증이 구성된 경우 키 ID와 값이 서버의 값과 일치하는지 확인해 주십시오.
예약된 컨피그레이션 백업 없음	Cisco ISE-PIC 컨피그레이션 백업이 예약되지 않았습니다.	컨피그레이션 백업에 대한 일정을 생성해 주십시오.
작업 DB 제거 실패	작업 데이터베이스에서 오래된 데이터를 제거할 수 없습니다. 이는 M&T 노드가 사용 중인 경우에 발생할 수 있습니다.	데이터 제거 감사 보고서에서 used_space가 threshold_space보다 작은지 확인해 주십시오. CLI를 사용하여 M&T 노드에 로그인하고 제거 작업을 수동으로 수행해 주십시오.

경보 이름	경보 설명	경보 해결 방법
복제 실패	보조 노드에서 복제된 메시지를 사용하지 못했습니다.	Cisco ISE-PIC GUI에 로그인하고 구축 페이지에서 수동 동기화를 수행해 주십시오. 영향을 받는 Cisco ISE-PIC 노드를 등록 취소했다가 다시 등록해 주십시오.
복원 실패	Cisco ISE-PIC 복원 작업에 실패했습니다.	Cisco ISE-PIC와 리포지토리 사이의 네트워크 연결을 확인해 주십시오. 리포지토리에 사용된 자격 증명이 올바른지 확인해 주십시오. 백업 파일이 손상되지 않았는지 확인해 주십시오. CLI에서 **reset-config** 명령을 실행하고 마지막으로 알려진 안전한 백업을 복원해 주십시오.
패치 실패	서버에서 패치 프로세스가 실패했습니다.	서버에서 패치 프로세스를 다시 실행해 주십시오.
패치 성공	서버에서 패치 프로세스가 성공했습니다.	-
복제 중지됨	ISE-PIC 노드가 PAN에서 컨피그레이션 데이터를 복제할 수 없습니다.	Cisco ISE-PIC GUI에 로그인하여 구축 페이지에서 수동 동기화를 수행하거나, 필수 필드를 사용하여 영향을 받는 ISE-PIC 노드를 등록 취소했다가 다시 등록해 주십시오.
엔드포인트 인증서 만료됨	엔드포인트 인증서가 일별 예약 작업에서 만료된 상태로 표시되었습니다.	새 엔드포인트 인증서를 받으려면 엔드포인트 디바이스를 다시 등록해 주십시오.
엔드포인트 인증서 제거됨	일별 예약 작업에서 만료된 엔드포인트 인증서가 제거되었습니다.	추가 작업 필요 없음 - 이는 관리자가 시작한 정리 작업입니다.
느린 복제 오류	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 정보	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
느린 복제 경고	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
EST 서비스 중단	EST 서비스가 중단되었습니다.	CA 및 EST 서비스가 실행 중이고 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완전한지 확인하십시오.
EST 서비스 작동 중	EST 서비스가 작동 중입니다.	관리자에게 EST 서비스가 작동하고 있음을 알리는 알림입니다.
Smart Call Home 통신 실패	Smart Call Home 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE-PIC와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
원격 분석 통신 장애	원격 분석 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
ISE 서비스		
AD Connector를 다시 시작해야 함	AD Connector가 예기치 않게 중지되었으므로 다시 시작해야 합니다.	이 문제가 계속되면 Cisco TAC에 지원을 요청해 주십시오.
Active Directory 포리스트를 사용할 수 없음	Active Directory 포리스트 GC(Global Catalog)를 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
인증 도메인을 사용할 수 없음	인증 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 매핑. 인증 비활성	ID 매핑 서비스에서 최근 15분간 사용자 인증 이벤트를 수집하지 않았습니다.	사용자 인증이 필요한 시점이라면(예: 근무 시간) Active Directory 도메인 컨트롤러에 대한 연결을 확인해 주십시오.
구성된 네임서버 작동 중지됨	구성된 네임서버가 작동 중지되었거나 사용 불가능합니다.	DNS 컨피그레이션 및 네트워크 연결을 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
AD: 머신 TGT 새로 고침 실패	ISE-PIC 서버 TGT(Ticket Granting Ticket) 새로 고침에 실패했습니다. 해당 TGT는 AD 연결 및 서비스에 사용됩니다.	Cisco ISE-PIC 머신 계정이 있으며 유효한지 확인해주십시오. 또한 가능한 클럭 오차, 복제, Kerberos 컨피그레이션 및/또는 네트워크 오류가 있는지도 확인해 주십시오.
AD: ISE 계정 비밀번호 업데이트 실패	ISE-PIC 서버에서 AD 머신 계정 비밀번호를 업데이트하지 못했습니다.	Cisco ISE-PIC 머신 계정 비밀번호가 변경되지 않았는지, 그리고 머신 계정이 비활성화되었거나 제한되어 있지 않은지 확인해 주십시오. KDC에 대한 연결을 확인해 주십시오.
가입한 도메인 사용 불가능	가입한 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 특성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 저장소 사용 불가능	Cisco ISE-PIC 정책 서비스 노드를 구성한 ID 저장소에 연결할 수 없습니다.	Cisco ISE-PIC와 ID 저장소 사이의 네트워크 연결을 확인해 주십시오.
AD: ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE-PIC 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE-PIC 머신 계정에 Active Directory에서 사용자 그룹을 가져올 권한이 있는지 확인 합니다.
시스템 상태		
높은 디스크 I/O 사용률	Cisco ISE-PIC 시스템의 디스크 I/O사용률이 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 디스크 공간 사용률	Cisco ISE-PIC 시스템의 디스크 공간사용률이 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.

경보 이름	경보 설명	경보 해결 방법
높은 로드 평균	Cisco ISE-PIC 시스템의 로드 평균이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 메모리 사용률	Cisco ISE-PIC 시스템의 메모리 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 작업 DB 사용률	Cisco ISE-PIC 모니터링 노드의 syslog 데이터 볼륨이 예상보다 많습니다.	작업 데이터에 대한 컨피그레이션 제거 창을 확인하고 줄이십시오.
상태 사용 불가능	모니터링 노드가 Cisco ISE-PIC 노드에서 상태를 받지 못했습니다.	Cisco ISE-PIC 노드가 작동되어 실행 중인지 확인해 주십시오. Cisco ISE-PIC 노드가 모니터링 노드와 통신할 수 있는지 확인해 주십시오.
프로세스 작동 중지	Cisco ISE-PIC 프로세스 중 하나가 실행되고 있지 않습니다.	Cisco ISE-PIC 애플리케이션을 다시 시작해 주십시오.
OCSP 트랜잭션 임계값에 도달함	OCSP 트랜잭션 임계값에 도달했습니다. 이 경보는 내부 OCSP 서비스에서 많은 양의 트래픽이 발생하는 경우에 트리거됩니다.	시스템의 리소스가 충분한지 확인해 주십시오.
라이센싱		
PIC 라이센스 만료됨	Cisco ISE-PIC 노드에 설치된 라이센스가 만료되었습니다.	새 라이센스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
30일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 30일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.
60일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 60일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.

경보 이름	경보 설명	경보 해결 방법
90일 이내에 만료되는 PIC 라이선스	Cisco ISE-PIC 노드에 설치된 라이센스는 90일 후에 만료됩니다.	ISE-PIC 라이센스의 연장에 대해서는 Cisco 영업팀에 문의하십시오.
시스템 오류		
로그 수집 오류	Cisco ISE-PIC 모니터링 컬렉터 프로세스가 정책 서비스 노드에서 생성된 감사 로그를 유지할 수 없습니다.	이는 정책 서비스 노드의 실제 기능에는 영향을 미치지 않습니다. 추가적인 해결 방법은 TAC에 문의해 주십시오.
예약된 보고서 내보내기 실패	내보낸 보고서(CSV 파일)를 구성한 리포지토리에 복사할 수 없습니다.	구성한 리포지토리를 확인해 주십시오. 리포지토리가 삭제되었으면 다시 추가해 주십시오. 리포지토리를 사용할 수 없거나 리포지토리에 연결할 수 없는 경우 리포지토리를 유효한 리포지토리로 다시 구성해 주십시오.

사용자 또는 엔드포인트를 Cisco ISE-PIC에 추가하는 경우에는 경보가 트리거되지 않습니다.

알람 설정

다음 표에서는 **Alarm Settings(**알람 설정**)** 창(**Settings(**설정**)** > **Alarm Settings(**알람 설정**))**에 대해 설명합니다.

필드 이름	설명
알람 유형	알람 유형입니다.
경보 이름	알람의 이름입니다.
설명	알람에 대한 설명입니다.
제안 조치	알람이 트리거될 때 수행할 작업입니다.
상태	알람 규칙을 활성화하거나 비활성화합니다.
심각도	알람의 심각도 레벨을 선택합니다. 유효한 옵션은 다음과 같습니다. • Critical(위험) : 심각한 오류 상태를 나타냅니다. • Warning(경고): 정상적이기는 하지만 중요한 상태를 나타냅니다. 기본 상태입니다. • Info(정상): 정보 메시지를 나타냅니다.

필드 이름	설명
시스템 로그 메시지 보내기	Cisco ISE-PIC에서 생성하는 각 시스템 알람에 대해 시스템 로그 메시지를 보냅니다.
쉼표로 구분하여 여러 이메일 입력	이메일 주소 또는 ISE-PIC 관리자 이름 또는 둘 다의 목록입니다.
이메일 메모**(0 ~ 4,000**자**)**	시스템 알람과 연결하려는 맞춤형 텍스트 메시지.

맞춤형 경보 추가

Cisco ISE-PIC에는 5개의 기본 알람 유형(컨피그레이션 변경됨, 높은 디스크 I/O 사용률, 높은 디스크 공간 사용률, 높은 메모리 사용률 및 ISE 인증 비활성 등)이 포함되어 있습니다. Cisco에서 정의한 시스템 알람은 Alarms Settings(알람 설정) 페이지(Settings(설정) > Alarms Settings(알람 설정))에 나열됩니다. 시스템 알람만 편집할 수 있습니다.

기존 시스템 알람 외에도 기존 알람 유형에서 사용자 지정 알람을 추가, 수정 또는 삭제할 수 있습니다.

각 경보 유형에 대해 경보를 최대 5개까지 생성할 수 있으며 총 경보 수는 200개로 제한됩니다.

경보를 추가하려면 다음을 수행합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings (**설정**)> Alarm Settings (**알람 설정**)**를 선택합니다.

단계 **2** **Alarm Configuration(**알람 구성**)** 탭 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부사항을 입력합니다. 자세한 내용은 알람 설정 섹션을 참고하십시오.

알람 유형에 따라 Alarm Configuration(알람 컨피그레이션) 페이지에 추가 특성이 표시됩니다. 예를 들어 구성 변경 알람에 대해서는 Object Name(개체 이름), Object Type(개체 유형) 및 Admin Name(관리자 이름) 필드가 표시됩니다. 각기 기준이 다른 동일 경보의 여러 인스턴스를 추가할 수 있습니다.

단계 **4** 제출을 클릭합니다.

들어오는 트래픽을 검증하는 **TCP** 덤프 유틸리티

TCP 덤프 유틸리티는 패킷을 스니핑합니다. 이 패킷을 사용하여 예상 패킷이 노드에 도달했는지 확인할 수 있습니다. 예를 들어 보고서에 들어오는 인증 또는 로그인이 나타나 있지 않은 경우 들어오는 트래픽이 없거나 들어오는 트래픽이 Cisco ISE에 도달되지 않는다는 의심이 있을 수 있습니다. 이 경우 이 도구를 실행하여 검증할 수 있습니다.

네트워크 문제를 해결하는 데 도움이 되도록 TCP 덤프 옵션을 구성한 다음 네트워크 트래픽에서 데이터를 수집할 수 있습니다.

TCP 덤프를 사용하여 네트워크 트래픽 모니터링

TCP Dump(TCP 덤프) 페이지에는 사용자가 생성하는 TCP 덤프 프로세스 파일이 나열됩니다. 각기 다른 용도로 다른 파일을 생성하고 필요에 따라 실행한 다음 필요하지 않은 경우 삭제할 수 있습니다.

크기, 파일 수 및 프로세스 실행 기간을 지정하여 수집되는 데이터를 제어할 수 있습니다. 프로세스가 제한 시간 전에 완료되고 최대 크기보다 작은 파일 둘 이상을 활성화한 경우 프로세스가 계속 진행되고 다른 덤프 파일이 생성됩니다.

결합된 인터페이스를 포함하여 더 많은 인터페이스에서 TCP 덤프를 실행할 수 있습니다.

사람이 읽을 수 있는 형식은 더 이상 옵션으로 제공되지 않며, 덤프 파일은 항상 원시 형식입니다.

저장소에 대한 IPv6 연결을 지원합니다.

시작하기 전에

TCP 덤프 페이지의 네트워크 인터페이스 드롭다운 목록에는 IPv4 또는 IPv6 주소가 구성되어 있는 NIC(Network Interface Cards)만 표시됩니다. 기본적으로 VMware에서는 모든 NIC가 연결되어 있으므로 모든 NIC에 IPv6 주소가 있으며 네트워크 인터페이스 드롭다운 목록에 표시됩니다.

단계 **1** TCP 덤프 유틸리티의 소스로 **Host Name(**호스트 이름**)**을 선택합니다.

단계 **2** 드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다.

단계 **3** Filter(필터) 필드에 필터 기준으로 사용할 부울 식을 입력합니다.

다음과 같은 표준 tcpdump 필터 식이 지원됩니다.

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 및 not 10.77.122.119

단계 **4** 이 TCP 덤프 프로세스의 파일 이름을 입력합니다.

단계 **5** TCP 덤프 로그 파일을 저장할 저장소를 선택합니다.

단계 **6** **File Size(**파일 크기**)**—최대 파일 크기를 선택합니다.

덤프가 이 파일 크기를 초과하면 새 파일이 열려 덤프를 계속합니다. 덤프가 새 파일을 계속 사용할 수 있는 횟수는 **Limit to(**다음으로 제한**)** 설정을 기준으로 제한됩니다.

단계 **7** **Limit to(**다음으로 제한**)**—덤프가 확장 할 수 있는 파일의 수를 제한합니다.

단계 **8** **Time Limit(**시간 제한**)**—종료 전에 덤프가 실행되는 기간을 설정합니다.

단계 **9** 라디오 버튼을 클릭해 On(켜기) 또는 Off(끄기)로 설정하여 Promiscuous Mode(무차별 모드)를 설정합니다. 기본값은 On(켜기)입니다.

무차별 모드는 네트워크 인터페이스가 시스템 CPU로 모든 트래픽을 전달하는 기본 패킷 스니핑 모드입니다. 이 모드는 On(켜기)으로 설정해 두는 것이 좋습니다.

참고 Cisco ISE는 1500MTU(점보 프레임)보다 큰 프레임을 지원하지 않습니다.

TCP 덤프 파일 저장

시작하기 전에

TCP 덤프를 사용하여 네트워크 트래픽 모니터링 섹션의 설명에 따라 작업을 정상적으로 완료한 상태여야 합니다.

참고 Cisco ISE CLI를 통해 TCP 덤프에 액세스할 수도 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI* 참조 설명서를 참고해 주십시오.

단계 **1** **Format(**형식**)** 드롭다운 목록에서 옵션을 선택합니다. **Human Readable(**사람이 읽을 수 있음**)**이 기본값입니다.

단계 **2** **Download(**다운로드**)**를 클릭하고 원하는 위치로 이동한 후에 **Save(**저장**)**를 클릭합니다.

단계 **3** 이전 덤프 파일을 먼저 저장하지 않고 제거하려면 **Delete(**삭제**)**를 클릭합니다.

TCP 덤프 설정

다음 표에서는 네트워크 인터페이스에서 패킷의 내용을 모니터링하고 네트워크에서 나타나는 문제를 해결하는 데 사용할 수 있는 **tcpdump** 유틸리티 페이지의 필드에 대해 설명합니다. 이 페이지의 탐색 경로는 **Troubleshoot(**문제 해결**)**.

표 ***26: TCP*** 덤프 설정

옵션	사용 지침
상태	• Stopped(중지됨) - tcpdump 유틸리티가 실행되고 있지 않습니다. • Start(시작) - tcpdump 유틸리티의 네트워크 모니터링을 시작하려면 클릭합니다. • Stop(중지) - tcpdump 유틸리티를 중지하려면 클릭합니다.
Host Name(호스트 이름)	드롭다운 목록에서 모니터링할 호스트 이름을 선택합니다.

옵션	사용 지침
Network Interface(네트워크 인터페이스)	드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다. 참고 모든 NIC(Network Interface Cards)가 Cisco ISE 관리 포털에 표시되도록 IPv4 또는 IPv6 주소를 사용하여 구성해야 합니다.
Promiscuous Mode(무차별 모드)	• On(켜기) - 무차별 모드를 켜려면 클릭합니다(기본값). • Off(켜기) - 무차별 모드를 끄려면 클릭합니다. 무차별 모드는 기본 패킷 스니핑 모드로, On(켜기)으로 설정해 두는 것이 좋습니다. 이 모드에서는 네트워크 인터페이스가 모든 트래픽을 시스템 CPU로 전달합니다.
Filter(필터)	필터 기준으로 사용할 부울 식을 입력합니다. 지원되는 표준 tcpdump 필터 식: ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123
Format(형식)	tcpdump 파일의 형식을 선택합니다.
Dump File(덤프 파일)	다음과 같은 마지막 덤프 파일에 대한 데이터를 표시합니다. 관리자가 2011년 4월 27일 수요일 20:42:38(UTC)에 마지막으로 생성함 `파일 크기: 3,744바이트 형식: 원시 패킷 데이터 호스트 이름: Positron 네트워크 인터페이스: GigabitEthernet 0 무차별 모드: 설정` • Download(다운로드) - 최신 덤프 파일을 다운로드하려면 클릭합니다. • Delete(삭제) - 최신 덤프 파일을 삭제하려면 클릭합니다.

로깅 메커니즘

Cisco ISE-PIC 로깅 메커니즘

시스템 로그 제거 설정 구성

다음 프로세스를 사용하여 로컬 로그 저장 기간을 설정하고 특정 기간이 지난 후 로컬 로그를 삭제합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Logging(**기록**)** > **Local Log Settings(**로컬 로그 설정**)**.

단계 **2** **Local Log Storage Period(**로컬 로그 저장 기간**)** 필드에 로그 엔트리를 컨피그레이션 소스에 보관할 최대 기간을 일 단위로 입력합니다.

localStore 폴더의 크기가 97GB에 도달하면 구성된 **Local Log Storage Period(**로컬 로그 저장 기간**)**가 끝나기 전에 일찍 로그가 삭제될 수 있습니다.

단계 **3** 저장 기간이 만료되기 전에 언제든지 기존 로그 파일을 삭제하려면 **Delete Logs Now(**지금 로그 삭제**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

디버그 로그

디버그 로그에서는 부트스트랩, 애플리케이션 컨피그레이션, 런타임, 구축, 모니터링, 보고 및 PKI(Public Key Infrastructure) 정보를 캡처합니다. 지난 30일 동안의 위험 및 경고 경보와 지난 7일 동안의 정보 경보가 디버그 로그에 포함됩니다.

개별 구성 요소에 대한 디버깅 로그 심각도 수준을 구성할 수 있습니다.

노드 또는 구성 요소에 대해 Reset to Default(기본값으로 재설정) 옵션을 사용하여 로그 레벨을 공장에서 제공한 기본값으로 다시 재설정할 수 있습니다.

로컬 서버에 디버그 로그를 저장할 수 있습니다.

참고 시스템이 백업 또는 업그레이드에서 복원된 경우 디버그 로그 컨피그레이션은 저장되지 않습니다.

디버그 로그 심각도 수준 구성

디버그 로그의 심각도 레벨을 구성할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration** > **Logging(**로깅**)** > **Debug Log Configuration(**디버그 로그 구성**)**.

단계 **2** 노드를 선택하고 **Edit(**편집**)**를 클릭합니다.

Debug Log Configuration(디버그 로그 컨피그레이션) 페이지에는 선택한 노드에서 실행 중인 서비스를 기준으로 하는 구성 요소 목록과 개별 구성 요소에 대해 설정된 현재 로그 레벨이 표시됩니다.

노드 또는 구성 요소에 대해 **Reset to Default(**기본값으로 재설정**)** 옵션을 사용하여 로그 레벨을 공장에서 제공한 기본값으로 다시 재설정할 수 있습니다.

단계 **3** 로그 심각도 수준을 구성하려는 구성 요소를 선택하고 **Edit(**편집**)**를 클릭합니다. **Log Level(**로그 레벨**)** 드롭다운 목록에서 원하는 로그 심각도 수준을 선택하고 **Save(**저장**)**를 클릭합니다.

참고 런타임 AAA 구성 요소의 로그 심각도 수준을 변경하면 해당 하위 구성 요소 prrt-JNI의 로그 레벨도 변경됩니다. 하위 구성 요소 로그 레벨을 변경해도 부모 구성 요소에는 영향을 주지 않습니다.

Active Directory 문제 해결

Active Directory와 Cisco ISE-PIC 통합을 위한 사전 요건

이 섹션에서는 Cisco ISE-PIC와 통합되도록 Active Directory를 구성하는 데 필요한 수동 단계를 설명합니다. 그러나 대부분의 경우 Cisco ISE-PIC가 Active Directory를 자동으로 구성할 수 있습니다. Active Directory와 Cisco ISE-PIC 통합의 사전 요구 사항은 다음과 같습니다.

- Active Directory 도메인 구성을 변경하는 데 필요한 AD 도메인 관리자 자격 증명이 있어야 합니다.
- NTP(Network Time Protocol) 서버 설정을 사용하여 Cisco ISE-PIC 서버와 Active Directory 간에 시간을 동기화합니다. Cisco ISE-PIC CLI에서 NTP 설정을 구성할 수 있습니다.
- Cisco ISE-PIC를 가입시키는 도메인에 Cisco ISE-PIC에서 액세스할 수 있으며 작동 가능한 글로벌 카탈로그 서버가 하나 이상 있어야 합니다.

다양한 작업을 수행하는 데 필요한 **Active Directory** 계정 권한

가입 작업	탈퇴 작업	**Cisco ISE-PIC** 머신 계정
가입 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE-PIC 머신 계정이 있는지 확인하는 용도) • 도메인에 Cisco ISE-PIC 머신 계정 생성(머신 계정이 아직 없는 경우) • 새 머신 계정에서 속성 설정(예: Cisco ISE-PIC 머신 계정 비밀번호, SPN, dnsHostname)	탈퇴 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE-PIC 머신 계정이 있는지 확인하는 용도) • 도메인에서 Cisco ISE-PIC 머신 계정 제거 강제 탈퇴를 수행하는 경우(비밀번호 없이 탈퇴) 도메인에서 머신 계정이 제거되지 않습니다.	Active Directory 연결과의 통신에 사용되는 ISE-PIC 머신 계정에는 다음 권한이 필요합니다. • 비밀번호 변경 • 연락된 사용자 및 머신에 해당하는 사용자 및 머신 개체 읽기 • 정보(예: 신뢰할 수 있는 도메인, 대체 UPN 접미사 등)를 확인하기 위한 Active Directory 쿼리 • tokenGroups 속성 읽기 Active Directory에서 머신 계정을 미리 생성할 수 있습니다. SAM 이름이 Cisco ISE-PIC 어플라이언스 호스트 이름과 일치하는 경우 가입 작업 중에 해당 항목을 찾아서 재사용해야 합니다. 여러 가입 작업이 수행되는 경우 Cisco ISE-PIC 내에서 가입별로 하나씩 여러 머신 계정이 유지 관리됩니다.

참고 가입 또는 탈퇴 작업에 사용하는 크리덴셜은 Cisco ISE-PIC에 저장되지 않습니다. 새로 생성된 Cisco ISE-PIC 머신 계정 크리덴셜만 저장됩니다.

Microsoft Active Directory에서 네트워크 액세스**: SAM**에 대한 원격 호출을 허용하는 클라이언트 제한 보안 정책이 수정되었습니다. 이로 인해 Cisco ISE는 15일마다 머신 계정 암호를 업데이트하지 못할 수 있습니다. 머신 계정 암호가 업데이트되지 않으면 Cisco ISE는 Microsoft Active Directory를 통해 더 이상 사용자를 인증하지 않습니다. 이 이벤트에 대해 알 수 있도록 Cisco ISE 대시보드에서 **AD: ISE password update failed(AD: ISE** 암호 업데이트 실패**)** 알람을 받게 됩니다.

사용자는 보안 정책을 통해 로컬 SAM(Security Accounts Manager) 데이터베이스 및 Microsoft Active Directory의 사용자 및 그룹을 열거할 수 있습니다. Cisco ISE가 머신 계정 암호를 업데이트할 수 있도록 하려면 Microsoft Active Directory의 컨피그레이션이 정확한지 확인하십시오. 영향을 받는 Windows 운영체제 및 Windows Server 버전, 네트워크에 미치는 영향 및 필요한 변경 사항에 대한 자세한 내용은 다음을 참조하십시오.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

통신을 위해 열어 두어야 하는 네트워크 포트

프로토콜	포트(원격-로컬)	대상	참고
DNS(TCP/UDP)	49,152 이상의 난수	DNS 서버/AD 도메인 컨트롤러	—
MSRPC	445	도메인 컨트롤러	—
Kerberos(TCP/UDP)	88	도메인 컨트롤러	MS AD/KDC
LDAP(TCP/UDP)	389	도메인 컨트롤러	—
LDAP(GC)	3268	글로벌 카탈로그 서버	—
NTP	123	NTP 서버/도메인 컨트롤러	—
IPC	80	보조 ISE-PIC 노드용	—

Easy Connect ISE-PIC

ISE-PIC Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. Active Directory 서버를 올바르게 구성해야 ISE 사용자가 서버에 연결하여 사용자 로그인 정보를 가져올 수 있습니다. 다음 섹션에서는 ISE-PIC를 지원하도록 Active Directory 도메인 컨트롤러를 구성하는 방법을 확인할 수 있습니다(Active Directory 측에서의 구성).

를 지원하도록 Active Directory 도메인 컨트롤러를 구성하려면(Active Directory 측에서의 구성) 다음 단계를 따르십시오.

참고 모든 도메인에서 모든 도메인 컨트롤러를 구성해야합니다.

1. ISE-PIC에서 Active Directory 조인 포인트 및 도메인 컨트롤러를 설정합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE-PIC 노드 가입, 20 페이지 및 도메인 컨트롤러 추가, 22 페이지를 참조하십시오.
2. 도메인 컨트롤러별 WMI를 구성합니다. 패시브 ID용 WMI 구성, 24 페이지를 참조하십시오.
3. Active Directory에서 다음 단계를 수행합니다.
   - 다음에 대한 Active Directory 설정 구성 패시브 ID 서비스, 174 페이지
4. (선택 사항) 다음 단계를 수행하여 Active Directory에서 ISE로 수행하는 자동 구성 문제를 해결합니다.
   - Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정, 177 페이지

• 도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한, 177 페이지
• 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 179 페이지
• WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 180 페이지
• AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여, 181 페이지

다음에 대한 Active Directory 설정 구성 패시브 ID 서비스

ISE-PIC Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. ISE-PIC는 Active Directory에 연결하여 사용자 로그인 정보를 가져옵니다.

Active Directory 도메인 컨트롤러에서 다음 단계를 수행해야 합니다.

단계 **1** 관련 Microsoft 패치가 Active Directory 도메인 컨트롤러에 설치되어 있는지 확인합니다.

a) Windows Server 2008에는 다음 패치가 필요합니다.

- http://support.microsoft.com/kb/958124

  이 패치는 Microsoft의 WMI에서 메모리 누수를 수정하여, ISE가 도메인 컨트롤러와의 성공적인 연결을 설정할 수 없게 합니다.

- http://support.microsoft.com/kb/973995

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 다른 메모리 유출을 수정합니다.

b) Windows Server 2008 R2에는 다음 패치가 필요합니다(SP1이 설치되어 있지 않은 경우).

- http://support.microsoft.com/kb/981314

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 메모리 유출을 수정합니다.

- http://support.microsoft.com/kb/2617858

  이 패치는 Windows Server 2008 R2에서 예기치 않게 발생하는 느린 시작 또는 로그인 프로세스를 수정합니다.

c) Windows 플랫폼의 WMI 관련 문제의 경우 다음 링크에 나열되어 있는 패치가 필요합니다.

- http://support.microsoft.com/kb/2591403

이러한 핫픽스는 WMI 서비스 및 관련 구성 요소의 작동 및 기능과 연관되어 있습니다.

단계 **2** Active Directory가 Windows 보안 로그에 사용자 로그인 이벤트를 기록하는지 확인합니다.

Audit Policy(감사 정책) 설정(Group Policy Management(그룹 정책 관리) 설정의 일부분)의 설정이 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 정상 로그온을 허용하는지 확인합니다(이는 기본 Windows 설정이지만 이 설정이 올바른지를 명시적으로 확인해야 함).

단계 **3** ISE-PIC가 Active Directory에 연결하려면 Active Directory 사용자에게 충분한 권한이 있어야 합니다. 다음 지침에서는 관리 도메인 그룹 사용자 또는 비관리 도메인 그룹 사용자에 대한 권한을 정의하는 방법을 보여줍니다.

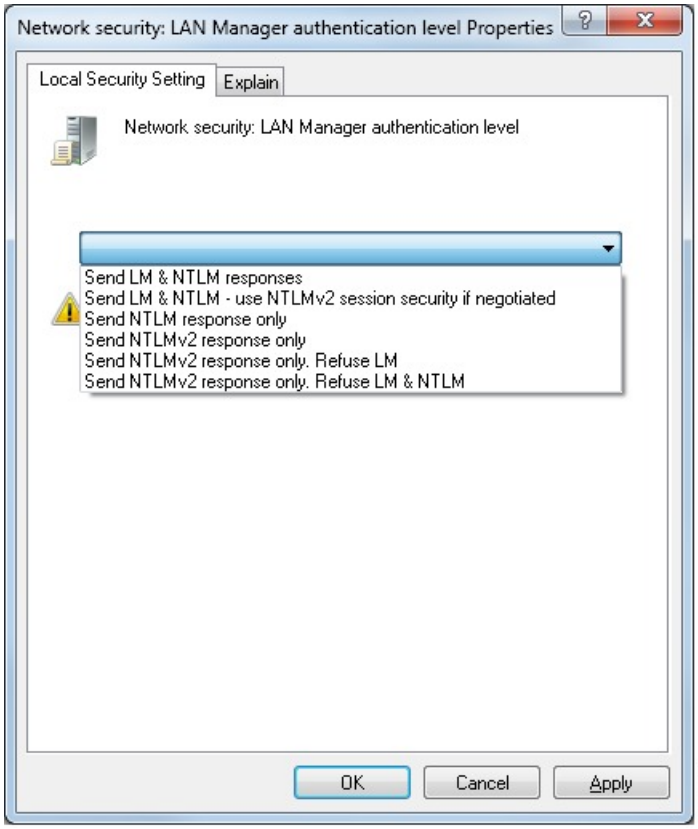
- Active Directory 사용자가 도메인 관리자 그룹의 멤버인 경우 필요한 권한
- Active Directory 사용자가 도메인 관리자 그룹의 멤버가 아닌 경우 필요한 권한

단계 **4** ISE-PIC에서 사용하는 Active Directory 사용자는 NTLM(NT LAN Manager) v1 또는 v2로 인증할 수 있습니다. ISE-PIC와 Active Directory 도메인 컨트롤러 간에 정상적으로 인증된 연결을 위해 Active Directory NTLM 설정이 ISE-PIC NTLM 설정과 일치하는지를 확인해야 합니다. 다음 표에는 모든 Microsoft NTLM 옵션과 지원되는 ISE-PIC NTLM 작업이 나와 있습니다. ISE-PIC가 NTLMv2로 설정되어 있으면 설명된 6개 옵션이 모두 지원됩니다. ISE-PIC가 NTLMv1을 지원하도록 설정되어 있으면 처음 5개 옵션만 지원됩니다.

표 ***27: ISE-PIC*** 및 ***AD NTLM*** 버전 설정에 따라 지원되는 인증 유형

ISE-PIC NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM response(LM 및 NTLM 응답 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send LM & NTLM - use NTLMv2 session security if negotiated(LM 및 NTLM 전송 - 협상 시 NTLMv2 세션 보안 사용) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLM response only(NTLM 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only(NTLMv2 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM(NTLMv2 응답만 전송하고 LM은 거부) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM & NTLM(NTLMv2 응답만 전송하고 LM 및 NTLM은 거부) 연결이 거부됨 연결이 허용됨	연결이 거부됨	연결이 허용됨

그림 *7: MS NTLM* 인증 유형 옵션



단계 **5** Active Directory 도메인 컨트롤러에서 `dllhost.exe`에 대한 트래픽을 허용하는 방화벽 규칙을 생성했는지 확인합니다.

방화벽을 끄거나, 특정 IP(ISE-PIC IP 주소)에서의 다음 포트에 대한 액세스를 허용할 수 있습니다.

- TCP 135: 일반 RPC 포트입니다. 비동기 RPC 호출을 수행하는 경우, 이 포트에서 수신 대기하는 서비스는 이 요청을 서비스하는 구성 요소에서 사용 중인 포트를 클라이언트에 알립니다.
- UDP 137: Netbios 이름 확인
- UDP 138: Netbios 데이터그램 서비스
- TCP 139: Netbios 세션 서비스
- TCP 445: SMB

더 많은 포트를 동적으로 할당되거나 수동으로 구성할 수 있습니다. 대상으로 %SystemRoot%\System32\dllhost.exe를 추가하는 방법을 권장합니다. 이 프로그램은 포트를 동적으로 관리합니다.

모든 방화벽 규칙을 특정 IP(ISE-PIC IP)에 할당할 수 있습니다.

Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정

Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2의 경우 도메인 관리자 그룹에는 기본적으로 Windows 운영체제의 특정 레지스트리 키에 대한 모든 권한이 없습니다. Microsoft Active Directory 관리자는 Microsoft Active Directory 사용자에게 다음 레지스트리 키에 대한 모든 권한을 부여해야 합니다.

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

다음 Microsoft Active Directory 버전의 경우에는 레지스트리를 변경할 필요가 없습니다.

- Windows 2003
- Windows 2003R2
- Windows 2008

모든 권한을 부여하려면 Microsoft Active Directory 관리자가 먼저 다음과 같이 키 소유권을 가져와야 합니다.

단계 **1** 키 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Owner(**소유자**)** 탭을 선택합니다.

단계 **2** **Permissions(**권한**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한

Windows 2012 R2의 경우 Microsoft AD 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여합니다.

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell에서 다음 명령을 사용하여 레지스트리 키에 대한 전체 권한이 부여되었는지 확인합니다.

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD 사용자가 도메인 관리자 그룹에는 없지만 도메인 사용자 그룹에는 있으면 다음 권한이 필요합니다.

- ISE-PIC가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

- 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 179 페이지
- WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 180 페이지

이러한 권한은 다음 Microsoft AD 버전에만 필요합니다.

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

ISE-PIC가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

ISE-PIC가 도메인 사용자로 연결하여 로그인 인증 이벤트를 검색할 수 있게 하려면 도메인 컨트롤러에 일부 레지스트리 키를 수동으로 추가해야 합니다. 도메인 컨트롤러 또는 도메인의 머신에서 에이전트는 필요하지 않습니다.

다음 레지스트리 스크립트에는 추가할 키가 나와 있습니다. 이 스크립트를 복사하여 텍스트 파일에 붙여 넣고 파일을 .reg 확장자로 저장한 다음 파일을 더블 클릭하여 레지스트리를 변경합니다. 레지스트리 키를 추가하려면 사용자가 루트 키의 소유자여야 합니다.

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"=" "
[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}] "DllSurrogate"="
 "
```

DllSurrogate 키의 값에는 공백이 두 개 포함되어야 합니다. 레지스트리를 수동으로 업데이트하는 경우 두 개의 공백만 포함하고 따옴표는 포함하지 않아야 합니다. 레지스트리를 수동으로 업데이트하는 동안 AppID, DllSurrogate 및 해당 값에 따옴표가 포함되지 않았는지 확인하십시오.

파일 맨 끝의 빈 줄을 포함하여 위 스크립트에 나와 있는 빈 줄은 그대로 유지합니다.

Windows 명령 프롬프트에서 다음 명령을 사용하여 레지스트리 키가 생성되었고 올바른 값을 가지고 있는지 확인합니다.

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e`

도메인 컨트롤러에서 **DCOM**을 사용하기 위한 권한

ISE-PIC 패시브 ID 서비스에 사용되는 Active Directory 사용자는 도메인 컨트롤러에서 DCOM을 사용할 권한이 있어야 합니다. **dcomcnfg** 명령줄 툴을 사용하여 권한을 구성하십시오.

단계 **1** 명령줄에서 **dcomcnfg** 툴을 실행합니다.

단계 **2** **`Component Services`**(구성 요소 서비스)를 펼칩니다.

단계 **3** 확장 컴퓨터 > 내 컴퓨터 .

단계 **4** 메뉴 모음에서 **Action(**작업**)**을 선택하고 **properties(**속성**)**를 클릭한 후 **COM Security(COM** 보안**)**를 클릭합니다.

단계 **5** Cisco ISE가 Access(액세스) 및 Launch(실행)에 모두 사용할 계정에 Allow(허용) 권한이 있는지 확인합니다. 해당 AMicrosoft Active Directory 사용자를 4개 옵션(**Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 모두에 대한 **Edit Limits(**제한 편집**)**와 **Edit Default(**기본값 편집**))**에 모두 추가해야 합니다.

단계 **6** **Access Permission(**액세스 권한**)** 및 **Launch and Activation Permission(**실행 및 활성화 권한**)** 둘 다에 대해 Local Access(로컬 액세스) 및 Remote Access를 모두 Allow(허용)합니다.

그림 ***8:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

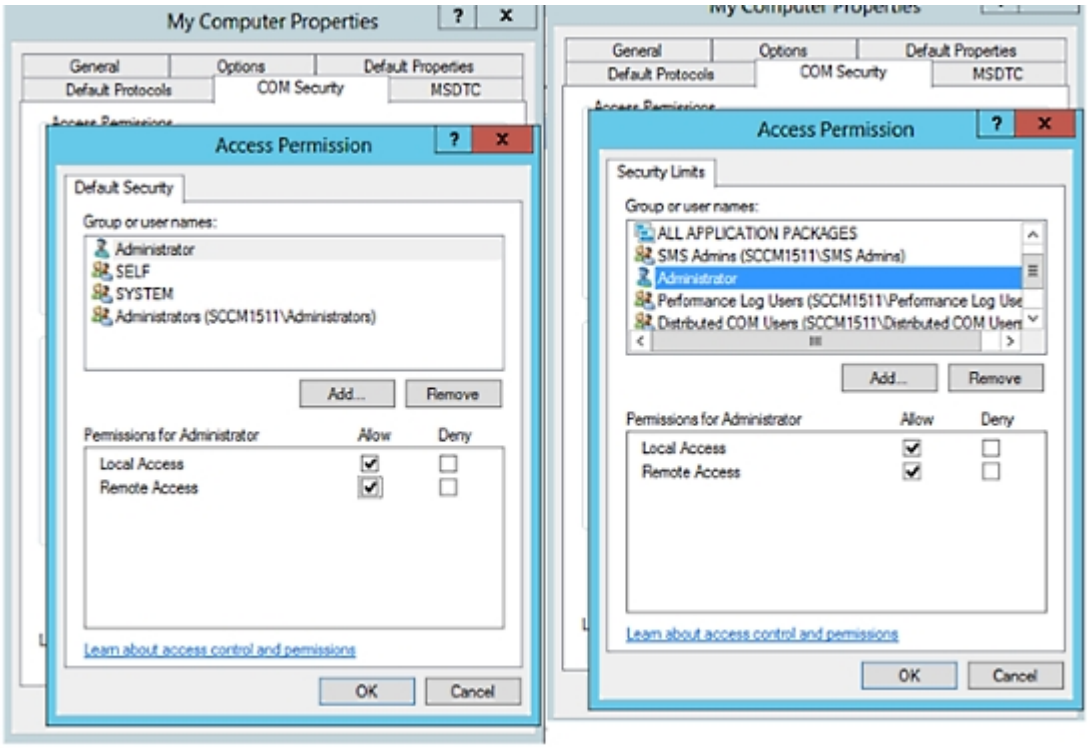
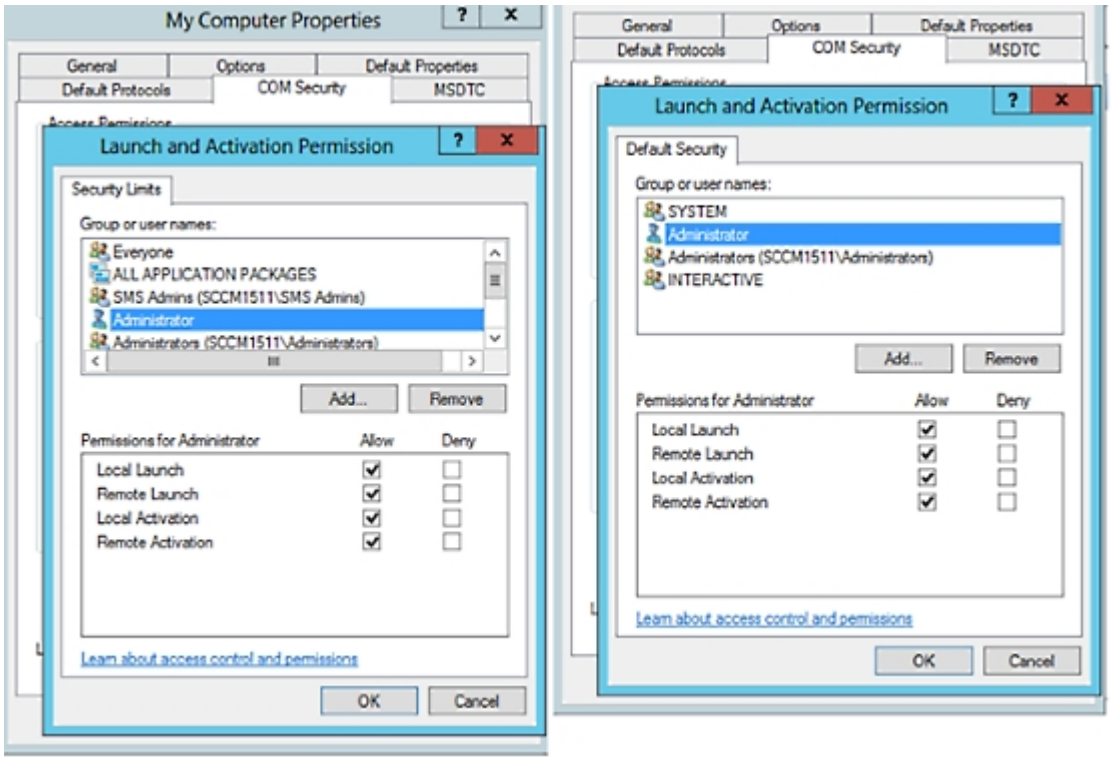


그림 *9:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

기본적으로 Microsoft Active Directory 사용자에게는 방법 실행 및 원격 활성화에 대한 권한이 없습니다. wmimgmt.msc MMC 콘솔을 사용하여 액세스 권한을 부여할 수 있습니다.

단계 **1** 다음 메뉴를 선택합니다. **Start(**시작**)** > **Run(**실행**)** 그런 다음 `wmimgmt.msc`를 입력합니다.

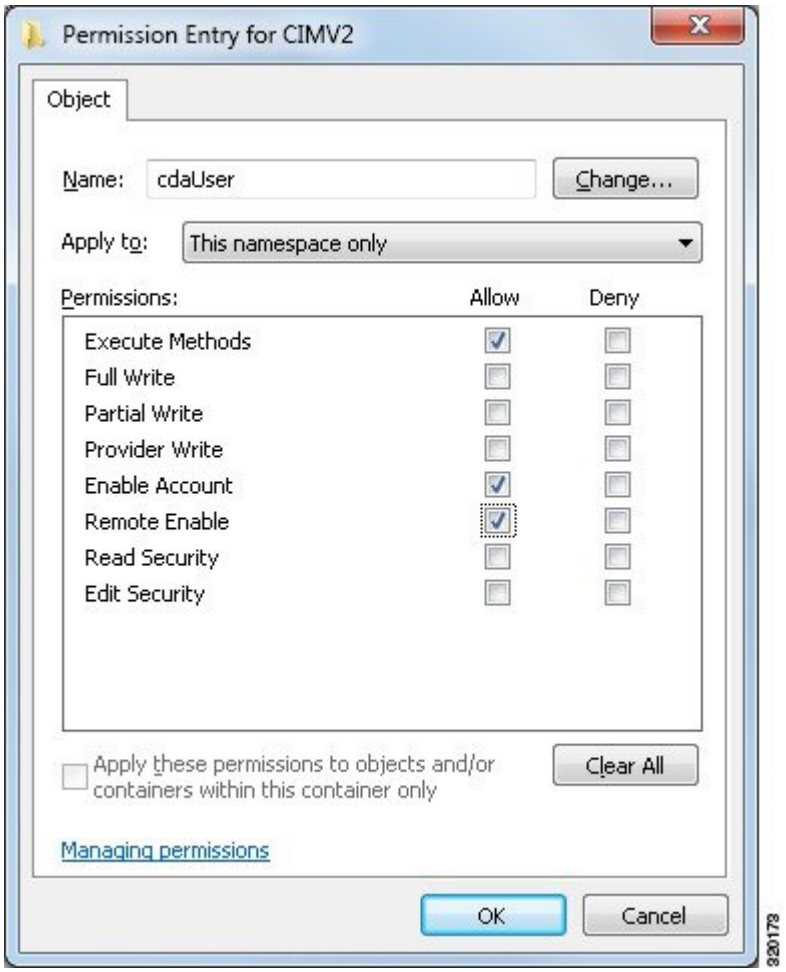
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

단계 **3** **Security(**보안**)** 탭에서 **Root(**루트**)**를 펼치고 **CIMV2**를 선택합니다.

단계 **4** **Security(**보안**)**를 클릭합니다.

단계 **5** Active Directory 사용자를 추가하고 아래 이미지에 나와 있는 대로 필요한 권한을 구성합니다.

그림 *10: WMI Root\CIMv2* 이름 공간에 필요한 권한



AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여

Windows 2008 이상에서는 Event Log Readers라는 그룹에 ISE-PIC ID 매핑 사용자를 추가하여 AD 도메인 컨트롤러 로그에 대한 액세스 권한을 부여할 수 있습니다.

모든 이전 버전 Windows에서는 아래에 나와 있는 것처럼 레지스트리 키를 편집해야 합니다.

단계 **1** 보안 이벤트 로그에 대한 액세스 권한을 위임하려면 계정의 SID를 찾습니다.

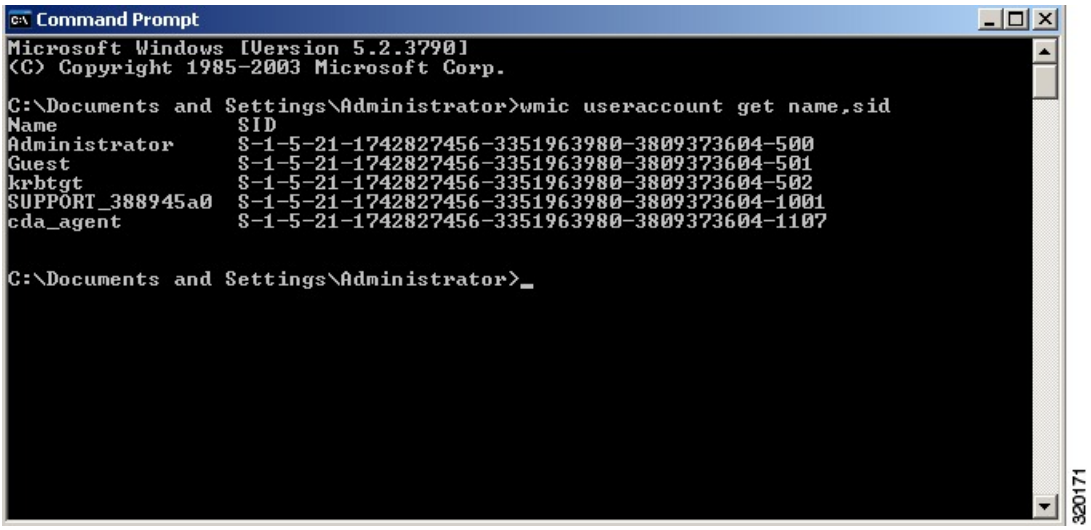
단계 **2** 명령줄에서 다음 명령을 사용하여 모든 SID 계정을 나열합니다. 이 명령은 아래 다이어그램에도 나와 있습니다.

```
wmic useraccount get name,sid
```

특정 사용자 이름 및 도메인의 경우 다음 명령을 사용할 수도 있습니다.

```
wmic useraccount where name="iseUser" get domain,name,sid
```

그림 *11:* 모든 *SID* 계정 나열



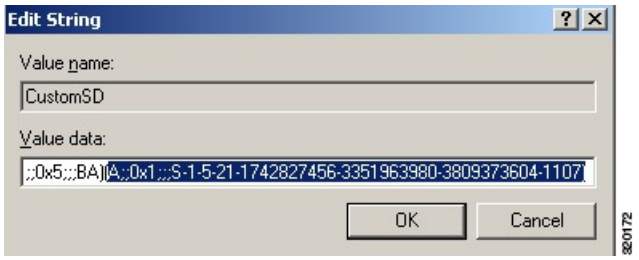
단계 **3** SID를 찾고 레지스트리 편집기를 연 후에 다음 위치로 이동합니다.

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

단계 **4** **Security(**보안**)**를 클릭하고 **CustomSD**를 두 번 클릭합니다.

예를 들어 ise_agent 계정 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`에 읽기 권한을 허용하려면 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`을 입력합니다.

그림 *12: CustomSD* 문자열 편집



단계 **5** 도메인 컨트롤러에서 WMI 서비스를 다시 시작합니다. 다음과 같이 두 가지 방법으로 WMI 서비스를 다시 시작할 수 있습니다.

a) CLI에서 다음 명령을 실행합니다.

net stop winmgmt

net start winmgmt

b) `Services.msc`를 실행합니다. 그러면 Windows 서비스 관리 툴이 열립니다. Windows 서비스 관리 윈도우에서 **Windows Management Instrumentation** 서비스를 찾아 마우스 오른쪽 버튼으로 클릭한 후에 **Restart(**다시 시작**)**를 선택합니다.

추가 문제 해결 정보 얻기

Cisco ISE-PIC에서는 관리 포털에서 지원 및 문제 해결 정보를 다운로드할 수 있습니다. 지원 번들을 사용하면 Cisco TAC(Technical Assistance Center)가 Cisco ISE-PIC의 문제 해결을 위한 진단 정보를 준비할 수 있습니다.

참고 TAC용 고급 문제 해결 정보를 제공하는 지원 번들과 디버그 로그는 해석하기가 어렵습니다. Cisco ISE-PIC에서 제공하는 다양한 보고서 및 문제 해결 도구를 사용하여 네트워크에서 발생하는 문제를 진단하고 해결할 수 있습니다.

Cisco ISE-PIC 지원 번들

지원 번들에 포함시킬 로그를 구성할 수 있습니다. 예를 들어 디버그 로그에 포함되도록 특정 서비스의 로그를 구성할 수 있습니다. 날짜를 기준으로 로그를 필터링할 수도 있습니다.

다운로드할 수 있는 로그는 다음과 같이 분류될 수 있습니다.

- 전체 구성 데이터베이스: 사람이 읽을 수 있는 XML 형식의 Cisco ISE-PIC 구성 데이터베이스를 포함합니다. 문제를 해결할 때 이 데이터베이스 구성을 다른 Cisco ISE 노드로 가져와 시나리오를 다시 생성할 수 있습니다.
- 디버그 로그: 부트스트랩, 애플리케이션 구성, 런타임, 구축, PKI(Public Key Infrastructure) 정보와 모니터링 및 보고 로그를 캡처합니다.

  디버그 로그는 특정 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그를 사용하려면 11장, "로깅"을 참고해 주십시오. 디버그 로그를 사용하지 않으면 모든 정보 메시지(INFO)가 지원 번들에 포함됩니다. 자세한 내용은 Cisco ISE-PIC 디버그 로그, 185 페이지를 참고하십시오.
- 로컬 로그: Cisco ISE에서 실행되는 다양한 프로세스의 시스템 로그 메시지를 포함합니다.
- 코어 파일: 크래시의 원인을 식별하는 데 도움이 되는 중요한 정보를 포함합니다. 이 로그는 애플리케이션이 크래시될 때 생성되며 힙 덤프를 포함합니다.
- 모니터링 및 보고 로그: 알림 및 보고서에 대한 정보를 포함합니다.
- 시스템 로그: Cisco ADE(Application Deployment Engine) 관련 정보를 포함합니다.
- 정책 구성: Cisco ISE에서 사람이 읽을 수 있는 형식으로 구성된 정책을 포함합니다.

Cisco ISE CLI에서 **backup-logs** 명령을 사용하여 이러한 로그를 다운로드할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI* 참조 설명서를 참고해 주십시오.

관리 포털에서 이러한 로그를 다운로드하도록 선택하는 경우 다음과 같이 해 주십시오.

- 디버그 로그 또는 시스템 로그 등의 로그 유형에 따라 로그 하위 집합만 다운로드합니다.

- 선택한 로그 유형에 대한 마지막 *n* 번호 파일만 다운로드합니다. 이 옵션을 사용하면 지원 번들의 크기와 다운로드에 소요되는 시간을 제어할 수 있습니다.

모니터링 로그는 모니터링, 보고 및 문제 해결 기능에 대한 정보를 제공합니다. 로그 다운로드에 대한 자세한 내용은 Cisco ISE-PIC 로그 파일 다운로드, 184 페이지를 참고하십시오.

지원 번들

지원 번들을 단순 tar.gpg 파일로 로컬 컴퓨터에 다운로드할 수 있습니다. 지원 번들은 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 형식으로 날짜 및 타임스탬프를 사용하여 이름이 지정됩니다. 브라우저에서 지원 번들을 적절한 위치에 저장하도록 메시지를 표시합니다. 지원 번들 내용을 추출하여 README.TXT 파일을 볼 수 있습니다. 이 파일에는 지원 번들의 내용과 함께 지원 번들에 포함되어 있는 ISE 데이터베이스의 내용을 가져오는 방법이 설명되어 있습니다.

Cisco ISE-PIC 로그 파일 다운로드

네트워크에서 문제를 해결하는 동안 자세한 정보를 확인하기 위해 Cisco ISE-PIC 로그 파일을 다운로드할 수 있습니다.

설치 및 업그레이드 문제를 해결하기 위해 ADE-OS가 포함된 시스템 로그 및 기타 로그 파일을 다운로드할 수도 있습니다.

시작하기 전에

- 디버그 로그 및 디버그 로그 레벨을 구성해야 합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Logging(기록)** > **Download Logs(로그 다운로드)** > **Appliance node list(어플라이언스 노드 목록)**.

단계 **2** 지원 번들을 다운로드할 노드를 클릭합니다.

단계 **3** **Support Bundle(지원 번들)** 탭에서 지원 번들에 입력할 매개변수를 선택합니다.

모든 로그를 포함하는 경우 지원 번들이 매우 커지며 다운로드 시간이 오래 걸립니다. 다운로드 프로세스를 최적화하려면 최근 *n*개 파일만 다운로드하도록 선택합니다.

단계 **4** 지원 번들을 생성할 시작 및 종료 날짜를 입력합니다.

단계 **5** 다음 중 하나를 선택합니다.

- Public Key Encryption(공개 키 암호화): 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 선택합니다.
- Shared Key Encryption(공유 키 암호화): 온프레미스에서 로컬로 문제를 해결하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 지원 번들의 암호화 키를 입력해야 합니다.

단계 **6** **Create Support Bundle(지원 번들 생성)**을 클릭합니다.

단계 **7** **Download(다운로드)**를 클릭하여 새로 생성한 지원 번들을 다운로드합니다.

지원 번들은 애플리케이션 브라우저를 실행 중인 클라이언트 시스템에 다운로드되는 tar.gpg 파일입니다.

다음에 수행할 작업

특정 구성 요소에 대한 디버그 로그를 다운로드합니다.

Cisco ISE-PIC 디버그 로그

디버그 로그는 다양한 Cisco ISE-PIC 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그에는 최근 30일 내에 생성된 위험 및 경고 경보와 함께 최근 7일 내에 생성된 정보 경보가 포함됩니다. 문제를 보고하는 동안 이러한 디버그 로그를 사용하고 문제 진단 및 확인을 위해 해당 로그를 보낼지 묻는 메시지가 표시될 수 있습니다.

참고 디버그 로그의 모니터링 등 로드가 많은 디버그 로그를 활성화하면 높은 로드에 대한 알람이 생성될 수 있습니다.

디버그 로그 가져오기

단계 **1** 디버그 로그를 가져올 구성 요소를 구성합니다.

단계 **2** 디버그 로그를 다운로드합니다.

Cisco ISE-PIC 구성 요소 및 해당 디버그 로그

참고 아래 목록은 ISE에서 사용 가능한 전체 구성 요소 목록입니다. 표에 나열된 일부 구성 요소는 ISE-PIC

와 관련이 없을 수 있습니다.

표 ***28:*** 구성 요소 및 해당 디버그 로그

구성 요소	디버그 로그
Active Directory	ad_agent.log
Cache Tracker	tracking.log
EDF(Entity Definition Framework)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log

구성 요소	디버그 로그
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
게스트 액세스 관리자	guest.log
게스트 액세스	guest.log
MyDevices	guest.log
포털	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log

구성 요소	디버그 로그
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

디버그 로그 다운로드

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Logging(**기록**)** > **Download Logs(**로그 다운로드**)**.

단계 **2** Appliance node(어플라이언스 노드) 목록에서 디버그 로그를 다운로드할 노드를 클릭합니다.

단계 **3** **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

디버그 로그 유형 및 디버그 로그의 목록이 표시됩니다. 이 목록은 디버그 로그 컨피그레이션을 기반으로 합니다.

단계 **4** 다운로드하려는 로그 파일을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에 저장합니다.

필요에 따라 이 프로세스를 반복하여 다른 로그 파일을 다운로드할 수 있습니다. **Debug Logs(**디버그 로그**)** 창에서 다운로드할 수 있는 추가 디버그 로그는 다음과 같습니다.

- isebootstrap.log: 부트스트래핑 로그 메시지를 제공합니다.
- monit.log: Watchdog 메시지를 제공합니다.
- pki.log - 타사 암호화 라이브러리 로그를 제공합니다.
- iseLocalStore.log: 로컬 저장소 파일에 대한 로그를 제공합니다.
- ad_agent.log: Microsoft Active Directory 타사 라이브러리 로그를 제공합니다.

- catalina.log: 타사 로그를 제공합니다.