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 항목을 참조하십시오.

다음과 같은 제공자 유형을 정의할 수 있습니다.

표 *1:* 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
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, 3 페이지
엔드포인트	다른 구성된 프로브와 함께 백그라운드에서 항상 실행되어 사용자가 여전히 연결되어 있는지를 확인합니다.		WMI	사용자가 계속 연결되어 있는지 여부	엔드포인트 프로브, 37 페이지
SPAN			SPAN(스위치에 설치됨) 및 Kerberos 메시지	• 사용자 이름 • IP 주소 • 도메인	SPAN, 13 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, 8 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), 15 페이지

- Active Directory 에이전트, 3 페이지
- 설정 관리, 8 페이지
- SPAN, 13 페이지
- Syslog Providers(시스템 로그 제공자), 15 페이지
- 패시브 ID 서비스 필터링, 37 페이지
- 엔드포인트 프로브, 37 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 Directory를 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 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 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성 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, 7 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 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 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성 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, 7 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, 4 페이지를 참조하십시오.

표 ***2: 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 ***3:*** 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 항목을 참조하십시오.
3. 패시브 ID 서비스용 ISE-PIC REST 서비스에 대한 Bridge(브리지)를 구성합니다., 9 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 클라이언을 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 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, 10 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 클라이언를 설정합니다. ISE-PIC REST Service로 API Calls(API 호출) 전송, 10 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., 9 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., 9 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, 11 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 *4: 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, 10 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, 14 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 ***5: 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, 16 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, 22 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, 16 페이지의 내용을 참조하십시오.
- 단일 메시지 헤더를 사용자 지정합니다. 시스템 로그 헤더 사용자 지정, 22 페이지의 내용을 참조하십시오.
- 템플릿을 생성하여 메시지 본문을 사용자 지정합니다. 시스템 로그 메시지 본문 사용자 지정, 21 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, 26 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, 16 페이지 항목 참조) 필요하다면 메시지 템플릿을 생성하여(자세한 내용은 시스템 로그 메시지 본문 사용자 지정, 21 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 ***6: 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, 22 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, 21 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, 26 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, 26 페이지을 참조하십시오.

다음을 사용자 맞춤화할 수 있습니다.

- 단일 메시지 헤더—시스템 로그 헤더 사용자 지정, 22 페이지
- 복수 메시지 본문—시스템 로그 메시지 본문 사용자 지정, 21 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, 16 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, 23 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, 23 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

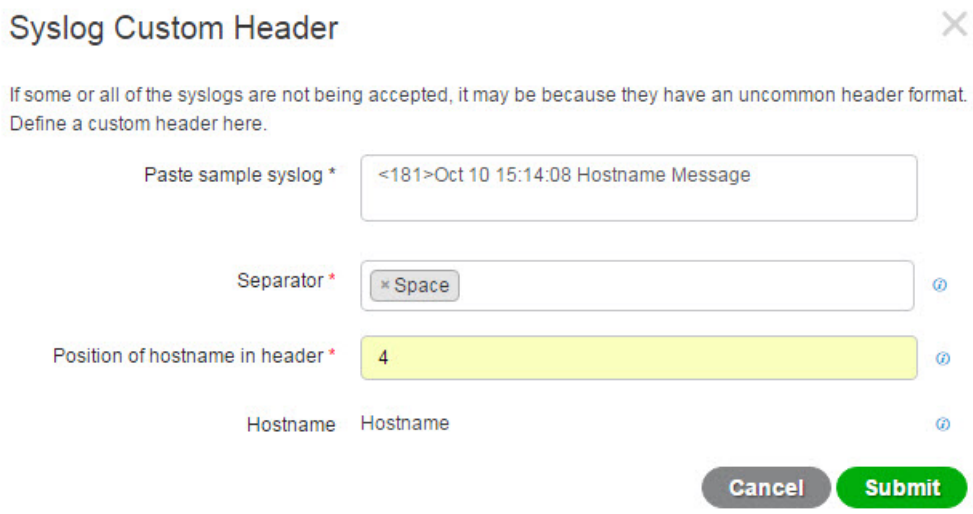
구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다.

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 ***1:*** 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 9: 맞춤형 템플릿용 정규식, 26 페이지 항목을 참고하십시오.

표 *7:* 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 9: 맞춤형 템플릿용 정규식, 26 페이지 항목을 참고하십시오.

표 *8:* 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 *9:* 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, 22 페이지 항목을 참조하십시오. 본문 사용자 지정에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 지정, 21 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, 22 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, 26 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, 26 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, 26 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, 26 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, 26 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, 26 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, 26 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, 26 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, 26 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}|[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, 26 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.

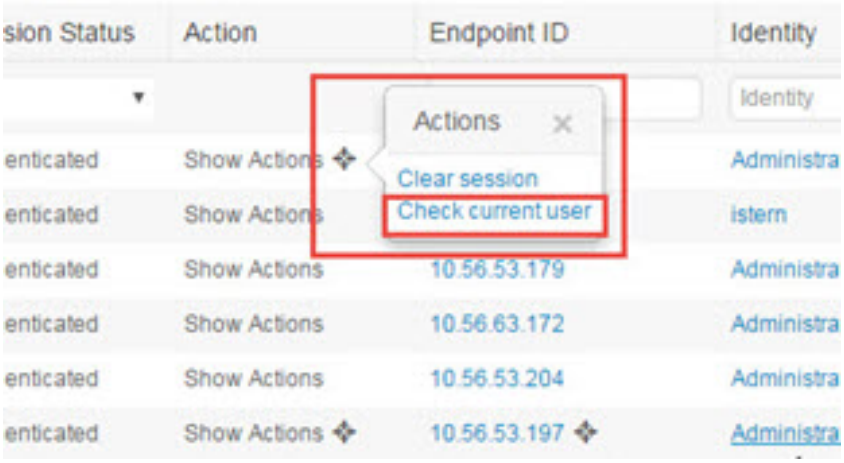
엔드포인트 프로브

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, 39 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 *2:* 현재 사용자 확인



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

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 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.