ISE 서비스, 목적 및 문제 해결 이해

목차

소개

이 문서에서는 ISE 서비스, 목적 및 문제 해결에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco Identity Services Engine에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서는 Cisco Identity Services Engine의 특정 소프트웨어 및 하드웨어 버전으로 제한되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Cisco ISE(Identity Services Engine)는 중앙 집중식 AAA(Policy Management, Authentication, Authorization, and Accounting)를 통해 고급 네트워크 보안을 제공하도록 설계된 포괄적인 솔루션입니다. 이를 통해 조직은 사용자, 장치 및 애플리케이션에 대한 네트워크 액세스를 관리하면서 보안, 규정 준수 및 원활한 사용자 환경을 보장할 수 있습니다.

이러한 목표를 달성하기 위해 Cisco ISE는 다양한 서비스를 사용하며, 각각은 시스템이 효율적으로 작동하도록 하는 특정 작업을 담당합니다. 이러한 서비스는 함께 작동하여 안전한 네트워크 액세스, 강력한 정책 시행, 자세한 로깅, 외부 시스템과의 원활한 통합, 효율적인 장치 프로파일링을 보장합니다.

ISE의 각 서비스는 솔루션의 무결성과 가용성을 유지하는 데 중요한 역할을 합니다. 일부 서비스는 데이터베이스 관리 및 인증과 같은 핵심 기능을 처리하는 반면, 다른 서비스는 장치 프로파일링, 인증서 관리 및 모니터링과 같은 고급 기능을 지원합니다.

이 문서에서는 Cisco ISE의 다양한 서비스에 대한 개요를 제공하고, 문제가 발생할 경우 그 목적, 중요성 및 잠재적인 문제 해결 단계를 설명합니다. 관리자 또는 네트워크 보안 전문가와 상관없이 이러한 서비스를 이해하면 ISE 구축이 원활하고 안전하게 실행되도록 보장할 수 있습니다.

ISE 서비스 이해 및 문제 해결

스크린샷에 언급된 서비스는 ISE에서 해당 기능을 지원하기 위해 활용됩니다. ISE 노드의 CLI를 통해 show application status ise 명령을 사용하여 ISE에서 사용 가능한 상태를 확인합니다. 다음은 ISE의 상태 또는 사용 가능한 서비스를 보여 주는 샘플 출력입니다.

```
honey/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          4101512
Database Server                        running          107 PROCESSES
Application Server                     running          4118209
Profiler Database                      running          4108739
ISE Indexing Engine                    running          4119606
AD Connector                           running          4121671
M&T Session Database                   running          4114154
M&T Log Processor                      running          4118388
Certificate Authority Service          running          4121560
EST Service                            running          61939
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          4105571
ISE API Gateway Database Service       running          4107770
ISE API Gateway Service                running          4113275
ISE pxGrid Direct Service              running          36228
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
ISE Node Exporter                      running          4122893
ISE Prometheus Service                 running          4124896
ISE Grafana Service                    running          4128455
ISE MNT LogAnalytics Elasticsearch     running          4130784
ISE Logstash Service                   running          4135868
ISE Kibana Service                     running          4137540
ISE Native IPSec Service               running          4142286
MFC Profiler                           running          52667
```

ISE에서 사용할 수 있는 서비스입니다.

이제 각 서비스에 대해 자세히 살펴보겠습니다.

데이터베이스 수신기

데이터베이스 리스너 서비스는 ISE와 데이터베이스 서버 간의 통신을 관리하는 데 도움이 되는 중요한 구성 요소입니다. ISE는 데이터베이스와 관련된 요청을 수신 대기하고 처리하며, ISE 시스템이 기본 데이터베이스에서 읽고 쓸 수 있도록 합니다.

ISE의 데이터베이스 리스너 서비스에 대한 주요 내용

1. 통신 인터페이스: ISE와 데이터베이스 서버 간의 통신 브리지 역할을 하여 시스템이 사용자 자격 증명, 세션 정보, 네트워크 정책 등과 같은 데이터를 검색하고 저장할 수 있도록 합니다.

2. 외부 데이터베이스 지원: 사용자 인증 및 정책 저장을 위해 외부 데이터베이스(예: Oracle 또는 Microsoft SQL Server)를 사용하도록 ISE를 구성할 수 있습니다. 데이터베이스 리스너 서비스는 ISE가 이 외부 데이터베이스에 안전하고 효율적으로 연결하고 상호 작용할 수 있도록 합니다.

3. 데이터 처리: 이 서비스는 ISE 시스템에서 데이터베이스 쿼리를 수신 대기한 다음 외부 데이터베이스에 대한 적절한 작업으로 변환합니다. 또한 레코드 삽입, 업데이트 또는 삭제와 같은 요청을 처리하고 데이터베이스에서 정보를 검색할 수 있습니다.

4. 데이터베이스 상태 모니터링: 통신 채널을 제공하는 것 외에도, 외부 데이터베이스에 대한 연결이 안정적이고 작동적이라는 것을 보장하는 데 도움이 된다. 연결에 실패하면 ISE는 컨피그레이션에 따라 로컬 스토리지로 폴백하거나 성능이 저하된 모드로 들어갑니다.

데이터베이스 서버

Database Server 서비스는 시스템에서 사용하는 데이터의 저장 및 검색을 관리합니다. ISE가 컨피그레이션, 정책 정보, 사용자 데이터, 인증 로그, 디바이스 프로필 및 기타 필요한 정보를 저장하는 데 사용하는 기본 데이터베이스와의 상호 작용을 처리합니다.

ISE의 데이터베이스 서버 서비스에 대한 핵심 사항

1. 내부 데이터 저장소 Database Server Service는 기본적으로 ISE가 운영 데이터를 로컬에 저장하는 데 사용하는 내장형 데이터베이스를 관리합니다. 여기에는 인증 및 권한 부여 레코드, 사용자 프로필, 네트워크 액세스 정책, 디바이스 및 엔드포인트 정보, 세션 정보 등의 데이터가 포함됩니다.

2. 임베디드 데이터베이스 대부분의 Cisco ISE 구축에서 시스템은 로컬 스토리지에 임베디드 PostgreSQL 데이터베이스를 사용합니다. 데이터베이스 서버 서비스는 이 데이터베이스가 원활하게 작동하고 데이터베이스에 저장된 데이터와 관련된 모든 쿼리, 업데이트 및 관리 작업을 처리합니다.

3. 데이터베이스 무결성: 서비스는 모든 트랜잭션이 제대로 처리되고 데이터베이스의 무결성이 유지되도록 합니다. 레코드 잠금, 데이터베이스 연결 관리, 데이터베이스 쿼리 실행 등의 작업을 처리합니다.

데이터베이스 리스너 및 데이터베이스 서버 서비스가 초기화 중이거나 실행되고 있지 않은지 확인 및 문제 해결

데이터베이스 리스너와 데이터베이스 서버는 다른 모든 서비스가 제대로 작동하려면 함께 실행해야 하는 필수 서비스입니다. 이러한 서비스가 실행 중이 아니거나 초기화 중에 멈춘 경우 이러한 문제 해결 단계는 복구에 도움이 됩니다.

1. application stop ise 및 application start ise 명령을 사용하여 ISE 서비스를 다시 시작합니다.

2. VM 노드인 경우 VM에서 노드를 다시 시작하면 서비스 복구에 도움이 됩니다.

3. 노드가 물리적 노드인 경우 CIMC에서 노드를 다시 시작/로드하면 서비스 복구에 도움이 됩니다.

4. 데이터베이스가 손상된 경우 Cisco TAC에 추가 트러블슈팅을 문의하십시오.

데이터베이스 리스너 및 데이터베이스 서버는 데이터베이스에 불일치가 있거나 데이터베이스를 제대로 초기화할 수 없는 경우 대개 중지되거나 시작되지 않습니다. 이러한 경우 application reset-config ise 명령을 사용하여 애플리케이션 재설정을 수행하면 데이터베이스의 복구 및 새로 시작하는 데 도움이 됩니다. application reset-config ise 명령을 실행하면 컨피그레이션과 인증서가 제거되지만 IP 주소 및 도메인 이름 세부 정보는 유지됩니다. 구축의 모든 노드에 이 명령을 적용하기 전에 Cisco TAC에 문의하여 추가 정보를 확인하고 잠재적인 영향을 파악하는 것이 좋습니다.

응용 프로그램 서버

Application Server는 ISE 플랫폼의 핵심 기능 및 서비스를 실행하고 관리하는 핵심 구성 요소입니다. ISE가 네트워크 액세스 제어, 인증, 권한 부여, 계정 관리 및 정책 관리에서 역할을 수행할 수 있도록 해주는 비즈니스 로직, 사용자 인터페이스 및 서비스를 호스팅합니다.

ISE의 애플리케이션 서버 서비스에 대한 주요 내용

1. 사용자 인터페이스(UI) Application Server Service는 ISE를 위한 웹 기반 UI(사용자 인터페이스)를 렌더링합니다. 이를 통해 관리자는 정책을 구성 및 관리하고, 로그와 보고서를 보고, ISE의 다른 기능과 상호 작용할 수 있습니다.

2. 서비스 관리: 정책 관리, 관리 작업, 분산 형 구축에서 다른 ISE 노드 와의 통신을 포함 하여 ISE가 제공 하는 다른 서비스를 처리 할 수 있습니다.

3. 중앙집중식 처리: 애플리케이션 서버 서비스는 ISE 아키텍처의 중심 역할을 하며, 네트워크 디바이스, 디렉토리 및 외부 서비스의 정책, 인증 요청 및 데이터를 이해하는 논리를 제공합니다.

응용 프로그램 서버가 초기화 중이거나 실행 중이 아님 확인

애플리케이션 서버는 인증서, 리소스, 구축, 라이센싱과 같은 몇 가지 웹 애플리케이션에 따라 달라집니다. 웹 응용 프로그램을 초기화하지 못하면 응용 프로그램 서버가 초기화 상태에서 중단된 상태로 유지됩니다. 애플리케이션 서버는 노드의 구성 데이터에 따라 Not running(**실행되지 않음**) → **Initializing(초기화)** → **Running(실행 중) 상태**에서 약 15~35분 정도 소요됩니다.

1. ISE의 관리자 인증서가 유효하고 모든 노드에 대한 구축에서 활성 상태인지 확인합니다.
2. 구축의 모든 노드가 기본 관리 노드와 동기화되어 있는지 확인합니다.
3. 노드가 VM인 경우 권장 리소스가 노드에 할당되었는지 확인합니다.

ISE 노드의 CLI에서 show application **status ise 명령**을 사용하여 애플리케이션 서버의 상태를 확인합니다. 애플리케이션 서버와 관련된 대부분의 로그는

Catalina.Out 및 Localhost.log 파일입니다.

언급된 조건이 충족되고 애플리케이션 서버가 초기화 상태로 유지되면 ISE의 CLI/GUI에서 지원 번들을 보호하십시오. application stop ise 및 application start ise 명령을 사용하여 서비스를 복구/다시 시작합니다.

프로파일러 데이터베이스

프로 파 일러 데이터베이스는 프로 파 일러 서비스에 의해 검색 된 네트워크 장치, 엔드 포인트 및 장치 프로파일에 대한 정보를 저장 하는 데 사용 되는 전문 데이터베이스 입니다. 프로파일러는 네트워크 특성 및 동작을 기반으로 네트워크 디바이스(예: 컴퓨터, 스마트폰, 프린터, IoT 디바이스 등)를 자동으로 식별하고 분류하는 ISE의 중요한 구성 요소입니다.

ISE의 프로파일러 데이터베이스 서비스에 대한 핵심 사항

1. 장치 프로파일링: 프로파일러 데이터베이스 서비스의 주요 기능은 프로파일링 프로세스를 지원하는 것입니다. ISE는 이 서비스를 사용하여 프로파일링 중에 수집하는 다음과 같은 정보를 저장합니다.

- 디바이스 유형(예: 스마트폰, 랩톱, 프린터, IoT 장치)
- 장치 운영 체제(예: Windows®, macOS®, Cisco IOS®, Android®)
- 장치 제조업체
- 디바이스를 분류하는 데 도움이 되는 네트워크 동작 또는 패턴

2. 프로파일러 정보: 디바이스 하드웨어 및 소프트웨어 프로파일과 같은 프로파일러 특성을 저장하며, 이는 디바이스를 사전 정의된 정책과 일치시키는 데 사용됩니다. 이 정보는 프로필을 기반으로 올바른 네트워크 액세스 정책 또는 VLAN에 디바이스를 동적으로 할당하는 데에도 사용됩니다.

3. 프로파일링 프로세스: 프로파일링 프로세스는 일반적으로 다음을 기반으로 합니다.

- 활성 프로파일링: ISE는 네트워크에 있는 디바이스에 정보를 적극적으로 쿼리합니다.
- 수동 프로파일링: ISE는 DHCP 요청, RADIUS 특성, HTTP 헤더 및 기타 네트워크 프로토콜과 같은 네트워크 트래픽에서 데이터를 수동적으로 수집하여 디바이스 유형을 결정합니다.

ISE 프로파일링 서비스 확인 및 문제 해결

1. ISE CLI에서 show application status ise 명령을 실행하여 프로파일러 데이터베이스 서비스가 실행 중인지 확인합니다.

2. 기본 관리 노드의 GUI에서 관리 > 배치로 이동하여 노드를 선택합니다. Edit(수정)를 클릭하고 세션 서비스와 프로파일링 서비스가 활성화되었는지 확인합니다.

3. 이제 관리 > 배치 > 노드를 선택합니다. 프로파일러 컨피그레이션으로 이동하고 엔드포인트 데이터 보안을 위해 필요한 프로브가 활성화되어 있는지 확인합니다.

4. Administration(관리) > System(시스템) > Profiling(프로파일링)으로 이동하고 CoA에 대해 구성된 프로파일러 설정을 확인합니다.

5. Context visibility(상황 가시성) > Endpoints(엔드포인트) > 엔드포인트를 선택하고 엔드포인트에 대한 여러 프로브에서 수집된 특성을 확인합니다.

프로파일링 문제 해결에 유용한 디버깅:

- 프로파일러(profiler.log)
- 런타임 AAA(prrt-server.log)
- nsf(ise-psc.log)
- nsf-session(ise.psc.log)

ISE 인덱싱 엔진

인덱싱 엔진은 ISE 데이터베이스에 저장된 데이터를 효율적으로 검색, 인덱싱 및 검색하는 서비스입니다. 특히 대량의 데이터를 처리하고 인증, 권한 부여, 모니터링 및 보고 작업에 필요한 정보에 빠르게 액세스할 수 있는 경우 ISE의 성능과 확장성을 향상시킵니다.

ISE의 ISE 인덱싱 엔진에 대한 핵심 사항

1. 데이터 인덱싱: ISE 인덱싱 엔진은 인증 로그, 세션 로그, 정책 히트, 프로파일링 데이터, 네트워크 액세스 레코드 등 ISE에 저장된 다양한 유형의 데이터에 대한 인덱스를 생성합니다. 인덱싱은 검색 및 쿼리를 보다 효율적으로 만들 수 있도록 이 데이터를 구성하는 데 도움이 됩니다.

2. 로그 관리 및 보고: 이 서비스는 보고 및 로그 쿼리의 성능을 개선하여 로그 관리에 중요한 역할을 합니다. 예를 들어, 특정 인증 이벤트를 검색할 때 인덱싱 엔진을 사용하면 원하는 레코드를 더 빠르게 검색할 수 있습니다. 이는 보안 모니터링 및 규정 준수 보고에 매우 중요합니다.

3. 자료 검색: 또한 인덱싱 엔진은 ISE가 필요할 때 기본 데이터베이스에서 인덱싱된 데이터를 효율적으로 검색할 수 있도록 하는 역할도 합니다. 이를 통해 ISE는 사용자 인터페이스, 외부 툴 또는 API의 쿼리에 대한 빠른 응답을 제공할 수 있습니다.

ISE 인덱싱 엔진이 실행 중이거나 초기화 중이 아닌지 확인합니다.

1. nslookup <**FQDN / IP address of the ISE node** > **명령**을 사용하여 CLI를 통해 정방향 및 역방향 DNS 조회가 클러스터**의** 모든 노드**에서** 작동하는지 확인합니다.
2. ISE 관리 인증서가 클러스터의 모든 노드에 대해 유효하고 활성 상태인지 확인합니다.
3. **show ntp** 명령을 사용하여 CLI를 통해 NTP가 작동 중이며 ISE 노드와 동기화되어 있는지 확인합니다.

인덱싱 엔진은 Context Visibility 및 Indexing 엔진이 사용하여 Context Visibility가 작동하도록 설치 및 실행해야 합니다. 인덱싱 엔진 문제 해결에 도움이 될 수 있는 유용한 로그는 문제 중에 **show logging system ade/ADE.log tail 명령**을 사용하여 지원 번들에서 보호되거나 CLI를 통해 꼬리가 잡힐 수 있는 **ADE.log** 파일입니다.

AD 커넥터

AD Connector(Active Directory Connector)는 ISE가 Microsoft AD(Active Directory)와 통합할 수 있게 해주는 서비스로서, ISE가 AD 자격 증명 및 그룹 멤버십을 기반으로 사용자를 인증, 권한 부여

및 관리할 수 있게 해줍니다. AD 커넥터는 ISE와 Active Directory 간의 브리지 역할을 하므로 ISE에서 NAC(네트워크 액세스 제어) 및 정책 시행을 위해 AD를 활용할 수 있습니다.

ISE에서 AD 커넥터 서비스의 주요 기능

1. Active Directory와의 통합: AD 커넥터 서비스는 ISE와 Active Directory 간의 브리지 역할을 합니다. ISE는 AD에 안전하게 연결할 수 있으므로 ISE가 사용자 인증 및 정책 시행을 위해 AD를 중앙 집중식 ID 저장소로 활용할 수 있습니다.

2. 동기화: AD 커넥터 서비스는 Active Directory에서 ISE로 사용자 및 그룹 데이터 동기화를 지원합니다. 이를 통해 ISE는 사용자와 그룹에 대한 최신 정보를 제공하며, 이는 정확한 정책 시행을 위해 매우 중요합니다.

3. 보안 통신: AD 커넥터 서비스는 LDAP over SSL(LDAPS)과 같은 프로토콜을 사용하여 ISE와 Active Directory 간에 보안 통신 채널을 설정하여 인증 및 쿼리 프로세스 중에 데이터 프라이버시와 무결성을 보장합니다.

4. 다중 Active Directory 도메인 지원: 이 서비스는 여러 Active Directory 도메인에 대한 연결을 지원할 수 있습니다. 이는 ISE가 서로 다른 AD 포리스트 또는 도메인의 사용자를 인증해야 하는 대규모 또는 다중 도메인 환경에서 특히 유용합니다.

5. 사용자 및 그룹 조회: 이를 통해 ISE는 AD에서 사용자 및 그룹 정보를 쿼리할 수 있습니다. 여기에는 사용자 이름, 그룹 멤버십 및 네트워크 액세스 정책을 적용하는 데 사용할 수 있는 기타 사용자 특성과 같은 세부사항이 포함될 수 있습니다. 예를 들어, 네트워크 액세스 정책은 사용자 AD 그룹 멤버십을 기반으로 적용할 수 있습니다(예: 서로 다른 그룹의 사용자에게 서로 다른 액세스 레벨 부여).

1. NTP가 노드와 동기화되어 있는지, AD와 ISE 간의 시간 차이가 5분 미만이어야 하는지 확인합니다.

2. DNS 서버가 AD와 관련된 FQDN 및 도메인을 확인할 수 있는지 확인합니다.

3. **공정 > 보고서 > 보고서 > 진단 > AD 커넥터 공정으로 이동하여**, AD와 관련된 이벤트나 보고서를 확인합니다.

트러블슈팅에 유용한 로그는 런타임 구성 **요소에 대한** 디버그 로그가 있는 ad_**agent.log입니다**.

M&T 세션 데이터베이스

M&T 세션 데이터베이스(모니터링 및 문제 해결 세션 데이터베이스)는 네트워크 액세스 이벤트에 대한 세션 관련 데이터를 저장하고 관리하는 데 중요한 역할을 합니다. M&T 세션 데이터베이스에는 사용자 인증, 디바이스 연결, 네트워크 액세스 이벤트 등 네트워크 활동을 모니터링, 문제 해결, 분석하는 데 필수적인 활성 세션에 대한 정보가 들어 있습니다.

ISE에서 M&T 세션 데이터베이스 서비스의 주요 기능

1. 세션 데이터 저장소: M&T 세션 데이터베이스 서비스는 네트워크의 사용자 및 디바이스 세션에 대한 데이터를 저장하고 인덱싱하는 역할을 합니다. 여기에는 세션 시작 및 종료 시간, 인증 결과, 사용자 또는 디바이스 ID, 관련 정책(예: 역할 할당 또는 VLAN 할당)이 포함됩니다. 데이터에는 또한 초기 인증 및 세션 이벤트를 추적하는 모든 어카운팅 메시지를 포함하여 세션 라이프사이클을

자세히 설명하는 RADIUS 어카운팅 정보도 포함됩니다.

2. 실시간 및 이력 자료 이 서비스는 실시간 세션 데이터(활성 세션) 및 내역 세션 데이터(이전 세션)에 대한 액세스를 제공합니다. 이를 통해 관리자는 지속적인 사용자 액세스를 모니터링할 수 있을 뿐만 아니라 과거 세션 로그를 다시 검토하여 문제를 조사하거나 액세스 이벤트를 검증할 수 있습니다. 실시간 세션 모니터링을 통해 현재 네트워크에 무단 디바이스가 없는지 확인할 수 있습니다.

3. 향상된 모니터링: 세션에 적용된 정책을 포함하여 사용자 및 장치 활동에 대한 통찰력을 제공하여 잠재적인 보안 문제 또는 무단 액세스를 탐지하는 데 도움을 줍니다.

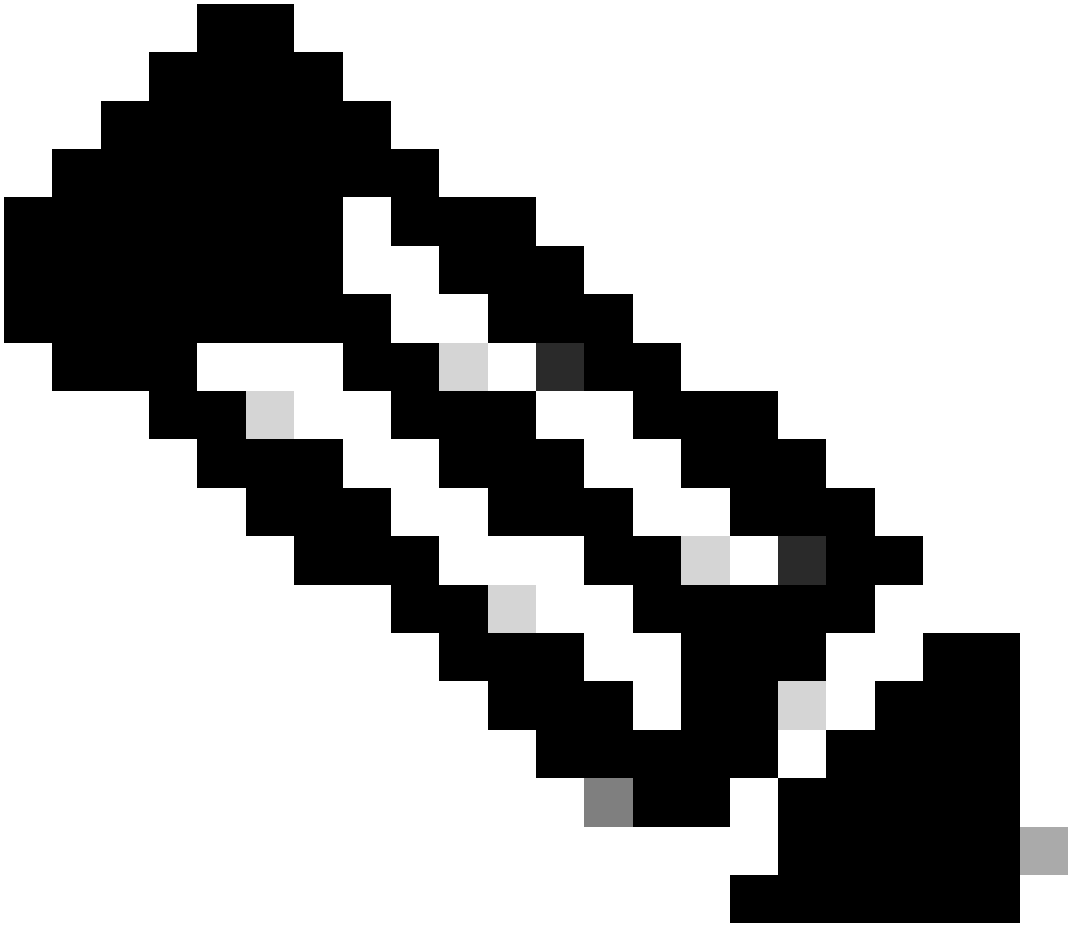
4. 감사 및 보고 업무 네트워크 액세스 이벤트 기록을 저장하고 규정 보고에 필요한 데이터를 제공하여 규정 준수 감사 및 보고를 용이하게 합니다.

ISE에서 M&T 세션 데이터베이스 확인 및 문제 해결

1. 노드에 권장 리소스가 할당되었는지 확인합니다.

2. **ISE CLI**에서 **show tech-**support를 보안하여 문제를 추가로 확인합니다.

3. ISE CLI에서 application configure ise 명령을 실행하여 M&T 세션 **데이터베이스**를 재설정하고 옵션 **1**을 선택합니다.



참고: M&T 데이터베이스 재설정은 배포에 미칠 영향을 확인한 후에만 수행해야 합니다. 추가 확인은 Cisco TAC에 문의하십시오.

알려진 결함

Cisco 버그 ID ·32364

M&T 로그 프로세서

M&T 로그 프로세서(모니터링 및 문제 해결 로그 프로세서)는 ISE 내의 다양한 서비스에서 생성된 로그 데이터를 수집, 처리 및 관리하는 구성 요소입니다. M&T(Monitoring and Troubleshooting) 프레임워크의 핵심 부분으로, 관리자가 ISE 시스템 내에서 네트워크 액세스 이벤트, 인증 시도, 정책 적용 및 기타 활동을 모니터링하고 문제를 해결할 수 있도록 지원합니다. M&T 로그 프로세서는 로그 항목의 처리를 특별히 처리하므로 ISE에서 보고, 감사 및 문제 해결에 필요한 정보를 저장, 분석 및 제공할 수 있습니다.

ISE에서 M&T 로그 프로세서 서비스의 주요 기능

1. 로그 수집 및 처리: M&T 로그 프로세서 서비스는 인증 요청, 권한 부여 결정, 계정 관리 메시지, 정책 시행 활동 등 다양한 ISE 구성 요소에 의해 생성된 로그를 수집 및 처리합니다. 이러한 로그에는 사용자, 디바이스 및 네트워크 액세스 시도에 대한 자세한 정보(예: 타임스탬프, 사용자 ID, 디바이스 유형, 적용된 정책, 액세스 요청의 성공 또는 실패, 실패 사유)가 포함됩니다.

2. 신고 및 준수사항 이 서비스에서 처리하는 로그는 규정 준수 보고에 매우 중요합니다. 대부분의 규정에서는 사용자 액세스 및 보안 이벤트의 로그를 보존해야 합니다. M&T 로그 프로세서 서비스는 모든 관련 로그가 처리되고 규정 준수 감사에 사용할 수 있도록 합니다. 사용자 액세스 로그, 인증 성공/실패율 또는 정책 적용 로그와 같은 로그 데이터를 기반으로 세부 보고서를 생성하는 데 도움이 됩니다.

ISE에서 M&T 로그 프로세서 서비스 확인 및 문제 해결

1. Cisco 설치 설명서에 따라 ISE 노드가 권장 리소스와 함께 구축되어 있는지 확인합니다.

2. 문제를 확인하려면 ISE CLI에서 **show logging system ade/ADE.log tail** 명령을 실행하여 관련 예외/오류를 확인합니다.

알려진 결함

Cisco 버그 ID ·15130

인증 기관 서비스

CA(Certificate Authority) 서비스는 통신 보안을 유지하고 디바이스, 사용자 및 네트워크 서비스를 인증하기 위해 디지털 인증서를 관리하는 데 도움이 되는 중요한 구성 요소입니다. 디지털 인증서는 신뢰할 수 있는 연결을 설정하고 클라이언트(컴퓨터, 스마트폰, 네트워크 장치)와 네트워크 인프라 구성 요소(스위치, 무선 액세스 포인트, VPN 게이트웨이) 간의 안전한 통신을 보장하는 데 필수적입니다. Cisco ISE의 CA 서비스는 802.1X 인증, VPN 액세스, 보안 통신, SSL/TLS 암호화 등 네트워크 보안에 여러 가지 용도로 사용되는 X.509 인증서와 함께 작동합니다.

ISE에서 CA(Certificate Authority) 서비스의 주요 기능

1. 인증서 관리: 인증 기관 서비스는 ISE 내에서 디지털 인증서의 생성, 발급, 관리 및 갱신을 담당합니다. 이러한 인증서는 네트워크 전체에서 다양한 인증 프로토콜 및 암호화 용도로 사용됩니다. 내부 인증 기관의 역할을 하거나 외부 CA와 통합할 수 있습니다(예: Microsoft AD CS, VeriSign 또는 DigiCert와 같은 공용 CA에서 인증서를 발급합니다.

2. 증명서의 발급 EAP-TLS 또는 유사한 인증서 기반 인증 방법이 필요한 환경의 경우 ISE는 NAD(Network Access Device), 사용자 또는 엔드포인트에 대해 인증서를 발급할 수 있습니다. ISE는 장치 및 사용자를 인증하기 위한 인증서를 자동으로 생성 및 배포하거나 외부 CA에서 인증서를 요청할 수 있습니다.

3. 인증서 등록: CA 서비스는 인증서를 사용하여 네트워크에 인증해야 하는 랩톱, 전화기 및 기타 네트워크 디바이스와 같은 엔드포인트에 대해 인증서 등록을 지원합니다. ISE는 SCEP(Simple Certificate Enrollment Protocol) 또는 ACME(Automated Certificate Management Environment)와 같은 프로토콜을 사용하여 디바이스의 인증서 등록을 용이하게 합니다.

4. 인증서 갱신: 이 서비스는 디바이스 및 사용자 모두에 대해 만료되는 인증서의 갱신을 자동화합니다. 인증서가 항상 유효하고 최신 상태인지 확인하여 만료된 인증서로 인한 서비스 중단을 방지합니다.

5. 외부 인증 기관과의 통합: ISE가 자체 CA로 작동할 수 있지만 외부 CA와 통합되는 경우가 더 많습니다(예: Microsoft Active Directory 인증서 서비스). CA 서비스는 필요에 따라 사용자, 디바이스 및 네트워크 리소스에 대한 인증서를 요청하면서 ISE와 외부 CA 간의 상호 작용을 관리할 수 있습니다.

EST 서비스

EST(Enrollment over Secure Transport) 서비스는 인증서 기반 인증 환경에서 네트워크 디바이스 및 사용자에게 디지털 인증서를 안전하게 발급하는 데 사용되는 프로토콜입니다. EST는 디바이스에서 안전하고 자동화된 방식으로 CA(Certificate Authority)의 인증서를 요청할 수 있는 인증서 등록 프로토콜입니다. EST 서비스는 디바이스가 인증서를 사용하여 네트워크에 인증해야 하는 802.1X 환경, VPN 연결 또는 BYOD(Bring Your Own Device) 시나리오와 같은 디바이스 인증에 특히 유용합니다.

ISE에서 EST 서비스의 주요 기능

1. 인증서 등록: EST 서비스는 인증을 위해 인증서가 필요한 디바이스(예: 스위치, 액세스 포인트 또는 엔드포인트)에 대해 보안 인증서 등록을 활성화하는 기능을 담당합니다. 이 등록은 보안 전송(일반적으로 HTTPS)을 통해 수행되므로 프로세스가 암호화되고 무단 액세스로부터 보호됩니다.

2. 인증서 취소 및 갱신 인증서가 등록되면 EST 서비스는 인증서 폐기 또는 갱신을 관리하는 역할도 수행합니다. 예를 들어, 디바이스는 현재 인증서가 만료되면 새 인증서를 요청해야 하며, EST는 이 프로세스를 자동화하는 데 도움이 될 수 있습니다.

3. 향상된 네트워크 액세스 제어: EST 서비스는 디바이스에서 인증서를 사용하여 인증할 수 있도록 함으로써 네트워크의 보안 상태를 강화합니다. 특히 802.1X 인증을 사용하는 환경에서는 더욱 그렇습니다.

인증 기관 및 EST 서비스가 실행 중/초기화 중이 아닌지 확인합니다.

1. Administration(관리) **> System(시스템) > Certificates(인증서) > Certificate Authority(인증 기관) > Internal CA settings(내부 CA 설정)로 이동합니다.** CA, EST 및 OCSP Responder Status(CA, EST 및 OCSP 응답자 상태)가 Sorted(정렬) 및 Enabled(활성화됨)인지 확인합니다.
2. 트러블슈팅에 도움이 될 수 있는 유용한 디버그는 set, provisioning , ca-service 및 ca-service-cert입니다. toise**-psc.log , catalina.out , caservice.log** 및 **error.log 파일을 참조하십시오.**
3. ISE 루트 CA 및 ISE 메시징 인증서가 구축에서 유효한지 확인합니다. ISE 루트 CA의 갱신이 필요한 경우 **Administration(관리) > Certificates(인증서) > Certificate Signing Requests(인증서 서명 요청) > Generate Certificate Signing Request(인증서 서명 요청 생성)로** 이동하여 Usage as **ISE Root CA(ISE 루트 CA로** 사용)를 선택합니다. Renew ISE Root **CA(ISE 루트 CA 갱신)를 클릭합니다**.

SXP 엔진 서비스

SXP 엔진 서비스는 SGT(Security Group Tag) 및 SXP(Security Group Exchange Protocol)를 사용

하여 ISE와 네트워크 디바이스 간의 통신을 관리하고 촉진하는 역할을 합니다. IP 주소나 MAC 주소보다는 장치의 보안 그룹을 기반으로 네트워크 액세스 제어를 적용하는 데 사용되는 TrustSec 정책을 지원하는 데 중요한 역할을 합니다. ISE의 SXP 엔진은 주로 보안 그룹 정보 교환에 사용되며, 이는 사용자 또는 장치 ID, 애플리케이션 및 위치를 기반으로 정책을 적용하는 데 도움이 됩니다. 라우터와 스위치 등 네트워크 디바이스 전반에 보안 정책을 적용하는 데 사용되는 SGT(Security Group Tag)를 디바이스가 공유할 수 있도록 합니다.

ISE에서 SXP 엔진 서비스의 주요 기능

1. TrustSec과의 통합: SXP는 일반적으로 유선 및 무선 네트워크 모두에 일관된 보안 정책을 시행하는 솔루션인 Cisco TrustSec을 활용하는 환경에 구축됩니다. SXP 엔진은 디바이스 간 SGT 통신을 용이하게 하므로 디바이스 또는 사용자의 보안 컨텍스트를 기반으로 동적 정책 시행이 가능합니다.

2. SGT(Security Group Tag): TrustSec의 정책 시행의 핵심은 SGT에 있습니다. 이러한 태그는 네트워크 트래픽을 분류하는 데 사용되며, SXP 프로토콜은 이러한 태그를 특정 사용자 또는 디바이스에 매핑하는 데 도움이 됩니다. 따라서 네트워크 액세스 및 트래픽 흐름에 대한 세분화된 정책 기반 제어가 가능합니다.

ISE의 SXP 엔진 서비스 확인 및 문제 해결

1. 기본적으로 SXP 엔진 서비스는 ISE에서 비활성화됩니다. 활성화하려면 ISE **GUI > Administration > Deployment**로 이동하여 **노드를 선택합니다.** Enable **SXP Service(SXP 서비스 활성화**) 확인란을 선택하고 인터페이스를 선택합니다. 그런 다음 show application status ise 명령을 사용하여 ISE CLI에서 SXP 엔진 **서비스의 상태를** 확인합니다.

2. 네트워크 통신 문제가 있는 경우 CLI에서 show interface 명령을 사용하여 SXP 엔진에 할당된 인터페이스에 유효한 IP 주소가 있는지 확인하고 네트워크에서 IP 서브넷이 허용되는지 확인합니다.

3. RADIUS 라이브 로그를 확인하여 ISE의 SXP 연결 이벤트를 확인합니다.

4. ISE 노드에서 SXP 구성 요소를 활성화하여 관련 로그 및 SXP와 관련된 예외를 디버깅합니다.

TC-NAC 서비스

TC-NAC Service(TrustSec Network Access Control)는 네트워크 디바이스에 TrustSec 정책을 적용하는 구성 요소로, 액세스 제어가 기존 IP 또는 MAC 주소가 아닌 SGT(Security Group Tag)를 기반으로 하는지 확인합니다.

TrustSec은 Cisco에서 개발한 프레임워크로, VLAN이나 IP 주소와 같은 레거시 메커니즘을 사용하지 않고 디바이스 역할, 사용자 또는 컨텍스트를 기반으로 네트워크 전반에 보안 정책을 적용할 수 있습니다. 디바이스를 여러 보안 그룹으로 그룹화하고 SGT로 태깅하여 더욱 세분화되고 동적인 네트워크 액세스 제어를 제공합니다.

ISE에서 TC-NAC 서비스의 주요 기능

1. 타사 NAC 시스템과의 통합: TC-NAC Service를 통해 ISE는 서드파티 네트워크 액세스 제어 솔루

션과 통신하고 상호 작용할 수 있습니다. 이 기능은 기존 NAC 인프라가 있지만 Cisco ISE와 통합하여 기능을 개선하거나, 추가 보안 정책을 활용하거나, Cisco의 다른 네트워크 보안 기능을 활용하려는 조직에 유용할 수 있습니다.

2. 원활한 정책집행의 지원 서드파티 NAC 솔루션과 통합할 경우 ISE는 정책 시행 및 의사 결정의 특정 측면을 맡을 수 있습니다. 이를 통해 Cisco 및 타사 NAC 시스템에서 모두 적용되는 정책이 네트워크 전체에서 일관되게 유지되도록 하여 더욱 통합된 정책 프레임워크를 구현할 수 있습니다.

3. 레거시 NAC 시스템 지원: TC-NAC Service는 레거시 NAC 시스템을 보유한 조직이 향상된 보안 기능을 위해 Cisco ISE를 채택하면서 해당 시스템을 계속 사용할 수 있도록 지원합니다. ISE는 이전 NAC 솔루션과 통합하고 라이프사이클을 확장하여 액세스 제어, 보안, 컴플라이언스 시행을 동시에 제공합니다.

4. 제3자 NAC 벤더 커뮤니케이션 촉진 이 서비스를 통해 ISE는 전용 프로토콜 또는 표준을 사용하는 서드파티 NAC 솔루션과의 통신을 용이하게 할 수 있습니다. ISE는 사용 중인 특정 NAC 솔루션에 따라 업계 표준 프로토콜(RADIUS, TACACS+ 또는 SNMP 등) 또는 사용자 지정 API를 통해 서드파티 NAC 시스템과 상호 작용할 수 있습니다.

ISE에서 TC-NAC 서비스 확인 및 문제 해결

1. Administration(관리) > Deployment(구축) > PSN **node(PSN 노드) > Enable Threat Centric NAC(Threat Centric NAC 활성화)로 이동하여 Threat Centric NAC가 활성화되었는지 확인합니다**.

2. SourceFire FireAMP 어댑터와 관련된 문제인 경우 네트워크에서 **포트 443**이 허용되는지 확인합니다.

3. **Operations(운영) > Threat-Centric NAC Live Logs(위협 중심 NAC 라이브 로그)**에서 엔드포인트 세션 세부사항을 확인합니다**.**

Threat Centric NAC에 의해 트리거된 경보:

- 어댑터에 연결할 수 없음(syslog ID: 91002): 어댑터에 연결할 수 없음을 나타냅니다.
- 어댑터 연결 실패(syslog ID: 91018): 어댑터가 연결 가능하지만 어댑터와 소스 서버 간의 연결이 끊겼음을 나타냅니다.
- 오류로 인해 어댑터가 중지되었습니다(syslog ID: 91006): 이 경보는 어댑터가 원하는 상태가 아닌 경우 트리거됩니다. 이 경보가 표시되면 어댑터 컨피그레이션 및 서버 연결을 확인합니다. 자세한 내용은 어댑터 로그를 참조하십시오.
- 어댑터 오류(syslog ID: 91009): Qualys 어댑터가 Qualys 사이트와의 연결을 설정하거나 Qualys 사이트에서 정보를 다운로드할 수 없음을 나타냅니다.

TC-NAC 문제를 해결하는 데 유용한 디버깅:

- va-runtime(varuntime.log)
- va-service(varuntime.log 및 vaaggregation.log)
- TC-NAC(ise-psc.log)
- anc(ise-psc.log)

PassiveID WMI 서비스

PassiveID WMI 서비스는 ISE가 WMI(Windows Management Instrumentation)를 네트워크의 엔드 포인트를 식별하고 프로파일링하기 위한 수동 메커니즘으로 사용하여 디바이스 프로파일링을 수행할 수 있도록 하는 서비스입니다. 특히 네트워크 액세스 제어 및 정책 시행을 위해 Windows OS를 실행하는 장치를 정확하게 식별해야 하는 환경에서 장치 프로파일링에 중요한 역할을 합니다.

ISE에서 PassiveID WMI 서비스의 주요 기능

1. 디바이스 ID 수집: PassiveID WMI 서비스를 사용하면 ISE가 WMI(Windows Management Instrumentation)를 사용하여 Windows 디바이스에서 ID 정보를 수동으로 수집할 수 있습니다. 또한 디바이스가 적극적으로 참여할 필요 없이 디바이스의 호스트 이름, OS 버전 및 기타 관련 속성과 같은 시스템 세부 정보를 수집합니다.

2. ISE 정책과의 통합: PassiveID WMI 서비스에서 수집한 정보는 ISE 정책 프레임워크에 통합됩니다. 유형, OS 및 보안 표준 준수와 같은 디바이스 특성을 기반으로 정책을 동적으로 적용하는 데 도움이 됩니다.

PassiveID WMI 서비스 확인 및 문제 해결

사용자 정보를 수신할 수 있는 가장 일반적인 소스이자 매우 안전하고 정확한 소스입니다. AD는 프로브로서 WMI 기술과 함께 작동하여 인증된 사용자 ID를 제공합니다.또한 프로브가 아닌 AD 자체는 다른 프로브가 사용자 데이터를 검색하는 소스 시스템(공급자)의 역할을 합니다.

문제 해결을 위해 유용한 디버그 및 정보가 필요합니다. 이러한 특성을 PassiveID WMI 문제에 대한 디버그 수준으로 설정하십시오.

- PassiveID(passiveID*)
- 런타임 로깅(prrt-server.log)
- Active Directory (ad)_agent.log) - 추적 레벨
- collector(collector.log)(세션이 게시된 경우 PassiveID,MnT 노드 및 액티브 pxGrid 노드)
- pxGrid(pxgrid/)(세션이 게시된 경우 보조 MnT 및 액티브 pxGrid 노드)

PassiveID WMI 문제 해결에 필요한 정보:

1. 예전엔 효과가 있었습니까? 최근에 변경된 사항이 있습니다. (업그레이드, ISE에 패치 설치/DC에 업그레이드)
2. 테스트 연결이 제대로 작동합니까(통합하기 전에 테스트 연결 확인)
3. AD에 가입하는 데 사용되는 사용자 이름 및 WMI에 사용되는 사용자 이름에 대한 세부 정보입니다(관리자 또는 비관리자 계정).
4. DC의 이벤트(4768, 4770)가 기록되었는지 확인합니다. (DC의 이벤트 뷰어 로그)
5. 로그 캡처: 수동 ID 및 런타임 로깅에 대한 디버그 수준을 설정한 다음 해당 DC, AD - 타임스탬프가 있는 추적 수준에 대해 wmi를 구성합니다.

PassiveID Syslog 서비스

PassiveID Syslog 서비스는 PassiveID 프로파일링 기능이 환경의 네트워크 디바이스에서 syslog

메시지를 수집 및 처리할 수 있도록 하는 서비스입니다. 이러한 syslog 메시지는 네트워크에 연결된 엔드포인트에 대한 중요한 정보를 포함하며, ISE는 이를 사용하여 네트워크 액세스 제어 및 정책 시행을 위해 이러한 디바이스를 프로파일링합니다.

수동 ID Syslog 서비스의 주요 기능

1. 수동 인증 패시브 ID Syslog 서비스를 통해 Cisco ISE는 사용자 및 디바이스 활동을 나타내는 네트워크 디바이스(스위치 또는 라우터 등)에서 syslog 메시지를 수집하여 사용자 및 디바이스를 수동으로 인증할 수 있습니다. 이 기능은 802.1X와 같은 기존의 활성 인증 방법이 적합하지 않거나 실행 불가능한 경우에 유용합니다.

2. 사건기록: 수동 ID Syslog 서비스는 syslog 프로토콜을 사용하여 네트워크에서 사용자 액세스 및 동작을 추적하는 네트워크 장치로부터 로그를 수신합니다. 이러한 로그에 포함된 정보에는 디바이스 로그인 시도, 액세스 포인트, 인터페이스 세부 정보 등이 포함될 수 있으며, 이는 ISE가 디바이스 또는 사용자를 수동적으로 식별하는 데 도움이 됩니다.

PassiveID API 서비스

PassiveID API 서비스는 네트워크에 연결된 디바이스 또는 사용자의 ID에 대한 정보가 필요한 시스템과의 통합을 가능하게 하는 서비스입니다. 일반적으로 네트워크 관리자가 모든 디바이스에 대해 802.1X와 같은 활성 네트워크 인증 프로토콜을 요구하지 않고 ID 기반 정책 및 작업을 수행하려는 환경에서 사용됩니다.

수동 ID API 서비스의 주요 기능

1. 외부 시스템과의 통합 Passive ID API를 사용하면 ISE가 서드파티 시스템 또는 네트워크 디바이스(예: 스위치, 라우터, 방화벽 또는 ID 관련 이벤트를 생성할 수 있는 모든 시스템)로부터 ID 정보를 받을 수 있습니다. 이러한 외부 시스템은 syslog 메시지, 인증 로그 또는 ISE가 사용자 또는 디바이스를 수동적으로 식별하는 데 도움이 될 수 있는 기타 관련 데이터와 같은 정보를 전송할 수 있습니다.

2. 수동 인증: 수동 ID API 서비스는 능동 인증이 필요하지 않은 ID 데이터를 수집하여 사용자 및 디바이스를 수동으로 인증하는 데 사용됩니다(예: 802.1X, MAB 또는 웹 인증이 필요 없음). 예를 들어, 네트워크 디바이스, Active Directory 로그 또는 보안 어플라이언스에서 정보를 캡처하여 사용자 또는 디바이스를 식별하는 데 사용할 수 있습니다.

3. 신원정보 매핑 Passive ID API를 사용하여 ID 데이터를 특정 보안 정책에 매핑할 수 있습니다. 이 정보는 사용자와 디바이스에 SGT(Security Group Tag) 또는 역할을 동적으로 할당하는 데 사용되며, 이는 네트워크 액세스 제어(예: 세그멘테이션 및 방화벽 정책)의 시행에 영향을 줍니다.

PassiveID 에이전트 서비스

PassiveID 에이전트 서비스는 엔드포인트(예: 컴퓨터, 랩톱, 모바일 디바이스)에 설치된 PassiveID 에이전트를 사용하여 디바이스 프로파일링을 활성화하는 서비스입니다. PassiveID Agent를 사용하면 ISE가 액티브 스캔 또는 디바이스와의 직접적인 상호 작용 없이 엔드포인트의 트래픽을 수신하여 네트워크의 디바이스에 대한 프로파일링 정보를 수집할 수 있습니다.

패시브 ID 에이전트 서비스의 주요 기능

1. 수동 사용자 및 장치 식별 패시브 ID 에이전트 서비스는 ID 관련 정보를 수동적으로 수집하며, 대개 네트워크 디바이스 또는 엔드포인트에서 이 데이터를 ISE로 전송합니다. 이 서비스를 통해 ISE는 디바이스에서 액티브 인증을 수행하지 않고도 사용자의 활동 또는 특성에 따라 사용자 및 디바이스를 인증하고 식별할 수 있습니다(예: 802.1X 자격 증명이 제공되지 않음).

2. 다른 Cisco 구성 요소와의 통합: Passive ID Agent는 스위치, 무선 컨트롤러, 액세스 포인트 등의 Cisco 네트워크 디바이스와 긴밀하게 협력하여 네트워크 트래픽, syslog 또는 기타 관리 시스템에서 ID 관련 정보를 수집합니다. 또한 Cisco TrustSec 및 Cisco Identity Services와 통합되어 이 데이터를 특정 SGT(Security Group Tag) 또는 기타 ID 기반 정책에 매핑할 수 있습니다.

3. 상황별 네트워크 접근 통제 패시브 ID 에이전트는 이 정보를 Cisco ISE에 보낸 다음 사용자 또는 디바이스의 ID 및 컨텍스트를 기반으로 적절한 액세스 제어 정책을 적용합니다. 여기에는 다음이 포함될 수 있습니다.

- 역할 기반 액세스 제어.
- 동적 VLAN 할당.
- 네트워크 세그멘테이션.
- 사용자 역할 또는 디바이스 보안 상태에 따라 보안 정책 시행

PassiveID 끝점 서비스

PassiveID 엔드포인트 서비스는 PassiveID 기술을 기반으로 네트워크에서 엔드포인트(디바이스)를 식별하고 프로파일링하는 역할을 담당하는 서비스입니다. 이 서비스는 ISE가 엔드포인트 자체와의 적극적인 상호 작용 없이 네트워크에 연결된 디바이스에 대한 정보를 수집, 처리 및 분류하는 데 도움이 됩니다. PassiveID Endpoint Service는 프로파일링, 네트워크 액세스 제어 및 보안 정책 시행에서 중요한 역할을 합니다.

PassiveID 엔드포인트 서비스의 주요 기능

1. 수동 사용자 및 장치 식별 PassiveID 엔드포인트 서비스는 Cisco ISE가 네트워크 활동 또는 시스템 로그의 정보를 활용하여 네트워크의 디바이스를 수동으로 식별하고 인증할 수 있게 합니다. 여기에는 MAC 주소, IP 주소 또는 AD(Active Directory)와 같은 외부 ID 저장소의 로그인 정보와 같은 네트워크 동작 또는 특성을 기반으로 사용자와 디바이스를 식별하는 것이 포함됩니다.

2. 엔드포인트에서의 데이터 수집 엔드포인트 서비스는 여러 소스에서 다양한 유형의 엔드포인트별 데이터를 수집합니다.

- Active Directory 또는 기타 디렉토리와 같은 외부 ID 저장소에서 사용자 로그인 정보입니다.
- IP 주소, MAC 주소 및 장치 유형과 같은 장치 특성(예: 디바이스가 Windows PC, 휴대폰 또는 IoT 디바이스인지 여부)
- DHCP 요청, ARP 요청 및 기타 네트워크 레이어 통신과 같은 엔드포인트 네트워크 활동

PassiveID SPAN 서비스

PassiveID SPAN 서비스는 엔드포인트 프로파일링을 위해 네트워크 디바이스에서 SPAN(Switched

Port Analyzer) 포트 미러링을 활용하여 네트워크 트래픽을 캡처 및 분석하는 서비스입니다. 이 서비스는 디바이스 자체에 활성 프로브 또는 에이전트를 설치하지 않고도 ISE가 네트워크 통신 패턴을 분석하여 네트워크의 엔드포인트(디바이스)에 대한 정보를 수동적으로 수집하는 데 도움이 됩니다.

PassiveID SPAN 서비스의 주요 기능

1. SPAN 트래픽에서 수동 ID 수집: PassiveID SPAN 서비스를 통해 ISE는 스위치의 SPAN 포트를 통해 미러링되거나 복사된 네트워크 트래픽을 기반으로 ID 데이터를 수집할 수 있습니다. SPAN 포트는 일반적으로 다른 포트 또는 VLAN의 네트워크 트래픽을 미러링하여 네트워크 모니터링에 사용됩니다. ISE는 이 트래픽을 캡처하여 다음과 같은 ID 정보를 수동적으로 수집할 수 있습니다.

- 디바이스의 MAC 주소.
- 디바이스와 연결된 IP 주소.
- 캡처된 트래픽에서 DHCP 요청 또는 기타 ID 관련 정보.
- 스위치 또는 무선 컨트롤러와 같은 네트워크 디바이스의 인증 로그

2. 사용자 및 기기 식별정보의 캡처 SPAN 서비스는 기본적으로 네트워크를 통과하는 트래픽을 수신하고 디바이스와 직접 상호 작용할 필요 없이 네트워크 패킷에서 키 ID 정보를 식별합니다. 여기에는 다음과 같은 데이터가 포함될 수 있습니다.

- EAP(Extensible Authentication Protocol)와 같은 프로토콜을 통해 인증하는 경우 사용자 ID입니다.
- MAC 주소 및 IP 주소를 기반으로 하는 디바이스 ID입니다.
- 관찰된 트래픽 패턴 및 이벤트를 기반으로 하는 디바이스 역할 및 동작

PassiveID 스택 확인 및 문제 해결(PassiveID SPAN 서비스, PassiveID Syslog 서비스, PassiveID 엔드포인트 서비스, PassiveID 에이전트, PassiveID API 서비스)

1. PassiveID 스택은 제공자 목록이며 PassiveID 스택의 모든 서비스는 기본적으로 비활성화되어 있습니다. ISE GUI > Administration > Deployment > Select the node, Enable Passive Identity Service로 이동하고 Save를 클릭합니다. PassiveID 스택 서비스 상태를 확인하려면 ISE 노드의 CLI에 로그인하고 show application status ise 명령을 실행합니다.

2. 패시브 ID 에이전트에 문제가 있는 경우 에이전트의 FQDN이 ISE 노드에서 확인 가능한지 확인합니다. 이를 수행하려면 ISE CLI에 로그인하고 nslookup < FQDN of Agent configured > 명령을 실행합니다.

3. ISE 인덱싱 엔진이 활성 상태이고 역방향 및 정방향 DNS 조회가 모두 ISE에 구성된 DNS 또는 이름 서버에 의해 확인되는지 확인합니다.

4. syslog 공급자와 원활한 통신을 보장하려면 네트워크에서 UDP 포트 40514 및 TCP 포트 11468이 열려 있는지 확인합니다.

5. 노드에서 SPAN 공급자를 구성하려면 ISE Passive Identity Service가 활성화되어 있는지 확인합니다. ISE CLI의 show interface 명령을 사용하여 SPAN 공급자에서 구성할 인터페이스를 ISE에서 사용할 수 있는지 확인합니다.

수동 ID 제공자에 따라 로그를 확인하려면 passiveid-syslog.log, passiveid-agent.log, passiveid-api.log, passiveid-endpoint.log, passiveid-span.log를 검토해야 합니다. 언급된 로그는 ISE 노드의 지원 번들에서 보호될 수 있습니다.

DHCP 서버(dhcpd)

dhcpd(DHCP Server) 서비스는 네트워크 디바이스에 DHCP(Dynamic Host Configuration Protocol) 기능을 제공하는 서비스입니다. 주로 네트워크에 연결하려는 디바이스(엔드포인트)에 IP 주소를 할당하는 데 사용됩니다. ISE에서 DHCP 서버는 네트워크에 연결할 때 IP 주소를 요청하는 엔드포인트에 IP 주소를 제공하는 데 중요한 역할을 합니다. 또한 이 서비스는 DNS 서버, 기본 게이트웨이 및 기타 네트워크 설정과 같은 추가 구성 정보를 제공할 수 있습니다.

ISE에서 DHCP 서버(dhcpd) 서비스의 주요 기능

1. 동적 IP 주소 할당: ISE의 dhcpd 서비스는 네트워크에 연결할 때 IP 주소를 요청하는 디바이스에 IP 주소 할당을 제공하는 DHCP 서버 역할을 합니다. 이는 BYOD(Bring Your Own Device) 환경이나 장치가 자동으로 IP 주소를 얻도록 구성된 경우와 같이 장치가 동적으로 네트워크에 연결되는 시나리오에서 중요합니다.

2. 프로필 기반 DHCP: dhcpd 서비스는 디바이스의 프로필에 따라 IP 주소를 할당할 수 있다. ISE가 디바이스를 프로파일링한 경우(예: 스마트폰, 노트북, IoT 기기)라고 판단하면 기기 유형이나 역할에 따라 적절한 IP 주소를 할당하거나 다른 설정을 적용할 수 있다.

3. DHCP 릴레이 지원 ISE가 실제 IP 주소 할당을 처리하지 않는 경우 ISE는 DHCP 릴레이 에이전트의 역할을 하여 디바이스에서 외부 DHCP 서버로 DHCP 요청을 전달할 수 있습니다. 이 경우 dhcpd 서비스는 디바이스에서 중앙 DHCP 서버로 요청을 전달할 수 있으며, ISE는 네트워크 정책 및 액세스 제어를 계속 적용할 수 있습니다.

DHCP 서버(dhcpd) 확인 및 문제 해결

1. Cisco TAC에 문의하여 DHCP 서버 패키지가 ISE에 설치되어 있는지 확인합니다.

2. ISE의 루트에 **로그인합니다 > rpm -qi dhcp**.

DNS 서버(명명된)

DNS 서버(명명된) 서비스는 ISE가 DNS(Domain Name System) 서버 또는 DNS 확인자로 작동하도록 허용하는 서비스입니다. 주로 도메인 이름을 IP 주소로, 그 반대로 해석하여 네트워크에 있는 디바이스 간의 통신을 촉진하는 역할을 담당합니다.

ISE에서 DNS 서버(명명된) 서비스의 주요 기능

1. ISE 통신을 위한 DNS 확인: ISE의 명명된 서비스는 도메인 이름을 IP 주소로 확인하는 데 도움이 됩니다. 이는 ISE가 IP 주소가 아닌 도메인 이름을 사용하여 다른 네트워크 디바이스 또는 외부 서비스(예: Radius 서버, Active Directory 또는 외부 NTP 서버)에 연결해야 할 때 특히 중요합니다.

- 예를 들어 ISE가 Radius 서버 또는 외부 디렉터리 서비스(예: Active Directory)에 연결해야 하

는 경우 해당 서버의 도메인 이름을 IP 주소로 확인해야 합니다.
- ISE는 이러한 도메인 이름을 확인하기 위해 시스템에 구성된 DNS 서버를 쿼리하여 원활한 통신을 보장합니다.

2. 외부 서비스에 대한 DNS 확인 DNS 서비스를 통해 ISE는 도메인 이름이 필요한 외부 서비스에 연결할 수 있습니다. 예를 들어, ISE는 다음과 같은 외부 서비스의 이름을 확인해야 합니다.

- 클라우드 기반 서비스.
- NTP(Network Time Protocol) 서버
- CA(Certificate Authorities) 또는 LDAP 서버

3. 다중 도메인 및 이중 DNS 서버: 이중화를 위해 여러 DNS 서버를 사용하도록 ISE를 구성할 수 있습니다. 한 DNS 서버를 사용할 수 없게 될 경우 ISE는 다른 DNS 서버로 폴백하여 지속적인 운영과 DNS 확인을 보장할 수 있습니다.

DNS 서버 확인 및 문제 해결(명명된)

1. ISE 노드의 CLI에서 **ping <IP** of DNS server **/ name server> 명령을** 사용하여 구축의 이름 서버 또는 DNS 서버에 **연결할 수 있는지** 확인합니다.

2. ISE CLI를 통해 nslookup **<**FQDN **/ IP address of ISE nodes> 명령을** 사용하여 ISE FQDN의 DNS 확인을 수행합니다.

ISE 메시징 서비스

ISE 메시징 서비스는 ISE 시스템 내의 다양한 서비스와 구성 요소 간의 비동기 통신을 지원하는 구성 요소입니다. ISE의 전체 시스템 아키텍처에서 중요한 역할을 하며, 플랫폼의 여러 부분에서 메시지를 보내고 받고, 작업을 관리하고, 활동을 동기화할 수 있습니다.

ISE 메시징 서비스의 주요 기능

1. 공정간 통신 ISE 메시징 서비스는 다양한 ISE 서비스 간 IPC(프로세스 간 통신)를 활성화하는 데 중요한 역할을 합니다. 인증, 권한 부여 및 정책 시행과 같은 다양한 ISE 모듈 및 서비스가 조정된 방식으로 데이터와 지침을 교환할 수 있도록 보장합니다.

2. 분산환경지원: 대규모 또는 분산형 ISE 구축(예: 멀티 노드 또는 고가용성 컨피그레이션)에서 메시징 서비스는 다양한 ISE 노드 간의 통신을 용이하게 합니다. 이렇게 하면 인증 요청, 사용자 세션, 정책 업데이트 등의 데이터가 ISE 시스템 내의 여러 노드에서 올바르게 동기화됩니다.

3. 정책 및 구성 동기화: 메시징 서비스는 ISE 노드 간의 컨피그레이션 및 정책 동기화에 사용됩니다. 기본 노드에 대한 컨피그레이션 변경 사항이 적용되면 서비스는 이러한 변경 사항이 시스템의 보조 또는 백업 노드로 전파되도록 합니다. 이는 일관성을 유지하고 여러 위치 또는 분산된 ISE 노드에 적용된 네트워크 액세스 정책이 동기화된 상태를 유지하도록 하는 데 필수적입니다.

ISE 메시징 서비스가 실행 중이거나 초기화 중이 아닌지 확인합니다.

1. 포트 TCP 8671이 방화벽에서 차단되지 않았는지 확인합니다. 이 포트는 ISE 장치 간의 노드 간 통신에 사용됩니다.

2. 대기열 링크 오류를 확인하고 오류가 있는 경우 ISE 메시징 및 ISE 루트 CA 인증서를 갱신합니다. 일반적으로 대기열 링크 오류는 내부 인증서 손상 문제로 인해 발생합니다. 대기열 링크 오류를 해결하려면 ISE - Queue Link Error 문서를 참조하여 ISE 메시징 및 ISE 루트 CA 인증서를 갱신합니다.

3. GUI -> Administration -> Certificates -> Select ISE Messaging Certificate(ISE 메시징 인증서 선택)에서 View(보기)를 클릭하여 인증서 상태를 확인합니다.

ISE 메시징 서비스 트러블슈팅에 유용한 로그는 지원 번들에서 사용할 수 있거나 문제 동안 show logging system ade/ADE.log tail 명령을 사용하여 CLI를 통해 꼬리를 수 있는 ade.log입니다.

4. ADE.log 로그에 rabbitmq가 표시되는 경우: 연결 거부 오류, ISE 루트에서 Rabbitmq 모듈에 대한 잠금을 제거하려면 Cisco TAC에 문의하십시오.

ISE API 게이트웨이 데이터베이스 서비스

ISE API 게이트웨이 데이터베이스 서비스는 ISE 시스템 내의 API 요청 및 응답과 관련된 데이터를 관리하고 처리하는 구성 요소입니다. ISE API Gateway를 ISE 데이터베이스와 연결하는 중재자 역할을 하므로 사용자 지정 애플리케이션이 서비스에서 관리하는 API 호출을 통해 ISE 내의 데이터를 업데이트하거나 수정할 수 있습니다(예: 액세스 정책 조정 또는 사용자 추가/제거).

ISE API 게이트웨이 데이터베이스 서비스의 주요 기능

1. ISE 데이터에 대한 API 액세스: ISE API 게이트웨이 데이터베이스 서비스는 브리지 역할을 하여 외부 애플리케이션이 ISE RESTful API를 통해 ISE 데이터베이스와 상호 작용할 수 있도록 합니다. 이러한 API는 다음과 같이 ISE 데이터베이스에 저장된 데이터를 검색하거나 수정하는 데 사용할 수 있습니다.

- 사용자 인증 로그
- 네트워크 액세스 정책.
- 장치 프로파일링 정보.
- 시스템 구성 및 설정.

2. 외부 시스템 통합 지원 이 서비스는 다음과 같은 외부 시스템과 ISE를 통합하는 데 중요한 역할을 합니다.

- 외부 인증 서버(LDAP, Active Directory, RADIUS).
- NMS(Network Management Systems)
- SIEM(보안 정보 및 이벤트 관리) 솔루션
- ISE 데이터와 상호 작용해야 하는 맞춤형 애플리케이션 또는 서비스입니다.

API 액세스를 제공함으로써 API 게이트웨이 데이터베이스 서비스는 이러한 외부 시스템이 ISE 데이터를 쿼리하거나, ISE에 업데이트를 전송하거나, 외부 이벤트에 대한 응답으로 ISE 내에서 특정 작업을 트리거할 수 있도록 합니다.

3. RESTful API 통신 지원 ISE는 HTTP/HTTPS를 통해 작동하도록 설계된 RESTful API를 표시합니다. API 게이트웨이 데이터베이스 서비스는 API 요청 및 응답의 흐름을 관리하며, 요청이 인증되고 처리되며 ISE 데이터베이스의 적절한 데이터가 응답에서 반환되도록 합니다.

ISE API 게이트웨이 서비스

ISE API 게이트웨이 서비스는 ISE 서비스, 데이터 및 기능에 대한 RESTful API 액세스를 제공하는 중요한 구성 요소입니다. ISE와 외부 시스템 간의 브리지 역할을 하므로 이러한 시스템이 ISE 네트워크 액세스 제어, 정책 적용, 인증 및 기타 서비스와 프로그래밍 방식으로 상호 작용할 수 있습니다. API Gateway는 타사 애플리케이션, 네트워크 관리 시스템 및 사용자 지정 애플리케이션이 수동 개입 또는 ISE 사용자 인터페이스에 대한 직접 액세스 없이 Cisco ISE와 상호 작용할 수 있도록 합니다.

ISE API 게이트웨이 서비스의 주요 기능

1. ISE에 대한 API 액세스 활성화: ISE API 게이트웨이 서비스는 외부 시스템이 RESTful API를 사용하여 Cisco ISE 데이터 및 정책에 안전하게 액세스하고 상호 작용할 수 있도록 지원합니다. 그러면 인증, 정책 시행, 세션 관리 등과 같은 ISE 기능에 프로그래밍 방식으로 액세스할 수 있습니다.

2. 체계적 통제: API 게이트웨이 서비스는 ISE 기능을 프로그래밍 방식으로 제어할 수 있습니다. 관리자 및 개발자는 API를 사용하여 다음을 수행할 수 있습니다.

- 네트워크 정책을 검색하거나 수정합니다.
- 사용자 세션 및 인증 로그를 쿼리하거나 관리합니다.
- 네트워크 액세스 제어 규칙을 생성하고 관리합니다.
- 디바이스 프로필에 액세스하거나 업데이트합니다.

이 컨트롤은 실시간 데이터를 기반으로 네트워크 액세스 정책을 동적으로 조정하거나 ISE를 더 광범위한 보안 자동화 플랫폼에 통합하는 등 자동화 또는 맞춤형 워크플로 오케스트레이션에 활용할 수 있습니다.

3. 모니터링 및 보고 업무 API 게이트웨이 서비스는 외부 시스템에서 운영 ISE 로그, 세션 기록 및 정책 시행 세부사항에서 데이터를 수집할 수 있도록 합니다. 이는 다음에 중요합니다.

- 규정 준수 보고.
- 보안 모니터링.
- 사고 대응

API 호출을 사용하여 로그, 감사 정보 및 이벤트를 가져올 수 있으므로 보안 팀은 중앙 집중식 대시보드 또는 보고 툴에서 ISE 활동을 모니터링할 수 있습니다.

ISE API 게이트웨이 서비스 및 ISE API 게이트웨이 데이터베이스 서비스 확인 및 문제 해결

1. ISE 노드의 관리자 인증서가 활성 상태이고 유효한지 확인합니다. Administration(관리) > Certificates(인증서) > Select the node(노드 선택) > Select Admin Certificate(관리 인증서 선택)로 이동합니다. View(보기)를 클릭하여 ISE 노드의 Admin Certificate(관리자 인증서) 상태를 확인합니다.

2. ise-api-gateway, api-gateway, apisservice 구성 요소를 디버깅하도록 설정하고 다음 명령을 사용하여 로그를 미룰 수 있습니다.

- show logging application ise-psc.log tail

- show logging application api-gateway.log tail

ISE pxGrid Direct 서비스

ISE pxGrid Direct Service는 ISE에서 pxGrid(Platform Exchange Grid) 기능을 지원하는 핵심 구성 요소입니다. pxGrid는 Cisco 네트워크 보안 솔루션과 타사 애플리케이션, 서비스 및 장치 간의 안전하고 표준화되고 확장 가능한 데이터 공유 및 통합을 지원하는 Cisco 기술입니다. ISE pxGrid Direct Service를 사용하면 중간 장치나 서비스를 사용할 필요 없이 ISE와 다른 pxGrid 호환 시스템 간에 직접 통신할 수 있습니다.

ISE pxGrid Direct 서비스의 주요 기능

1. 타사 시스템과의 직접 통합: ISE pxGrid Direct Service를 통해 ISE는 방화벽, 라우터, NAC 솔루션, SIEM 플랫폼 및 기타 보안 어플라이언스와 같은 서드파티 네트워크 보안 시스템과 직접 통합할 수 있습니다. 이러한 시스템에서는 네트워크 액세스 이벤트, 보안 사고 및 상황별 네트워크 데이터와 관련된 정보를 교환할 수 있습니다.

2. 상황 공유: pxGrid의 주요 기능 중 하나는 상황 정보(예: 디바이스 ID, 사용자 역할, 보안 상태, 네트워크 액세스 정보)의 공유입니다. pxGrid Direct Service를 통해 ISE는 RADIUS 또는 TACACS+와 같은 기존 방법에 의존하지 않고 이 컨텍스트를 다른 디바이스 또는 애플리케이션과 직접 공유할 수 있습니다.

3. 단순통신: ISE는 pxGrid를 사용하여 표준화된 프로토콜을 사용하여 서드파티 솔루션과 통신하고 정보를 교환할 수 있습니다. 따라서 각 개별 서드파티 솔루션에 대해 맞춤형 통합이 필요하지 않으므로 통합 프로세스가 간소화됩니다.

4. 보안 및 규정 준수 강화: 또한 pxGrid Direct Service는 네트워크 에코시스템의 모든 시스템이 사용자, 디바이스, 보안 정책에 대한 동일한 실시간 상황 데이터에 액세스할 수 있도록 보장함으로써 보안 상태 및 규정 준수를 향상시킵니다. 이를 통해 전체 환경에 걸쳐 네트워크 보안 정책을 보다 효율적으로 시행할 수 있습니다.

ISPxgrid Direct 서비스 확인 및 문제 해결

1. Cisco TAC에 문의하여 /tmp **폴더에 edda*.lock***이 있는지 확인합니다. 대답이 "예"인 경우 Cisco TAC에서 잠금을 제거하고 루트에서 Pxgrid Direct 서비스를 다시 시작합니다.

2. 문제 **해결을** 위해 ISE 노드에서 디버깅할 PxGrid Direct 구성 요소를 설정합니다. 다음 명령을 사용하여 ISE 지원 번들 또는 ISE CLI를 통해 로그를 보호할 수 있습니다.

show logging application pxgriddirect-service.log

show logging application pxgriddirect-connector.log

언급된 로그는 Cisco ISE에서 가져와 수신한 엔드포인트 데이터에 대한 정보를 Pxgrid Connector의 연결 상태와 함께 제공합니다.

세그먼테이션 정책 서비스

Segmentation Policy Service는 사용자 ID, 디바이스 상태 또는 기타 상황 정보를 기반으로 네트워크 세그멘테이션 정책을 시행하는 핵심 구성 요소입니다. 또한 특정 네트워크 세그먼트에 대한 사용자 및 디바이스 액세스를 제어하여 인증된 사용자 또는 규정 준수 디바이스만 네트워크의 특정 부분에 액세스할 수 있도록 합니다. 네트워크 세그멘테이션은 네트워크의 공격 표면을 줄이고, 위협의 측면 이동을 방지하고, 규정 준수를 보장하는 데 필수적입니다. ISE의 세그멘테이션 정책 서비스는 네트워크 전체에서 이러한 네트워크 세그멘테이션 규칙을 동적으로 유연하게 적용하는 데 사용됩니다.

세그먼테이션 정책 서비스의 주요 기능

1. 네트워크 세그먼트 정의 ISE의 세그멘테이션 정책 서비스를 통해 관리자는 사용자 또는 디바이스의 특성에 따라 다양한 네트워크 세그먼트(서브넷 또는 VLAN)를 정의할 수 있습니다. 예를 들면 다음과 같습니다.

- 보안 상태가 서로 다른 디바이스를 서로 다른 세그먼트에 할당할 수 있습니다(예: 한 VLAN의 신뢰할 수 있는 디바이스 및 다른 VLAN의 신뢰할 수 없는 디바이스).
- 서로 다른 부서 또는 역할의 사용자를 서로 다른 네트워크 세그먼트에 할당하여 최소 권한을 적용하고 민감한 리소스에 대한 액세스를 제한할 수 있습니다.

2. 동적 세분화 이 서비스를 통해 동적 네트워크 세그멘테이션이 가능합니다. 즉, 실시간 조건에 따라 네트워크 세그먼트 또는 VLAN을 변경할 수 있습니다. 예를 들면 다음과 같습니다.

- 사용자는 역할 또는 디바이스 상태에 따라 특정 VLAN에 할당될 수 있습니다.
- 규정을 준수하지 않는 것으로 간주되거나 오래된 운영 체제를 실행 중인 디바이스는 수정될 때까지 격리 또는 게스트 VLAN으로 이동할 수 있습니다.

3. 정책적 집행: 세그멘테이션 정책 서비스는 정책을 사용하여 디바이스 또는 사용자를 어떤 세그먼트에 배치할지 결정합니다. 이러한 정책은 다음과 같은 다양한 요소를 고려할 수 있습니다.

- 사용자 ID: 사용자 역할 또는 특성 기준.
- 디바이스 상태: 디바이스의 상태 또는 규정 준수 상태(예: 최신 안티바이러스 소프트웨어를 실행 중입니까?)
- 위치: 네트워크에서 사용자 또는 디바이스의 물리적 위치(예: 사무실, 게스트 영역, 원격 액세스).
- 액세스 시간: 액세스 요청이 이루어지는 요일 또는 요일.

4. 보안정책의 시행 세그멘테이션 정책 서비스는 RADIUS 및 VLAN 할당과 같은 업계 표준을 활용하여 네트워크 디바이스(스위치, 라우터, 방화벽 등) 전반에 걸쳐 보안 정책이 일관성 있게 적용되도록 합니다. 이를 통해 Cisco ISE는 네트워크 인프라 디바이스와 통신하여 필요한 세그멘테이션 정책을 시행할 수 있습니다.

세그먼테이션 정책 서비스 확인 및 문제 해결

1. Work Centers(작업 센터) > TrustSec > Overview(개요) > Dashboard(대시보드)로 이동하여 세그멘테이션이 올바르게 구성되어 있는지 확인합니다.

2. Work Centers(작업 센터) > TrustSec > Reports(보고서), TrustSec reports(TrustSec 보고서)를 선택하여 세그멘테이션 정책 서비스 상태 및 보고서를 확인합니다.

REST 인증 서비스

REST 인증 서비스는 RESTful API를 사용하여 인증 기능을 제공하는 서비스입니다. 외부 애플리케이션 및 시스템이 표준 REST 프로토콜을 사용하여 HTTP(S)를 통해 ISE와 상호 작용하여 사용자 또는 디바이스를 인증할 수 있도록 합니다. 이 서비스는 Cisco ISE 인증 기능을 사용자 또는 디바이스를 인증해야 하지만 기존 방법(예: RADIUS 또는 TACACS+)을 사용할 수 없는 타사 애플리케이션 또는 시스템과 원활하게 통합할 수 있게 해줍니다.

REST 인증 서비스의 주요 기능

1. RESTful 인증: REST 인증 서비스는 REST API 프로토콜을 통해 인증 요청을 활성화합니다. 이렇게 하면 외부 시스템(예: ISE를 인증 서버로 사용하는 사용자 또는 디바이스를 인증하는 애플리케이션, 서드파티 네트워크 디바이스 또는 서비스)입니다. RADIUS 또는 TACACS+와 같은 기존 인증 프로토콜이 아닌 RESTful 웹 서비스 호출을 통해 인증할 수 있습니다.

2. 외부 애플리케이션과의 통합: 이 서비스는 사용자 또는 디바이스를 인증해야 하지만 기존 인증 방법(예: RADIUS 또는 TACACS+)을 사용하지 않는 외부 애플리케이션을 위해 설계되었습니다. 대신 REST API를 통해 ISE와 상호 작용하여 ISE 인증을 웹 기반 또는 클라우드 네이티브 애플리케이션에 더 간편하게 통합할 수 있습니다.

3. 유연하고 확장 가능한 인증: REST 인증 서비스는 네트워크 디바이스 또는 온프레미스 솔루션에 국한되지 않는 확장 가능한 인증 방법을 제공합니다. ISE에 자격 증명과 정책을 쿼리하여 사용자 또는 디바이스를 인증해야 하는 클라우드 서비스, 모바일 애플리케이션 및 기타 웹 기반 플랫폼에서 사용할 수 있습니다.

4. 적용 용이성 REST API는 표준화된 인터페이스를 제공하며, 기존 방식에 비해 최신 소프트웨어 및 애플리케이션과 더 쉽게 통합되고 적용할 수 있습니다. JSON 형식의 응답을 제공하며 GET, POST, PUT 및 DELETE와 같은 HTTP 메서드를 사용하여 인증을 위해 ISE를 통합하는 웹 개발자 및 시스템에서 더 쉽게 액세스할 수 있습니다.

Rest Auth 확인 및 문제 해결

1. Open API 관련 문제를 해결하려면 apiservice 구성 요소를 디버그로 설정합니다.

2. ERS API 관련 문제를 해결하려면 ers 구성 요소를 디버그로 설정합니다.

API 서비스 GUI 페이지인 경우: https://{iseip}:{port}/api/swagger-ui/index.html 또는 https://{iseip}:9060/ers/sdk에 액세스할 수 있습니다. API 서비스가 예상대로 작동한다고 결론을 내렸습니다.

API에 대한 자세한 내용은 API 설명서를 참조하십시오.

SSE 커넥터

SSE 커넥터(Secure Software-Defined Edge Connector)는 ISE를 Cisco SD-Access(Secure Software-Defined Access) 솔루션과 통합하는 서비스입니다. SSE 커넥터를 사용하면 ISE가 Cisco DNA Center와 안전하게 통신할 수 있어 SD 액세스 환경에서 자동화된 네트워크 정책, 세그멘테이

션 및 에지 보안 관리가 가능합니다.

SSE 커넥터의 주요 기능

1. 타사 보안시스템과의 통합 SSE 커넥터는 Cisco ISE를 방화벽, IPS(Intrusion Prevention Systems), NAC(Network Access Control) 솔루션, SIEM(Security Information and Event Management) 시스템 등의 서드파티 보안 시스템과 쉽게 통합할 수 있도록 지원합니다. 이러한 외부 시스템은 ISE에서 데이터를 안전하게 전송하거나 수신할 수 있으며, 이를 통해 더 동적인 정책 시행을 위해 사용할 수 있습니다.

2. 실시간 위협정보: ISE를 다른 보안 시스템과 연결함으로써 SSE Connector는 실시간 위협 인텔리전스를 교환할 수 있도록 합니다. 이 정보에는 의심스러운 활동, 손상된 엔드포인트 또는 기타 보안 시스템에서 탐지한 악의적인 동작이 포함될 수 있으므로 ISE에서 현재 위협 레벨 또는 디바이스 상태를 기반으로 액세스 정책을 동적으로 조정할 수 있습니다.

3. 자동화된 치료: SSE Connector에서 활성화된 통합은 자동화된 교정 워크플로를 지원할 수 있습니다. 예를 들어, 시스템이 외부 보안 어플라이언스에 의해 손상된 것으로 플래그가 지정된 경우 ISE는 네트워크 액세스를 차단하는 정책을 자동으로 시행하거나 추가 조사를 위해 엔드포인트를 교정 네트워크 세그먼트로 리디렉션할 수 있습니다.

SSE 커넥터 확인 및 문제 해결

1. SSE 커넥터는 ISE에서 PassiveID 서비스가 활성화된 경우에만 활성화됩니다.

2 . debug의 sse-connector(connector.log) 구성 요소는 SSE 커넥터 관련 메시지에 대한 자세한 정보를 제공합니다.

Hermes(pxGrid 클라우드 에이전트)

Hermes(pxGrid Cloud Agent)는 클라우드 환경에서 ISE와 pxGrid(Platform Exchange Grid) 에코시스템 간의 통합을 지원하는 구성 요소입니다. Hermes는 ISE와 클라우드 기반 서비스 또는 플랫폼 간의 통신을 지원하는 데 사용되는 클라우드 기반 에이전트로, 서로 다른 네트워크 및 보안 시스템 전반에서 상황 정보를 공유하기 위한 pxGrid 프레임워크를 지원합니다.

Hermes(pxGrid Cloud Agent)의 주요 기능

1. 클라우드와 온프레미스 간 통합 Hermes(pxGrid Cloud Agent)는 클라우드 기반 서비스와 온프레미스 ISE 인프라 간의 원활한 통합을 지원하도록 설계되었습니다. 기존 온프레미스 네트워크 환경 이상으로 pxGrid의 기능을 확장하여 클라우드 기반 애플리케이션 및 서비스 전반에 안전한 데이터 교환 및 정책 시행이 가능합니다.

2 . pxGrid 에코시스템 지원: pxGrid는 네트워크 보안 솔루션 전반에서 상황 및 정보를 안전하게 공유하기 위한 Cisco 플랫폼입니다. Hermes는 pxGrid의 클라우드 에이전트 역할을 하여 ISE와 다양한 클라우드 기반 서비스 간에 안전한 실시간 통신을 가능하게 합니다. 이러한 통합을 통해 네트워크 보안 정책을 온프레미스 및 클라우드 환경 모두에서 일관되게 적용할 수 있으므로 보안을 더욱 쉽게 관리하고 적용할 수 있습니다.

3. 클라우드 기반 엔드포인트 가시성: Hermes의 주요 장점 중 하나는 ISE가 온프레미스 엔드포인트에 대한 가시성을 제공하는 것과 유사하게 클라우드 기반 엔드포인트에 대한 가시성을 제공한다는 점입니다. 컴플라이언스 상태, 보안 상태, ID 정보 등 클라우드의 디바이스와 사용자에 대한 데이터를 수집할 수 있습니다. 이를 통해 ISE는 온프레미스 디바이스와 마찬가지로 클라우드 엔드포인트에서 네트워크 액세스 정책을 시행할 수 있습니다.

4. ISE를 클라우드 환경으로 원활하게 확장하는 방법 Hermes의 주요 이점 중 하나는 ISE 온프레미스 환경과 점점 늘어나는 클라우드 네이티브 애플리케이션 간의 원활한 브리지를 제공한다는 것입니다. 따라서 기존 인프라를 완전히 정비하지 않고도 ISE 보안 정책, 인증 방법 및 액세스 제어를 클라우드 서비스로 더 쉽게 확장할 수 있습니다.

Hermes(Pxgrid 클라우드 에이전트) 확인 및 문제 해결

1. 기본적으로 Hermes 서비스는 비활성화되어 있으며 ISE를 Cisco PxGrid 클라우드에 연결하면 Hermes 서비스가 활성화됩니다. 따라서 ISE에서 Hermes 서비스가 비활성화된 경우 ISE **GUI > Administration > Deployment**에서 Pxgrid Cloud 옵션이 활성화되었는지 확인하고 **ISE 노드를 선택합니다**. Pxgrid 클라우드**를 수정하고 활성화합니다.**

2. Pxgrid 클라우드와 관련된 문제를 해결하는 데 유용한 디버깅은 hermes**.log** 및 pxcloud**.log**입니다. 이러한 디버깅은 Pxgrid 클라우드가 활성화된 Pxgrid 노드에서만 사용할 수 있습니다.

McTrust(Meraki 동기화 서비스)

McTrust(Meraki Sync Service)는 Cisco ISE와 Cisco Meraki 시스템 간의 통합을 가능하게 하는 서비스로서, 특히 네트워크 디바이스 및 액세스 정책을 동기화하고 관리할 수 있습니다. McTrust 서비스는 Meraki의 클라우드 매니지드 네트워크 인프라와 ISE 온프레미스 ID 및 정책 관리 시스템 간에 사용자 및 디바이스 정보를 동기화하는 커넥터 역할을 합니다.

McTrust의 주요 기능(Meraki Sync Service)

1. Meraki 디바이스와의 원활한 통합 McTrust를 통해 ISE는 Meraki의 클라우드 매니지드 디바이스와 동기화 및 통합할 수 있습니다. 여기에는 Meraki 포트폴리오의 일부인 Meraki 액세스 포인트, 스위치, 보안 어플라이언스와 같은 디바이스가 포함됩니다. ISE가 Meraki 인프라와 직접 통신할 수 있으므로 Meraki 관리 디바이스에 네트워크 액세스 제어 정책을 보다 쉽게 적용할 수 있습니다.

2. 장치동기화 자동화: Meraki 동기화 서비스는 ISE 정책을 Meraki 네트워크 디바이스와 자동으로 동기화합니다. 즉, ISE의 네트워크 액세스 제어 정책에 대한 변경 사항이 수동 개입 없이 Meraki 디바이스에 자동으로 반영됩니다. 따라서 관리자는 Meraki 및 ISE 플랫폼 모두에서 네트워크 액세스를 더 쉽게 관리할 수 있습니다.

3. Meraki 관리형 장치에 대한 정책 집행: McTrust를 사용하면 ISE가 인증 및 디바이스 상태를 기반으로 Meraki 디바이스에 네트워크 액세스 정책을 적용할 수 있습니다. 액세스를 요청하는 디바이스 또는 사용자의 보안 상태에 따라 VLAN 할당 조정, ACL(Access Control List) 적용, 특정 네트워크 리소스에 대한 액세스 제한 등의 정책을 Meraki 네트워크 요소에 동적으로 할당할 수 있습니다.

4. Meraki 대시보드 통합: McTrust는 ISE를 Meraki 대시보드와 직접 통합하여 통합 관리 인터페이스를 제공합니다. 이러한 통합을 통해 관리자는 Meraki 클라우드 매니지드 인터페이스 내에서

Meraki 디바이스와 ISE 매니지드 리소스 모두에 대한 네트워크 정책 및 액세스 제어 규칙을 보고 관리할 수 있습니다.

McTrust 확인 및 문제 해결(Meraki Sync Service)

1. ISE GUI -> Work Centers -> TrustSec -> Integrations -> Sync status에 로그인합니다. 발견된 모든 문제/오류를 확인합니다.

2. ISE 노드의 모든 관리자 인증서가 활성 상태이고 유효한지 확인합니다.

Meraki 동기화 서비스 트러블슈팅에 유용한 디버그는 meraki-connector.log입니다.

ISE 노드 내보내기

ISE 노드 내보내기 서비스는 ISE 시스템, 특히 ISE 노드(관리 노드, 모니터링 노드 또는 정책 서비스 노드)에서 성능 메트릭을 모니터링하고 수집하는 데 사용되는 구성 요소입니다.

ISE 노드 내보내기의 주요 기능

1.메트릭 내보내기: ISE 노드 엑스포터는 CPU 사용량, 메모리 사용량, 디스크 사용률, 네트워크 통계, 시스템 로드 및 기타 운영 체제 레벨 메트릭과 같은 다양한 성능 관련 메트릭을 제공합니다. 이러한 메트릭은 ISE 노드의 상태 및 성능을 모니터링하는 데 사용되며 Grafana와 같은 모니터링 대시보드에서 시각화할 수 있습니다.

2. 시스템 상태 모니터링: 성능 데이터를 Prometheus로 내보내면 ISE Node Exporter에서 ISE 노드의 상태 및 운영 상태를 지속적으로 모니터링할 수 있습니다. 관리자는 미리 정의된 임계값을 기반으로 알림을 생성하여 성능 저하 또는 시스템 문제를 알릴 수 있습니다.

3. 프로메테우스 통합 ISE 노드 엑스포터는 일반적으로 신뢰성과 확장성을 위해 설계된 오픈 소스 모니터링 및 알림 툴킷인 Prometheus와 함께 사용됩니다. 노드 엑스포터는 Prometheus에서 폐기할 수 있는 시스템 레벨 메트릭을 공개하여 시계열 데이터를 수집하고 저장합니다.

ISE Prometheus 서비스

ISE Prometheus 서비스는 ISE 시스템에서 성능 메트릭을 모니터링하고 수집할 수 있도록 Prometheus를 ISE와 통합하는 서비스입니다. Prometheus는 시계열 데이터를 수집, 저장 및 분석하는 데 사용되는 오픈 소스 모니터링 및 알림 툴킷이며, ISE Prometheus Service를 통해 ISE는 모니터링을 위해 내부 메트릭을 Prometheus에 노출할 수 있습니다.

ISE Prometheus Service의 주요 기능

1. 모니터링을 위한 메트릭 수집: ISE Prometheus Service는 ISE 시스템과 관련된 다양한 운영 및 성능 메트릭을 내보내도록 설계되었습니다. 이러한 메트릭에는 일반적으로 CPU 사용률 및 시스템 로드, 메모리 사용량, 디스크 사용량 및 I/O 성능, 네트워크 통계, 인증 요청 통계, 정책 시행 통계, 시스템 상태 및 가동 시간 데이터가 포함되지만 이에 국한되지 않습니다

2. 프로메테우스 통합 Prometheus 서비스는 ISE가 Prometheus와 호환되는 형식으로 데이터를 노

출할 수 있도록 허용하며, 이는 정기적으로 이 데이터를 삭제합니다. 그런 다음 Prometheus는 데이터를 시계열 데이터베이스에 저장하므로 ISE 시스템의 추세 및 기록 성능을 추적할 수 있습니다.

3. 그라파나를 이용한 시각화 및 보고 ISE의 Prometheus Service는 인기 있는 오픈 소스 시각화 도구인 Grafana와 원활하게 통합됩니다. 관리자는 메트릭을 Prometheus로 내보낸 후 Grafana 대시보드를 사용하여 데이터를 실시간으로 시각화할 수 있습니다. 이를 통해 성능 병목 현상, 시스템 트렌드, ISE 구축의 잠재적 문제를 쉽게 식별할 수 있습니다.

ISE Grafana 서비스

ISE Grafana Service는 모니터링 및 데이터 시각화를 위한 오픈 소스 플랫폼인 Grafana를 사용하여 시스템 성능 메트릭의 시각화를 제공하는 서비스입니다. Prometheus와 통합되어 ISE에서 수집된 실시간 및 기록 데이터를 표시하므로 관리자는 ISE 시스템의 상태, 성능 및 사용법에 대한 통찰력을 제공하는 대화형 대시보드를 생성할 수 있습니다.

ISE Grafana Service의 주요 기능

1. 맞춤형 대시보드: Grafana는 맞춤 설정이 가능하므로 관리자가 특정 모니터링 요구 사항에 따라 대시보드를 만들고 수정할 수 있습니다. Prometheus에서 특정 데이터 포인트를 추출하기 위해 사용자 지정 쿼리를 만들 수 있으며, 이러한 쿼리는 그래프, 테이블, 히트맵 등과 같은 다양한 형식으로 시각화할 수 있습니다.

2. 분산 ISE 구축을 위한 중앙 집중식 모니터링: 여러 ISE 노드가 서로 다른 위치에 구축된 분산 ISE 구축의 경우 Grafana는 각 노드에서 수집된 모든 시스템 메트릭을 중앙에서 볼 수 있습니다. 이를 통해 관리자는 단일 위치에서 전체 ISE 구축의 성능을 모니터링할 수 있습니다.

3. 이력 자료 및 동향 분석: Grafana는 Prometheus에 저장된 데이터를 사용하여 시스템 메트릭의 기록 분석을 지원하므로 관리자는 시간의 경과에 따른 추세를 추적할 수 있습니다. 예를 들어, 지난 한 달 동안 CPU 사용량이 어떻게 변경되었는지 또는 인증 성공률이 어떻게 변동했는지 모니터링할 수 있습니다. 이 기록 데이터는 용량 계획, 트렌드 분석, 장기적 문제 파악에 유용합니다.

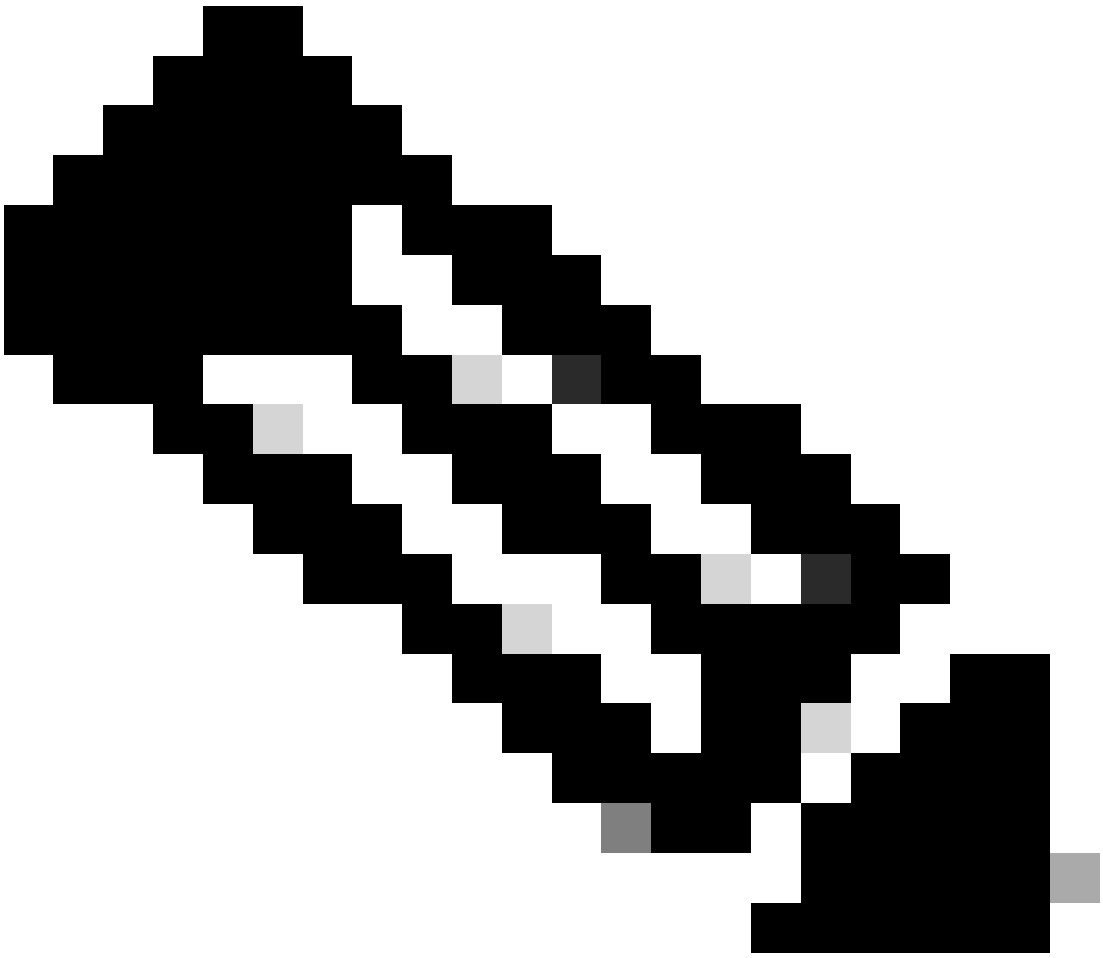
ISE Grafana Service, ISE Prometheus Service, ISE Node Exporter 확인 및 문제 해결

1. ISE Grafana Service, ISE Prometheus Service 및 ISE Node Exporter Service는 함께 작동하며 Grafana Stack Services라고 합니다. 이러한 서비스 트러블슈팅을 위해 사용할 특정 디버깅이 없습니다. 그러나 이러한 명령은 문제 해결에 도움이 됩니다.

show logging application ise-prometheus/prometheus.log

show logging application ise-node-exporter/node-exporter.log

show logging application ise-grafana/grafana.log



참고: 모니터링이 활성화된 경우 ISE 노드 내보내기, ISE Prometheus 서비스 및 ISE Grafana 서비스가 실행 중이어야 하며 이러한 서비스가 중단되면 데이터 수집 중에 문제가 발생합니다 .

ISE MNT 로그분석 Elasticsearch

ISE MNT LogAnalytics Elasticsearch는 Elasticsearch를 ISE 모니터링 및 문제 해결(MNT) 기능과 통합하는 구성 요소입니다. ISE 로그 및 이벤트와 관련된 로그 어그리게이션, 검색 및 분석에 사용됩니다. Elasticsearch는 널리 사용되는 분산 검색 및 분석 엔진이며, ISE와 통합할 경우 ISE 구성 요소에서 생성된 로그 데이터를 저장, 분석 및 시각화하는 시스템 기능을 향상시킵니다.

ISE MNT LogAnalytics Elasticsearch의 주요 기능

1. 로그 저장 및 인덱싱 ISE의 Elasticsearch 서비스는 ISE에서 생성된 로그 데이터를 저장하고 인덱싱하는 역할을 합니다. Elasticsearch는 분산형 검색 및 분석 엔진이며, 이를 통해 특정 이벤트, 오류 또는 시스템 활동을 빠르게 검색, 쿼리 및 검색할 수 있는 방식으로 ISE 로그를 저장할 수 있습니다.

2. 로그 분석과의 통합 ISE MNT LogAnalytics Elasticsearch는 로그 분석과 함께 작동하여 포괄적인 로깅 솔루션을 제공합니다. ISE는 인증, 정책 시행, 시스템 운영 및 기타 활동과 관련된 로그 데이터를 수집할 수 있습니다. 이 데이터는 Elasticsearch에 저장되므로 더 쉽게 세부 분석을 수행하고 ISE 동작에 대한 통찰력을 얻을 수 있습니다.

3. 중앙집중식 로깅(Centralized Logging) ISE는 Elasticsearch와 통합하여 중앙 집중식 로깅 솔루션을 제공하는데, 이는 분산 로그 수집이 필요한 환경에 매우 중요합니다. 이를 통해 관리자는 여러 ISE 노드의 로그를 통합된 단일 인터페이스에서 보고 분석할 수 있으므로, 문제 해결 및 ISE 성능 모니터링이 더 쉬워집니다.

4. 로그 분석 및 문제 해결: ISE MNT LogAnalytics Elasticsearch 서비스는 관리자가 로그 데이터에 쉽게 액세스하여 시스템 동작을 분석하고 문제를 해결할 수 있도록 지원합니다. 예를 들어 인증 실패가 갑자기 급증하거나 예기치 않은 시스템 중단이 발생하면 Elasticsearch에서 로그 데이터를 빠르게 쿼리하여 근본 원인을 식별할 수 있습니다.

ISE M&T LogAnalytics Elasticsearch 확인 및 문제 해결

1. ISE에서 로그 분석 서비스를 비활성화하고 다시 활성화하면 도움이 됩니다. Operations(운영) > System 360 > Settings(설정) > Log analytics(로그 분석)로 이동합니다(토글 옵션을 사용하여 비활성화 및 활성화).

2. ISE 루트에서 M&T LogAnalytics를 다시 시작하면 문제가 해결됩니다. 이 작업을 수행하려면 Cisco TAC에 문의하십시오.

알려진 결함

Cisco 버그 ID ·66198

ISE Logstash 서비스

ISE Logstash Service는 오픈 소스 데이터 처리 파이프라인인 Logstash를 로그 수집, 변환 및 포워딩을 위해 ISE와 통합하는 구성 요소입니다. Logstash는 로그 수집기 및 로그 전달자 역할을 하므로 ISE 로그를 처리하고 분석, 저장 및 모니터링을 위해 다른 시스템으로 전송할 수 있습니다. Logstash는 로그 또는 기타 데이터를 수집, 구문 분석, 저장, 분석 및 시각화를 위해 다른 소스에서 중앙 위치로 전달하는 강력한 오픈 소스 툴입니다. ISE의 컨텍스트에서 ISE Logstash Service는 로그를 처리하고 중앙 집중식 로깅 시스템으로 전달하는 데 사용됩니다. 이 시스템에서는 로그를 추가로 분석, 모니터링 및 시각화할 수 있습니다.

ISE Logstash Service의 주요 기능

1. 로그 수집 및 전달: ISE Logstash Service의 기본 기능은 다양한 ISE 구성 요소(예: 인증 로그, 시스템 로그, 정책 시행 로그 등)에서 로그 데이터를 수집하고 저장 및 분석을 위해 중앙 위치(일반적으로 Elasticsearch 또는 다른 로그 관리 시스템)로 전달하는 것입니다.

2. 로그 구문 분석: Logstash는 수집된 로그를 구조화된 형식으로 구문 분석할 수 있습니다. 원시 로그 데이터를 처리하고 그로부터 의미 있는 정보를 추출하여 로그 항목을 쿼리 및 분석하기 쉬운 형식으로 변환합니다. Elasticsearch 또는 다른 시스템에 데이터를 전달하기 전에 데이터를 필터링, 구문 분석 및 보강하는 작업이 포함될 수 있습니다.

ISE Logstash 서비스 확인 및 문제 해결

1. 사용할 특정 디버그가 없습니다. 그러나 **show logging application ise-logstash/logstash.log은** 서비스 상태에 대한 통찰력을 제공합니다.

2. ISE에서 로그 분석 서비스를 비활성화하고 다시 활성화하면 도움이 됩니다. **Operations(운영) > System 360 > Settings(설정) > Log analytics(로그 분석)로** 이동합니다(토글 옵션을 사용하여 비활성화 및 활성화).

Logstash 서비스와 관련된 알려진 결함

Cisco 버그 ID ·74832

Cisco 버그 ID ·58596

ISE 키바나 서비스

ISE Kibana Service는 오픈 소스 데이터 시각화 도구인 Kibana를 ISE 로깅 및 모니터링 인프라와 통합하는 구성 요소입니다. Kibana는 (로그 데이터를 저장하고 인덱싱하는) Elasticsearch와 함께 작동하여 ISE 로그 및 성능 메트릭을 시각화, 검색 및 분석할 수 있는 강력한 플랫폼을 제공합니다.

ISE Kibana Service의 주요 기능

1. 자료가상화: ISE Kibana Service를 통해 관리자는 ISE에서 수집된 로그 데이터를 시각적으로 표시할 수 있습니다. 여기에는 다음이 포함될 수 있습니다.

- 인증, 정책 시행, 사용자 활동 및 시스템 상태의 추세에 대한 차트, 그래프 및 테이블
- 파이 차트, 선 그래프 및 막대 차트를 통해 실패한 로그인 수, 세션 기간 또는 시간의 경과에 따른 오류 등과 같은 특정 메트릭을 추적할 수 있습니다.

ISE Kibana 서비스 확인 및 문제 해결

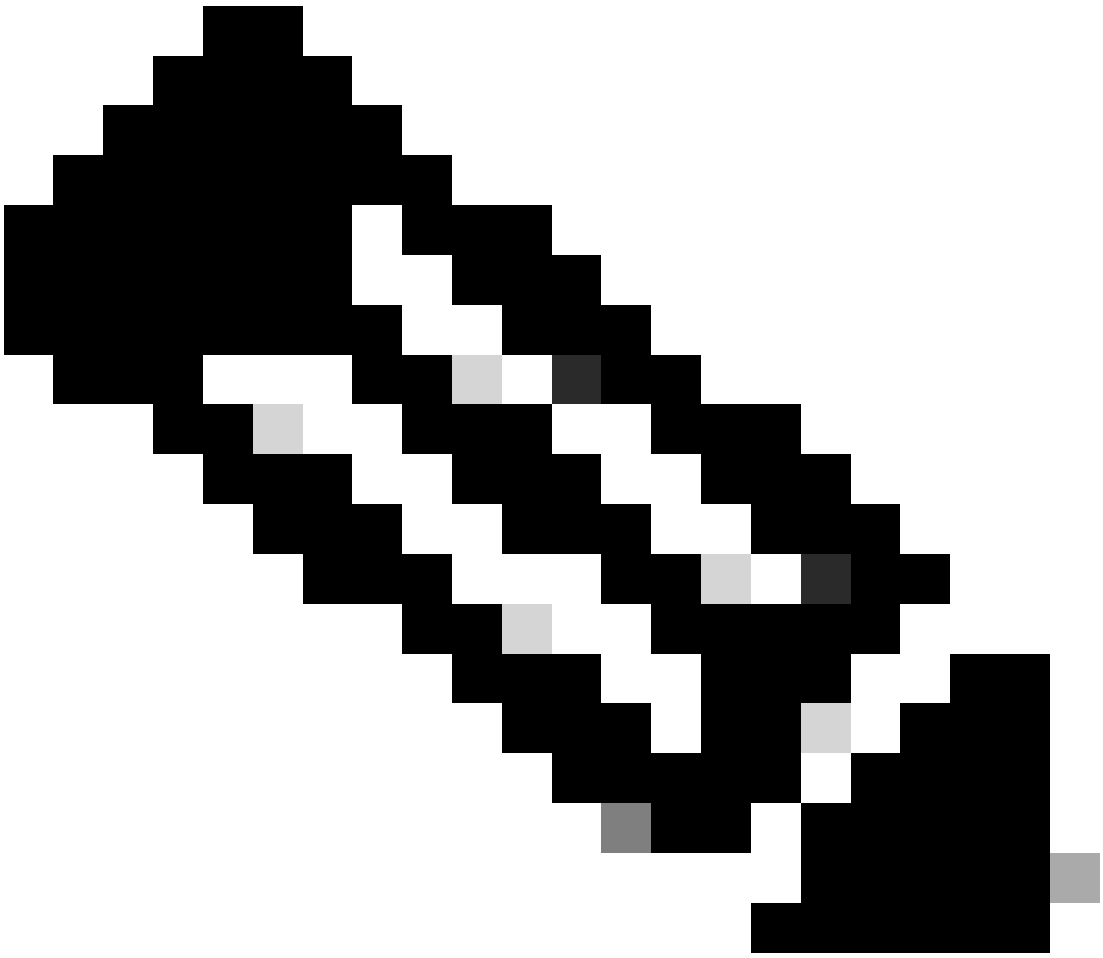
1. ISE kibana 서비스가 실행되고 있지 않으면 ISE에서 로그 분석을 사용하지 않도록 설정하고 다시 사용하도록 설정합니다. Operations(운영) > System 360 > Settings(설정), Log analytics(로그 분석)로 이동합니다(토글 옵션을 사용하여 사용 및 사용 안 함).

2. 많은 시나리오에서 /etc/hosts 폴더에 중복 항목이 있을 수 있으므로 문제가 발생합니다. 중복 항목을 제거하려면 TAC에 문의하십시오.

키바나 문제와 관련된 알려진 결함

Cisco 버그 ID ·78050

Cisco 버그 ID ·59848



참고: 로그 분석이 활성화되면 ISE MNT LogAnalytics Elasticsearch, ISE Logstash Service, ISE Kibana Service가 실행되고 있어야 하며 이러한 서비스가 중단되면 데이터 수집 중에 문제가 발생합니다.

ISE 네이티브 IPSec 서비스

ISE 기본 IPSec 서비스는 ISE 노드 간 또는 ISE와 기타 네트워크 디바이스 간의 보안 통신을 제공하는 IPSec(Internet Protocol Security)을 기본적으로 지원합니다. IPSec은 통신 세션에서 각 IP 패킷을 인증하고 암호화하여 네트워크 통신을 보호하는 데 사용되는 프로토콜 모음입니다. 기본 IPSec 서비스는 광범위한 보안 및 네트워크 액세스 관리 프레임워크의 일부입니다. IPsec VPN 연결을 처리하고 관리할 수 있는 기능을 제공하여 ISE 시스템과 원격 엔드포인트 간에 전송되는 데이터를 보호합니다. 여기에는 클라이언트 디바이스, 네트워크 액세스 디바이스(예: 라우터 또는 방화벽) 또는 기타 ISE 노드와의 상호 작용이 포함될 수 있으며, 여기서 IPsec 암호화 및 터널링은 중요한 정보를 보호하는 데 필요합니다.

ISE Native IPSec Service의 주요 기능

1. IPsec을 통한 보안 통신 ISE Native IPSec Service의 기본 기능은 IPsec을 사용하여 보안 통신 채

널을 설정하고 유지하는 것입니다. 여기에는 ISE와 다른 디바이스 간에 전송되는 데이터가 가로채기, 변조 및 무단 액세스로부터 보호되도록 하기 위한 암호화 및 인증 메커니즘이 사용됩니다.

2. IPsec VPN 연결: ISE Native IPSec Service는 IPsec 프로토콜을 사용하여 데이터 전송을 위한 안전한 암호화 터널을 제공하는 VPN 연결을 지원합니다. 이는 특히 신뢰할 수 없는 네트워크(예: 인터넷)를 통해 ISE 환경에 안전하게 액세스해야 하는 원격 근무자, 지사 또는 기타 위치에 유용합니다.

3. 원격 액세스 VPN 지원: Native IPSec Service는 원격 액세스 VPN 컨피그레이션에 참여할 수 있습니다. 원격 직원 또는 지사와 같이 오프사이트에 있는 사용자 또는 디바이스가 IPsec 터널을 통해 ISE 시스템에 안전하게 연결됩니다. 이 서비스는 ISE 환경에 도달하기 전에 모든 원격 액세스 트래픽이 암호화되고 인증되도록 보장합니다.

4.IPsec VPN 클라이언트 호환성: ISE 네이티브 IPSec 서비스는 IPsec VPN 클라이언트와의 호환성을 보장합니다. 또한 일반적인 클라이언트 구성을 지원하므로 민감한 데이터를 위험에 노출시키지 않고 장치가 네트워크에 안전하게 연결할 수 있습니다.

기본 IPSec 서비스 확인 및 문제 해결

1. 네이티브 IPSec 서비스에 사용할 특정 디버그가 없습니다. ISE CLI를 통해 show logging application strongswan/charon.log tail 명령을 사용하여 로그를 확인합니다.

2. 터널에 문제가 있는 경우 GUI > Administration > System > Settings > Protocols > IPSec > Native IPSec을 통해 터널 설정 상태를 확인합니다.

MFC 프로파일러

MFC 프로파일러는 네트워크 장치 및 엔드포인트 프로파일링에 사용되는 특수 구성 요소입니다. 프로파일링은 ISE가 네트워크의 디바이스를 식별하고 분류하며 디바이스 및 동작의 유형에 따라 적절한 네트워크 정책을 적용할 수 있도록 하기 때문에 네트워크 액세스 제어의 핵심 부분입니다.

ISE에서 MFC 프로파일러 서비스의 주요 기능

1. 트래픽 프로파일링: ISE의 MFC 프로파일러 서비스는 트래픽 데이터의 수집 및 프로파일링을 담당합니다. 사용 중인 애플리케이션 유형, 액세스한 서비스, 디바이스에서 표시되는 트래픽 패턴 등 엔드포인트가 네트워크에서 어떻게 작동하는지 모니터링합니다. 이 데이터는 각 엔드포인트의 프로필을 작성하는 데 도움이 됩니다.

2. 엔드포인트 프로파일링: MFC 프로파일러 서비스를 사용하면 ISE에서 해당 동작에 따라 엔드포인트를 식별하고 분류할 수 있습니다. 예를 들어 트래픽 패턴을 기반으로 엔드포인트가 프린터, 컴퓨터 또는 모바일 디바이스인지 탐지합니다. 이를 통해 다양한 유형의 디바이스에 대해 더 구체적인 정책을 시행하여 보안 및 운영 효율성을 높일 수 있습니다.

MFC 프로파일러 서비스 확인 및 문제 해결

1. ISE GUI -> Administration -> Profiling -> MFC profiling and AI 규칙으로 이동하여 서비스가 활성화되어 있는지 확인합니다.

2. 서비스가 활성화되었지만 ISE CLI에서 show application status ise 명령을 통해 비활성화됨/실행되지 않음으로 표시되는 경우. 1단계를 참조하여 ISE에서 MFC 프로파일링 서비스를 비활성화했다가 다시 활성화합니다.

문제 해결에 유용한 디버그: 디버그의 MFC 프로파일러 구성 요소입니다. ISE CLI를 통해 show logging application ise-pi-profiler.log tail 명령을 사용하여 지원 번들에서 로그를 확인하거나 로그를 테일링할 수 있습니다.

MFC 프로파일러가 비활성 상태 대신 실행 중이 아닌 것으로 표시되는 데 알려진 오류:

Cisco 버그 ID ·72853

핵심 사항

1. 서비스를 복구하려면 ISE CLI를 통해 application stop ise 및 application start ise 명령을 사용하여 서비스를 재시작합니다.

2. 문제가 있는 경우 ISE GUI/ISE CLI에서 캡처할 지원 번들이 있는지 확인하여 문제를 추가로 확인합니다. GUI 및 CLI를 통한 ISE 지원 번들 생성을 위한 참조 링크: Identity Services Engine에서 지원 번들 수집

3. 문제가 리소스, 로드 평균, 디스크 사용률 등과 관련된 경우 분석을 위해 스레드 덤프 및 힙 덤프를 수집해야 합니다.

4. 노드를 다시 로드하기 전에 Cisco TAC에 문의하고 추가 분석을 위해 보안 로그를 제공합니다.

ISE의 표준 문제

ISE 서비스의 문제 외에도, 이러한 문제는 기본적인 트러블슈팅 단계와 함께 ISE 노드에서 발견되는 몇 가지 문제입니다.

높은 로드 평균, 리소스 사용률 문제(CPU / 메모리 / 디스크), 리소스 부족 확인

1. ISE CLI를 통해 show inventory 명령을 사용하여 Cisco 권장 리소스가 노드에 할당되었는지 확인합니다.

2. ISE 노드의 CLI에서 tech top 명령을 실행하여 ISE의 리소스 사용률을 확인합니다.

3. ISE CLI를 통해 show disk 명령을 사용하여 디스크 사용률을 확인합니다.

4. 비활성 엔드포인트를 제거하고 노드의 로컬 디스크를 지우고 업그레이드 정리를 수행합니다.

문제가 지속되면 Cisco TAC에 문의하여 문제가 발생한 노드에서 보안 지원 번들, 힙 덤프 및 스레드 덤프를 제공합니다.

힙 덤프를 보호하려면 ISE 노드의 CLI에 로그인하고 application configure ise **명령을** 실행합니다. **옵션 22를** 선택합니다.

스레드 덤프를 보호하려면 ISE 노드의 CLI에 로그인하고 **application configure ise 명령을** 실행하고 **옵션 23을** 선택합니다. 스레드 덤프는 지원 번들에 포함되어 있거나 **show logging application**

appserver/catalina.out 명령을 사용하여 ISE CLI를 통해 **전달될** 수 있습니다.

모니터링 문제 확인 및 문제 해결

ISE의 MnT(Monitoring and Troubleshooting) 기능은 모니터링, 보고 및 알림 기능을 제공하는 ISE 아키텍처의 주요 블록 중 하나입니다.

ISE는 다음을 포함한 여러 위치에 모니터링 정보를 표시합니다.

- Cisco ISE 홈 페이지
- 컨텍스트 가시성 보기
- RADIUS 라이브 로그 및 라이브 세션
- 전역 검색
- 위협 중심 NAC 라이브 로그
- TACACS 라이브 로그

Monitoring and Troubleshooting Category(모니터링 및 트러블슈팅 카테고리)에서 관찰된 일반적인 문제:

1. Radius/TACACS 라이브 로그를 사용할 수 없음
2. 라이브 세션을 사용할 수 없음
3. 상태 요약을 사용할 수 없음
4. MnT 노드에서 나타나는 성능(높은 CPU/메모리) 문제

문제를 좁히기 위해 MnT 노드에서 디버그를 활성화합니다.

1. Cisco-mnt
2. 컬렉터
3. Cpm-mnt
4. 런타임 로깅

이 정보는 debug에 언급된 구성 요소 외에도 문제 해결에 도움이 될 수 있습니다.

1. 라이브 세션도 영향을 받습니까? 아니면 라이브 로그만 영향을 받습니까?
2. Radius 또는 TACACS 로그가 영향을 받습니까? 아니면 둘 다 받습니까?
3. MnT 노드에서 CPU 사용률이 높거나 스왑 공간이 많이 사용된다고 보십니까?
4. MnT 노드에 몇 개의 버퍼 파일이 표시됩니까? 버퍼 파일은 다음 위치에서 찾을 수 있습니다. /opt/CSCOcpm/mnt/data/collector
5. 메모리 및 CPU 예약이 활성화되었는지 여부. 활성화되지 않은 경우 활성화하십시오.
6. 최근 MnT/config/session DB 재설정이 수행되었습니까?
7. PSN에서 MnT 노드로 syslog가 전송됩니까?

MnT용 Syslog 서비스를 사용하는 경우 문제 해결을 위해 이 정보가 필요합니다.

1. 보안 syslog 대상을 사용하고 계십니까? 그렇지 않으면 스레드에 교착 상태가 발생하여 컬렉터가 작동하지 않는 것으로 알려져 있으므로 비활성화하십시오.
2. 보안 syslog 대상을 사용 중입니까? Administration(관리)->Logging(로깅)->Remote Logging Targets(원격 로깅 대상)->Secure Syslog collector 1 and 2(보안 Syslog 컬렉터 1 및 2)에서 인증서 매핑이 올바르게 설정되었는지 확인하십시오

3. 로깅 범주가 적절하게 설정되었는지(사용하지 않는/원치 않는 로깅 범주를 제거하는 것이 권장 - MnT 노드의 로드를 줄임) 확인하고 로깅 대상이 올바르게 구성되었는지 확인합니다.
4. 지원 번들의 awrrep *.html 파일을 확인하여 어떤 구성 요소가 더 자주 syslog를 전송하는지 파악하고 힌트를 얻습니다. 예를 들어 TACACS 테이블이 삽입 또는 업데이트 쿼리와 함께 표시되는 경우, 어떤 syslog가 더 자주 전송되는지 파악하기 위해 컬렉터 로그를 확인하여 상관관계를 분석할 수 있습니다

문제가 MnT 노드의 성능과 관련된 경우 다음 정보가 필요합니다.

1. MnT 노드의 ISE CLI에서 제공하는 tech top 출력.

2. CPU가 높으면 메모리 또는 스왑 공간 사용률도 높습니까?

3. 힙 덤프 및 스레드 덤프가 보호된 지원 번들.

참조

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3
- ISE에서 디버깅 문제 해결 및 활성화

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.