문제 해결

Cisco ISE에서 서비스 모니터링 및 문제 해결

모니터링 및 문제 해결(MnT) 서비스는 모든 Cisco ISE 런타임 서비스에 사용할 수 있는 포괄적인 ID 솔루션입니다. **Operations(**운영**)** 메뉴에는 다음 구성 요소가 포함되어 있으며 기본 PAN(Policy Administration Node)에서만 볼 수 있습니다. **Operations(**운영**)** 메뉴는 기본 모니터링 노드에 표시되지 않습니다.

- 모니터링: 네트워크에 대한 액세스 활동의 상태를 나타내는 의미 있는 데이터를 실시간으로 표시합니다. 이 정보는 쉽게 해석할 수 있으며 작동 조건에 영향을 미칠 수 있습니다.
- 문제 해결: 네트워크의 액세스 문제를 해결하기 위한 상황별 지침을 제공합니다. 이를 통해 관리자가 사용자의 문제를 해결하고 시기 적절하게 해결 방법을 제공할 수 있습니다.

- 보고: 관리자가 트렌드를 분석하고 시스템 성능 및 네트워크 활동을 모니터링하는 데 사용할 수 있는 표준 보고서 카탈로그를 제공합니다. 다양한 방법으로 보고서를 맞춤화하고 나중에 사용하기 위해 저장할 수 있습니다. 모든 보고서(**Health Summary(**상태 요약 보고서**)** 제외)에서 와일드카드와 여러 값을 사용하여 **Identity(ID)**, **Endpoint ID(**엔드포인트 **ID)** 및 **ISE Node(ISE** 노드**)** 필드에 대해 기록을 검색할 수 있습니다.

ISE Community Resource(ISE 커뮤니티 리소스)

문제 해결 TechNote의 전체 목록은 ISE Troubleshooting TechNotes를 참고하십시오.

Cisco ISE에서 TAC 지원 케이스 열기

Cisco ISE에서 케이스를 제기하여 구축 문제에 대한 지원을 요청하십시오. Cisco ISE 포털의 TAC 지원 케이스 기능을 사용하면, 문제가 발생한 특정 노드에 대한 지원 사례를 쉽게 제기할 수 있습니다. 제시된 양식을 통해 제공하는 정보와 함께 노드의 일련 번호 및 사용중인 Cisco ISE 버전과 같은 정보도 Cisco TAC로 전송됩니다.

참고 이 기능은 Cisco ISE 릴리스 3.0 패치 1 이상에서 사용할 수 있습니다.

단계 **1** Cisco ISE 포털의 홈 창에서 오른쪽 상단 모서리에 있는 물음표 아이콘을 클릭합니다.

단계 **2** 표시되는 인터랙티브 도움말 메뉴에서 **Resources(**리소스**)**를 클릭하고 드롭 다운 목록에서 **TAC Support Cases(TAC** 지원 케이스**)**를 선택합니다.

단계 **3** 표시되는 새 창에서 cisco.com 자격증명을 사용하여 로그인합니다. 기능에 액세스할 수 없다는 오류 메시지가 표시되면 고객 지원에 문의하여 Cisco ISE 계약의 약관을 검토하십시오.

단계 **4** 로그인하면 **Cases(**케이스**)** 창이 표시됩니다. **Open A Case(**케이스 열기**)**를 클릭합니다.

단계 **5** **Open Case(**케이스 열기**)** 양식에서

1. 드롭 다운 목록에서 케이스를 열 최대 4 개의 노드를 선택합니다. 기본 PAN 및 MnT 노드가 기본적으로 선택됩니다.
2. **Title(**제목**)** 및 **Description(**설명**)** 필드에 문제의 세부정보를 입력합니다.
3. **Contract ID(**계약 **ID)** 및 **Product Name(**제품 이름**)** 필드에 필수 정보를 입력합니다.
4. (선택 사항) 다음에 대한 값을 선택합니다.
    1. **Tech(**기술**)** : Cisco ISE 릴리스 드롭 다운 목록에서 선택합니다. 여기서 **Cisco Identity Services Engine-2.6**은 릴리스 2.6 이상을 나타냅니다.
    2. **Sub Tech(**하위 기술**)**: Cisco ISE 기능의 드롭 다운 목록에서 문제 영역을 선택합니다.
    3. **Problem Code(**문제 코드**)**: 드롭 다운 목록에서 해당 값을 선택합니다.

다음에 수행할 작업

이를 통해 Cisco TAC는 문제의 세부정보를 수신하고 문제를 조사 및 해결하기 위해 연락을 드릴 것입니다. 여기서 생성되는 케이스는 기본적으로 심각도 레벨 3입니다. 심각도가 더 높은 케이스(1 및 2)의 경우 Cisco TAC에 문의하여 케이스를 엽니다.

TAC Support Cases(TAC 지원 케이스**)** 창에서 케이스 세부정보를 확인합니다. 표시된 케이스 목록에서 검토할 케이스의 확인란을 선택합니다. 케이스 세부정보 및 이 케이스에 대한 TAC의 업데이트가 포함된 메모 목록을 보려면 **View Case(**케이스 보기**)**를 클릭합니다. 케이스에 나만의 메모를 추가하려면 **Add Notes(**메모 추가**)**를 클릭합니다.

케이스를 닫으려면 **Close Case(**케이스 닫기**)** 버튼을 클릭합니다. 케이스를 닫을 때 그 사유를 제시해야 합니다.

상태 확인

Cisco ISE 릴리스 3.0에는 Cisco ISE 구축의 모든 노드를 진단하는 온디맨드 상태 확인 옵션이 도입되었습니다. 작업 전에 모든 노드에서 상태 확인을 실행하면 다운타임을 줄이고 중요한 문제를 식별하여 Cisco ISE 시스템의 전반적인 기능을 개선할 수 있습니다. 상태 확인은 구성 요소의 작동 상태를 알려주고 Cisco ISE 구성 요소가 손상된 경우 즉시 문제 해결 권장 사항을 안내합니다.

표 ***1:*** 상태 확인 구축

구축 유형	설명
플랫폼 지원 확인	이렇게 하면 구축에서 지원되는 플랫폼을 확인합니다. 34xx 및 기타 지원되지 않는 플랫폼 세부 정보를 확인하고 시스템에 최소 12 코어 CPU, 300GB 하드 디스크, 16GB 메모리가 있는지 확인합니다.
구축 검증	동기화 또는 진행 중인 구축 노드의 상태를 확인할 수 있습니다.
DNS 확인 가능성	호스트 이름 및 IP 주소의 정방향 및 역방향 조회를 확인합니다.
신뢰 저장소 인증서 검증	신뢰 저장소 인증서가 유효하거나 만료되었는지를 나타냅니다.
시스템 인증서 검증	각 노드에 대한 시스템 인증서 검증을 확인합니다.
디스크 공간 확인	플랫폼 지원 확인에 있는 하드 디스크를 확인합니다. 그리고 추가 업그레이드 절차를 위해 디스크의 사용 가능한 공간을 확인합니다.
NTP 연결성 및 시간 소스 확인	시스템에 구성된 NTP 및 시간 소스가 NTP 서버에서 오는지 확인합니다.

구축 유형	설명
로드 평균 확인	지정된 간격으로 시스템의 로드를 자주 확인합니다. 빈도는 1분, 5분 및 15분 간격입니다.
MDM 검증	구성된 MDM 서버와 PSN 서버 간의 연결을 확인합니다.
라이선스 검증	스마트 라이선스가 구성되어 있고 유효한지 확인합니다. 스마트 라이선스가 구성되지 않고 유효한 사용자인 경우, 라이선스를 구성하고 검증하도록 요청하는 경고가 표시됩니다.
서비스 또는 프로세스 실패	서비스 또는 애플리케이션이 실행 중이거나 장애가 발생한 상태를 나타냅니다.
I/O 대역폭 성능 확인	디스크 읽기 쓰기 속도를 확인합니다.

참고 구축 옆의 숫자는 노드의 수와 상태 확인 세부 사항을 나타냅니다. 예를 들어, 구축에 0/2가 있는 경우 0은 실패/진행/완료 상태의 노드 수를 나타내며 2는 구축의 노드 수를 나타냅니다.

참고 상태 확인 중에 노드가 15분 동안 응답을 반환하지 않으면 해당 노드에 대한 상태 확인 시간이 초과하게 됩니다.

상태 확인 시작

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Health Checks(**상태 확인**)**.

단계 **2** **Start health checks(**상태 확인 시작**)**를 클릭합니다.

정보 팝업 창에 다음 메시지가 표시됩니다.

상태 확인이 트리거되었습니다.

단계 **3** **Ok(**확인**)**를 클릭하여 상태를 확인합니다.

단계 **4** **Health Checks(**상태 확인**)** 창에서 각 구성 요소의 상태를 볼 수 있습니다. 다음 색상은 Cisco ISE 구성 요소의 상태를 나타냅니다.

색상	상태	작업
빨간색	좋지 않음	상자에서 제공되는 문제 해결 권장 사항을 보려면 드롭 다운 옵션을 클릭합니다. 문제를 해결하고 새로 고침 아이콘을 클릭합니다.
주황색	좋음 참고 구성 요소의 상태가 작업을 수행하기에 적합합니다. 그러나 향후 일부 기능에 영향을 미칠 수 있는 문제가 있습니다.	상자에서 제공되는 문제 해결 권장 사항을 보려면 드롭 다운 옵션을 클릭합니다.
녹색	좋음	추가 작업은 필요하지 않습니다.
파란색	좋음	정보 아이콘을 클릭하여 기능에 대한 중요 정보를 확인합니다.

단계 **5** **Download Reports(**보고서 다운로드**)**를 클릭합니다.

HealthChecksReport.json 파일은 Cisco ISE 구축의 자세한 상태 정보와 함께 로컬 시스템에 저장됩니다.

상태 확인이 트리거된 후 상태는 다음 3시간 동안 **Health Check(**상태 확인**)** 창에 유지됩니다. **Health Checks(**상태 확인**)** 창이 새로 고쳐지거나 만료될 때까지 상태 확인을 실행할 수 없습니다.

네트워크 권한 프레임워크 이벤트 플로우 프로세스

NPF(Network Privilege Framework) 인증 및 권한 부여 이벤트 플로우에서는 다음 표에서 설명하는 프로세스가 적용됩니다.

프로세스 단계	설명
1	NAD(Network Access Device)는 일반 권한 부여 또는 플렉스 권한 부여를 수행합니다.
2	웹 권한 부여를 통해 알 수 없는 에이전트없는 ID가 프로파일링됩니다.
3	RADIUS 서버가 ID를 인증하고 권한을 부여합니다.
4	포트에서 ID에 대해 권한 부여가 프로비저닝됩니다.

프로세스 단계	설명
5	권한이 부여되지 않은 엔드포인트 트래픽이 삭제됩니다.

모니터링 및 문제 해결 기능에 대한 사용자 역할 및 권한

모니터링 및 문제 해결 기능은 기본 사용자 역할과 연결됩니다. 수행할 수 있는 작업은 할당된 사용자 역할과 직접적으로 관련됩니다.

각 사용자 역할에 대해 설정된 권한 및 제한에 대한 자세한 내용은 *Cisco ISE* 관리자 가이드의 "Cisco ISE 관리 가이드: 개요" 장에서 "Cisco ISE 관리자 그룹" 섹션을 참고하십시오.

참고 Cisco TAC의 감독 없이 루트 쉘(shell)을 사용하여 Cisco ISE에 액세스하는 것은 지원되지 않으며 Cisco는 그로 인해 발생할 수 있는 서비스 중단에 대해 책임을 지지 않습니다.

모니터링 데이터베이스에 저장된 데이터

Cisco ISE 모니터링 서비스는 특수 모니터링 데이터베이스에 데이터를 수집하고 저장합니다. 네트워크 기능을 모니터링하는 데 사용되는 데이터 비율과 양에 따라 모니터링 전용 노드가 필요할 수 있습니다. Cisco ISE 네트워크가 정책 서비스 노드 또는 네트워크 디바이스에서 많은 양의 로깅 데이터를 수집하는 경우 모니터링 전용 Cisco ISE 노드를 사용하는 것이 좋습니다.

모니터링 데이터베이스에 저장된 정보를 관리하려면 데이터베이스에 대한 전체 백업과 증분 백업을 수행합니다. 여기에는 원치 않는 데이터를 비우기한 다음 데이터베이스를 복구하는 과정도 포함됩니다.

Cisco ISE 텔레메트리

텔레메트리는 네트워크의 시스템 및 디바이스를 모니터링하여 제품 사용 방식에 대한 피드백을 Cisco에 제공합니다. Cisco는 이 정보를 사용하여 제품을 개선합니다.

텔레메트리는 기본적으로 활성화됩니다. 이 기능을 비활성화하려면,

1. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Network Success Diagnostics(**네트워크 성공 진단**)** > **Telemetry(**텔레메트리**)**
2. **Enable Telemetry(**텔레메트리 비활성화**)** 확인란을 선택 취소하면 텔레메트리가 비활성화됩니다.

   - **Cisco** 계정: 텔레메트리에서 이메일을 받을 수 있도록 Cisco 계정을 입력합니다. 또한 사용자에게 영향을 미칠 수 있는 심각한 문제를 발견할 경우 이 ID를 사용하여 연락을 취할 수도 있습니다.

- 전송 게이트웨이: Cisco ISE와 Cisco의 외부 텔레메트리 서버 간에 프록시를 사용하여 추가 보안을 제공할 수 있습니다. 이 경우 해당 확인란을 선택하고 프록시 서버의 FQDN을 입력합니다. 텔레메트리에는 프록시가 필요하지 않습니다.

  Cisco는 전송 게이트웨이용 소프트웨어를 제공합니다. Cisco.com에서 다운로드할 수 있습니다. 이 소프트웨어는 Linux 서버에서 실행됩니다. RHEL 서버에서 전송 게이트웨이 소프트웨어를 구축하는 방법에 대한 자세한 내용은 Smart Call Home Deployment Guide를 참조하십시오. 이 Cisco 소프트웨어를 사용하는 경우 URL 값은 **<FQDN of proxyserver>/Transportgateway/services/DeviceRequestHandler**입니다. 이 게이트웨이를 사용하여 스마트 라이선싱 서버에 연결할 수도 있습니다. 전송 게이트웨이 버전 3.5부터는 포트를 변경할 수 없지만 FQDN 대신 IP 주소를 입력할 수 있습니다.

텔레메트리가 수집하는 정보

텔레메트리는 Cisco에 다음과 같은 정보를 전송합니다.

노드:

각 **PAN(Policy Administration Node)**의 경우

- 현재 포스처 엔드포인트 수
- 현재 pxGrid 클라이언트 수
- 현재 MDM에서 관리하는 엔드포인트 수
- 현재 게스트 사용자 수
- 해당 텔레메트리 기록의 시작 및 종료 날짜
- FIPS 상태

각 **PSN(Policy Service Node)**의 경우

- 프로파일러 프로브 수
- 노드 서비스 유형
- 사용된 패시브 ID

모든 노드의 경우

- 총 및 활성 NAD
- CPU 코어 수
- VM 지원 디스크 공간
- VM 메모리 및 CPU 설정
- 시스템 이름
- 일련 번호

- VID 및 PID
- 업타임
- 마지막 CLI 로그인

MnT 노드 수

pxGrid 노드 수

라이선스

- 라이선스 만료 여부
- 사용 가능한 Cisco ISE Essentials 라이선스 수, 사용된 최대 수
- 사용 가능한 Cisco ISE Advantage 라이선스 수, 사용된 최대 수
- 사용 가능한 Cisco ISE Premium 라이선스 수, 사용된 최대 수
- 소형, 중형 및 대형 VM 라이선스 수
- 평가판 라이선스 사용 여부
- 스마트 어카운트 이름
- TACACS 디바이스 수
- 만료 날짜, 남은 일수, 라이선스 기간
- 서비스 유형, 기본 및 보조 UDI

포스처

- 비활성 정책 수
- 마지막 포스처 피드 업데이트
- 활성 정책 수
- 포스처 피드 업데이트

게스트 사용자

- 해당 날짜에 인증된 최대 게스트 수
- 해당 날짜의 최대 활성 게스트 수
- 해당 날짜의 최대 BYOD 사용자 수
- 인증된 게스트의 외부 ID 정보

NAD(Network Access Devices)

- 권한 부여: 활성화된 ACL, VLAN, 정책 규모
- NDG 맵 및 NAD 계층 구조

- 인증:
  - RADIUS, RSA ID, LDAP, ODBC 및 Active Directory ID 저장소 수
  - 관리자가 아닌 로컬 사용자 수
  - NDG 맵 및 NAD 맵
  - 정책 라인 수

권한 부여, 활성 VLAN, 정책 수, 활성화된 ACL 수:

- 상태, VID, PT
- 평균 로드, 메모리 사용률
- PAP, MnT, pxGrid 및 PIC 노드 수
- 이름, 프로파일 이름, 프로파일 ID

NAD 프로파일

각 NAD 프로파일:

- 이름 및 ID
- Cisco 디바이스
- TACACS 지원
- RADIUS 지원
- TrustSec 지원
- 기본 프로파일

프로파일러

- 마지막 피드 업데이트 날짜
- 자동 업데이트 활성화 여부
- 프로파일링된 엔드포인트, 엔드포인트 유형, 알 수 없는 엔드포인트, 알 수 없는 백분율 및 총 엔드포인트 수
- 맞춤형 프로파일 수
- 일련 번호, 범위, 엔드포인트 유형, 맞춤형 프로파일

MDM(Mobile Device Management)

- MDM 노드 목록
- 날짜 범위의 경우 현재 MDM 엔드포인트 수, 현재 게스트 사용자 수, 현재 포스처 사용자 수
- pxGrid 클라이언트 수

- 노드 수

Cisco ISE 프로세스를 모니터링하는 SNMP 트랩

Cisco ISE의 일반 SNMP 트랩

SNMP 트랩을 사용하면 Cisco ISE의 상태를 모니터링할 수 있습니다. Cisco ISE 서버에 액세스하지 않고 Cisco ISE를 모니터링하려는 경우 Cisco ISE에서 MIB 브라우저를 SNMP 호스트로 구성할 수 있습니다. 그런 다음 MIB 브라우저에서 Cisco ISE의 상태를 모니터링할 수 있습니다.

snmp-server host 및 **snmp-server trap** 명령에 대한 자세한 내용은 Cisco Identity Services Engine CLI 참조 가이드를 참고하십시오.

Cisco ISE는 SNMPv1, SNMPv2c 및 SNMPv3을 지원합니다.

CLI에서 SNMP 호스트를 구성하는 경우 Cisco ISE는 다음과 같은 일반 시스템 트랩을 전송합니다.

- Cold start: 디바이스를 재부팅할 때.
- Linkup: 이더넷 인터페이스가 작동중일 때.
- Linkdown: 이더넷 인터페이스가 중단되어 있을 때.
- Authentication failure: 커뮤니티 문자열이 일치하지 않을 때.

다음 표에는 Cisco ISE에서 기본적으로 생성되는 일반 SNMP 트랩이 나와 있습니다.

OID	설명	트랩 예
.1.3.6.1.4.1.8072.4.0.3 \n NET-SNMP-AGENT-MIB::nsNotifyRestart	에이전트가 재시작되었음을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyRestart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix
.1.3.6.1.4.1.8072.4.0.2 \n NET-SNMP-AGENT-MIB::nsNotifyShutdown	에이전트가 종료되는 중임을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: NET-SNMP-AGENT-MIB::nsNotifyShutdown SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpNotificationPrefix

OID	설명	트랩 예
.1.3.6.1.6.3.1.1.5.4 \n IF-MIB::linkUp	에이전트 역할을 수행하는 SNMP 엔티티가 통신 링크 중 하나에 대한 ifOperStatus 개체가 다운 상태를 유지하고 (notPresent 상태가 아닌) 다른 상태로 전환된 것을 탐지했음을 나타냅니다. 이 다른 상태는 ifOperStatus의 포함된 값으로 표시됩니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (478) 0:00:04.78 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkUp IF-MIB::ifIndex.12 = INTEGER: 12 IF-MIB::ifAdminStatus.12 = INTEGER: up(1) IF-MIB::ifOperStatus.12 = INTEGER: up(1) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

OID	설명	트랩 예
.1.3.6.1.6.3.1.1.5.3 \n IF-MIB::linkDown	에이전트 역할을 수행하는 SNMP 엔티티가 통신 링크 중 하나에 대한 ifOperStatus 개체가 (notPresent 상태가 아닌) 다른 상태에서 다운 상태로 전환되려는 것을 탐지했음을 나타냅니다. 이 다른 상태는 ifOperStatus의 포함된 값으로 표시됩니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (479) 0:00:04.79 SNMPv2-MIB::snmpTrapOID.0 = OID: IF-MIB::linkDown IF-MIB::ifIndex.5 = INTEGER: 5 IF-MIB::ifAdminStatus.5 = INTEGER: up(1) IF-MIB::ifOperStatus.5 = INTEGER: down(2) SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
.1.3.6.1.6.3.1.1.5.1 \n SNMPv2-MIB::coldStart	알림 생성자 애플리케이션을 지원하는 SNMP 엔티티가 자체적으로 다시 초기화되고 해당 컨피그레이션이 변경되었을 수 있음을 나타냅니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8) 0:00:00.08 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-MIB::coldStart SNMPv2-MIB::snmpTrapEnterprise.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10

Cisco ISE의 프로세스 모니터링 SNMP 트랩

Cisco ISE CLI에서 SNMP 호스트를 구성하는 경우 Cisco ISE에서는 Cisco ISE 프로세스 상태에 대한 hrSWRunName 트랩을 SNMP 관리자로 전송할 수 있습니다. Cisco ISE는 cron 작업을 사용하여 이러한 트랩을 트리거합니다. 크론 작업은 Monit에서 Cisco ISE 프로세스 상태를 검색합니다. CLI에서 **SNMP** 서버 호스트 명령을 구성하고 나면 cron 작업이 5분마다 실행되어 Cisco ISE를 모니터링합니다.

참고 관리자가 ISE 프로세스를 수동으로 중지하면 해당 프로세스에 대한 모니터링도 중지되며 SNMP 관리자로 트랩이 전송되지 않습니다. 프로세스가 실수로 종료되어 자동으로 복구되지 않는 경우에만 프로세스 중지 SNMP 트랩이 SNMP 관리자에게 전송됩니다.

다음은 Cisco ISE의 프로세스 모니터링 SNMP 트랩에 대한 전체 목록입니다.

OID	설명	트랩 예
.1.3.6.1.2.1.25.4.2.1.2 \n HOST-RESOURCES-MIB::hrSWRunName	제조업체, 수정 버전 및 일반적으로 알려진 이름을 포함하여 실행중인 소프트웨어에 대한 텍스트 설명입니다. 이 소프트웨어가 로컬로 설치된 경우 해당 hrSWInstalledName에 사용된 것과 동일한 문자열이어야 합니다. 고려되는 서비스는 app-server, rsyslog, redis-server, ad-connector, mnt-collector, mnt-processor, ca-server est-server 및 elasticsearch입니다.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (63692139) 7 days, 8:55:21.39 SNMPv2-MIB::snmpTrapOID.0 = OID: HOSTRESOURCES- MIB::hrSWRunName HOSTRESOURCES- MIB::hrSWRunName = STRING: "redis-server:Running"

Cisco ISE는 구성된 SNMP 서버로 다음 상태에 대한 트랩을 전송합니다.

- Process Start(프로세스 시작)(monitored[모니터링됨] 상태)
- Process Stop(프로세스 중지)(not monitored[모니터링되지 않음] 상태)
- Execution Failed(실행 장애): 프로세스 상태가 "Monitored(모니터링됨)"에서 "Execution Failed(실행 장애)"로 변경되면 트랩이 전송됩니다.

- Does not exists(없음): 프로세스 상태가 "Monitored(모니터링됨)"에서 "Does Not Exists(없음)"로 변경되면 트랩이 전송됩니다.

SNMP 서버에서는 각 객체에 대해 고유 객체 ID(OID)가 생성되며 특정 값이 이 OID에 할당됩니다. SNMP 서버의 OID 값으로 객체를 찾을 수 있습니다. 실행 중인 트랩의 OID 값은 *"running(실행 중)"*이며 not monitored(모니터링되지 않음), does not exist(없음) 및 execution failed(실행 장애) 트랩의 OID 값은 *"stopped(중지됨)"*입니다.

Cisco ISE는 HOST-RESOURCES MIB에 속하는 hrSWRunName의 OID를 사용하여 트랩을 전송하고 이 OID 값을 < *PROCESS NAME* > - <*PROCESS STATUS* >로, 예를 들면 "실행 시간 - 실행"으로 설정합니다.

Cisco ISE가 SNMP 서버로 SNMP 트랩을 보내지 않도록 하려면 Cisco ISE CLI에서 SNMP 컨피그레이션을 제거합니다. 이 작업은 SNMP 관리자로부터의 SNMP 트랩 전송 및 폴링을 중지합니다.

Cisco ISE의 디스크 사용률 **SNMP** 트랩

Cisco ISE 파티션이 그 디스크 사용률 임계값에 도달하고 구성된 여유 공간이 모두 사용되면 디스크 사용률 트랩이 전송됩니다.

다음은 Cisco ISE에서 구성할 수 있는 디스크 사용 SNMP 트랩의 전체 목록입니다.

OID	설명	트랩 예
.1.3.6.1.4.1.2021.9.1.9 \n UCD-SNMP-MIB::dskPercent	디스크에서 사용된 공간의 백분율.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198297) 13 days, 16:19:42.97 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPercent UCD-SNMP-MIB::dskPercent = INTEGER: 13
.1.3.6.1.4.1.2021.9.1.2 \n UCD-SNMP-MIB::dskPath	디스크가 마운트된 경로. dskPath는 ISE admin 명령의 출력에서 모든 마운트 포인트에 대한 트랩을 전송할 수 있습니다**show disks**.	DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (118198304) 13 days, 16:19:43.04 SNMPv2-MIB::snmpTrapOID.0 = OID: UCD-SNMP-MIB::dskPath UCD-SNMP-MIB::dskPath = STRING: /opt

Cisco ISE 경보

경보는 네트워크의 위험 조건에 대해 알리며 경보 dashlet에 표시됩니다. 또한 데이터 제거 이벤트와 같은 시스템 활동에 대한 정보도 제공합니다. 시스템 활동에 대한 알림을 어떤 식으로 받으려는지 구성할 수 있습니다. 아니면 경보를 완전히 비활성화할 수도 있습니다. 특정 경보에 대한 임계값도 구성할 수 있습니다.

대부분의 경보에는 일정이 연결되어 있지 않으며 이벤트가 발생한 직후에 경보가 전송됩니다. 특정한 시점에 보존되는 경보 수는 최신 경보를 기준으로 15,000개입니다.

이벤트가 다시 발생하는 경우 약 1시간 동안 동일한 경보가 표시되지 않습니다. 이벤트가 다시 발생하는 기간 동안에는 트리거에 따라 경보가 다시 표시되려면 약 1시간이 소요될 수 있습니다.

다음 표에는 모든 Cisco ISE 경보, 설명 및 해당 해결 방법이 나와 있습니다.

표 ***2: Cisco ISE*** 경보

경보 이름	경보 설명	경보 해결 방법
관리 및 운영 관리 감사		
구축 업그레이드 장애	ISE 노드에서 업그레이드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 실패 이유와 정정 작업을 확인해 주십시오.
업그레이드 번들 다운로드 장애	ISE 노드에서 업그레이드 번들 다운로드에 장애가 발생했습니다.	장애가 발생한 노드의 ADE.log에서 업그레이드 실패 이유와 정정 작업을 확인해 주십시오.
SXP 연결 장애	SXP 연결에 장애가 발생했습니다.	SXP 서비스가 실행 중인지 확인해 주십시오. 피어의 호환성을 확인해 주십시오.
모든 디바이스에 적용된 Cisco 프로파일	네트워크 디바이스 프로파일은 MAB, Dot1X, CoA, 웹 리디렉션 등 네트워크 액세스 디바이스의 기능을 정의합니다. ISE 2.0 업그레이드의 일부분으로 기본 Cisco 네트워크 디바이스 프로파일이 모든 네트워크 디바이스에 적용되었습니다.	적절한 프로파일을 할당하려면 Cisco 제품이 아닌 네트워크 디바이스의 컨피그레이션을 편집하는 것이 좋습니다.
CRL에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	CRL 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 LDAP 연결이 다시 연결됨	OCSP 확인 결과 LDAP 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. LDAP 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 LDAP 서버에 설치해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CRL에서 취소된 인증서를 발견하여 보안 시스템 로그 연결이 다시 연결됨	CRL 확인 결과 시스템 로그 연결에 사용된 인증서가 취소되었습니다.	CRL 컨피그레이션이 유효한지 확인해 주십시오. 시스템 로그 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 시스템 로그 서버에 설치해 주십시오.
OCSP에서 취소된 인증서를 발견하여 보안 시스템 로그 연결이 다시 연결됨	OCSP 확인 결과 시스템 로그 연결에 사용된 인증서가 취소되었습니다.	OCSP 컨피그레이션이 유효한지 확인해 주십시오. 시스템 로그 서버 인증서 및 해당 발급자 인증서가 취소되지 않았는지 확인해 주십시오. 취소된 경우 새 인증서를 발급하여 시스템 로그 서버에 설치해 주십시오.
관리자 계정 잠금/비활성화	비밀번호 만료 또는 잘못된 로그인 시도로 인해 관리자 계정이 잠기거나 비활성화되었습니다. 자세한 내용은 관리자 비밀번호 정책을 참고해 주십시오.	관리자 비밀번호는 다른 관리자가 GUI 또는 CLI를 사용하여 재설정할 수 있습니다.
ERS에서 더 이상 사용되지 않는 URL을 식별함	ERS에서 더 이상 사용되지 않는 URL을 식별함	요청 URL이 더 이상 사용되지 않으므로 해당 URL을 사용하지 않는 것이 좋습니다.
ERS에서 오래된 URL을 식별함	ERS에서 오래된 URL을 식별함	요청한 URL이 오래되었으므로 최신 URL을 사용하는 것이 좋습니다. 이 URL는 향후 릴리스에서 제거되지 않습니다.
ERS 요청 content-type 헤더가 오래됨	ERS 요청 content-type 헤더가 오래되었습니다.	요청 content-type 헤더에 나와 있는 요청 리소스 버전이 오래되었습니다. 이는 리소스 스키마가 수정되었음을 의미합니다. 하나 이상의 속성이 추가되었거나 제거되었을 수 있습니다. 오래된 스키마 문제를 해결하기 위해 ERS 엔진은 기본값을 사용합니다.
ERS XML 입력에서 XSS 또는 삽입 공격이 의심됨	ERS XML 입력에서 XSS 또는 삽입 공격이 의심됩니다.	xml 입력을 검토하십시오.

경보 이름	경보 설명	경보 해결 방법
백업 실패	ISE 백업 작업이 실패했습니다.	Cisco ISE와 저장소 사이의 네트워크 연결을 확인해 주십시오. 다음 사항을 확인해 주십시오. • 저장소에 사용되는 자격 증명이 올바릅니다. • 저장소에 충분한 디스크 공간이 있습니다. • 저장소 사용자에게 쓰기 권한이 있습니다.
CA 서버 작동 중지됨	CA 서버가 작동 중지되었습니다.	CA 서비스가 CA 서버에서 작동되어 실행 중인지 확인해 주십시오.
CA 서버 작동	CA 서버가 작동합니다.	관리자에게 CA 서버가 작동하고 있음을 알리는 알림입니다.
인증서 만료	이 인증서가 곧 만료됩니다. 인증서가 만료되면 Cisco ISE가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 취소됨	관리자가 내부 CA에 의해 엔드포인트로 발급된 인증서를 취소했습니다.	처음부터 새 인증서로 프로비저닝될 때까지 BYOD 흐름을 진행해 주십시오.
인증서 프로비저닝 초기화 오류	인증서 프로비저닝 초기화에 실패했습니다.	주체에서 동일한 CN(CommonName) 속성 값을 가진 여러 인증서가 발견되었습니다. 인증서 체인을 작성할 수 없습니다. SCEP 서버의 인증서를 비롯하여 시스템의 모든 인증서를 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
인증서 복제 실패	보조 노드에 대한 인증서 복제에 실패했습니다.	보조 노드의 인증서가 유효하지 않거나 다른 영구적인 오류 조건이 있습니다. 보조 노드에 기존의 충돌하는 인증서가 있는지 확인해 주십시오. 충돌하는 인증서가 있는 경우, 보조 노드에서 기존 인증서를 삭제하고 기본 노드에서 새 인증서를 내보내고 인증서를 삭제한 다음 가져와 복제를 다시 시도하도록 해 주십시오.
인증서 복제 일시적 실패	보조 노드에 대한 인증서 복제가 일시적으로 실패했습니다.	네트워크 중단과 같은 일시적 상태로 인해 인증서가 보조 노드로 복제되지 않았습니다. 복제가 성공할 때까지 재시도됩니다.
인증서 만료됨	이 인증서가 만료되었습니다. Cisco ISE가 클라이언트와의 보안 통신을 설정하지 못할 수 있습니다. 노드 간 통신에도 영향을 미칠 수 있습니다.	인증서를 바꾸십시오. 신뢰 인증서의 경우 발급 CA(Certificate Authority)에 문의해 주십시오. CA 서명 로컬 인증서의 경우 CSR을 생성하고 CA에 새 인증서를 생성해 달라고 요청해 주십시오. 자체 서명된 로컬 인증서의 경우 Cisco ISE를 사용하여 만료 날짜를 연장해 주십시오. 더 이상 사용되지 않는 경우 인증서를 삭제할 수 있습니다.
인증서 요청 전달 실패	인증서 요청 전달에 실패했습니다.	들어오는 인증 요청이 발신자의 속성과 일치하는지 확인해 주십시오.
컨피그레이션 변경됨	Cisco ISE 컨피그레이션이 업데이트되었습니다. 이 경보는 사용자 및 엔드포인트에서 컨피그레이션이 변경된 경우에는 트리거되지 않습니다.	컨피그레이션 변경이 예상되는지 확인해 주십시오.
CRL 검색 실패	서버에서 CRL을 검색할 수 없습니다. 이는 지정된 CRL을 사용할 수 없는 경우에 발생할 수 있습니다.	다운로드 URL이 올바르고 서비스에 사용할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
DNS 확인 실패	노드에서 DNS 확인에 실패했습니다.	**ip name-server** 명령으로 구성한 DNS 서버에 연결할 수 있는지 확인해 주십시오. **DNS Resolution failed for CNAME <hostname of the node>** 에 해당하는 경보를 받는 경우 각 ISE 노드의 A 기록와 함께 CNAME RR을 생성해야 합니다.
펌웨어 업데이트 필요	이 호스트에서 펌웨어를 업데이트해야 합니다.	펌웨어 업데이트를 받으려면 Cisco TAC에 문의하십시오.
불충분한 가상 머신 리소스	이 호스트에서 CPU, RAM, 디스크 공간 또는 IOPS와 같은 VM(Virtual Machine) 리소스가 충분하지 않습니다.	Cisco ISE 하드웨어 설치 설명서에 명시된 VM 호스트에 대한 최소 요건을 확인해 주십시오.
NTP 서비스 실패	이 노드에서 NTP 서비스 작동이 중지되었습니다.	이는 NTP 서버와 Cisco ISE 노드 사이의 시간 차이가 크기 때문에 (1,000초 이상) 발생할 수 있습니다. NTP 서버가 적절히 작동 중인지 확인하고 **ntp server <servername>** CLI 명령을 사용하여 NTP 서비스를 다시 시작하여 시간 격차 문제를 해결해 주십시오.
NTP 동기화 실패	이 노드에 구성된 모든 NTP 서버에 연결할 수 없습니다.	문제를 해결하려면 CLI에서 **show ntp** 명령을 실행해 주십시오. Cisco ISE에서 NTP 서버에 연결할 수 있는지 확인해 주십시오. NTP 인증이 구성된 경우 키 ID와 값이 서버의 값과 일치하는지 확인해 주십시오.
예약된 컨피그레이션 백업 없음	Cisco ISE 컨피그레이션 백업이 예약되지 않았습니다.	컨피그레이션 백업에 대한 일정을 생성해 주십시오.
작업 DB 제거 실패	작업 데이터베이스에서 오래된 데이터를 제거할 수 없습니다. 이는 MnT 노드가 사용 중인 경우 발생합니다.	데이터 비우기 감사 보고서에서 used_space가 threshold_space보다 작은지 확인해 주십시오. CLI를 사용하여 MnT 노드에 로그인하고 제거 작업을 수동으로 수행해 주십시오.

경보 이름	경보 설명	경보 해결 방법
프로파일러 SNMP 요청 실패	SNMP 요청 시간이 초과되었거나 SNMP 커뮤니티 또는 사용자 인증 데이터가 잘못되었는지 확인해 주십시오.	SNMP가 NAD에서 실행되고 있는지 확인하고 Cisco ISE의 SNMP 컨피그레이션이 NAD와 일치하는지 확인해 주십시오.
복제 실패	보조 노드에서 복제된 메시지를 사용하지 못했습니다.	Cisco ISE GUI에 로그인하고 구축 페이지에서 수동 동기화를 수행해 주십시오. 영향을 받는 Cisco ISE 노드를 등록 취소했다가 다시 등록해 주십시오.
복원 실패	Cisco ISE 복원 작업에 실패했습니다.	Cisco ISE와 저장소 사이의 네트워크 연결을 확인해주십시오. 저장소에 사용된 자격 증명이 올바른지 확인해 주십시오. 백업 파일이 손상되지 않았는지 확인해 주십시오. CLI에서 **reset-config** 명령을 실행하고 마지막으로 알려진 안전한 백업을 복원해 주십시오.
패치 실패	서버에서 패치 프로세스가 실패했습니다.	서버에서 패치 프로세스를 다시 실행해 주십시오.
패치 성공	서버에서 패치 프로세스가 성공했습니다.	-
외부 MDM 서버 API 버전 불일치	외부 MDM 서버 API 버전이 Cisco ISE에서 구성한 버전과 일치하지 않습니다.	MDM 서버 API 버전이 Cisco ISE에서 구성한 버전과 일치하는지 확인해 주십시오. 필요한 경우 Cisco ISE MDM 서버 컨피그레이션을 업데이트해 주십시오.
외부 MDM 서버 연결 실패	외부 MDM 서버에 대한 연결에 실패했습니다.	MDM 서버가 작동하며 Cisco ISE-MDM API 서비스가 MDM 서버에서 실행되고 있는지 확인해 주십시오.
외부 MDM 서버 응답 오류	외부 MDM 서버 응답 오류입니다.	MDM 서버에서 Cisco ISE-MDM API 서비스가 제대로 실행되고 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
복제 중지됨	ISE 노드가 PAN에서 컨피그레이션 데이터를 복제할 수 없습니다.	Cisco ISE GUI에 로그인하여 구축 페이지에서 수동 동기화를 수행하거나, 필수 필드를 사용하여 영향을 받는 ISE 노드를 등록 취소했다가 다시 등록해 주십시오.
엔드포인트 인증서 만료됨	엔드포인트 인증서가 일별 예약 작업에서 만료된 상태로 표시되었습니다.	새 엔드포인트 인증서를 받으려면 엔드포인트 디바이스를 다시 등록해 주십시오.
엔드포인트 인증서 제거됨	일별 예약 작업에서 만료된 엔드포인트 인증서가 제거되었습니다.	필요 조치가 없습니다. 이는 관리자가 시작한 정리 작업입니다.
엔드포인트 제거 활동	엔드포인트에서 지난 24시간 동안의 활동을 제거합니다. 이 경보는 야간에 트리거됩니다.	**Operations(**작업**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Purge Activities(**엔드포인트 제거 활동**)**를 선택해 제거 활동을 검토해 주십시오.
느린 복제 오류	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 정보	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
느린 복제 경고	느린 복제 또는 중단된 복제가 탐지되었습니다.	노드에 연결할 수 있는지, 그리고 노드가 구축에 포함되어 있는지 확인해 주십시오.
PAN 자동 페일오버 - 페일오버 실패	보조 관리 노드로의 프로모션 요청이 실패했습니다.	추가 작업에 대해서는 경보 세부 정보를 참고해 주십시오.
PAN 자동 페일오버 - 페일오버 트리거됨	기본 역할에 대한 보조 관리 노드의 페일오버가 성공적으로 트리거되었습니다.	보조 PAN 프로모션이 완료될 때까지 기다렸다가 이전의 기본 PAN을 작동해 주십시오.
PAN 자동 페일오버 - 상태 검사 비활성	PAN이 지정된 모니터링 노드로부터 상태 검사 모니터링 요청을 받지 못했습니다.	보고된 모니터링 노드가 작동 중지되었거나 동기화가 중단되었는지 확인하고 필요한 경우 수동 동기화를 트리거해 주십시오.

경보 이름	경보 설명	경보 해결 방법
PAN 자동 페일오버 - 유효하지 않은 상태 검사	자동 페일오버에 대해 유효하지 않은 상태 검사 모니터링 요청이 수신되었습니다.	상태 검사 모니터링 노드의 동기화가 중단되었는지 확인하고 필요한 경우 수동 동기화를 트리거해 주십시오.
PAN 자동 페일오버 - 기본 관리 노드 작동 중지	기본 관리 노드가 작동 중지되었거나 모니터링 노드에서 연결할 수 없습니다.	PAN을 작동시키거나 페일오버가 발생할 때까지 기다리십시오.
PAN 자동 페일오버 - 페일오버 시도 거부됨	보조 관리 노드가 상태 검사 모니터 노드에 의해 생성된 프로모션 요청을 거부했습니다.	추가 작업에 대해서는 경보 세부정보를 참고해 주십시오.
EST 서비스 중단	EST 서비스가 중단되었습니다.	CA 및 EST 서비스가 실행 중이고 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완전한지 확인하십시오.
EST 서비스 작동 중	EST 서비스가 작동 중입니다.	관리자에게 EST 서비스가 작동하고 있음을 알리는 알림입니다.
Smart Call Home 통신 실패	Smart Call Home 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
원격 분석 통신 장애	원격 분석 메시지가 성공적으로 전송되지 않았습니다.	Cisco ISE와 Cisco 시스템 사이의 네트워크 연결을 확인해 주십시오.
어댑터에 연결할 수 없음	Cisco ISE가 어댑터에 연결할 수 없습니다.	어댑터 로그를 확인해 장애 관련 세부정보를 확인하십시오.
어댑터 오류	어댑터에 오류가 발생했습니다.	경보 설명을 확인하십시오.
어댑터 연결 실패	어댑터가 소스 서버에 연결할 수 없습니다.	소스 서버에 연결할 수 있는지 확인하십시오.
오류 때문에 어댑터 중지됨	어댑터에 오류가 발생하여 바람직한 상태에 있지 않습니다.	어댑터 구성이 올바르고 소스 서버에 연결할 수 있는지 확인합니다. 어댑터 로그를 참조해 오류 관련 세부정보를 확인하십시오.
서비스 구성 요소 오류	서비스 구성 요소에 오류가 발생했습니다.	경보 설명을 확인하십시오.
서비스 구성 요소 정보	서비스 구성 요소가 알림을 전송했습니다.	없음

경보 이름	경보 설명	경보 해결 방법
ISE 서비스		
과도한 TACACS 인증 시도	ISE 정책 서비스 노드에서 예상되는 TACACS 인증 비율보다 더 높은 인증 시도가 발생했습니다.	• 네트워크 디바이스에서 재인증 타이머를 확인해 주십시오. • ISE 인프라의 네트워크 연결을 확인해 주십시오.
과도한 TACACS 인증 시도 장애	ISE 정책 서비스 노드에서 장애가 발생한 TACACS 인증의 예상 비율보다 더 높은 인증 시도 장애가 발생했습니다.	• 인증 단계를 확인하여 근본 원인을 파악해 주십시오. • ISE/NAD 컨피그레이션에서 ID 및 암호 불일치를 확인해 주십시오.
MSE 위치 서버에 다시 액세스할 수 있음	MSE 위치 서버에 다시 액세스할 수 있습니다.	없음
MSE 위치 서버에 액세스할 수 없습니다.	MSE 위치 서버가 액세스할 수 없거나 다운된 상태입니다.	MSE 위치 서버가 작동 및 실행 중이며 ISE 노드에서 액세스 가능한지 확인해 주십시오.
AD Connector를 다시 시작해야 함	AD Connector가 예기치 않게 중지되었으므로 다시 시작해야 합니다.	이 문제가 계속되면 Cisco TAC에 지원을 요청해 주십시오.
Active Directory 포리스트를 사용할 수 없음	Active Directory 포리스트 글로벌 카탈로그를 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
인증 도메인을 사용할 수 없음	인증 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ISE 인증 비활성	Cisco ISE 정책 서비스 노드가 네트워크 디바이스에서 인증 요청을 받지 않습니다.	• ISE/NAD 컨피그레이션을 확인해 주십시오. • ISE/NAD 인프라의 네트워크 연결을 확인해 주십시오.
ID 매핑. 인증 비활성	ID 매핑 서비스에서 최근 15분간 사용자 인증 이벤트를 수집하지 않았습니다.	사용자 인증이 필요한 시점이라면(예: 근무 시간) Active Directory 도메인 컨트롤러에 대한 연결을 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
CoA 실패	네트워크 디바이스가 Cisco ISE 정책 서비스 노드에서 실행한 CoA(Change of Authorization) 요청을 거부했습니다.	네트워크 디바이스가 Cisco ISE에서 CoA를 허용하도록 구성되었는지 확인해 주십시오. 유효한 세션에 대해 CoA가 실행되었는지 확인해 주십시오.
구성된 네임서버 작동 중지됨	구성된 네임서버가 작동 중지되었거나 사용 불가능합니다.	DNS 컨피그레이션 및 네트워크 연결을 확인해 주십시오.
신청자가 응답을 중지함	Cisco ISE가 120초 전에 클라이언트에 마지막 메시지를 보냈지만 클라이언트로부터 응답이 없습니다.	• 신청자가 Cisco ISE와 완전한 EAP 대화를 수행하도록 올바르게 구성되었는지 확인해 주십시오. • NAS가 신청자와 EAP 메시지를 전송하도록 올바르게 구성되었는지 확인해 주십시오. • EAP 대화를 위한 신청자 또는 NAS의 시간 제한이 짧지 않은지 확인해 주십시오.
과도한 인증 시도	Cisco ISE 정책 서비스 노드에서 예상되는 인증 비율보다 더 높은 인증 시도가 발생했습니다.	네트워크 디바이스에서 재인증 타이머를 확인해 주십시오. Cisco ISE 인프라의 네트워크 연결을 확인해 주십시오. 임계값을 충족하는 경우 과도한 인증 시도 및 과도한 실패 시도 경보가 트리거됩니다. 설명 열 옆에 표시되는 숫자는 최근 15분간 Cisco ISE에 대해 인증이 완료되었거나 실패한 총 인증 수입니다.

경보 이름	경보 설명	경보 해결 방법
과도한 실패 시도	Cisco ISE 정책 서비스 노드에서 예상되는 실패한 인증 비율보다 더 높은 인증 시도가 발생했습니다.	인증 단계를 확인하여 근본 원인을 파악해 주십시오. Cisco ISE/NAD 컨피그레이션에서 ID 및 암호 불일치가 있는지 확인해 주십시오. 임계값을 충족하는 경우 과도한 인증 시도 및 과도한 실패 시도 경보가 트리거됩니다. 설명 열 옆에 표시되는 숫자는 최근 15분간 Cisco ISE에 대해 인증이 완료되었거나 실패한 총 인증 수입니다.
AD: 머신 TGT 새로 고침 실패	ISE 서버 TGT(Ticket Granting Ticket) 새로 고침에 실패했습니다. TGT는 AD 연결 및 서비스에 사용됩니다.	ISE 머신 계정이 있으며 유효한지 확인해 주십시오. 또한 가능한 클럭 오차, 복제, Kerberos 컨피그레이션 또는 네트워크 오류가 있는지 아니면 두 오류가 모두 있는지도 확인해 주십시오.
AD: ISE 계정 비밀번호 업데이트 실패	ISE 서버에서 AD 머신 계정 비밀번호를 업데이트하지 못했습니다.	ISE 머신 계정 비밀번호가 변경되지 않았는지, 그리고 머신 계정이 비활성화되었거나 제한되어 있지 않은지 확인해 주십시오. KDC에 대한 연결을 확인해 주십시오.
가입한 도메인 사용 불가능	가입한 도메인을 사용할 수 없거나 인증, 권한 부여, 그리고 그룹 및 속성 검색에 사용할 수 없습니다.	DNS 컨피그레이션, Kerberos 컨피그레이션, 오류 조건 및 네트워크 연결을 확인해 주십시오.
ID 저장소 사용 불가능	Cisco ISE 정책 서비스 노드를 구성한 ID 저장소에 연결할 수 없습니다.	Cisco ISE와 ID 저장소 사이의 네트워크 연결을 확인해 주십시오.
잘못 구성된 네트워크 디바이스 탐지	Cisco ISE가 NAS에서 너무 많은 RADIUS 계정 관리 정보를 탐지했습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	NAS에서 너무 많은 중복 RADIUS 계정 관리 정보가 ISE로 전송되었습니다. 정확한 계정 관리 빈도로 NAS를 구성해 주십시오.

경보 이름	경보 설명	경보 해결 방법
잘못 구성된 신청자 탐지	Cisco ISE가 네트워크에서 잘못 구성된 신청자를 탐지했습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	신청자의 컨피그레이션이 올바른지 확인해 주십시오.
계정 관리 시작 없음	Cisco ISE 정책 서비스 노드가 세션에 권한을 부여했지만 네트워크 디바이스로부터 계정 관리 시작을 받지 못했습니다.	네트워크 디바이스에 RADIUS 계정 관리가 구성되어 있는지 확인해 주십시오. 네트워크 디바이스 컨피그레이션에서 로컬 권한 부여를 확인해 주십시오.
알 수 없는 NAD	Cisco ISE 정책 서비스 노드가 Cisco ISE에 구성되어 있지 않은 네트워크 디바이스에서 인증 요청을 받았습니다.	네트워크 디바이스가 정식 요청인지 확인한 다음 컨피그레이션에 추가해 주십시오. 암호가 일치하는지 확인해 주십시오.
SGACL 삭제	SGACL(Secure Group Access) 삭제가 발생했습니다. 이는 SGACL 정책 위반으로 인해 Trustsec 지원 디바이스에서 패킷이 삭제되는 경우에 발생합니다.	RBACL 삭제 요약 보고서를 실행하고 SGACL 삭제를 발생시킨 소스를 검토합니다. CoA를 잘못된 소스에 실행하여 세션에 다시 권한을 부여하거나 세션 연결을 끊으십시오.
RADIUS 요청 삭제됨	NAD의 인증/계정 관리 요청이 자동으로 버려집니다. 이는 알 수 없는 NAD, 공유 암호 불일치 또는 RFC에 따른 유효하지 않은 패킷 콘텐츠로 인해 발생할 수 있습니다. 이 경보는 기본적으로 비활성화되어 있습니다. 이 경보를 활성화하려면 경보 활성화 및 구성을 참조하십시오.	Cisco ISE에서 NAD/AAA 클라이언트의 컨피그레이션이 유효한지 확인해 주십시오. NAD/AAA 클라이언트 및 Cisco ISE의 공유 암호가 일치하는지 확인해 주십시오. AAA 클라이언트 및 네트워크 디바이스에 하드웨어 문제 또는 RADIUS 호환성 문제가 없는지 확인해 주십시오. 또한 디바이스를 Cisco ISE에 연결하는 네트워크에 하드웨어 문제가 없는지 확인해 주십시오.
EAP 세션 할당 실패	EAP 세션 제한에 도달했으므로 RADIUS 요청이 삭제되었습니다. 이 상태는 너무 많은 병렬 EAP 인증 요청으로 인해 발생할 수 있습니다.	몇 초간 기다렸다가 새 EAP 세션에서 다른 RADIUS 요청을 호출해 주십시오. 계속 시스템 오버로드가 발생하는 경우 ISE 서버를 다시 시작해 주십시오.

경보 이름	경보 설명	경보 해결 방법
RADIUS 상황 할당 실패	시스템 오버로드로 인해 RADIUS 요청이 삭제되었습니다. 이 상태는 너무 많은 병렬 인증 요청으로 인해 발생할 수 있습니다.	몇 초간 기다렸다가 새 RADIUS 요청을 호출해 주십시오. 계속 시스템 오버로드가 발생하는 경우 ISE 서버를 다시 시작해 주십시오.
AD: ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE 머신 계정에 그룹을 가져오는 데 필요한 권한이 없습니다.	Cisco ISE 머신 계정에 Active Directory에서 사용자 그룹을 가져올 권한이 있는지 확인합니다.
시스템 상태		
높은 디스크 I/O 사용률	Cisco ISE 시스템의 디스크 I/O사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 디스크 공간 사용률	Cisco ISE 시스템의 디스크 공간 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.

경보 이름	경보 설명	경보 해결 방법
높은 로드 평균	Cisco ISE 시스템의 로드 평균이 높습니다.	시스템의 리소스가 충분한지 확인해 주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오. 기본 및 보조 MNT 노드의 오전 2시 타임 스탬프에 대해 높은 로드 평균 경보가 표시되는 경우, 해당 시간에 DBMS 통계가 실행되는 것 때문에 CPU 사용량이 높을 수 있습니다. DBMS 통계가 완료되면 CPU 사용량이 정상으로 돌아옵니다. 매주 일요일 오전 1시에 주간 유지 관리 작업으로 인해 높은 로드 평균 경보가 트리거됩니다. 이 유지 관리 작업은 1GB 이상의 공간을 차지하는 모든 인덱스를 재구축합니다. 이 경보는 무시해도 됩니다.
높은 메모리 사용률	Cisco ISE 시스템의 메모리 사용률이 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
높은 작업 DB 사용률	Cisco ISE 모니터링 노드의 시스템 로그 데이터 볼륨이 예상보다 많습니다.	작업 데이터에 대한 컨피그레이션 제거 창을 확인하고 줄이십시오.
높은 인증 레이턴시	Cisco ISE 시스템의 인증 레이턴시가 높습니다.	시스템의 리소스가 충분한지 확인해주십시오. 시스템의 실제 작업량(예: 인증 수, 프로파일러 활동 등)을 확인해 주십시오. 다른 서버를 추가하여 로드를 분산시켜 주십시오.
상태 사용 불가능	모니터링 노드가 Cisco ISE 노드에서 상태를 받지 못했습니다.	Cisco ISE 노드가 준비되어 실행 중이며 모니터링 노드와 통신할 수 있는지 확인해 주십시오.

경보 이름	경보 설명	경보 해결 방법
프로세스 작동 중지	Cisco ISE 프로세스 중 하나가 실행되고 있지 않습니다.	Cisco ISE 애플리케이션을 다시 시작해 주십시오.
프로파일러 큐 크기 제한에 도달함	ISE 프로파일러 큐 크기 제한에 도달했습니다. 큐 크기 제한에 도달한 후 수신된 이벤트는 삭제됩니다.	시스템에 충분한 리소스가 있는지 확인하고 엔드포인트 속성 필터이 활성화되어 있는지 확인해 주십시오.
OCSP 트랜잭션 임계값에 도달함	OCSP 트랜잭션 임계값에 도달했습니다. 이 경보는 내부 OCSP 서비스에서 많은 양의 트래픽이 발생하는 경우에 트리거됩니다.	시스템의 리소스가 충분한지 확인해 주십시오.
라이선싱		
라이선스가 곧 만료됨	Cisco ISE 노드에 설치된 라이선스가 만료될 예정입니다.	Cisco ISE의 라이선싱 창에서 라이선스 사용 현황을 확인해 주십시오.
라이선스 만료됨	Cisco ISE 노드에 설치된 라이선스가 만료되었습니다.	새 라이선스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
라이선스 위반	Cisco ISE 노드에서 허용되는 라이선스 수가 초과되었거나 곧 초과됨을 탐지했습니다.	추가 라이선스를 구입하려면 Cisco 계정 팀에 문의해 주십시오.
스마트 라이선싱 인증 만료	스마트 라이선싱 인증이 만료되었습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하거나 Cisco Smart Software Manager의 네트워크 연결을 확인하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선스 인증 갱신 실패	Cisco Smart Software Manager를 이용한 인증 갱신에 실패했습니다.	**Cisco ISE** 라이선스 관리 창을 참조하여, **Licenses(**라이선스**)** 표에 있는 **Refresh(**새로고침**)** 버튼을 이용해 Cisco Smart Software Manager로 인증을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 인증 갱신 성공	Cisco Smart Software Manager를 이용한 인증 갱신에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 인증 갱신이 성공했음을 알리는 알림입니다.

경보 이름	경보 설명	경보 해결 방법
스마트 라이선싱 통신 장애	Cisco Smart Software Manager를 이용한 Cisco ISE 통신에 장애가 발생했습니다.	Cisco Smart Software Manager와의 네트워크 연결을 확인하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 통신 복원	Cisco Smart Software Manager를 이용한 Cisco ISE 통신이 복원되었습니다.	Cisco Smart Software Manager와의 네트워크 연결이 복원되었음을 알리는 알림입니다.
스마트 라이선싱 등록 취소 실패	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 실패했습니다.	자세한 내용은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 등록 취소 성공	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 등록 취소에 성공했음을 알리는 알림입니다.
스마트 라이선싱 비활성화	스마트 라이선스가 Cisco ISE에서 비활성화되어 기존 라이선스를 사용하고 있습니다.	스마트 라이선싱을 다시 활성화하는 방법은 **License Administration(**라이선스 관리**)** 창을 참조하십시오. Cisco ISE에서 스마트 라이선싱을 사용하는 방법을 알고 싶다면 Cisco ISE 관리 가이드를 참조하거나 Cisco 파트너에게 문의하십시오.
스마트 라이선싱 평가 기간 만료	스마트 라이선싱 평가 기간이 만료되었습니다.	Cisco Smart Software Manager를 이용해 Cisco ISE를 등록하는 방법은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오.
스마트 라이선스 HA 역할 변경	스마트 라이선스를 사용하는 동안 고가용성 역할 변경이 발생했습니다.	Cisco ISE의 HA 역할이 변경되었음을 알리는 알림입니다.

경보 이름	경보 설명	경보 해결 방법
스마트 라이선싱 Id 인증서 만료	스마트 라이선싱 인증서가 만료되었습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 Id 인증서 갱신 실패	Cisco Smart Software Manager를 이용한 스마트 라이선싱 등록 갱신에 실패했습니다.	**Cisco ISE** 라이선스 관리 창을 참조해 스마트 라이선싱 등록을 수동으로 갱신하십시오. 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 Id 인증서 갱신 성공	Cisco Smart Software Manager를 이용한 스마트 라이선싱 등록 갱신에 성공했습니다.	Cisco Smart Software Manager를 등록 갱신에 성공했음을 알리는 알림입니다.
스마트 라이선싱 잘못된 요청	잘못된 요청이 Cisco Smart Software Manager에 전달되었습니다.	자세한 내용은 **Cisco ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 규정 위반	Cisco ISE 라이선스가 규정을 준수하지 않습니다.	자세한 내용은 **ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. 새 라이선스를 구입하려면 파트너나 Cisco 계정 팀에 문의해 주십시오.
스마트 라이선싱 등록 실패	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 실패했습니다.	자세한 내용은 **ISE License Administration(Cisco ISE** 라이선스 관리**)** 창을 참조하십시오. Cisco Smart Software Manager에 로그인하거나, 문제가 해결되지 않는다면 Cisco 파트너에 문의하십시오.
스마트 라이선싱 등록 성공	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 성공했습니다.	Cisco Smart Software Manager를 이용한 Cisco ISE 등록에 성공했음을 알리는 알림입니다.
시스템 오류		

경보 이름	경보 설명	경보 해결 방법
로그 수집 오류	Cisco ISE 모니터링 컬렉터 프로세스가 정책 서비스 노드에서 생성된 감사 로그를 유지할 수 없습니다.	이는 정책 서비스 노드의 실제 기능에는 영향을 미치지 않습니다. 추가적인 해결 방법은 Cisco TAC에 문의해 주십시오.
예약된 보고서 내보내기 실패	내보낸 보고서(CSV 파일)를 구성한 저장소에 복사할 수 없습니다.	구성한 저장소를 확인해 주십시오. 저장소가 삭제되었으면 다시 추가해 주십시오. 저장소를 사용할 수 없거나 저장소에 연결할 수 없는 경우 저장소를 유효한 저장소로 다시 구성해 주십시오.
TrustSec		
알 수 없는 SGT가 프로비저닝됨	알 수 없는 SGT가 프로비저닝되었습니다.	ISE가 권한 부여 플로우 과정에서 알 수 없는 SGT를 프로비저닝했습니다. 알 수 없는 SGT를 알려진 플로우의 일부로 할당해서는 안 됩니다.
일부 TrustSec 네트워크 디바이스에 최신 ISE IP-SGT 매핑 컨피그레이션이 없음	일부 TrustSec 네트워크 디바이스에 최신 ISE IP-SGT 매핑 컨피그레이션이 없습니다.	ISE가 다른 IP-SGT 매핑 집합이 포함된 일부 네트워크 디바이스를 식별했습니다. **IP-SGT** 매핑 구축 옵션을 사용하여 디바이스를 업데이트해 주십시오.
TrustSec SSH 연결 장애	TrustSec SSH 연결에 실패했습니다.	ISE가 네트워크 디바이스에 대한 SSH 연결을 설정하지 못했습니다. **Network Device(**네트워크 디바이스**)** 창의 네트워크 디바이스 SSH 자격 증명이 네트워크 디바이스에 구성되어 있는 자격 증명과 비슷한지 확인해 주십시오. ISE(IP 주소)와의 네트워크 디바이스 사용 SSH 연결을 확인해 주십시오.
TrustSec에서 ISE가 1.0 이외의 TLS 버전에서 작동하도록 설정되었음을 식별함	TrustSec에서 식별된 ISE가 1.0 이외의 TLS 버전과 작동하도록 설정되었습니다.	TrustSec는 TLS 버전 1.0만 지원합니다.

경보 이름	경보 설명	경보 해결 방법
Trustsec PAC 검증 장애	Trustsec PAC 검증에 실패했습니다.	ISE가 네트워크 디바이스에서 전송한 PAC를 검증할 수 없습니다. **Network Device(**네트워크 디바이스**)** 창 및 디바이스 CLI에서 TrustSec 디바이스 자격 증명을 확인해 주십시오. 디바이스가 ISE 서버에 의해 프로비저닝된 유효한 PAC를 사용하는지 확인해 주십시오.
Trustsec 환경 데이터 다운로드 실패	Trustsec 환경 데이터 다운로드에 실패했습니다.	Cisco ISE에서 불법적인 환경 데이터 요청을 수신했습니다. 다음을 확인합니다. • PAC가 요청에 존재하며 유효합니다. • 모든 속성이 요청에 존재합니다.
TrustSec CoA 메시지 무시	TrustSec CoA 메시지가 무시되었습니다.	Cisco ISE에서 TrustSec CoA 메시지를 전송했지만 응답을 받지 못했습니다. 네트워크 디바이스가 CoA를 지원하는지 확인합니다. 디바이스 컨피그레이션을 확인합니다.
TrustSec 기본 이그레스 정책 수정	TrustSec 기본 이그레스 정책이 수정되었습니다.	TrustSec 기본 이그레스 정책 셀이 수정되었습니다. 보안 정책과 일치하는지 확인하십시오.

참고 사용자 또는 엔드포인트를 Cisco ISE에 추가하는 경우에는 경보가 트리거되지 않습니다.

경보 설정

다음 표에서는 **Alarm Settings(**경보 설정**)** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)** > **Alarm Configuration(**경보 컨피그레이션**)** > **Add(**추가**)**)

필드 이름	설명
경보 유형	경보 유형

필드 이름	설명
경보 이름	경보의 이름입니다.
Description(설명**)**	경보에 대한 설명입니다.
제안 작업	경보가 트리거될 때 수행할 작업입니다.
Status(상태**)**	경보 규칙을 활성화하거나 비활성화합니다.
심각도	경보의 심각도 레벨을 선택합니다. 유효한 옵션은 다음과 같습니다. • Critical (위험) : 심각한 오류 상태를 나타냅니다. • Warning(경고): 정상적이기는 하지만 중요한 상태를 나타냅니다. 기본 상태입니다. • Info(정보) - 이 옵션은 정보 메시지를 나타냅니다.
시스템 로그 메시지 보내기	Cisco ISE가 생성하는 각 시스템 경보에 대해 시스템 로그 메시지를 보냅니다.
쉼표로 구분하여 여러 이메일 입력	이메일 주소 또는 ISE 관리자 이름 또는 둘 다의 목록입니다.
이메일 메모**(0 ~ 4,000**자**)**	시스템 경보와 연결하려는 맞춤형 텍스트 메시지.

맞춤형 경보 추가

Cisco ISE에는 높은 메모리 사용률 및 구성 변경과 같은 12가지 기본 경보 유형이 포함되어 있습니다. Cisco에서 정의한 시스템 경보는 **Alarms Settings(**경보 설정**)** 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**)에 나열됩니다. 시스템 경보만 편집할 수 있습니다.

기존 시스템 경보 외에도 기존 경보 유형에서 사용자 맞춤화 경보를 추가, 수정 또는 삭제할 수 있습니다.

경보 유형별로 최대 5개의 경보를 생성할 수 있습니다. 총 경보 수는 200개로 제한됩니다.

Alarm Settings(경보 설정**)** 창의 **Alarm Configuration(**경보 구성**)** 탭에서 **Conditions(**조건**)** 열에는 4가지 경보, 즉 High Authentication Latency(높은 인증 레이턴시), High Disk I/O Utilization(높은 디스크 I/O 사용률), High Disk Space Utilization(높은 디스크 공간 사용률) 및 High Memory Utilization(높은 메모리 공간 사용률)에 대한 세부정보가 표시됩니다 이러한 각 경보에는 구성 가능한 임계값이 있습니다. 그러나 임계값이 구성된 경우에도 **Conditions(**조건**)** 열에 세부정보가 표시되지 않을 수 있습니다. 이 경우 경보의 관련 임계값 필드를 다시 편집하여 **Conditions(**조건**)** 열의 세부정보를 확인합니다.

경보를 추가하려면 다음을 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**

단계 **2** **Alarm Configuration(**경보 구성**)** 탭 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부정보를 입력합니다. 자세한 내용은 경보 설정 섹션을 참고하십시오.

경보 유형(High Memory Utilization(높은 메모리 사용률), Excessive RADIUS Authentication Attempts(과도한 RADIUS 인증 시도), Excessive TACACS Authentication Attempts(과도한 TACACS 인증 시도) 등)에 따라 **Alarm Configuration(**경보 구성**)** 창에 추가 속성이 표시됩니다. 예를 들어 구성 변경 경보에 대해서는 **Object Name(**개체 이름**)**, **Object Type(**개체 유형**)** 및 **Admin Name(**관리자 이름**)** 필드가 표시됩니다. 각기 기준이 다른 동일 경보의 여러 인스턴스를 추가할 수 있습니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

Cisco ISE 경보 알림 및 임계값

Cisco ISE 경보를 활성화 또는 비활성화하고 위험 조건에 대한 알림을 받도록 경보 알림 동작을 구성할 수 있습니다. 특정 경보의 경우 과도한 실패 시도 경보에 대한 최대 실패 시도 횟수 또는 높은 디스크 사용률 경보에 대한 최대 디스크 사용률과 같은 임계값을 구성할 수 있습니다.

경보 단위로 알림 설정을 구성할 수 있습니다. 각 경보(시스템 정의 경보와 사용자 맞춤화 경보 둘 다)에 대해 알림을 받아야 하는 사용자의 이메일 ID를 입력할 수 있습니다.

참고 경보 규칙 레벨에 지정되어 있는 수신자 이메일 주소는 전역 수신자 이메일 주소 설정을 재정의합니다.

경보 활성화 및 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Alarm Settings(**경보 설정**)**

단계 **2** 기본 경보 목록에서 경보를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Enable(**활성화**)** 또는 **Disable(**비활성화**)**을 선택합니다.

단계 **4** 해당하는 경우 경보 임계값을 구성합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

모니터링을 위한 **Cisco ISE** 경보

Cisco ISE는 위험 시스템 조건이 발생할 때마다 항상 알림을 보내는 시스템 경보를 제공합니다. Cisco ISE에서 생성된 경보는 경보 dashlet에 표시됩니다. 이러한 알림은 자동으로 경보 dashlet에 표시됩니다.

경보 dashlet에는 최근 경보 목록이 표시되며 여기서 경보 세부정보를 보기 위한 경보를 선택할 수 있습니다. 관리자는 또한 이메일 및 시스템 로그 메시지를 통해 경보 알림을 받을 수도 있습니다.

모니터링 경보 보기

단계 **1** Cisco ISE **Dashboard(**대시보드**)**로 이동합니다.

단계 **2** **Alarms(**경보**)** dashlet에서 원하는 경보를 클릭합니다. 경보 세부정보 및 제안 작업이 포함된 새 윈도우가 열립니다.

단계 **3** 경보를 새로 고침하려면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **4** 경보를 확인하여 경보를 읽은 것으로 표시하면 경보 카운터(경보가 생성된 횟수)가 감소합니다. 타임스탬프 옆에 있는 확인란을 선택하여 확인할 경보를 선택할 수 있습니다.

현재 창에 표시된 모든 경보를 읽은 것으로 표시하려면 **Acknowledge(**확인**)** 드롭다운 목록에서 **Acknowledge Selected(**선택한 경보 확인**)**를 선택합니다. 기본적으로 이 창에는 100개의 행이 표시됩니다. **Rows/Page(**행/페이지**)** 드롭다운 목록에서 원하는 값을 선택하여 표시할 다른 행 수를 선택할 수 있습니다.

현재 창에 표시되어 있는지 여부와 관계없이 모든 경보를 읽은 것으로 표시하려면 **Acknowledge(**확인**)** 드롭다운 목록에서 **Acknowledge All(**모두 확인**)**을 선택합니다.

참고 제목 행에서 **Time Stamp(**타임스탬프**)** 근처에 있는 확인란을 선택하면 창에 표시되는 모든 경보가 선택됩니다. 그러나 선택한 경보 중 하나 이상에 대한 확인란의 선택을 취소하면 모든 기능 선택이 취소됩니다. 이제 **Time Stamp(**타임스탬프**)** 근처의 확인란이 선택되지 않은 것을 확인할 수 있습니다.

단계 **5** 선택한 경보에 해당하는 **Details(**세부정보**)** 링크를 클릭합니다. 선택한 경보에 해당하는 세부정보가 포함된 새 창이 열립니다.

참고 페르소나를 변경하기 전에 생성된 경보에 해당하는 **Details(**세부정보**)** 링크에는 데이터가 표시되지 않습니다.

로그 수집

모니터링 서비스는 로그 및 컨피그레이션 데이터를 수집하고 데이터를 저장한 다음 처리하여 보고서와 경보를 생성합니다. 구축 서버에서 수집된 로그 세부정보를 볼 수 있습니다.

경보 시스템 로그 컬렉션 위치

경보 알림을 시스템 로그 메시지로 보내도록 모니터링 기능을 구성하는 경우 알림을 받을 시스템 로그 대상이 필요합니다. 경보 시스템 로그 대상은 경보 시스템 로그 메시지가 전송되는 대상입니다.

참고 Cisco ISE 모니터링을 위해서는 로깅 소스 인터페이스 컨피그레이션에서 NAS(Network Access Server) IP 주소를 사용해야 합니다. Cisco ISE 모니터링에 사용할 스위치를 구성해야 합니다.

또한 시스템 로그 메시지를 받을 수 있는 시스템 로그 서버로 시스템이 구성되어 있어야 합니다. 경보 시스템 로그 대상을 생성, 편집 및 삭제할 수 있습니다.

원격 로깅 대상을 경보 대상으로 구성하려면 이 절차를 수행합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **New Logging Target(**새 로깅 대상**)** 창에서 로깅 대상에 대한 필수 세부정보를 제출하고 **Include Alarms for this Target(**이 대상에 대한 경보 포함**)** 확인란을 선택합니다.

RADIUS 라이브 로그

다음 표에서는 최근 RADIUS 인증이 표시되는 Live Logs(RADIUS 라이브 로그) 창의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**입니다. 기본 PAN에서만 RADIUS 라이브 로그를 볼 수 있습니다.

표 ***3: RADIUS*** 라이브 로그

필드 이름	설명
Time(시간**)**	모니터링 및 문제 해결 수집 에이전트가 로그를 수신한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.

필드 이름	설명
Details(세부정보**)**	Details(세부정보) 열 아래의 아이콘을 클릭하면 새 브라우저 창에서 **Authentication Detail Report(**인증 세부정보 보고서**)**가 열립니다. 이 보고서는 인증 및 관련 속성, 인증 플로우에 대한 정보를 제공합니다. **Authentication Details(**인증 세부정보**)** 상자에서 **Response Time(**응답 시간**)**은 Cisco ISE가 인증 플로우를 처리하는 데 걸리는 총 시간입니다. 예를 들어 인증이 3개의 왕복 메시지로 구성되어 있고 첫 메시지는 300ms, 그 다음 메시지는 150ms, 마지막 메시지는 100ms의 처리 시간이 소요된 경우 **Response Time(**응답 시간**)**은 300 + 150 + 100 = 550ms입니다. 참고 48시간 넘게 활성 상태인 엔드포인트의 세부정보는 볼 수 없습니다. 48시간 넘게 활성 상태인 엔드포인트의 **Details(**세부정보**)** 아이콘을 클릭하면 다음 메시지가 포함된 페이지가 표시될 수 있습니다. No Data available for this record(이 기록에 데이터가 없습니다). Either the data is purged or authentication for this session record happened a week ago(데이터가 삭제되었거나이 세션 기록에 대한 인증이 일주일 전에 발생했습니다). Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session('PassiveID' 또는 'PassiveID Visibility' 세션인 경우에는 ISE가 아닌 세션에 대한 인증 세부정보만 포함됩니다).
Repeat Count(반복 횟수**)**	지난 24시간 동안 ID, 네트워크 디바이스 및 권한 부여가 변경되지 않고 인증 요청이 반복된 횟수를 표시합니다.

필드 이름	설명
ID	인증과 연결된 로그인한 사용자 이름을 표시합니다. ID 저장소에 사용자 이름이 없는 경우 INVALID로 표시됩니다. 인증이 다른 이유로 인해 실패하는 경우 USERNAME으로 표시됩니다. 참고 이는 사용자에게만 적용되며, MAC 주소에는 적용되지 않습니다. 디버깅을 지원하기 위해 Cisco ISE가 잘못된 사용자 이름을 표시하도록 할 수 있습니다. 이렇게 하려면 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Security Settings(**보안 설정**)**에서 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 확인란을 선택합니다. 또한 **Disclose Invalid Usernames(**잘못된 사용자 이름 공개**)** 옵션이 시간 초과되도록 구성하여 이 옵션을 수동으로 해제할 필요가 없게 할 수 있습니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	iPhone, Android, MacBook, Xbox 등으로 프로파일이 지정된 엔드포인트 유형을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
Authorization Policy(권한 부여 정책**)**	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Network Device(네트워크 디바이스**)**	네트워크 액세스 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	엔드포인트가 연결되어 있는 포트 번호를 표시합니다.
Identity Group(ID 그룹**)**	로그가 생성된 대상인 사용자나 엔드포인트에 할당되는 ID 그룹을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.

필드 이름	설명
Server(서버**)**	로그가 생성된 정책 서비스를 나타냅니다.
MDM Server Name(MDM 서버 이름**)**	MDM 서버의 이름을 표시합니다.
Event(이벤트**)**	이벤트 상태를 표시합니다.
Failure Reason(실패 이유**)**	인증이 실패한 경우 자세한 실패 이유를 표시합니다.
Auth Method(인증 방법**)**	MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Session ID(세션 **ID)**	세션 ID를 표시합니다.

참고 **RADIUS Live Logs(RADIUS** 라이브 로그**)** 및 **TACACS+ Live Logs(TACACS+** 라이브 로그**)** 창에는 각 정책 권한 부여 규칙의 첫 번째 속성에 대한 "Queried PIP" 항목이 표시됩니다. 권한 부여 규칙 내의 모든 속성이 이전 규칙에 대해 이미 쿼리된 사전과 관련된 경우 추가 "Queried PIP" 항목이 표시되지 않습니다.

RADIUS **Live Logs(**라이브 로그**)** 창에서는 다음을 수행할 수 있습니다.

- 데이터를 CSV 또는 PDF 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 사용자 맞춤화 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

TACACS 라이브 로그

다음 표에서는 TACACS+ AAA 세부정보가 표시되는 TACACS Live Logs(TACACS 라이브 로그) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(운영)** > **RADIUS** > **Live Logs(라이브 로그)**입니다. 기본 PAN에서만 TACACS 라이브 로그를 볼 수 있습니다.

표 *4: TACACS* 라이브 로그

필드 이름	사용 지침
생성 시간	특정 이벤트가 트리거된 시간을 기준으로 시스템 로그 생성 시간을 표시합니다.
Logged Time(기록된 시간**)**	모니터링 노드에서 시스템 로그를 처리하고 저장한 시간을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Status(상태**)**	인증 성공 여부를 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다. 인증이 통과한 경우 녹색으로 표시되고, 인증이 실패한 경우 빨간색으로 표시됩니다.
Details(세부정보**)**	돋보기를 클릭하면 표시되는 보고서를 드릴다운하여 선택한 인증 시나리오에 대한 추가 세부정보를 확인할 수 있습니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Session Key(세션 키**)**	ISE가 네트워크 디바이스에 반환하는 세션 키(EAP 성공 또는 EAP 장애 메시지에서 확인 가능)를 표시합니다.
Username(사용자 이름**)**	디바이스 관리자의 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Type(유형**)**	두 가지 유형인 Authentication(인증)과 Authorization(권한 부여)으로 구성됩니다. 인증, 권한 부여 또는 둘 다에서 통과했거나 장애가 발생한 사용자 이름을 표시합니다. 이 열은 필수 항목이므로 선택을 취소할 수 없습니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.

필드 이름	사용 지침
ISE Node(ISE 노드**)**	액세스 요청이 처리되는 ISE 노드의 이름을 표시합니다.
Network Device Name(네트워크 디바이스 이름**)**	네트워크 디바이스의 이름을 표시합니다.
Network Device IP(네트워크 디바이스 **IP)**	액세스 요청이 처리되는 네트워크 디바이스의 IP 주소를 표시합니다.
네트워크 디바이스 그룹	네트워크 디바이스가 속한 해당 네트워크 디바이스 그룹의 이름을 표시합니다.
디바이스 유형	다른 네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 디바이스 유형 정책을 표시합니다.
Location(위치**)**	네트워크 디바이스의 액세스 요청을 처리하는 데 사용되는 위치 기반 정책을 표시합니다.
Device Port(디바이스 포트**)**	액세스 요청을 수행하는 디바이스 포트 번호를 표시합니다.
Failure Reason(실패 이유**)**	네트워크 디바이스에서 수행한 액세스 요청을 거부하는 이유를 표시합니다.
Remote Address(원격 주소**)**	최종 무선국을 고유하게 식별하는 IP 주소, MAC 주소 또는 기타 문자열을 표시합니다.
Matched Command Set(일치하는 명령 집합**)**	MatchedCommandSet 속성 값이 있으면 표시하고, MatchedCommandSet 속성 값이 비어 있거나 속성 자체가 시스템 로그에 없으면 빈 값을 표시합니다.
Shell Profile(셸 프로파일**)**	네트워크 디바이스에서 명령을 실행하기 위해 디바이스 관리자에게 부여된 권한을 표시합니다.

TACACS Live Logs(TACACS 라이브 로그) 페이지에서는 다음을 수행할 수 있습니다.

- 데이터를 csv 또는 pdf 형식으로 내보냅니다.
- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.
- 열 값을 정렬합니다.

참고 모든 사용자 맞춤 설정은 사용자 기본 설정으로 저장됩니다.

라이브 인증

Live Authentications(라이브 인증**)** 창에서 발생하는 최근 RADIUS 인증을 모니터링할 수 있습니다. 이 창에는 지난 24시간 동안의 상위 10개 RADIUS 인증이 표시됩니다. 이 섹션에서는 **Live Authentications(**라이브 인증**)** 창의 기능에 대해 설명합니다.

Live Authentications(라이브 인증**)** 창에는 발생하는 인증 이벤트에 해당하는 라이브 인증 항목이 표시됩니다. 이 창에는 인증 항목 외에 이벤트에 해당하는 라이브 세션 항목도 표시됩니다. 원하는 세션을 드릴다운하여 세션에 해당하는 상세 보고서를 볼 수도 있습니다.

Live Authentications(라이브 인증**)** 창에는 최근 RADIUS 인증이 발생한 순서에 따라 테이블 형식으로 표시됩니다. **Live Authentications(**라이브 인증**)** 창 하단에 표시되는 마지막 업데이트에는 서버 날짜, 시간 및 표준 시간대가 표시됩니다.

참고 액세스 요청 패킷의 비밀번호 속성이 비어 있는 경우 오류 메시지가 트리거되고 액세스 요청이 실패합니다.

단일 엔드포인트 인증이 성공한 경우 두 항목이 **Live Authentications(**라이브 인증**)** 창에 표시됩니다. 하나는 인증 기록에 해당하고 다른 하나는 세션 기록(세션 라이브 보기에서 가져옴)에 해당합니다. 이후에 디바이스에서 또 다른 인증이 성공적으로 수행되면 세션 기록에 해당하는 반복 카운터가 증가합니다. **Live Authentications(**라이브 인증**)** 창에 나타나는 반복 카운터에는 숨겨진 중복 RADIUS 인증 성공 메시지의 수가 표시됩니다.

기본적으로 표시되는 라이브 인증 데이터 범주를 참고하십시오. 이러한 항목은 최근 RADIUS 인증 섹션에 설명되어 있습니다.

모든 열을 표시하거나 선택한 데이터 열만 표시할 수 있습니다. 표시할 열을 선택한 후에는 선택 사항을 저장할 수 있습니다.

라이브 인증 모니터링

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**

단계 **2** **Refresh(**새로 고침**)** 드롭다운 목록에서 시간 간격을 선택하여 데이터 새로 고침 속도를 변경합니다.

단계 **3** **Refresh(**새로 고침**)** 아이콘을 클릭하여 데이터를 수동으로 업데이트합니다.

단계 **4** **Show(**표시**)** 드롭다운 목록의 옵션을 선택하여 표시되는 기록 수를 변경합니다.

단계 **5** **Within(**시간 범위**)** 드롭다운 목록에서 옵션을 선택하여 시간 간격을 지정합니다.

단계 **6** **Add or Remove Columns(**열 추가 또는 제거**)**를 클릭하고 드롭다운 목록에서 옵션을 선택하여 표시되는 열을 변경합니다.

단계 **7** 드롭다운 목록 맨 아래에서 **Save(**저장**)**를 클릭하여 수정 사항을 저장합니다.

단계 **8** **Show Live Sessions(**라이브 세션 표시**)**를 클릭하여 라이브 RADIUS 세션을 확인합니다.

라이브 세션에 대해 동적 CoA(Change of Authorization) 기능을 사용하면 활성 RADIUS 세션을 동적으로 제어할 수 있습니다. NAD(Network Access Device)에 대해 재인증 또는 연결 끊기 요청을 보낼 수 있습니다.

Live Authentications(라이브 인증) 페이지에서 데이터 필터링

Live Authentications(라이브 인증) 페이지의 필터를 사용하면 필요한 정보를 필터링하고 네트워크 인증 문제를 빠르게 해결할 수 있습니다. Authentication(인증)(라이브 로그) 페이지에서 기록을 필터링하여 원하는 기록만 볼 수 있습니다. 인증 로그에는 다양한 세부정보가 포함되어 있으며, 특정 사용자나 위치로부터의 인증을 필터링하면 데이터를 빠르게 스캔할 수 있습니다. Live Authentications(라이브 인증) 페이지의 필드에서 사용할 수 있는 다양한 연산자를 통해 검색 조건에 따라 기록을 필터링할 수 있습니다.

- 'abc': 'abc' 포함
- '!abc': 'abc' 미포함
- '{}': 비어 있음
- '!{}': 비어 있지 않음
- 'abc*': 'abc'로 시작됨
- '*abc': 'abc'로 끝남
- '\!', '*', '\{', '\\' : Esc

Escape(이스케이프) 옵션을 사용하면 필터로 사용되는 특수 문자를 비롯한 특수 문자로 텍스트를 필터링할 수 있습니다. 특수 문자 앞에는 백슬래시(\)를 접두사로 추가해야 합니다. 예를 들어 ID가 "Employee!"인 사용자의 인증 기록을 확인하려면 **Identity Filter(ID** 필터**)** 필드에 "Employee\!"를 입력합니다. 이 예제에서 Cisco ISE는 느낌표(!)를 특수 문자가 아닌 리터럴 문자로 간주합니다.

또한 **Status(**상태**)** 필드에서 통과한 인증 기록, 실패한 인증, 라이브 세션 등만 필터링할 수도 있습니다. 녹색 확인 표시를 클릭하면 이전에 통과한 모든 인증이 필터링됩니다. 빨간색 십자 표시를 클릭하면 실패한 모든 인증이 필터링됩니다. 파란색 i 아이콘을 클릭하면 모든 라이브 세션이 필터링됩니다. 이러한 옵션의 조합을 표시하도록 선택할 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)**

단계 **2** 라이브 인증 표시 페이지에서 원하는 필드를 기준으로 데이터를 필터링합니다.

통과/실패한 인증이나 라이브 인증을 기준으로 결과를 필터링할 수 있습니다.

RADIUS 라이브 세션

다음 표에서는 라이브 인증을 표시하는, RADIUS **Live Sessions(**라이브 세션**)** 창의 필드를 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 RADIUS 라이브 세션의 Primary PAN(기본 PAN)에서만 볼 수 있습니다.

표 ***5: RADIUS*** 라이브 세션

필드 이름	설명
Initiated(시작됨**)**	세션이 시작된 타임스탬프를 표시합니다.
Updated(업데이트됨**)**	변경으로 인해 세션이 마지막으로 업데이트된 타임스탬프를 표시합니다.
Account Session Time(계정 세션 시간**)**	사용자 세션의 시간 범위를 초 단위로 표시합니다.
Session Status(세션 상태**)**	엔드포인트 디바이스의 현재 상태를 표시합니다.
Action(CoA 작업**)**	**Actions(**작업**)** 아이콘을 클릭하여 활성 RADIUS 세션을 다시 인증하거나 활성 RADIUS 세션의 연결을 끊습니다.
Repeat Count(반복 횟수**)**	사용자 또는 엔드포인트를 재인증하는 횟수를 표시합니다.
Endpoint ID(엔드포인트 **ID)**	엔드포인트의 고유한 식별자(일반적으로는 MAC 또는 IP 주소)를 표시합니다.
ID	엔드포인트 디바이스의 사용자 이름을 표시합니다.
IP Address(IP 주소**)**	엔드포인트 디바이스의 IP 주소를 표시합니다.
Audit Session ID(감사 세션 **ID)**	고유 세션 ID를 표시합니다.
Account Session ID(계정 세션 **ID)**	네트워크 디바이스에서 제공하는 고유 ID를 표시합니다.
Endpoint Profile(엔드포인트 프로파일**)**	디바이스에 대한 엔드포인트 프로파일을 표시합니다.
Posture Status(포스처 상태**)**	포스처 검증의 상태 및 인증에 대한 세부정보를 표시합니다.
Security Group(보안 그룹**)**	인증 로그로 식별된 그룹을 표시합니다.
Server(서버**)**	로그가 생성된 정책 서비스 노드를 나타냅니다.

필드 이름	설명
Auth Method(인증 방법**)**	PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), IEE 802.1x 또는 dot1x 등과 같이 RADIUS 프로토콜에서 사용하는 인증 방법을 표시합니다.
Authentication Protocol(인증 프로토콜**)**	PEAP(Protected Extensible Authentication Protocol), EAP(Extensible Authentication Protocol) 등 사용되는 인증 프로토콜을 표시합니다.
Authentication Policy(인증 정책**)**	특정 인증에 대해 선택한 정책의 이름을 표시합니다.
권한 부여 정책	특정 권한 부여에 대해 선택한 정책의 이름을 표시합니다.
Authorization Profiles(권한 부여 프로파일**)**	인증에 사용된 권한 부여 프로파일을 표시합니다.
NAS IP Address(NAS IP 주소**)**	네트워크 디바이스의 IP 주소를 표시합니다.
Device Port(디바이스 포트**)**	네트워크 디바이스에 연결된 포트를 표시합니다.
PRA Action(PRA 작업**)**	네트워크에서 클라이언트가 규정 준수를 위해 올바르게 포스처된 후 클라이언트에 대해 수행되는 정기적 재평가 작업을 표시합니다.
ANC Status(ANC 상태**)**	디바이스의 적응형 네트워크 제어 상태를 Quarantine(격리), Unquarantine(격리 해제) 또는 Shutdown(종료)으로 표시합니다.
WLC Roam(WLC 로밍**)**	로밍 중에 엔드포인트가 WLC 간에 전달되었음을 추적하는 데 사용되는 부울(Y/N)을 표시합니다. cisco-av-pair=nas-update의 값은 Y 또는 N입니다. 참고 Cisco ISE는 WLC의 nas-update=true 속성을 사용하여 세션이 로밍 상태인지 여부를 식별합니다. 원래 WLC가 nas-update=true인 계정 관리 중지 속성을 전송하는 경우 재인증을 방지하기 위해 ISE에서 세션이 삭제되지 않습니다. 로밍이 실패하는 경우 ISE는 5일 동안 활동이 없으면 세션을 지웁니다.
Packets In(수신 패킷**)**	수신된 패킷 수를 표시합니다.
Packets Out(전송 패킷**)**	전송된 패킷 수를 표시합니다.
Bytes In(수신 바이트**)**	수신된 바이트 수를 표시합니다.

필드 이름	설명
Bytes Out(전송 바이트**)**	전송된 바이트 수를 표시합니다.
Session Source(세션 소스**)**	RADIUS 세션인지 아니면 패시브 ID 세션인지를 나타냅니다.
User Domain Name(사용자 도메인 이름**)**	사용자의 등록된 DNS 이름을 표시합니다.
Host Domain Name(호스트 도메인 이름**)**	호스트의 등록된 DNS 이름을 표시합니다.
User NetBIOS Name(사용자 **NetBIOS** 이름**)**	사용자의 NetBIOS 이름을 표시합니다.
Host NetBIOS Name(호스트 **NetBIOS** 이름**)**	호스트의 NetBIOS 이름을 표시합니다.
라이선스 유형	사용하는 라이선스 유형을 표시합니다.
라이선스 세부정보	라이선스 세부정보를 표시합니다.

필드 이름	설명
Provider(사업자**)**	엔드포인트 이벤트는 다양한 시스템 로그 소스에서 학습됩니다. 이러한 시스템 로그 소스를 제공자라고 합니다. • WMI(Windows Management Instrumentation)—WMI는 운영체제, 장치, 애플리케이션 및 서비스 관련 관리 정보에 액세스하기 위한 공통 인터페이스와 개체 모델을 제공하는 Windows 서비스입니다. • 에이전트: 클라이언트나 다른 프로그램을 대신하여 클라이언트에서 실행되는 프로그램입니다. • 시스템 로그: 클라이언트가 메시지를 전송하는 로깅 서버입니다. • REST: 클라이언트가 터미널 서버를 통해 인증됩니다. 이 시스템 로그 소스에 대한 TS Agent ID(TS 에이전트 ID), Source Port Start(소스 포트 시작), Source Port End(소스 포트 끝), Source First Port(소스 최초 포트) 값이 표시됩니다. • Span: 네트워크 정보가 span 프로브를 사용해 검색됩니다. • DHCP: DHCP 이벤트입니다. • 엔드포인트 참고 엔드포인트 세션에서 서로 다른 제공자에서 발생한 두 이벤트를 파악하면, 제공자는 라이브 세션 페이지에 쉼표로 구분된 값으로 표시됩니다.
MAC 주소**(MAC Address)**	클라이언트의 MAC 주소를 표시합니다.
엔드포인트 확인 시간	엔드포인트 프로브가 엔드포인트를 마지막으로 확인한 시간을 표시합니다.

필드 이름	설명
Endpoint Check Result(엔드포인트 확인 결과**)**	엔드포인트 프로브의 결과를 표시합니다. 가능한 값은 다음과 같습니다. • 연결 불가 • 사용자 로그아웃 • 활성 사용자
Source Port Start(소스 포트 시작**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 첫 번째 포트 번호를 표시합니다.
Source Port End(소스 포트 종료**)**	(값은 REST 제공자에 대해서만 표시됨) 포트 범위의 마지막 포트 번호를 표시합니다.
Source First Port(소스 첫 번째 포트**)**	(값은 REST 제공자에 대해서만 표시됨) 터미널 서버 에이전트가 할당한 첫 번째 포트를 표시합니다. 터미널 서버는 모뎀이나 네트워크 인터페이스 없이도 여러 엔드포인트가 연결될 수 있고 여러 엔드포인트와 LAN 네트워크 간의 연결을 촉진하는 서버 또는 네트워크 디바이스를 말합니다. 여러 엔드포인트가 같은 IP 주소를 이용하는 것처럼 보이기 때문에 특정 사용자의 IP 주소를 식별하기가 어렵습니다. 따라서 특정 사용자를 식별하기 위해 각 사용자에 포트 범위를 할당하는 터미널 서버 에이전트가 서버에 설치됩니다. 이렇게 하면 IP 주소-포트-사용자 매핑을 만들 수 있습니다.
TS 에이전트 **ID**	(값은 REST 제공자에 대해서만 표시됨) 엔드포인트에 설치된 터미널 서버 에이전트의 고유 ID를 표시합니다.
AD User Resolved Identities(AD 사용자가 확인한 **ID)**	(값은 AD 사용자에 대해서만 표시됨) 일치하는 잠재적 계정을 표시합니다.
AD User Resolved DNs(AD 사용자가 확인한 **DN)**	(값은 AD 사용자에 대해서만 폿시됨) AD 사용자의 Distinguished Name(고유 이름) 을 표시합니다 (예: CN=chris,CN=Users,DC=R1,DC=com).

요약 내보내기

지난 7일 동안 모든 사용자가 내보낸 보고서의 세부정보를 상태와 함께 볼 수 있습니다. 내보내기 요약에는 수동 보고서와 예약 보고서가 모두 포함됩니다. 내보내기 요약 페이지는 2분마다 자동으로

새로 고쳐집니다. 내보내기 요약 페이지를 수동으로 새로 고치려면 새로 고침 아이콘을 클릭하십시오.

슈퍼 관리자는 진행 중이거나 대기열에 있는 내보내기를 취소할 수 있습니다. 다른 사용자는 본인이 시작한 내보내기 프로세스만 취소할 수 있습니다.

기본적으로는 특정 시점에 보고서를 3번만 수동으로 내보낼 수 있으며, 수동으로 트리거된 나머지 보고서는 대기열에 추가됩니다. 예약된 보고서 내보내기에는 이러한 제한이 없습니다.

참고 대기열에 있는 모든 보고서가 다시 예약되며, 진행 중이거나 취소 중인 상태의 보고서는 Cisco ISE 서버가 재시작되면 실패로 표시됩니다.

참고 기본 MnT 노드가 다운되면 예약된 보고서 내보내기 작업이 보조 MnT 노드에서 실행됩니다.

다음 표에서는 Export Summary(요약 내보내기) 페이지의 필드에 대해 설명합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Export Summary(**요약 내보내기**)**입니다.

표 ***6:*** 요약 내보내기

필드 이름	설명
Report Exported(내보낸 보고서**)**	보고서의 이름을 표시합니다.
Exported By(내보낸 사람**)**	내보내기 프로세스를 시작한 사용자의 역할을 표시합니다.
Scheduled(예약됨**)**	보고서 내보내기가 예약된 내보내기인지 표시합니다.
Triggered On(트리거됨**)**	내보내기 프로세스가 시스템에서 트리거된 시간을 표시합니다.
Repository(저장소**)**	내보낸 데이터를 저장할 저장소 이름을 표시합니다.
Filter Parameters(필터 파라미터**)**	보고서를 내보내는 동안 선택한 필터 파라미터를 표시합니다.

필드 이름	설명
Status(상태**)**	내보낸 보고서의 상태를 표시합니다. 다음 중 하나일 수 있습니다. • 대기열에 있음 • 진행 중 • 완료됨 • 취소 중 • 취소됨 • 실패 • 건너뜀 참고 실패 상태에는 실패 이유가 표시됩니다. 건너뜀 상태는 기본 MnT 노드가 다운되어 예약된 보고서 내보내기를 건너뛰었음을 나타냅니다.

Export Summary(내보내기 요약) 페이지에서 다음을 수행할 수 있습니다.

- 요건에 따라 열을 보이거나 숨깁니다.
- 빠른 필터 또는 맞춤형 필터를 사용하여 데이터를 필터링합니다. 나중에 사용하기 위해 필터를 저장할 수도 있습니다.
- 열을 다시 정렬하고 열의 폭을 조정합니다.

인증 요약(Authentication Summary) 보고서

인증 요청과 관련된 속성에 따른 특정 사용자, 디바이스 또는 검색 기준에 대한 네트워크 액세스 문제를 해결할 수 있습니다. 이를 위해서는 인증 요약 보고서를 실행합니다.

네트워크 액세스 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Device Administration(**디바이스 관리**)** > **Authentication Summary Report(**인증 요약 보고서**)**.

단계 **2** 보고서에서 오류 사유를 필터링합니다.

단계 **3** 네트워크 액세스 문제를 해결하려면 보고서의 오류 사유별 인증 섹션 내 데이터를 검토합니다.

참고 인증 요약(Authentication Summary) 보고서에는 실패했거나 성공한 인증에 해당하는 최신 데이터가 수집되어 표시되므로, 보고서 내용이 표시될 때까지는 몇 분 정도 걸립니다.

구축 및 지원 정보에 대한 **Cisco Support Diagnostics**

개요

Cisco Support Diagnostics Connector는 Cisco TAC(Technical Assistance Center) 및 Cisco 지원 엔지니어가 기본 관리 노드에서 구축 정보를 가져올 수 있도록 지원하는 새로운 기능입니다. TAC는 커넥터를 통해 구축의 특정 노드에 대한 지원 정보를 가져올 수 있게 됩니다. 이 데이터를 사용하면 문제를 보다 신속하고 효과적으로 해결할 수 있습니다.

Cisco ISE 관리 포털을 통해 Cisco Support Diagnostics Connector를 활성화할 수 있습니다. 이 기능을 사용하면 SSE(Security Services Exchange) 클라우드 포털을 활용하여 구축의 기본 정책 관리 노드와 Cisco Support Diagnostics를 양방향으로 연결할 수 있습니다.

사전 요건

- Cisco Support Diagnostics를 활성화하거나 비활성화하려면 슈퍼 관리자 또는 시스템 관리자 역할이 필요합니다.

Cisco Support Diagnostics Connector 구성

Cisco Support Diagnostics 기능을 활성화하려면 다음 단계를 수행합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Network Success Diagnostics(**네트워크 성공 진단**)** > **Cisco Support Diagnostics** > **Cisco Support Diagnostics Setting(Cisco Support Diagnostics** 설정**)**으로 이동합니다.
- 이 기능은 기본적으로 비활성화되어 있습니다. 비활성화된 경우 **Enable Cisco Support Diagnostics(Cisco Support Diagnostics** 활성화**)** 확인란을 선택하여 Cisco Support Diagnostics를 활성화합니다.

Cisco Support Diagnostics 양방향 연결 확인

Cisco ISE가 Cisco Support Diagnostics에 성공적으로 등록되었는지와 Security Services Exchange 포털을 통해 양방향 연결이 설정되었는지 확인하려면 다음 단계를 수행합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Change Configuration Audit(**컨피그레이션 변경 감사**)**으로 이동합니다.
- 다음과 같이 이벤트 보고서를 확인합니다.
  1. Cisco Support Diagnostics가 활성화됩니다.
  2. ISE 서버가 Cisco Support Diagnostics에 등록되었습니다.
  3. ISE SSE 서비스가 Cisco Support Diagnostics에 등록되었습니다.
  4. Cisco Support Diagnostics 양방향 연결이 활성화됩니다.

- Operations Audit(운영 감사) 창(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations**(운영) > **Reports**(보고서) > **Reports**(보고서) > **Audit**(감사) > **Operations Audit**(운영 감사))으로 이동하여 Cisco Support Diagnostics에 구성된 활성화, 비활성화, 등록, 미등록, 기입, 미기입 서비스에 대한 세부정보를 확인해도 됩니다.

문제 해결 정보

Cisco Support Diagnostics 양방향 연결이 끊긴 것으로 표시되면 다음을 확인합니다.

- 스마트 라이선싱: 스마트 라이선싱을 비활성화하면 Cisco Support Diagnostics가 자동으로 비활성화됩니다. 스마트 라이선싱을 재활성화하여 커넥터를 활성화합니다.
- **Security Services Exchange** 클라우드에 대한 연결: Cisco Support Diagnostics가 활성화된 경우 Cisco ISE는 Security Services Exchange 포털로 설정된 영구 연결을 지속적으로 확인합니다. 이 연결이 끊어진 것으로 확인되면 "Alarms: The Cisco Support Diagnostics bi-directional connectivity is broken.(경보: Cisco Support Diagnostics 양방향 연결이 끊겼습니다.)" 경보가 트리거됩니다. 이전에 제공된 컨피그레이션 단계를 사용하여 기능을 다시 활성화하십시오.
-

관련 정보

관리자는 ERS API를 사용하여 다음과 같은 특정 작업을 수행할 수 있습니다.

- 특정 노드에서 지원 정보를 트리거합니다.
- 트리거된 지원 번들의 상태를 가져옵니다.
- 지원 번들을 다운로드합니다.
- 구축 정보를 가져옵니다.

사용 및 기타 정보는 ERS SDK 페이지를 참조하십시오.

진단 문제 해결 도구

진단 도구를 사용하면 Cisco ISE 네트워크를 진단하여 문제를 해결하고 문제 해결 방법에 대한 자세한 지침을 제공할 수 있습니다. 이러한 도구를 사용하여 인증 문제를 해결하고 Trustsec 디바이스를 포함하여 네트워크에 있는 네트워크 디바이스의 컨피그레이션을 평가할 수 있습니다.

RADIUS 인증 문제 해결 도구

이 도구를 사용하면 예기치 않은 인증 결과가 있는 경우 문제 해결을 위해 RADIUS 인증 또는 Active Directory 관련 RADIUS 인증을 검색하고 선택할 수 있습니다. 인증을 통과할 것으로 기대했지만 실패했을 경우 또는 사용자나 머신에서 특정 권한 수준을 가질 것을 예상했지만 사용자나 머신에 해당 권한이 없는 경우 이 도구를 사용하십시오.

- 문제 해결을 위해 사용자 이름, 엔드포인트 ID, NAS(Network Access Service) IP 주소 및 인증 실패 이유를 기준으로 RADIUS 인증을 검색하면 Cisco ISE에는 시스템(현재) 날짜의 인증만 표시됩니다.
- 문제 해결을 위해 NAS 포트를 기준으로 RADIUS 인증을 검색하면 Cisco ISE에는 지난달의 시작부터 현재 날짜까지 모든 NAS 포트 값이 표시됩니다.

참고 NAS IP 주소 및 엔드포인트 ID 필드를 기준으로 RADIUS 인증을 검색하면 검색은 먼저 작업 데이터베이스에서 수행된 다음 컨피그레이션 데이터베이스에서 수행됩니다.

예기치 않은 **RADIUS** 인증 결과 관련 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **RADIUS Authentication Troubleshooting(RADIUS** 인증 문제 해결**)**

단계 **2** 필요에 따라 필드에서 검색 기준을 지정합니다.

단계 **3** **Search(**검색**)**를 클릭하여 검색 기준과 일치하는 RADIUS 인증을 표시합니다.

AD 관련 인증을 검색하는 경우 구축에 Active Directory 서버가 구성되어 있지 않으면 'AD가 구성되어 있지 않음' 메시지가 표시됩니다.

단계 **4** 표에서 RADIUS 인증 기록을 선택하고 **Troubleshoot(**문제 해결**)**을 클릭합니다.

AD 관련 인증 문제를 해결해야 하는 경우 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory** > **AD node(AD** 노드**)** 아래의 진단 도구에 액세스합니다.

단계 **5** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정한 후에 **Submit(**제출**)**을 클릭합니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

단계 **7** 문제 해결이 완료된 후 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

단계 **8** 진단 내용, 문제 해결을 위한 단계 및 문제 해결 요약을 확인하려면 **Done(**완료**)**을 클릭합니다.

네트워크 디바이스 명령 진단 도구 실행

네트워크 디바이스 실행 명령 진단 도구를 사용하면 네트워크 디바이스에 대해 **show** 명령을 실행할 수 있습니다.

표시되는 결과는 콘솔에 표시되는 것과 동일합니다. 이 도구를 사용하면 디바이스 컨피그레이션의 모든 문제를 식별할 수 있습니다.

네트워크 디바이스의 컨피그레이션을 확인하거나 네트워크 디바이스가 구성된 방법을 확인하려면 이 도구를 활용하면 됩니다.

네트워크 디바이스 실행 명령 진단 도구에 액세스하려면 다음 탐색 경로 중 하나를 선택하십시오.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Troubleshoot(**문제 해결**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.

표시되는 **Execute Network Device Command(**네트워크 디바이스 실행 명령**)** 창에서 해당 필드에 실행할 네트워크 디바이스의 IP 주소와 show 명령을 입력합니다. **Run(**실행**)**을 클릭합니다.

구성 확인을 위해 **Cisco IOS** 표시 명령 실행

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**.

단계 **2** 해당 필드에 정보를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭하여 지정한 네트워크 디바이스에서 명령을 실행합니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 네트워크 디바이스에서 명령을 실행하고 출력을 확인합니다.

컨피그레이션 검증기 평가 도구

이 진단 도구를 사용하여 네트워크 디바이스의 컨피그레이션을 평가하고 컨피그레이션 문제를 모두 식별할 수 있습니다. Expert Troubleshooter는 디바이스의 컨피그레이션을 표준 컨피그레이션과 비교합니다.

에이전트리스 포스처 문제 해결

에이전트리스 포스처 보고서는 에이전트가 없는 포스처가 정상적으로 작동하지 않을 때 활용할 수 있는 기본 문제 해결 도구입니다. 이 보고서에는 스크립트 업로드 완료, 스크립트 업로드 실패, 스크립트 실행 완료 등의 이벤트를 포함하는 에이전트리스 플로우 단계와 알려진 실패 이유가 표시됩니다.

다음 두 위치에서 에이전트리스 포스처 문제 해결에 액세스할 수 있습니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Live Logs(**라이브 로그**)**: 문제를 해결하려는 클라이언트의 Posture Status(포스처 상태) 열에서 3개의 세로 점을 클릭합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Troubleshoot(**문제 해결**) > Diagnostics(**진단**) > General Tools(**일반 도구**) > Agentless Posture Troubleshooting(**에이전트리스 포스처 문제 해결**)**을 선택합니다.

에이전트리스 포스처 문제 해결 도구는 지정된 클라이언트에 대한 에이전트리스 포스처 활동을 수집합니다. **Agentless Posture Flow(**에이전트리스 포스처 플로우**)**는 포스처를 시작하고 현재 활성 상태인 클라이언트와 Cisco ISE 간의 모든 상호 작용을 표시합니다. **Only Download Client Logs(**클라이언트 로그만 다운로드**)**에서는 클라이언트에서 지난 24시간 동안의 포스처 플로우가 포함된 로그를 생성합니다. 클라이언트는 언제든지 로그를 삭제할 수 있습니다. 수집이 완료되면 로그의 ZIP 파일을 내보낼 수 있습니다.

보고서

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Reports(**보고서**) > Reports(**보고서**) > Endpoints and Users(**엔드포인트 및 사용자**) > Agentless Posture(**에이전트리스 포스처**)**를 선택하여 에이전트리스 포스처를 실행하는 모든 엔드포인트를 확인합니다.

네트워크 디바이스 컨피그레이션 문제 해결

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Evaluate Configuration Validator(**구성 검증기 평가**)**를 선택합니다.

단계 **2** 구성을 평가할 네트워크 디바이스의 IP 주소를 **Network Device IP(**네트워크 디바이스 **IP)** 필드에 입력합니다.

단계 **3** 확인란을 선택하고 권장 템플릿과 비교할 구성 옵션 옆의 라디오 버튼을 클릭합니다.

단계 **4** **Run(**실행**)**을 클릭합니다.

단계 **5** 표시되는 **Progress Details...(**진행 세부정보**)** 영역에서 **Click Here to Enter Credentials(**여기를 클릭하여 자격 증명 입력**)**를 클릭합니다. **Credentials Window(**자격 증명 창**)** 대화 상자에서 네트워크 디바이스와의 연결을 설정하는 데 필요한 연결 매개변수 및 자격 증명을 입력하고 **Submit(**제출**)**를 클릭합니다

워크플로우를 취소하려면 **Progress Details...(**진행 세부정보**...)** 창에서 **Click Here to Cancel the Running Workflow(**여기를 클릭하여 실행 중인 워크플로우 취소**)**를 클릭합니다.

단계 **6** 분석할 인터페이스 옆의 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

단계 **7** 구성 평가에 대한 자세한 내용을 보려면 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

엔드포인트 포스처 장애 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Posture Troubleshooting(**포스처 문제 해결**)**을 선택합니다.

단계 **2** 해당 필드에 정보를 입력합니다.

단계 **3** **Search(**검색**)**를 클릭합니다.

단계 **4** 이벤트에 대한 설명을 찾고 해결책을 확인하려면 목록에서 이벤트를 선택하고 **Troubleshoot(**문제 해결**)**을 클릭합니다.

세션 추적 테스트 케이스

이 툴을 사용하면 정책 플로우를 예측 가능한 방식으로 테스트하여 실제 트래픽을 실제 디바이스에서 생성할 필요 없이 정책이 구성된 방식을 확인하고 검증할 수 있습니다.

테스트 사례에 사용할 속성 및 해당 값의 목록을 구성할 수 있습니다. 이러한 세부정보는 정책의 런타임 호출을 시뮬레이션하기 위해 정책 시스템과의 상호 작용을 수행하는 데 사용됩니다.

사전을 사용하여 속성을 구성할 수 있습니다. 단순 RADIUS 인증에 적용 가능한 모든 사전이 **Attributes(**속성**)** 필드에 나열됩니다.

참고 단순 RADIUS 인증에 대해서만 테스트 케이스를 구성할 수 있습니다.

세션 추적 테스트 케이스 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Troubleshoot(**문제 해결**) > Diagnostic Tools(**진단 도구**) > General Tools(**일반 도구**) > Session Trace Test Cases(**세션 추적 테스트 케이스**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Test Details(**테스트 세부정보**)** 탭에서 테스트 케이스의 이름과 설명을 입력합니다.

단계 **4** 사전 정의된 테스트 케이스 중 하나를 선택하거나 필수 속성 및 해당 값을 구성합니다. 다음과 같은 미리 정의된 테스트 케이스를 사용할 수 있습니다.

- 기본 인증 액세스
- 프로파일링된 Cisco 폰
- 호환되는 디바이스 액세스
- Wi-Fi 게스트(리디렉션)
- Wi-Fi 게스트(액세스)

미리 정의된 테스트 케이스를 선택하면 Cisco ISE가 테스트 케이스의 관련 속성을 자동으로 채웁니다. 이러한 속성에 기본값을 사용하거나 표시된 옵션에서 원하는 값을 선택할 수 있습니다. 테스트 케이스에 사용자 맞춤화 속성을 더 추가할 수도 있습니다.

테스트 케이스에 추가하는 속성 및 값은 Text(텍스트) 필드에 나열됩니다(Custom Attributes(사용자 맞춤화 속성) 필드 아래). Text(텍스트) 필드에서 콘텐츠를 편집하면 Cisco ISE에서 업데이트된 콘텐츠의 유효성과 syntax(명령문)를 확인합니다.

Test Details(테스트 세부정보) 페이지 하단에서 모든 속성의 요약을 볼 수 있습니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

Cisco ISE는 테스트 세부정보를 저장하기 전에 속성 및 해당 값을 검증하고 오류가 있는 경우 이를 표시합니다.

단계 **6** **Test Visualizer(**시각화 테스트**)** 탭에서 이 테스트 케이스를 실행할 노드를 선택합니다.

참고 정책 서비스 페르소나가 있는 노드만 **ISE Node(ISE** 노드**)** 드롭다운 목록에 표시됩니다.

User Groups/Attributes(사용자 그룹/속성**)**를 클릭하여 외부 ID 저장소에서 사용자의 그룹 및 속성을 검색합니다.

단계 **7** **Execute(**실행**)**를 클릭합니다.

Cisco ISE는 테스트 케이스를 실행하고 테스트 케이스의 단계별 결과를 표 형식으로 나타냅니다. 정책 단계, 일치 규칙 및 결과 개체가 표시됩니다. 각 단계의 세부정보를 보려면 녹색 아이콘을 클릭합니다.

단계 **8** 이전 테스트 실행의 결과를 보려면 **Previous Test Executions(**이전 테스트 실행**)** 탭을 클릭합니다. 또한 두 개의 테스트 케이스를 선택하고 비교할 수 있습니다. Cisco ISE는 각 테스트 케이스의 속성에 대한 비교 보기를 표 형식으로 표시합니다.

RADIUS Live Logs(RADIUS 라이브 로그) 페이지에서 세션 추적 테스트 케이스 툴을 시작할 수 있습니다. Live Logs(라이브 로그) 페이지에서 항목을 선택하고 Actions(작업) 아이콘(Details(세부정보) 열)을 클릭하여 세션 추적 테스트 케이스 툴을 시작할 수 있습니다. Cisco ISE는 해당 로그 항목에서 관련 속성 및 해당 값을 추출합니다. 필요한 경우 이러한 속성 및 값을 수정하고 테스트 케이스를 실행할 수 있습니다.

고급 문제 해결을 위한 기술 지원 터널

Cisco ISE는 Cisco IronPort Tunnel 인프라를 사용하여 Cisco 기술 지원 엔지니어가 ISE 서버에 연결해 시스템의 문제를 해결할 수 있는 보안 터널을 생성합니다. Cisco ISE는 SSH를 사용하여 터널을 통한 보안 연결을 생성합니다.

관리자는 터널 액세스를 제어할 수 있습니다. 즉, 지원 엔지니어에게 액세스 권한을 부여할 시기와 기간을 선택할 수 있습니다. Cisco 고객 지원에서는 사용자 개입 없이 터널을 설정할 수 없습니다. 서비스 로그인에 대한 알림이 수신됩니다. 언제든지 터널 연결을 비활성화할 수 있습니다. 기본적으로 기술 지원 터널은 72시간 동안 열려 있습니다. 기본적으로 기술 지원 터널은 72시간 동안 열려 있지만 모든 문제해결 작업이 완료되면 관리자나 지원 엔지니어가 터널을 닫는 것이 좋습니다. 필요한 경우 터널 오픈 기간을 72시간보다 길게 연장하도록 선택할 수 있습니다.

tech support-tunnel enable 명령을 사용하여 터널 연결을 시작합니다.

tech support-tunnel status 명령은 연결 상태를 표시합니다. 이 명령은 연결 설정 여부, 인증 장애 발생 여부 또는 서버에 연결할 수 없는지 여부에 대한 정보를 제공합니다. 터널 서버에 연결할 수는 있지만 ISE가 인증을 할 수 없으면 ISE는 30분 동안 5분마다 다시 인증을 시도하며 그 후에는 터널이 비활성화됩니다.

tech support-tunnel disable 명령을 사용하여 터널 연결을 비활성화할 수 있습니다. 이 명령을 실행하면 지원 엔지니어가 현재 로그인되어 있어도 기존 터널의 연결이 끊깁니다.

ISE 서버에서 터널 연결을 이미 설정한 경우에는 생성된 SSH 키를 ISE 서버에서 사용할 수 있습니다. 나중에 지원 터널을 활성화하려고 하면 이전에 생성되었던 SSH 키를 재사용할지를 묻는 메시지가 표시됩니다. 같은 키를 사용하거나 새 키를 생성하도록 선택할 수 있습니다. 또한 **tech support-tunnel resetkey** 명령을 사용하여 키를 수동으로 재설정할 수도 있습니다. 터널 연결이 활성화되어 있을 때 이 명령을 실행하면 연결을 먼저 비활성화하라는 메시지가 표시됩니다. 기존 연결을 비활성화하지 않고 계속 사용하도록 선택하면 기존 연결이 비활성화된 후에 키가 재설정됩니다. 연결을 비활성화하도록 선택하면 터널 연결이 끊기고 키가 즉시 재설정됩니다.

터널 연결을 설정한 후에는 **tech support-tunnel extend** 명령을 사용하여 연결을 연장할 수 있습니다.

tech support-tunnel 명령의 사용 지침은 CCisco Identity Services Engine CLI Reference Guide를 참고하십시오.

기술 지원 터널 설정

Cisco ISE CLI(Command Line Interface)를 통해 보안 터널을 설정할 수 있습니다.

단계 **1** Cisco ISE CLI에서 다음 명령을 입력합니다.

tech support-tunnel enable

시스템에서 터널의 비밀번호와 별칭을 입력하라는 메시지를 표시합니다.

단계 **2** 비밀번호를 입력합니다.

단계 **3** (선택 사항) 터널의 별칭을 입력합니다.

시스템에서 SSH 키를 생성하고 비밀번호, 디바이스 일련 번호 및 SSH 키를 표시합니다. 지원 엔지니어가 시스템에 연결할 수 있도록 이 정보를 Cisco 고객 지원에 전달해야 합니다.

단계 **4** 비밀번호, 디바이스 일련 번호 및 SSH 키를 복사하여 Cisco 고객 지원에 전송합니다.

이제 지원 엔지니어가 ISE 서버에 안전하게 연결할 수 있습니다. 서비스 로그인에 대한 정기 알림이 수신됩니다.

들어오는 트래픽을 검증하는 **TCP** 덤프 유틸리티

TCP 덤프 유틸리티는 패킷을 스니핑합니다. 이 패킷을 사용하여 예상 패킷이 노드에 도달했는지 확인할 수 있습니다. 예를 들어 보고서에 들어오는 인증 또는 로그인이 나타나 있지 않은 경우 들어오는 트래픽이 없거나 들어오는 트래픽이 Cisco ISE에 도달되지 않는다는 의심이 있을 수 있습니다. 이 경우 이 도구를 실행하여 검증할 수 있습니다.

네트워크 문제를 해결하는 데 도움이 되도록 TCP 덤프 옵션을 구성한 다음 네트워크 트래픽에서 데이터를 수집할 수 있습니다.

TCP 덤프를 사용하여 네트워크 트래픽 모니터링

TCP Dump(TCP 덤프) 페이지에는 생성한 TCP 덤프 프로세스 파일이 나열됩니다. 다양한 용도로 다른 파일을 생성하고 필요에 따라 실행한 다음, 필요하지 않은 경우 삭제할 수 있습니다.

크기, 파일 수 및 프로세스 실행 기간을 지정하여 수집되는 데이터를 제어할 수 있습니다. 프로세스가 제한 시간 전에 완료되고 최대 크기보다 작은 파일 둘 이상을 활성화한 경우 프로세스가 계속 진행되고 다른 덤프 파일이 생성됩니다.

결합된 인터페이스를 포함하여 더 많은 인터페이스에서 TCP 덤프를 실행할 수 있습니다.

사람이 읽을 수 있는 형식은 더 이상 옵션으로 제공되지 않으며, 덤프 파일은 항상 원시 형식입니다.

저장소에 대한 IPv6 연결을 지원합니다.

시작하기 전에

TCP Dump(TCP 덤프) 페이지의 Network Interface(네트워크 인터페이스) 드롭다운 목록에는 IPv4 또는 IPv6 주소가 구성되어 있는 NIC(Network Interface Cards)만 표시됩니다. 기본적으로 VMware에서는 모든 NIC가 연결되어 있으므로 모든 NIC에 IPv6 주소가 있으며 네트워크 인터페이스 드롭다운 목록에 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **TCP Dump(TCP** 덤프**)**.

단계 **2** TCP 덤프 유틸리티의 소스로 **Host Name(**호스트 이름**)**을 선택합니다.

단계 **3** 드롭다운 목록에서 모니터링할 네트워크 인터페이스를 선택합니다.

단계 **4** Filter(필터) 필드에 필터링할 부울 식을 입력합니다.

다음과 같은 표준 tcpdump 필터 식이 지원됩니다.

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 및 not 10.77.122.119

단계 **5** 이 TCP 덤프 프로세스의 파일 이름을 입력합니다.

단계 **6** TCP 덤프 로그 파일을 저장할 저장소를 선택합니다.

단계 **7** **File Size(**파일 크기**)** - 최대 파일 크기를 선택합니다.

덤프가 이 파일 크기를 초과하면 새 파일이 열려 덤프를 계속합니다. 덤프가 새 파일을 계속 사용할 수 있는 횟수는 **Limit to(**다음으로 제한**)** 설정을 기준으로 제한됩니다.

단계 **8** **Limit to(**다음으로 제한**)** - 덤프가 확장할 수 있는 파일의 수를 제한합니다.

단계 **9** **Time Limit(**시간 제한**)** - 종료 전에 덤프가 실행되는 기간을 구성합니다.

단계 **10** 라디오 버튼을 클릭해 On(켜기) 또는 Off(끄기)로 설정하여 Promiscuous Mode(무차별 모드)를 설정합니다. 기본값은 On(켜기)입니다.

무차별 모드는 네트워크 인터페이스가 시스템 CPU로 모든 트래픽을 전달하는 기본 패킷 스니핑 모드입니다. 이 모드는 On(켜기)으로 설정해 두는 것이 좋습니다.

참고 Cisco ISE는 1500MTU(점보 프레임)보다 큰 프레임을 지원하지 않습니다.

TCP 덤프 파일 저장

시작하기 전에

TCP 덤프를 사용하여 네트워크 트래픽 모니터링 섹션의 설명에 따라 작업을 정상적으로 완료한 상태여야 합니다.

참고 Cisco ISE CLI를 통해 TCP Dump에 액세스할 수도 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **TCP Dump(TCP** 덤프**)**.

단계 **2** **Format(**형식**)** 드롭다운 목록에서 옵션을 선택합니다. **Human Readable(**사람이 읽을 수 있음**)**이 기본값입니다.

단계 **3** **Download(**다운로드**)**를 클릭하고 원하는 위치로 이동한 후에 **Save(**저장**)**를 클릭합니다.

단계 **4** 이전 덤프 파일을 먼저 저장하지 않고 제거하려면 **Delete(**삭제**)**를 클릭합니다.

엔드포인트 또는 사용자의 예기치 않은 SGACL 비교

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **Egress (SGACL) Policy(**이그레스**(SGACL)** 정책**)**.

단계 **2** SGACL 정책을 비교할 TrustSec 디바이스의 네트워크 디바이스 IP 주소를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 제안 해결 단계를 확인합니다.

이그레스 정책 진단 흐름

이그레스 정책 진단 도구는 비교를 위해 다음 표에서 설명하는 프로세스를 사용합니다.

프로세스 단계	설명
1	사용자가 입력한 IP 주소에 디바이스를 연결하고 각 소스 및 대상 SGT 페어에 대해 ACL(Access Control List, 액세스 제어 목록)을 가져옵니다.
2	Cisco ISE에 구성되어 있는 이그레스 정책을 확인하고 각 소스 및 대상 SGT 쌍에 대해 ACL을 가져옵니다.
3	Cisco ISE에서 가져온 SGACL 정책과 네트워크 디바이스에서 가져온 SGACL 정책을 비교합니다.
4	SGACL이 일치하지 않으면 소스 및 대상 SGT 쌍을 표시합니다. 또한 일치하는 엔트리도 추가 정보로 표시합니다.

SXP-IP 매핑을 사용하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Trustsec Tools(TrustSec** 도구**)** > **SXP-IP Mappings(SXP-IP** 매핑**)**.

단계 **2** 네트워크 디바이스의 IP 주소를 입력합니다.

단계 **3** **Select(**선택**)**를 클릭합니다.

단계 **4** **Run(**실행**)**, **User Input Required(**사용자 입력 필요**)**를 차례로 클릭하고 필요한 필드를 수정합니다.

Expert Troubleshooter가 네트워크 디바이스에서 TrustSec SXP 연결을 검색하며, 피어 SXP 디바이스를 선택하라는 메시지가 다시 표시됩니다.

단계 **5** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필요한 정보를 입력합니다.

단계 **6** SXP 매핑을 비교할 피어 SXP 디바이스의 확인란을 선택하고 일반 연결 매개변수를 입력합니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

단계 **8** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 해결 단계를 확인합니다.

IP-SGT 매핑을 사용하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **IP User SGT(IP** 사용자 **SGT)**를 선택합니다.

단계 **2** 필요에 따라 필드에 정보를 입력합니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

추가 입력을 요청하는 메시지가 표시됩니다.

단계 **4** **User Input Required(**사용자 입력 필요**)**를 클릭하고 필드의 내용을 필요한 대로 수정합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

단계 **6** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 진단 및 해결 단계를 확인합니다.

디바이스 **SGT** 도구

Trustsec 솔루션에서 활성화된 디바이스의 경우 각 네트워크 디바이스는 RADIUS 인증을 통해 SGT 값이 할당됩니다. 디바이스 SGT 진단 도구는 네트워크 디바이스(관리자가 제공하는 IP 주소 사용)에 연결하여 네트워크 디바이스 SGT 값을 얻습니다. 그런 다음 RADIUS 인증 기록에서 가장 최근에 할당된 SGT 값을 확인합니다. 마지막으로 디바이스-SGT 쌍이 테이블 형식으로 표시되며 SGT 값이 동일한지, 아니면 다른지 나타냅니다.

디바이스 **SGT** 매핑을 비교하여 **TrustSec**이 활성화된 네트워크의 연결 문제 해결

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **TrustSec Tools(TrustSec** 도구**)** > **Device SGT(**디바이스 **SGT)**

단계 **2** 필요에 따라 필드에 정보를 입력합니다.

텔넷의 기본 포트 번호는 23이고 SSH의 기본 포트 번호는 22입니다.

단계 **3** **Run(**실행**)**을 클릭합니다.

단계 **4** **Show Results Summary(**결과 요약 표시**)**를 클릭하여 디바이스 SGT 비교 결과를 확인합니다.

추가 문제 해결 정보 얻기

Cisco ISE에서는 관리 포털에서 지원 및 문제 해결 정보를 다운로드할 수 있습니다. 지원 번들을 사용하면 Cisco TAC(Technical Assistance Center)가 Cisco ISE의 문제 해결을 위한 진단 정보를 준비할 수 있습니다.

참고 TAC용 고급 문제 해결 정보를 제공하는 지원 번들과 디버그 로그는 해석하기가 어렵습니다. Cisco ISE에서 제공하는 다양한 보고서 및 문제 해결 도구를 사용하여 네트워크에서 발생하는 문제를 진단하고 해결할 수 있습니다.

Cisco ISE 지원 번들

지원 번들에 포함시킬 로그를 구성할 수 있습니다. 예를 들어 디버그 로그에 포함되도록 특정 서비스의 로그를 구성할 수 있습니다. 날짜를 기준으로 로그를 필터링할 수도 있습니다.

다운로드할 수 있는 로그는 다음과 같이 분류될 수 있습니다.

- 전체 구성 데이터베이스: 사람이 읽을 수 있는 XML 형식의 Cisco ISE 구성 데이터베이스를 포함합니다. 문제를 해결할 때 이 데이터베이스 구성을 다른 Cisco ISE 노드로 가져와 시나리오를 다시 생성할 수 있습니다.
- 디버그 로그: 부트스트랩, 애플리케이션 구성, 런타임, 구축, PKI(Public Key Infrastructure) 정보와 모니터링 및 보고 로그를 캡처합니다.

  디버그 로그는 특정 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그를 사용하려면 11장, "로깅"을 참고해 주십시오. 디버그 로그를 사용하지 않으면 모든 정보 메시지(INFO)가 지원 번들에 포함됩니다. 자세한 내용은 Cisco ISE 디버그 로그, 66 페이지를 참고하십시오.
- 로컬 로그: Cisco ISE에서 실행되는 다양한 프로세스의 시스템 로그 메시지를 포함합니다.
- 코어 파일: 크래시의 원인을 식별하는 데 도움이 되는 중요한 정보를 포함합니다. 이 로그는 애플리케이션이 크래시될 때 생성되며 힙 덤프를 포함합니다.
- 모니터링 및 보고 로그: 알림 및 보고서에 대한 정보를 포함합니다.
- 시스템 로그: Cisco ADE(Application Deployment Engine) 관련 정보를 포함합니다.
- 정책 구성: Cisco ISE에서 사람이 읽을 수 있는 형식으로 구성된 정책을 포함합니다.

Cisco ISE CLI에서 **backup-logs** 명령을 사용하여 이러한 로그를 다운로드할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

참고 인라인 포스처 노드의 경우 관리 포털에서 지원 번들을 다운로드할 수 없습니다. Cisco ISE CLI에서 **backup-logs** 명령을 사용해야 합니다.

관리 포털에서 이러한 로그를 다운로드하도록 선택하는 경우 다음과 같이 해 주십시오.

- 디버그 로그 또는 시스템 로그 등의 로그 유형에 따라 로그 하위 집합만 다운로드합니다.
- 선택한 로그 유형에 대한 마지막 *n* 번호 파일만 다운로드합니다. 이 옵션을 사용하면 지원 번들의 크기와 다운로드에 소요되는 시간을 제어할 수 있습니다.

모니터링 로그는 모니터링, 보고 및 문제 해결 기능에 대한 정보를 제공합니다. 로그 다운로드에 대한 자세한 내용은 Cisco ISE 로그 파일 다운로드, 65 페이지를 참고하십시오.

지원 번들

지원 번들을 단순 tar.gpg 파일로 로컬 컴퓨터에 다운로드할 수 있습니다. 지원 번들은 ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar..gpg 형식으로 날짜 및 타임스탬프를 사용하여 이름이 지정됩니다. 브라우저에서 지원 번들을 적절한 위치에 저장하도록 메시지를 표시합니다. 지원 번들 콘텐츠를 추출하여 README.TXT 파일을 볼 수 있습니다. 이 파일에는 지원 번들의 콘텐츠와 함께 지원 번들에 포함되어 있는 ISE 데이터베이스의 콘텐츠를 가져오는 방법이 설명되어 있습니다.

Cisco ISE 로그 파일 다운로드

네트워크에서 문제를 해결하는 동안 자세한 정보를 확인하기 위해 Cisco ISE 로그 파일을 다운로드할 수 있습니다.

설치 및 업그레이드 문제를 해결하기 위해 ADE-OS가 포함된 시스템 로그 및 기타 로그 파일을 다운로드할 수도 있습니다.

지원 번들을 다운로드하는 동안 암호화 키를 수동으로 입력하는 대신 이제 암호화를 위한 공개 키를 사용하도록 선택할 수 있습니다. 이 옵션을 선택하면 지원 번들 암호화 및 암호 해독에 Cisco PKI가 사용됩니다. Cisco TAC에서 공개 키와 개인 키를 유지 관리합니다. Cisco ISE는 공개 키를 사용하여 지원 번들을 암호화합니다. Cisco TAC는 개인 키를 사용하여 지원 번들을 암호 해독할 수 있습니다. 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 사용합니다. 문제를 온프레미스(구내 장비)에서 문제 해결하려는 경우에는 공유 키 암호화를 사용합니다.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- 디버그 로그 및 디버그 로그 레벨을 구성해야 합니다.

단계 **1** **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**.

단계 **3** 지원 번들을 다운로드할 노드를 클릭합니다.

단계 **4** **Support Bundle(**지원 번들**)** 탭에서 지원 번들에 입력할 매개변수를 선택합니다.

모든 로그를 포함하는 경우 지원 번들이 매우 커지며 다운로드 시간이 오래 걸립니다. 다운로드 프로세스를 최적화하려면 최근 *n*개 파일만 다운로드하도록 선택합니다.

단계 **5** 지원 번들을 생성할 시작 및 종료 날짜를 입력합니다.

단계 **6** 다음 중 하나를 선택합니다.

- Public Key Encryption(공개 키 암호화): 문제 해결을 위해 Cisco TAC에 지원 번들을 제공하려면 이 옵션을 선택합니다.

- Shared Key Encryption(공유 키 암호화): 온프레미스에서 로컬로 문제를 해결하려는 경우 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 지원 번들의 암호화 키를 입력해야 합니다.

단계 **7** 지원 번들용 암호화 키를 입력하고 한 번 더 입력합니다.

단계 **8** **Create Support Bundle(**지원 번들 생성**)**을 클릭합니다.

단계 **9** **Download(**다운로드**)**를 클릭하여 새로 생성한 지원 번들을 다운로드합니다.

지원 번들은 애플리케이션 브라우저를 실행 중인 클라이언트 시스템에 다운로드되는 tar.gpg 파일입니다.

다음에 수행할 작업

특정 구성 요소에 대한 디버그 로그를 다운로드합니다.

Cisco ISE 디버그 로그

디버그 로그는 다양한 Cisco ISE 구성 요소에 대한 문제 해결 정보를 제공합니다. 디버그 로그에는 최근 30일 내에 생성된 위험 및 경고 경보와 함께 최근 7일 내에 생성된 정보 경보가 포함됩니다. 문제를 보고하는 동안 이러한 디버그 로그를 사용하고 문제 진단 및 확인을 위해 해당 로그를 보낼지 묻는 메시지가 표시될 수 있습니다.

참고 디버그 로그의 모니터링 등 로드가 많은 디버그 로그를 활성화하면 높은 로드에 대한 경보가 생성될 수 있습니다.

디버그 로그 가져오기

단계 **1** 디버그 로그를 가져올 구성 요소를 구성합니다.

단계 **2** 디버그 로그를 다운로드합니다.

Cisco ISE 구성 요소 및 해당 디버그 로그

표 *7:* 구성 요소 및 해당 디버그 로그

구성 요소	디버그 로그
Active Directory	ad_agent.log
Cache Tracker	tracking.log
EDF(Entity Definition Framework)	edf.log
JMS	ise-psc.log
License	ise-psc.log

구성 요소	디버그 로그
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
게스트 액세스 관리자	guest.log
게스트 액세스	guest.log
MyDevices	guest.log
포털	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log

구성 요소	디버그 로그
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

기능별 디버그 마법사 설정

디버그 마법사에는 Cisco ISE 노드의 문제를 해결하는 데 사용할 수 있는 디버그 템플릿이 포함되어 있습니다. 디버그 프로파일 및 디버그 로그를 구성 할 수 있습니다.

Debug Profile Configuration(디버그 프로파일 컨피그레이션**)** 창에서 템플릿 내부의 개별 구성 요소에 대한 디버그 로그 심각도 레벨을 구성할 수 있습니다.

Debug Profile Configuration(디버그 프로파일 컨피그레이션**)** 창에서 디버그 로그의 심각도 레벨을 구성할 수 있습니다. 디버그 로그에서는 부트스트랩, 애플리케이션 컨피그레이션, 런타임, 구축, 모니터링, 보고 및 PKI(Public Key Infrastructure) 정보를 캡처합니다.

참고

- 노드별 로그 레벨은 디버그 마법사 프로파일보다 우선합니다.
- 동일한 구성 요소를 편집하는 여러 프로파일을 활성화할 때는 추적의 우선 순위가 가장 높은 경우에 로그 레벨이 높을수록 우선 순위가 높습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Profile Configuration(**디버그 프로파일 컨피그레이션**)**에서 디버그 프로파일을 구성할 수 있습니다.

단계 **2** 새 프로파일을 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 프로파일의 **Name(**이름**)**과 **Description(**설명**)**을 입력합니다.
프로파일에 포함할 구성 요소 옆의 확인란을 선택하고 각 구성 요소에 대해 해당하는 **Log Level(**로그 레벨**)**을 설정합니다.

단계 **4** **Save(**저장**)**를 클릭하여 프로파일을 저장합니다.

단계 **5** ISE 노드를 즉시 활성화하려면 **Enable(**활성화**)**을 클릭합니다. 그렇지 않은 경우 **Do it Later(**나중에**)**를 클릭합니다.

단계 **6** **Enable(**활성화**)**을 클릭하는 경우, 프로파일을 활성화하려는 ISE 노드 옆의 확인란을 선택합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Profile Configuration(**디버그 프로파일 컨피그레이션**)**에서 디버그 로그를 구성할 수 있습니다.

단계 **9** 라디오 버튼을 클릭하여 노드를 선택합니다.

단계 **10** 라디오 버튼을 클릭하여 구성 요소를 선택하고 **Edit(**편집**)**를 클릭하여 구성 요소의 **Component Name(**구성 요소 이름**)**, **Log Level(**로그 레벨**)**, **Description(**설명**)** 및 **Log File Name(**로그 파일 이름**)**을 변경합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

디버그 로그 다운로드

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)** > **Appliance node list(**어플라이언스 노드 목록**)**.

단계 **3** Appliance node(어플라이언스 노드) 목록에서 디버그 로그를 다운로드할 노드를 클릭합니다.

단계 **4** **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

디버그 로그 유형 및 디버그 로그의 목록이 표시됩니다. 이 목록은 디버그 로그 컨피그레이션을 기반으로 합니다.

단계 **5** 다운로드하려는 로그 파일을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에 저장합니다.

필요에 따라 이 프로세스를 반복하여 다른 로그 파일을 다운로드할 수 있습니다. **Debug Logs(**디버그 로그**)** 창에서 다운로드할 수 있는 추가 디버그 로그는 다음과 같습니다.

- isebootstrap.log: 부트스트래핑 로그 메시지를 제공합니다.
- monit.log: Watchdog 메시지를 제공합니다.
- pki.log: 타사 암호화 라이브러리 로그를 제공합니다.

- iseLocalStore.log: 로컬 저장소 파일에 대한 로그를 제공합니다.
- ad_agent.log: Microsoft Active Directory 타사 라이브러리 로그를 제공합니다.
- catalina.log: 타사 로그를 제공합니다.