유지 관리 및 모니터링

적응형 네트워크 제어

ANC(Adaptive Network Control)는 관리 노드에서 실행되는 서비스입니다. 이 서비스는 엔드포인트의 네트워크 액세스를 모니터링하고 제어합니다. ANC는 ISE 관리자가 관리자 GUI에서 호출하며 타사 시스템에서 pxGrid를 통해 호출할 수도 있습니다. ANC는 유선 및 무선 구축을 지원하며, 이를 위해서는 Premier 라이선스가 필요합니다.

ANC를 사용하여 시스템의 전체 권한 부여 정책을 수정하지 않고도 권한 부여 상태를 변경할 수 있습니다. ANC에서는 엔드포인트를 격리할 때 권한 부여 상태를 설정할 수 있습니다. 따라서 ANCPolicy를 확인하도록 정의된 권한 부여 정책은 네트워크 액세스를 제한하거나 거부할 수 있습니다. 전체 네트워크 액세스가 가능하도록 엔드포인트를 격리 해제할 수 있습니다. 네트워크에서 엔드포인트 연결이 끊어진 NAS(Network Attached System)의 포트를 종료할 수도 있습니다.

한 번에 격리할 수 있는 사용자 수에는 제한이 없습니다. 또한 격리 기간 길이에도 시간 제약 조건이 없습니다.

ANC를 통해 네트워크 액세스를 모니터링하고 제어하려면 다음 작업을 수행하십시오.

- 격리: 예외 정책(권한 부여 정책)을 사용하여 네트워크에 대한 엔드포인트 액세스를 제한하거나 거부할 수 있습니다. ANCPolicy에 따라 다른 권한 부여 프로파일(권한)을 할당하려면 예외 정책을 생성해야 합니다. 격리 상태로 설정하면 근본적으로 엔드포인트가 기본 VLAN에서 지정된 격리 VLAN으로 이동합니다. 엔드포인트와 동일한 NAS에서 지원되는 격리 VLAN을 먼저 정의해야 합니다.
- 격리 해제: 엔드포인트의 네트워크에 대한 전체 액세스를 허용하는 격리 상태를 되돌릴 수 있습니다. 이는 엔드포인트를 원래 VLAN으로 되돌리면 발생합니다.
- 종료: NAS의 포트를 비활성화하고 네트워크에서 엔드포인트 연결을 끊을 수 있습니다. 엔드포인트가 연결된 NAS에서 포트가 종료되면 NAS에서 포트를 다시 수동으로 재설정합니다. 이렇게 하면 엔드포인트를 네트워크에 연결할 수 있으며, 이는 무선 구축에 사용할 수 없습니다.

격리 및 격리 해제 작업은 활성 엔드포인트의 세션 디렉토리 보고서에서 트리거될 수 있습니다.

참고 격리된 세션이 격리 해제된 경우 새로 격리 해제된 세션의 시작 방법은 스위치 컨피그레이션에 지정된 인증 방법에 따라 달라집니다.

참고 Cisco ISE 1.4부터 ANC가 EPS(Endpoint Protection Services)를 대체합니다. ANC는 추가 분류 및 성능 개선을 제공합니다. 때때로 일부 ANC 작업에서 ERS 속성을 사용하는 것이 가능할 수도 있지만, ANC 속성을 사용하는 것이 좋습니다.

Cisco ISE에서 적응형 네트워크 제어 활성화

ANC는 기본적으로 비활성화되어 있습니다. ANC는 PxGrid가 활성화된 경우에만 활성화되며, 관리 포털에서 서비스를 수동으로 비활성화할 때까지 활성화된 상태로 유지됩니다.

네트워크 액세스 설정 구성

ANC를 사용하면 엔드포인트의 네트워크 액세스 상태를 격리, 격리 해제 또는 포트 종료로 재설정할 수 있습니다. 이는 네트워크의 엔드 포인트에 대한 권한 부여 정도를 정의합니다.

엔드포인트 IP 주소 또는 MAC 주소를 사용하여 엔드포인트가 연결되어 있는 NAS(Network Access Server) 포트를 종료하거나 엔드포인트를 격리 또는 격리 해제할 수 있습니다. 격리 및 격리 해제 작업은 동시에 수행하지 않는 경우 같은 엔드포인트에 대해 여러 번 수행할 수 있습니다. 네트워크에서 악의적인 엔드포인트가 검색되면 ANC를 사용해 NAS 포트를 닫는 방법으로 엔드포인트 액세스를 종료할 수 있습니다.

ANC 정책을 엔드포인트에 할당하려면 다음을 수행합니다.

시작하기 전에

- ANC를 활성화합니다.
- ANC용 권한 부여 프로파일 및 예외 유형 권한 권한 부여 정책을 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Adaptive Network Control(**적응형 네트워크 제어**)** > **Policy List(**정책 목록**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** ANC 정책의 이름을 입력하고 EPS 작업을 지정합니다. 다음 옵션을 사용할 수 있습니다.

- 격리
- Shut_Down
- Port_Bounce

작업은 하나 또는 여러 개 선택할 수 있지만 Shut_Down 및 Port_Bounce는 다른 ANC 작업과 결합할 수 없습니다.

단계 **4** **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택하고 정책 집합을 확장합니다.

단계 **5** ANCPolicy 속성을 사용하여 ANC 정책을 해당하는 권한 부여 정책과 연결합니다.

단계 **6** **Operations(**작업**) > Adaptive Network Control(**적응형 네트워크 제어**) > Endpoint Assignment(**엔드포인트 할당**)**를 선택합니다.

단계 **7** **Add(**추가**)**를 클릭합니다.

단계 **8** 엔드포인트의 IP 주소 또는 MAC 주소를 입력하고 **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 정책을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ANC를 통해 네트워크 액세스에 대한 권한 부여 프로파일 생성

ANC에서 사용할 권한 부여 프로파일을 생성하십시오. 이렇게 하면 Standard Authorization Profiles(표준 권한 부여 프로파일) 목록에 해당 권한 부여 프로파일이 표시됩니다. 네트워크에서 엔드포인트를 인증하고 권한을 부여할 수 있지만, 해당 엔드포인트는 네트워크에만 액세스하도록 제한됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 권한 부여 프로파일의 고유한 이름과 설명을 입력하고 **Access Type(**액세스 유형**)**은 **ACCESS_ACCEPT**로 업데이트합니다.

단계 **4** **DACL Name(DACL** 이름**)** 확인란을 선택하고 드롭다운 목록에서 **DENY_ALL_TRAFFIC**을 선택합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

예외 권한 부여 정책은 특수한 조건이나 권한 또는 즉각적인 요건에 대한 제한적 액세스 권한을 부여하는 데 사용됩니다. ANC 권한 부여의 경우에는 모든 표준 권한 부여 정책보다 먼저 처리되는 격리 예외 정책을 생성해야 합니다. 다음 조건을 사용하여 예외 규칙을 생성하십시오.

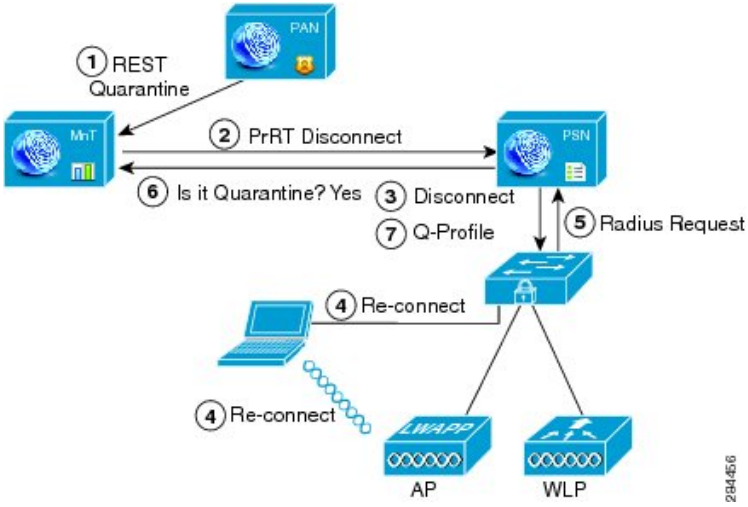
Session:ANCPolicy EQUALS Quarantine

ANC 격리 및 격리 해제 흐름

ANC를 사용하여 선택한 엔드포인트를 격리해 네트워크에 대한 액세스를 제한할 수 있습니다. 엔드포인트를 격리하고 상태에 따라 다른 권한 부여 프로파일을 할당하는 예외 권한 부여 정책을 설정할 수 있습니다. 권한 부여 프로파일은 지정된 네트워크 서비스에 대한 액세스를 허용하는 권한 부여 정책에 정의하는 권한의 컨테이너 역할을 합니다. 권한 부여가 완료되면 네트워크 액세스 요청에 대한 권한이 부여됩니다. 그런 다음 엔드포인트가 검증되면 네트워크에 대한 전체 액세스를 허용하도록 엔드포인트를 격리 해제할 수 있습니다.

이 그림에 나타난 격리 플로우에서는 권한 부여 규칙이 구성되었으며 ANC 세션이 설정된 것으로 가정합니다.

그림 ***1: ANC*** 격리 플로우



1. 클라이언트 디바이스가 무선 디바이스(WLC)를 통해 네트워크에 로그인하고, 관리 노드(PAP)에서 모니터링 노드(MnT)로 격리 REST API 호출이 실행됩니다.
2. 그런 다음 모니터링 노드는 정책 서비스 Cisco ISE 노드(PDP)를 통해 PrRT를 호출하여 CoA(Certificate of Authorization)를 불러옵니다.
3. 클라이언트 디바이스 연결이 끊어집니다.
4. 클라이언트 디바이스가 다시 인증되고 재연결됩니다.
5. 클라이언트 디바이스에 대한 RADIUS 요청이 모니터링 노드로 다시 보내집니다.
6. 확인이 진행되는 동안 클라이언트 디바이스가 격리됩니다.
7. Q-Profile 권한 부여 정책이 적용되고 클라이언트 디바이스가 검증됩니다.
8. 클라이언트 디바이스가 격리 해제되고 네트워크에 대한 전체 액세스가 제공됩니다.

ANC NAS 포트 종료 흐름

엔드포인트 IP 주소 또는 MAC 주소를 사용하여 엔드포인트가 연결되어 있는 NAS 포트를 종료할 수 있습니다.

종료하면 MAC 주소에 대해 지정된 IP 주소를 기반으로 NAS 포트를 닫을 수 있습니다. 엔드포인트를 네트워크에 다시 연결하려면 포트를 수동으로 복구해야 합니다. 이러한 복구는 유선 미디어를 통해 연결된 엔드포인트에만 적용됩니다.

일부 디바이스에서는 종료가 지원되지 않을 수도 있습니다. 그러나 대부분의 스위치는 종료 명령을 지원합니다. getResult() 명령을 사용하여 종료가 정상적으로 실행되는지를 확인할 수 있습니다.

아래 그림에는 ANC 종료 흐름이 나와 있습니다. 클라이언트 디바이스에서는 이 디바이스가 네트워크에 액세스하는 데 사용하는 NAS에서 종료 작업이 수행됩니다.

그림 ***2: ANC*** 종료 흐름

엔드포인트 제거 설정

ID 그룹 및 기타 조건을 기준으로 규칙을 구성하여 엔드포인트 제거 정책을 정의할 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Purge(**엔드포인트 제거**)**를 선택합니다. 지정된 엔드포인트를 제거하지 않고 선택한 프로파일링 조건을 기준으로 하여 엔드포인트를 제거할 수 있습니다.

엔드포인트 제거 작업을 예약할 수 있습니다. 이 엔드포인트 제거 예약은 기본적으로 활성화되어 있습니다. Cisco ISE는 기본적으로 30일 초과하는 엔드포인트 및 등록된 디바이스를 삭제합니다. 제거 작업은 기본 PAN에서 구성한 표준 시간대를 기준으로 매일 오전 1시(자정)에 실행됩니다.

엔드포인트 제거는 3분마다 5천개가 넘는 엔드포인트를 삭제합니다.

아래에는 엔드포인트를 비우기하는 데 사용할 수 있는 몇 가지 조건이 예제와 함께 나와 있습니다.

- InactivityDays - 엔드포인트에 대한 마지막 프로파일링 활동 또는 업데이트 이후로 경과한 일 수입니다.
  - 이 조건 시간이 흐르면서 누적된 오래된 디바이스를 제거합니다. 여기에는 대게 일반적으로 임시 게스트 또는 개인 디바이스 또는 사용 중단된 디바이스가 포함됩니다. 이러한 엔드포인트는 더 이상 활성화되지 않거나 가까운 미래에 표시되지 않을 가능성이 높아 구축에서 문제가 발생할 소지가 있습니다. 혹시라도 다시 연결되는 경우 필요에 따라 재검색되거나 프로파일링되거나 등록됩니다.
  - 엔드포인트에서 업데이트가 있을 때는 프로파일링이 활성화된 경우에만 InactivityDays가 0으로 재설정됩니다.
- ElapsedDays - 객체가 생성된 이후로 경과한 일 수입니다.
  - 이 조건은 게스트 또는 계약자 엔드포인트 또는 네트워크 액세스에 WebAuth를 사용하는 직원과 같이 지정된 기간 동안 인증되지 않은 또는 조건부 액세스가 부여된 엔드포인트에 사용될 수 있습니다. 허용되는 연결 유예 기간이 지난 후에는 완전히 다시 인증되고 등록되어야 합니다.
- PurgeDate - 엔드포인트를 제거하는 날짜입니다.

- 이 옵션은 생성 시간 또는 시작 시간에 관계없이 특정 시간 동안 액세스가 부여된 특수 이벤트 또는 그룹에 사용할 수 있습니다. 이 경우 모든 엔드포인트를 동시에 제거할 수 있습니다. 예를 들어 무역 박람회, 컨퍼런스 또는 주간 교육 과정에서 각 주마다 새 멤버가 참여하는 경우 절대 일, 주, 월이 아니라 특정 주나 월에 액세스가 부여됩니다.

격리된 엔드포인트가 정책 변경 후 인증을 갱신하지 않음

문제

정책 변경 또는 ID 추가 후 인증이 실패하며 재인증이 수행되지 않습니다. 인증이 실패하거나 해당 엔드포인트가 네트워크에 계속 연결할 수 없습니다. 이 문제는 사용자 역할에 할당된 포스처 정책에 따라 포스처 평가를 수행할 수 없는 클라이언트 머신에서 발생하는 경우가 많습니다.

가능한 원인

클라이언트 머신의 인증 타이머 설정 또는 스위치의 인증 간격이 올바르게 설정되어 있지 않습니다.

해결책

이 문제를 해결할 수 있는 몇 가지 방법은 다음과 같습니다.

1. Cisco ISE의 세션 상태 요약 보고서에서 지정된 NAD 또는 스위치를 확인하여 인터페이스에 적절한 인증 간격이 구성되어 있는지 파악합니다.
2. NAD/스위치에서 "show running configuration"을 입력한 다음 인터페이스가 적절한 "authentication timer start" 설정으로 구성되어 있는지 확인합니다. "authentication timer restart 15" 및 "authentication timer reauthenticate 15" 등을 예로 들 수 있습니다.
3. Cisco ISE에서 수행되었을 수 있는 컨피그레이션 변경 이후 "interface shutdown" 및 "no shutdown"을 입력하여 NAD/스위치에서 포트를 반송하고 재인증을 강제로 수행해 봅니다.

참고 CoA에는 MAC 주소 또는 세션 ID가 필요하므로 네트워크 디바이스 SNMP 보고서에 표시되어 있는 포트는 반송하지 않는 것이 좋습니다.

IP 주소 또는 MAC 주소를 찾을 수 없으면 ANC 작업이 실패함

엔드포인트에 대한 활성 세션에 IP 주소 관련 정보가 포함되어 있지 않으면 엔드포인트에서 수행하는 ANC 작업이 실패합니다. 해당 엔드포인트의 MAC 주소 및 세션 ID에도 이 규칙이 적용됩니다.

참고 ANC를 통해 엔드포인트의 권한 부여 상태를 변경하려는 경우에는 해당 엔드포인트의 IP 주소 또는 MAC 주소를 제공해야 합니다. IP 주소 또는 MAC 주소를 엔드포인트에 대한 활성 세션에서 찾을 수 없는 경우 다음과 같은 오류 메시지가 표시됩니다.

No active session found for this MAC address, IP Address or Session ID(□ MAC □□, IP □□ □□ □□ ID□ □□ □□ □ □□ □□ □ □□□□).

.

외부에서 인증된 관리자가 **ANC** 작업을 수행할 수 없음

외부에서 인증된 관리자가 라이브 세션에서 CoA-격리를 실행하려고 하면 Cisco ISE에서 다음 오류 메시지가 반환됩니다.

xx:xx:xx:xx:xx:xx□ □□ CoA □□ □□□ □□□ □ □□□□. □□: □□□□ □□□□ □□ □ □□□□. □□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□□.

외부에서 인증된 관리자가 ANC 작업을 Cisco ISE의 **Operations(**작업**)**에서 엔드포인트의 IP 주소 또는 MAC 주소를 사용하여 수행하는 경우 Cisco ISE에서는 다음 오류 메시지가 반환됩니다.

□□ □□: □□□□ □□□□ □□ □ □□□□. □□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□□.

백업 데이터 유형

Cisco ISE에서는 기본 PAN 또는 모니터링 노드의 데이터를 백업할 수 있습니다. 백업은 CLI 또는 사용자 인터페이스에서 수행할 수 있습니다.

Cisco ISE에서는 다음 데이터 유형을 백업할 수 있습니다.

- 컨피그레이션 데이터 - 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. 백업은 GUI 또는 CLI를 사용하여 기본 PAN을 통해 수행할 수 있습니다.
- 작업 데이터 - 모니터링 및 문제 해결 데이터를 포함합니다. 백업은 기본 PAN GUI를 통해 또는 모니터링 노드용 CLI를 사용하여 수행할 수 있습니다.

Cisco ISE가 VMware에서 실행될 때는 ISE 데이터 백업용으로 VMware 스냅샷이 지원되지 않습니다.

참고 VMware 스냅샷은 지정된 시점에 VM의 상태를 저장하므로, Cisco ISE는 VMware 스냅샷으로 ISE 데이터를 백업하는 기능은 지원하지 않습니다. 멀티 노드 Cisco ISE 구축에서는 모든 노드의 데이터가 현재 데이터베이스 정보와 지속적으로 동기화됩니다. 스냅샷을 복원하면 데이터베이스 복제 및 동기화 문제가 발생할 수 있습니다. 데이터 보관 및 복구를 위해 Cisco ISE에 포함된 백업 기능을 사용하는 것이 좋습니다.

VMware 스냅샷 또는 서드파티 백업 서비스를 사용하여 Cisco ISE 데이터를 백업하면 Cisco ISE 서비스가 중단될 수 있습니다. VMware 또는 CommVault SAN 레벨 백업과 같은 기타 서드파티 백업 서비스에서 백업을 시작하면 충돌이 일관되게 유지되도록 파일 시스템이 정지되어 Cisco ISE 기능이 정지될 수 있습니다. Cisco ISE 구축에서 서비스를 다시 시작하려면 재부팅해야 합니다.

복원 작업은 이전 Cisco ISE 버전의 백업 파일을 사용하여 수행하고 이후 버전에서 복원할 수 있습니다. 예를 들어 Cisco ISE, 릴리스 1.3 또는 1.4의 ISE 노드 백업이 있는 경우 Cisco ISE, 릴리스 2.1에서 복원할 수 있습니다.

Cisco ISE, 릴리스 3.0은 릴리스 2.4 이상에서 가져온 백업을 복원하도록 지원합니다.

저장소 백업 및 복구

Cisco ISE에서는 관리 포털을 통해 저장소를 생성하거나 삭제할 수 있습니다. 다음과 같은 저장소 유형을 생성할 수 있습니다.

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

참고 저장소는 각 디바이스에 대해 로컬입니다.

모든 구축 유형(소규모, 중간 규모, 대규모)에 대해 저장소 크기를 최소 100GB로 설정하는 것이 좋습니다.

다음 표에는 Cisco ISE 작업과 외부 저장소 유형 간의 지원 가능성 정보가 나와 있습니다.

표 *1:* 외부 저장소에 대한 지원 가능성 매트릭스

Repository Type(저장소 유형**)**	컨피그레이션 백업	컨피그레이션 복원	업그레이드	운영 백업	운영 복원	지원 번들	사용자 인터페이스의 검증	사용자 인터페이스에서 보고서 내보내기	사용자 인터페이스에서 정책 내보내기
FTP	√	√	√	√	√	√	√	√	√
SFTP	√	√	√	√	√	√	√	√	√
TFTP	√	√	√	√	√	√	X	√	√
HTTP	X	X	√	X	X	X	X	X	X
HTTPS	X	*X*	√	X	X	X	X	X	X
NFS	√	√	√	√	√	√	√	√	√

저장소 생성

CLI 및 GUI를 사용하여 저장소를 생성할 수 있습니다. 다음과 같은 이유로 인해 GUI를 사용하는 것이 좋습니다.

- CLI를 통해 생성하는 저장소는 로컬에 저장되며 다른 구축 노드로 복제되지 않습니다. 이러한 저장소는 GUI의 저장소 페이지에 나열되지 않습니다.
- 기본 PAN에서 생성하는 저장소는 다른 구축 노드로 복제됩니다.

키는 GUI의 기본 PAN에서만 생성되므로 업그레이드 중에 새 기본 관리자의 GUI에서 키를 다시 생성하고 SFTP 서버로 내보내야 합니다. 구축 환경에서 노드를 제거하는 경우 비관리 노드의 GUI에서 키를 생성하고 SFTP 서버로 내보내야 합니다.

RSA 공개 키 인증을 사용하여 Cisco ISE에서 SFTP 저장소를 구성할 수 있습니다. 관리자가 생성한 비밀번호를 사용하여 데이터베이스 및 로그를 암호화하는 대신 보안 키를 사용하는 RSA 공개 키 인증을 선택할 수 있습니다. RSA 공개 키로 생성된 SFTP 저장소의 경우 GUI를 통해 생성된 저장소는 CLI에서 복제되지 않으며 CLI를 통해 생성된 저장소는 GUI에서 복제되지 않습니다. CLI 및 GUI에서 동일한 저장소를 구성하려면 CLI 및 GUI 모두에서 RSA 공개 키를 생성하고 두 키를 모두 SFTP 서버로 내보냅니다.

참고 Cisco ISE는 FIPS 모드가 ISE에서 활성화되지 않은 경우에도 FIPS 모드에서 아웃바운드 SSH 또는 SFTP 연결을 시작합니다. ISE와 통신하는 원격 SSH 또는 SFTP 서버가 FIPS 140-2 승인 암호화 알고리즘을 허용하는지 확인합니다.

Cisco ISE는 임베디드 FIPS 140-2 검증 암호화 모듈을 사용합니다. FIPS 규정 준수 클레임에 대한 자세한 내용은 FIPS 규정 준수 편지를 참고해 주십시오.

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- RSA 공개 키 인증을 사용하여 SFTP 저장소를 생성하려면 다음 단계를 수행합니다.
  - SFTP 저장소에서 RSA 공개 키 인증을 활성화합니다.
  - **crypto host_key add** 명령을 사용하여 Cisco ISE CLI에서 SFTP 서버의 호스트 키를 입력합니다. 호스트 키 문자열은 저장소 구성 페이지의 **Path(**경로**)** 필드에 입력하는 호스트 이름과 일치해야 합니다.
  - 키 페어를 생성하고 GUI에서 공개 키를 로컬 시스템으로 내보냅니다. Cisco ISE CLI에서 **crypto key generate rsa passphrase** *test123* 명령을 사용하여 키 페어를 생성합니다. 여기서 passphrase는 4자보다 커야 하며 모든 저장소(로컬 디스크 또는 기타 구성된 저장소)로 내보내야 합니다.
  - 내보낸 RSA 공개 키를 PKI 지원 SFTP 서버에 복사하고 "authorized_keys" 파일에 추가합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**.

단계 **3** 새 저장소를 추가하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 새 저장소를 설정하는 데 필요한 값을 입력합니다. 필드에 대한 설명은 저장소 설정, 12 페이지를 참고하십시오.

단계 **5** 저장소를 생성하려면 **Submit(**제출**)**을 클릭합니다.

단계 **6** 왼쪽의 **Operations(**운영**)** 탐색창에서 **Repository(**저장소**)**를 클릭하거나 **Repository(**저장소**)** 창 위쪽의 **Repository List(**저장소 목록**)** 링크를 클릭해 저장소 목록 페이지로 이동하여 저장소가 정상적으로 생성되었는지 확인합니다.

다음에 수행할 작업

- 생성한 저장소가 유효한지 확인합니다. **Repository Listing(**저장소 목록**)** 창에서 확인할 수 있습니다. 해당 저장소를 선택하고 **Validate(**검증**)**를 클릭합니다. 또는 Cisco ISE 명령줄 인터페이스에서 다음 명령을 실행할 수 있습니다.

  show repository *repository-name*

여기서 *repository_name*은 생성한 저장소의 이름입니다.

참고 저장소를 생성할 때 입력한 경로가 없으면 다음 오류가 표시됩니다.

```
%Invalid Directory
```

- 온디맨드 백업을 실행하거나 백업을 예약합니다.

저장소 설정

다음 표에서는 백업 파일을 저장하기 위한 저장소를 생성하는 데 사용할 수 있는 **Repository List(**저장소 목록**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)** 입니다.

표 ***2:*** 저장소 설정

필드	사용 지침
Repository(저장소**)**	저장소의 이름을 입력합니다. 영숫자 문자를 입력할 수 있으며 최대 길이는 80자입니다.
Protocol(프로토콜**)**	사용 가능한 프로토콜 중에서 사용하려는 프로토콜 하나를 선택합니다.
Server Name(서버 이름**)**	(TFTP, HTTP, HTTPS, FTP, SFTP 및 NFS의 경우 필수) 저장소를 생성할 서버의 호스트 이름 또는 IPv4 주소(IPv4 또는 IPv6)를 입력합니다. 참고 IPv6 주소를 사용해 저장소를 추가하는 경우 ISE eth0 인터페이스가 IPv6 주소로 구성되어야 합니다.
경로	저장소의 경로를 입력합니다. 경로는 유효해야 하며 저장소를 생성할 때 이미 있는 상태여야 합니다. 이 값은 서버의 루트 디렉토리를 나타내는 슬래시 두 개(//) 또는 하나(/)로 시작할 수 있습니다. 그러나 FTP 프로토콜의 경우 슬래시 하나(/)는 루트 디렉토리가 아닌 로컬 디바이스 홈 디렉토리의 FTP를 나타냅니다.
PKI 인증 활성화	(선택 사항, SFTP 저장소에만 적용 가능) SFTP 저장소에서 RSA 공개 키 인증을 활성화하려면 이 확인란을 선택합니다.

필드	사용 지침
사용자 이름	(FTP, SFTP 의 경우 필수) 지정한 서버에 대한 쓰기 권한이 있는 사용자 이름을 입력합니다. 영숫자 문자만 입력할 수 있습니다.
Password(비밀번호**)**	(FTP, SFTP 의 경우 필수) 지정한 서버에 액세스하는 데 사용할 비밀번호를 입력합니다. 비밀번호는 0~9, a~z, A~Z, -, ., |, @, #,$, ^, &, *, (,), +, = 문자를 포함할 수 있습니다.

관련 항목

저장소 백업 및 복구, 9 페이지
저장소 생성, 10 페이지

SFTP 저장소에서 RSA 공개 키 인증 활성화

SFTP 서버에서 각 노드에는 CLI와 GUI용으로 하나씩, 2개의 RSA 공개 키가 있어야 합니다. SFTP 저장소에서 RSA 공개 키 인증을 활성화하려면 다음 단계를 수행합니다.

단계 **1** */etc/ssh/sshd_config.file*을 편집할 권한이 있는 계정으로 SFTP 서버에 로그인합니다.

참고 *sshd_config* 파일의 위치는 운영체제 설치에 따라 달라질 수 있습니다.

단계 **2** **vi /etc/ssh/sshd_config** 명령을 입력합니다.

sshd_config 파일의 내용이 나열됩니다.

단계 **3** RSA 공개 키 인증을 활성화하려면 다음 줄에서 "#" 기호를 제거합니다.

- RSAAuthentication: yes(예)
- PubkeyAuthentication: yes(예)

  참고 공개 인증 키가 no인 경우 yes로 변경합니다.

- AuthorizedKeysFile ~/.ssh/authorized_keys

온디맨드 및 예약된 백업

기본 PAN 및 기본 모니터링 노드에 대한 온디맨드 백업을 구성할 수 있습니다. 데이터를 즉시 백업하려면 온디맨드 백업을 수행합니다.

Cisco ISE에서는 한 번, 매일, 매주, 매월 실행되도록 예약할 수 있는 시스템 레벨 백업을 예약할 수 있습니다. 백업 작업에는 시간이 오래 걸릴 수 있으므로 중단되지 않도록 백업을 예약할 수 있습니다. 관리 포털에서 백업을 예약할 수 있습니다.

참고 내부 CA를 사용하는 경우 CLI를 사용하여 인증서 및 키를 내보내야 합니다. 관리 포털에서 수행하는 백업은 CA 체인을 백업하지 않습니다.

자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드의 "기본 설정" 장에서 "Cisco ISE CA 인증서 및 키 내보내기" 섹션을 참고하십시오.

관련 항목

유지 관리 설정

온디맨드 백업 수행

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복구 기능이 내부 CA(Certificate Authority) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복구하는 경우 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE 노드에서 CA 인증서를 내보내고 대상 시스템에 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발급한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  장점**:** 원래 소스 인증서 또는 원래 대상 인증서가 모두 사용되지 않아 안전하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발급된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 온디맨드 백업을 수행하기 전에 Cisco ISE의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 백업 파일을 저장할 저장소를 생성했는지 확인합니다.
- 로컬 저장소를 사용하여 백업해서는 안 됩니다. 원격 모니터링 노드의 로컬 저장소에는 모니터링 데이터를 백업할 수 없습니다.
- 백업을 가져오기 전에 모든 인증서 관련 변경을 수행해야 합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

참고 CD-ROM, HTTP, HTTPS 또는 TFTP 저장소 유형은 백업 및 복구 작업에서 지원되지 않습니다. 이러한 저장소 유형은 읽기 전용이거나 프로토콜이 파일 나열을 지원하지 않기 때문입니다. 백업을 복원하려면 저장소를 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 백업 유형을 Configuration(구성) 또는 Operational(운영) 중에서 선택합니다.

단계 **4** **Backup Now(**지금 백업**)**를 클릭합니다.

단계 **5** 필요한 값을 입력하여 백업을 수행합니다.

단계 **6** **Backup(**백업**)**을 클릭합니다.

단계 **7** 백업이 정상적으로 완료되었는지 확인합니다.

Cisco ISE는 백업 파일 이름에 타임스탬프를 추가하여 파일을 지정된 저장소에 저장합니다. Cisco ISE는 타임스탬프 외에 CFG 태그(구성 백업의 경우) 및 OPS 태그(운영 백업의 경우)도 추가합니다. 백업 파일이 지정된 저장소에 있는지 확인합니다.

분산형 구축에서는 백업을 실행할 때 노드를 승격하거나 노드의 역할을 변경하지 마십시오. 노드 역할을 변경해도 모든 프로세스가 종료되는 것은 아니며 백업을 동시에 실행하는 경우 데이터가 다소 불일치할 수도 있습니다. 백업이 완료될 때까지 기다린 후에 노드 역할을 변경해 주십시오.

백업이 실행 중일 때는 노드를 승격하지 마십시오. 이렇게 하면 모든 프로세스가 종료되며 백업을 동시에 실행하는 경우 데이터가 다소 불일치할 수도 있습니다. 백업이 완료될 때까지 기다린 후에 노드를 변경해 주십시오.

참고 백업이 실행 중일 때 높은 CPU 사용률이 관찰되고 높은 로드 평균 경보가 표시될 수 있습니다. 백업이 완료되면 CPU 사용률이 정상으로 돌아옵니다.

관련 항목

Cisco ISE 복원 작업, 20 페이지

인증 및 권한 부여 정책 컨피그레이션 내보내기, 26 페이지

온디맨드 백업 설정

다음 표에서는 임의의 시점에 백업을 가져오는 데 사용할 수 있는 **On-Demand Backup(**온디맨드 백업**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup & Restore(**백업 및 복구**)**입니다.

표 *3:* 온디맨드 백업 설정

필드 이름	사용 지침
Type(유형**)**	다음 중 하나를 선택합니다. • **Configuration Data Backup(**컨피그레이션 데이터 백업**)**: 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. • **Operational Data Backup(**운영 데이터 백업**)**: 모니터링 및 문제 해결 데이터를 포함합니다.
Backup Name(백업 이름**)**	백업 파일의 이름을 입력합니다.
Repository Name(저장소 이름**)**	백업 파일을 저장할 저장소입니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 백업을 실행하기 전에 저장소를 생성해야 합니다.
Encryption Key(암호화 키**)**	이 키는 백업 파일을 암호를 해독하는 데 사용됩니다.

관련 항목

백업 데이터 유형, 8 페이지
온디맨드 및 예약된 백업, 13 페이지
백업 기록, 19 페이지
백업 실패, 19 페이지
Cisco ISE 복원 작업, 20 페이지
인증 및 권한 부여 정책 컨피그레이션 내보내기, 26 페이지
분산형 환경에서 기본 및 보조 노드 동기화, 28 페이지
온디맨드 백업 수행, 14 페이지

백업 예약

온디맨드 백업을 수행하여 컨피그레이션 또는 모니터링(운영) 데이터를 즉시 백업할 수 있습니다. 복구 작업에서는 백업을 가져오는 시간의 컨피그레이션 상태로 Cisco ISE를 복원합니다.

중요 백업 및 복구를 수행 중인 경우, 복구는 대상 시스템의 신뢰할 수 있는 인증서 목록을 소스 시스템의 인증서 목록으로 덮어씁니다. 백업 및 복구 기능이 내부 CA(Certificate Authority) 인증서와 연계된 개인 키를 포함하지 않는다는 점이 매우 중요합니다.

한 시스템에서 다른 시스템으로 백업 및 복구하는 경우, 오류를 방지하려면 다음 옵션 중 하나를 선택해야 합니다.

- 옵션 **1:**

  CLI를 통해 소스 ISE 노드에서 CA 인증서를 내보내고 대상 시스템에 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발급한 모든 인증서는 계속해서 신뢰됩니다. 대상 시스템에서 발행된 모든 신규 인증서는 동일한 키를 사용하여 서명됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

- 옵션 **2:**

  복원 프로세스 이후에 내부 CA용으로 모든 신규 인증서를 생성합니다.

  장점**:** 원래 소스 인증서 또는 원래 대상 인증서가 사용되므로 안전하기 때문에 권장되는 옵션입니다. 원래 소스 시스템에서 발행된 인증서는 계속해서 신뢰됩니다.

  단점**:** 복구 기능을 사용하기 전에 대상 시스템에서 발급된 모든 인증서는 신뢰되지 않으며 재발급해야 합니다.

시작하기 전에

- 백업을 예약하기 전에 Cisco ISE의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 저장소를 구성했는지 확인합니다.
- 로컬 저장소를 사용하여 백업해서는 안 됩니다. 원격 모니터링 노드의 로컬 저장소에는 모니터링 데이터를 백업할 수 없습니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- Cisco ISE 1.1 이하 릴리스에서 Cisco ISE 1.2로 업그레이드한 경우에는 예약 백업을 재구성해야 합니다. *Cisco Identity Services Engine* 업그레이드 설명서 릴리스 *1.2*의 알려진 업그레이드 문제 섹션을 참고해 주십시오.

참고 CD-ROM, HTTP, HTTPS 또는 TFTP 저장소 유형은 백업 및 복구 작업에서 지원되지 않습니다. 이러한 저장소 유형은 읽기 전용이거나 프로토콜이 파일 나열을 지원하지 않기 때문입니다.

예약 백업 설정

다음 표에서는 전체 또는 증분 백업을 복구하는 데 사용할 수 있는 Scheduled Backup(예약 백업) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**입니다.

표 *4:* 예약 백업 설정

필드 이름	사용 지침
Type(유형**)**	다음 중 하나를 선택합니다. • **Configuration Data Backup(**컨피그레이션 데이터 백업**)**: 애플리케이션별 데이터와 Cisco ADE 운영체제 컨피그레이션 데이터를 모두 포함합니다. • **Operational Data Backup(**운영 데이터 백업**)**: 모니터링 및 문제 해결 데이터를 포함합니다.
Name(이름**)**	백업 파일의 이름을 입력합니다. 선택에 대한 설명이 포함된 이름을 입력할 수 있습니다. Cisco ISE는 백업 파일명에 타임스탬프를 추가하여 해당 파일을 저장소에 저장합니다. 일련의 백업을 구성하더라도 고유한 백업 파일명을 갖게 됩니다. Scheduled Backup(예약 백업) 목록 창에서 백업 파일명이 "backup_occur"로 추가되어 **kron** 수행 작업 파일임을 나타냅니다.
Description(설명**)**	백업의 설명을 입력합니다.
Repository Name(저장소 이름**)**	백업 파일이 저장되는 저장소를 선택합니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 백업을 실행하기 전에 저장소를 생성해야 합니다.
Encryption Key(암호화 키**)**	백업 파일을 암호화하고 암호를 해독하는 데 사용할 키를 입력합니다.
Schedule Options(예약 옵션**)**	예약 백업의 빈도를 선택하고 그에 따라 기타 옵션을 입력합니다.

관련 항목

백업 데이터 유형, 8 페이지
온디맨드 및 예약된 백업, 13 페이지
백업 기록, 19 페이지
백업 실패, 19 페이지
Cisco ISE 복원 작업, 20 페이지
인증 및 권한 부여 정책 컨피그레이션 내보내기, 26 페이지
분산형 환경에서 기본 및 보조 노드 동기화, 28 페이지
CLI를 사용한 복원, 19 페이지
백업 예약, 17 페이지

CLI를 사용한 복원

CLI와 GUI 둘 다에서 백업을 예약할 수 있지만 GUI를 사용하는 것이 좋습니다. 그러나 보조 모니터링 노드에 대한 운영 백업을 수행하려는 경우 CLI에서만 가능합니다.

백업 기록

백업 기록에서는 예약 백업 및 온디맨드 백업에 대한 기본 정보를 제공합니다. 백업 이름, 백업 파일 크기, 백업이 저장된 저장소 및 백업을 가져온 시점을 나타내는 타임스탬프가 나열됩니다. 이 정보는 운영 감사 보고서와 함께 Backup and Restore(백업 및 복구) 페이지의 History(기록) 표에서 사용할 수 있습니다.

실패한 백업의 경우 Cisco ISE가 경보를 트리거합니다. 백업 기록 페이지에 실패 이유가 제공됩니다. 실패 이유는 운영 감사 보고서에서도 확인할 수 있습니다. 실패 이유가 없거나 명확지 않은 경우 Cisco ISE CLI에서 **backup-logs** 명령을 실행하여 ADE.log에서 자세한 내용을 확인할 수 있습니다.

백업 작업이 진행 중인 경우 **show backup status** CLI 명령을 사용하여 백업 작업의 진행 상황을 확인할 수 있습니다.

백업 기록은 Cisco ADE 운영체제 컨피그레이션 데이터와 함께 저장됩니다. 이 기록은 애플리케이션이 업그레이드된 후에도 계속 해당 위치에 유지되며 PAN을 재이미지화하는 경우에만 제거됩니다.

백업 실패

백업이 실패하는 경우 다음 사항을 확인해 주십시오.

- NTP 동기화 또는 서비스 장애 문제가 있는지 확인합니다. Cisco ISE의 NTP 서비스가 작동하지 않으면 Cisco ISE에서 NTP 서비스 장애 경보를 생성합니다. Cisco ISE가 구성된 모든 NTP 서버와 동기화할 수 없는 경우 Cisco ISE에서 NTP 동기화 실패 경보를 생성합니다. NTP 서비스가 중지되었거나 동기화 문제가 있는 경우 Cisco ISE 백업이 실패할 수 있습니다. Alarms(경보) dashlet을 확인하고 NTP 동기화 또는 서비스 문제를 해결한 후에 백업 작업을 다시 시도하십시오.
- 다른 백업이 동시에 실행되고 있지 않은지 확인합니다.
- 구성한 저장소에 대해 사용 가능한 디스크 공간을 확인합니다.

- 모니터링 데이터가 할당된 모니터링 데이터베이스 크기의 75%를 사용한 경우 모니터링(운영) 백업이 실패합니다. 예를 들어 모니터링 노드에 600GB가 할당되어 있고 모니터링 데이터가 스토리지의 450GB 이상을 사용한 경우 모니터링 백업이 실패합니다.
- 데이터베이스 디스크 사용량이 90%를 초과하면 데이터베이스 크기를 할당된 크기의 75% 이하로 유지하기 위해 제거가 발생합니다.

- 제거가 진행 중인지 확인합니다. 제거가 진행 중일 때에는 백업 및 복구 작업이 수행되지 않습니다.
- 저장소가 올바르게 구성되었는지 확인합니다.

Cisco ISE 복원 작업

기본 또는 독립형 관리 노드에서 컨피그레이션 데이터를 복원할 수 있습니다. 기본 PAN에서 데이터를 복원한 후에는 보조 노드를 기본 PAN과 수동으로 동기화해야 합니다.

운영 데이터를 복원하는 프로세스는 구축 유형에 따라 다릅니다.

참고 Cisco ISE의 새 백업/복원 사용자 인터페이스에서는 백업 파일 이름에 메타데이터를 사용합니다. 그러므로 백업이 완료된 후에 백업 파일 이름을 수동으로 수정해서는 안 됩니다. 백업 파일 이름을 수동으로 수정할 경우 Cisco ISE 백업/복원 사용자 인터페이스에서 백업 파일을 인식할 수 없습니다. 백업 파일 이름을 수정해야 하는 경우 Cisco ISE CLI를 사용하여 백업을 복원해야 합니다.

데이터 복원 지침

다음은 Cisco ISE 백업 데이터를 복원할 때 따라야 하는 지침입니다.

- Cisco ISE를 사용하면 ISE 노드 (A)에서 백업을 가져와서 호스트네임이 동일한(IP 주소는 다름) 다른 ISE 노드 (B)에서 복구할 수 있습니다. 그러나 노드 B에서 백업을 복구한 후에는 인증서 및 포털 그룹 태그에 문제가 발생할 수 있으므로 노드 B의 호스트네임을 변경하지 마십시오.
- 특정 표준 시간대에서 기본 PAN의 백업을 가져온 다음 다른 표준 시간대에서 다른 Cisco ISE 노드에 해당 백업을 복원하려는 경우 복원 프로세스가 실패할 수 있습니다. 백업 파일의 타임스탬프가 백업을 복원하는 Cisco ISE 노드의 시스템 시간보다 이후이면 이러한 오류가 발생합니다. 백업을 가져오고 1일 후에 동일 백업을 복원하는 경우 백업 파일의 타임스탬프가 시스템 시간 이전에 되어 복원 프로세스가 정상적으로 진행됩니다.
- 백업을 가져온 호스트와 다른 호스트 이름으로 기본 PAN에서 백업을 복원하면 기본 PAN이 독립형 모드로 설정됩니다. 그러면 구축이 손상되고 보조 노드가 작동하지 않게 됩니다. 이 경우 독립형 모드를 기본 노드로 지정하고 보조 노드에서 컨피그레이션을 재설정한 후에 기본 노드에 보조 노드를 등록해야 합니다. Cisco ISE 노드에서 컨피그레이션을 재설정하려면 Cisco ISE CLI에서 다음 명령을 입력합니다.
  - **application reset-config ise**

- 초기 Cisco ISE 설치 및 설정 후에는 시스템 표준 시간대를 변경하지 않는 것이 좋습니다.
- 구축의 노드 하나 이상에서 인증서 컨피그레이션을 변경한 경우에는 다른 백업을 가져와 독립형 Cisco ISE 노드 또는 기본 PAN에서 데이터를 복원해야 합니다. 이렇게 하지 않는 경우 이전 백업을 사용하여 데이터를 복원하려고 하면 노드 간의 통신이 실패할 수 있습니다.
- 기본 PAN에서 컨피그레이션 백업을 복원한 후에는 이전에 내보낸 Cisco ISE CA 인증서 및 키를 가져올 수 있습니다.

참고 Cisco ISE CA 인증서 및 키를 내보내지 않은 경우 기본 PAN에서 컨피그레이션 백업을 복원한 후에 기본 PAN 및 PSN(Policy Service Nodes)에서 루트 CA 및 종속 CA를 생성합니다.

- 올바른 FQDN (플래티넘 데이터베이스의 FQDN)을 사용하지 않고 플래티넘 데이터베이스를 복원하려는 경우 CA 인증서를 다시 생성해야 합니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Signing Requests(**인증서 서명 요청**)** > **Replace ISE Root CA certificate chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 선택합니다. 그러나 올바른 FQDN을 사용하여 플래티넘 데이터베이스를 복원하는 경우 CA 인증서가 자동으로 다시 생성됩니다.
- Cisco ISE가 백업 파일을 저장하는 위치인 데이터 저장소가 필요합니다. 온디맨드 또는 예약 백업을 실행하려면 저장소를 생성해야 합니다.
- 독립형 관리 노드에 오류가 발생하는 경우에는 컨피그레이션 백업을 실행하여 해당 노드를 복원해야 합니다. 기본 PAN에 오류가 발생하는 경우에는 분산형 설정을 통해 보조 관리 노드를 기본 노드로 승격할 수 있습니다. 기본 PAN이 작동하면 기본 PAN에서 데이터를 복원할 수 있습니다.

참고 Cisco ISE는 문제 해결용으로 로그 및 구성 파일을 수집하는 데 사용할 수 있는 **backup-logs** CLI 명령도 제공합니다.

CLI에서 컨피그레이션 또는 모니터링 백업 복원

Cisco ISE CLI를 통해 컨피그레이션 데이터를 복원하려면 EXEC 모드에서 **restore** 명령을 사용합니다. 컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 다음 명령을 사용합니다.

filename repository-name encryption-key name **restore repository encryption-key hash|plain include-adeos**

구문 설명

restore	컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 이 명령을 입력합니다.

filename	저장소에 있는 백업된 파일의 이름입니다. 최대 120개의 영숫자를 지원합니다. 참고 파일 이름 뒤에 .tar.gpg 확장자를 추가해야 합니다(예: myfile.tar.gpg).
repository	백업이 포함되어 있는 저장소를 지정합니다.
repository-name	복원할 백업이 있는 저장소의 이름입니다.
encryption-key	(선택 사항) 백업을 복원할 사용자 맞춤화 암호화 키를 지정합니다.
hash	백업을 복원하기 위해 해시된 암호 키입니다. 뒤에 오는 암호화된(해시된) 암호 키를 지정합니다. 최대 40자를 지원합니다.
plain	백업을 복원하기 위한 일반 텍스트 암호 키입니다. 뒤에 오는 암호화되지 않은 일반 텍스트 암호 키를 지정합니다. 최대 15자를 지원합니다.
encryption-key name	암호화 키를 입력합니다.
include-adeos	(선택 사항, 컨피그레이션 백업에만 해당함) 컨피그레이션 백업에서 ADE-OS 컨피그레이션을 복원하려는 경우 이 명령 연산자 매개변수를 입력합니다. 컨피그레이션 백업을 복원할 때 이 매개변수를 포함하지 않으면 Cisco ISE 애플리케이션 컨피그레이션 데이터만 복원됩니다.

기본값

기본 동작 또는 값은 없습니다.

명령 모드

EXEC

사용 지침

Cisco ISE에서 restore 명령을 사용하는 경우 Cisco ISE 서버가 자동으로 다시 시작됩니다.

데이터를 복원할 때 암호화 키는 선택 사항입니다. 암호화 키를 제공하지 않은 이전 백업을 지원하려는 경우 암호화 키 없이 **restore** 명령을 사용하면 됩니다.

예

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain
 Lab12345
```

```
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore.  Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#
```

관련 명령

	Description(설명)
backup	백업을 수행하고(Cisco ISE 및 Cisco ADE OS) 저장소에 백업을 저장합니다.
backup-logs	시스템 로그를 백업합니다.
repository	백업 컨피그레이션을 위한 저장소 하위 모드로 진입합니다.
show repository	특정 저장소에 있는 사용 가능한 백업 파일을 표시합니다.
show backup history	시스템 백업 기록을 표시합니다.
show backup status	백업 작업의 상태를 표시합니다.
show restore status	복원 작업의 상태를 표시합니다.

보조 노드에 대한 애플리케이션 복원 후의 동기화 상태 및 복제 상태가 동기화되지 않음인 경우 해당 보조 노드의 인증서를 PAN으로 다시 가져온 다음 수동 동기화를 수행해야 합니다.

GUI에서 컨피그레이션 백업 복원

관리 포털에서 컨피그레이션 백업을 복원할 수 있습니다. GUI에는 현재 릴리스에서 생성한 백업만 나열됩니다. 이 릴리스 이전의 백업을 복원하려면 CLI에서 restore 명령을 사용해 주십시오.

시작하기 전에

기본 PAN 자동 페일오버 컨피그레이션이 구축에서 활성화되어 있는 경우 꺼져 있는지 확인합니다. 컨피그레이션 백업을 복원할 때는 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스

가 다시 시작되는 동안 작업이 지연될 수 있습니다. 서비스가 다시 시작될 때의 이러한 지연으로 인해 보조 관리 노드의 자동 페일오버가 시작될 수 있습니다.

구축 시 시간 컨피그레이션 백업의 듀얼 노드 구축인 경우 다음을 확인합니다.

- 복원의 소스 및 대상 노드는 컨피그레이션 백업에 사용된 것과 동일합니다. 대상 노드는 독립형 또는 기본 노드일 수 있습니다.
- 복원의 소스 및 대상 노드는 컨피그레이션 백업에 사용된 것과 다릅니다. 대상 노드는 독립형이어야 합니다.

참고 컨피그레이션 데이터베이스 백업을 복원하고 기본 PAN에서만 루트 CA를 다시 생성할 수 있습니다. 그러나 등록된 PAN에서는 컨피그레이션 데이터베이스 백업을 복원할 수 없습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 컨피그레이션 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **4** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **5** **Restore(**복원**)**를 클릭합니다.

다음에 수행할 작업

Cisco ISE CA 서비스를 사용하는 경우 다음을 수행해야 합니다.

1. 전체 Cisco ISE CA 루트 체인을 재생성합니다.
2. PAN에서 Cisco ISE CA 인증서와 키의 백업을 가져온 다음 보조 관리 노드에서 복원합니다. 그러면 기본 PAN 장애 시 보조 PAN이 루트 CA 또는 외부 PKI의 하위 CA로 작동할 수 있으며, 이 경우 보조 PAN을 기본 PAN으로 승격합니다.

모니터링 데이터베이스 복원

모니터링 데이터베이스를 복원하는 프로세스는 구축 유형에 따라 다릅니다. 다음 섹션에서는 독립형 및 분산형 구축에서 모니터링 데이터베이스를 복원하는 방법을 설명합니다.

CLI를 사용하여 이전 Cisco ISE 릴리스에서 온디맨드 모니터링 데이터베이스 백업을 복원해야 합니다. Cisco ISE 릴리스에서 예약 백업을 복원하는 기능은 지원되지 않습니다.

참고 데이터를 가져온 노드와 다른 노드로 데이터를 복원하려는 경우 새 노드를 가리키도록 로깅 대상 설정을 구성해야 합니다. 이렇게 하면 모니터링 시스템 로그가 적절한 노드로 전송됩니다.

독립형 환경에서 모니터링(운영) 백업 복원

GUI에는 현재 릴리스에서 생성한 백업만 나열됩니다. 이전 릴리스에서 가져온 백업을 복원하려면 CLI에서 restore 명령을 사용해 주십시오.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**를 선택합니다.

단계 **3** 운영 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **4** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **5** **Restore(**복원**)**를 클릭합니다.

관리 및 모니터링 페르소나를 사용하여 모니터링 백업 복원

관리 및 모니터링 페르소나를 사용하여 분산형 환경의 모니터링 백업을 복구할 수 있습니다.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** 기본 및 보조 PAN을 사용하는 경우 PAN을 동기화합니다.

PAN을 동기화할 때 PAN을 선택하고, 이를 활성 기본 상태로 승격해야 합니다.

단계 **2** 모니터링 노드의 등록을 취소하기 전에 모니터링 페르소나를 구축의 다른 노드에 할당합니다.

모든 구축에는 작동하는 모니터링 노드가 하나 이상 있어야 합니다.

단계 **3** 백업할 모니터링 노드를 등록 취소합니다.

단계 **4** 새로 등록 취소한 노드로 모니터링 백업을 복원합니다.

단계 **5** 새로 복원한 노드를 현재 관리 노드에 등록합니다.

단계 **6** 새로 복구하고 등록한 노드를 활성 모니터링 노드로 승격합니다.

모니터링 페르소나를 사용하여 모니터링 백업 복원

모니터링 페르소나만 사용하여 분산형 환경의 모니터링 백업을 복원할 수 있습니다.

시작하기 전에

- 이전 모니터링 데이터를 비웁니다.
- 백업을 예약하거나 온디맨드 백업을 수행합니다.

단계 **1** 복구할 노드의 등록 취소를 준비합니다. 이 작업은 구축의 다른 노드에 모니터링 페르소나를 할당하여 수행됩니다.

구축에는 작동하는 모니터링 노드가 하나 이상 있어야 합니다.

단계 **2** 복원할 노드를 등록 취소합니다.

참고 등록 취소가 완료될 때까지 기다렸다가 복원을 진행합니다. 노드가 독립형 상태여야 복원을 계속할 수 있습니다.

단계 **3** 새로 등록 취소한 노드로 모니터링 백업을 복원합니다.

단계 **4** 새로 복원한 노드를 현재 관리 노드에 등록합니다.

단계 **5** 새로 복원하고 등록한 노드를 PAN으로 승격합니다.

복원 기록

운영 감사 보고서 창에서 모든 복원 작업, 로그 이벤트 및 상태에 대한 정보를 가져올 수 있습니다.

참고 그러나 운영 감사 보고서 창에서는 이전 복원 작업에 해당하는 시작 시간에 대한 정보를 제공하지 않습니다.

문제 해결 정보를 확인하려면 Cisco ISE CLI에서 **backup-logs** 명령을 실행하고 ADE.log 파일을 확인해야 합니다.

복원 작업이 진행 중인 동안에는 모든 Cisco ISE 서비스가 중지됩니다. **show restore status** CLI 명령을 사용하여 복구 작업의 진행률을 확인할 수 있습니다.

인증 및 권한 부여 정책 컨피그레이션 내보내기

컨피그레이션 오류를 식별하고 문제 해결용으로 사용하기 위해 오프라인에서 읽을 수 있는 XML 파일 형식으로 인증 및 권한 부여 정책 컨피그레이션을 내보낼 수 있습니다. 이 XML 파일은 인증 및 권한 부여 정책 규칙, 단순/복합 정책 조건, DACL(Discretionary Access Control Lists) 및 권한 부여 정책을 포함합니다. XML 파일을 이메일로 보내거나 로컬 시스템에 저장하도록 선택할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup & Restore(**백업 및 복구**)**를 선택합니다.

단계 **2** **Policy Export(**정책 내보내기**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력합니다.

단계 **4** **Export(**내보내기**)**를 클릭합니다.

WordPad 등의 텍스트 편집기를 사용하여 XML 파일의 내용을 확인합니다.

정책 내보내기 예약 설정

다음 표에서는 **Schedule Policy Export(**정책 내보내기 예약**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)** > **Policy Export(**정책 내보내기**)**입니다.

표 ***5:*** 정책 내보내기 예약 설정

필드 이름	사용 지침
암호화	
Encryption Key(암호화 키**)**	내보내기 데이터를 암호화하고 암호를 해독하는 데 사용할 키를 입력합니다. 이 필드는 **Export with Encryption Key(**암호화 키를 사용해 내보내기**)** 옵션을 선택한 경우에만 활성화됩니다.
Destination(대상**)**	
Download file to local computer(파일을 로컬 컴퓨터에 다운로드**)**	정책 내보내기 파일을 로컬 시스템에 다운로드할 수 있습니다.
다음 사용자에게 이메일로 파일 보내기	이메일 주소가 여러 개인 경우 쉼표로 구분하십시오.
Repository(저장소**)**	정책 데이터를 내보낼 저장소를 선택합니다. 여기에 저장소 이름을 입력할 수는 없습니다. 드롭다운 목록에서 사용 가능한 저장소를 선택하는 것만 가능합니다. 정책 내보내기를 예약하기 전에 저장소를 생성해야 합니다.
Export Now(지금 내보내기**)**	데이터를 로컬 컴퓨터로 내보내거나 이메일 첨부 파일로 보내려면 이 옵션을 클릭합니다. 저장소로는 내보낼 수 없습니다. 저장소 내보내기만 예약이 가능합니다.

필드 이름	사용 지침
Schedule(일정**)**	
Schedule Options(예약 옵션**)**	내보내기 일정의 빈도를 선택하고 그에 따라 나머지 세부정보를 입력합니다.

분산형 환경에서 기본 및 보조 노드 동기화

분산형 환경에서는 PAN에서 백업 파일을 복원한 후 기본 노드와 보조 노드의 Cisco ISE 데이터베이스가 자동으로 동기화되지 않는 경우가 있습니다. 이러한 현상이 발생하는 경우 PAN에서 보조 ISE 노드로의 전체 복제를 수동으로 강제 수행할 수 있습니다. PAN에서 보조 노드로만 동기화를 강제 수행할 수 있습니다. syncup 작업 중에는 컨피그레이션을 변경할 수 없습니다. Cisco ISE에서는 동기화가 완료된 후에만 다른 Cisco ISE 관리 포털 페이지로 이동하여 컨피그레이션을 변경하도록 허용합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Backup and Restore(**백업 및 복구**)**

단계 **3** 복제 상태가 동기화되지 않음인 보조 ISE 노드 옆의 확인란을 선택합니다.

단계 **4** **Syncup**을 클릭하고 노드가 PAN과 동기화될 때까지 기다립니다. 이 프로세스가 완료될 때까지 기다려야 Cisco ISE 관리 포털에 다시 액세스할 수 있습니다.

분산형 구축에서 손실된 노드 복구

이 섹션에서는 분산형 구축에서 손실된 노드를 복구하는 데 사용할 수 있는 문제 해결 정보를 제공합니다. 다음 활용 사례 중 일부에서는 백업 및 복구 기능을, 다른 일부에서는 복제 기능을 사용하여 손실된 데이터를 복구합니다.

분산형구축에서 기존 IP 주소 및 호스트 이름을 사용한 손실 노드 복구

시나리오

분산형 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 복구 후에 기존 IP 주소와 호스트 이름을 사용하려고 합니다.

예를 들어 N1(기본 정책 관리 노드 또는 기본 PAN) 및 N2(보조 정책 관리 노드 또는 보조 PAN)의 두 개 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다.

가정

구축의 모든 Cisco ISE 노드가 제거되었습니다. 같은 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 및 N2 노드를 모두 대체해야 합니다. 이제 N1 및 N2 노드에 독립형 컨피그레이션이 사용됩니다.
2. N1 및 N2 노드의 UDI를 사용하여 라이선스를 가져온 다음 N1 노드에 설치합니다.
3. 그런 다음 교체된 N1 노드에서 백업을 복원해야 합니다. 복원 스크립트는 N2에서 데이터 동기화를 시도하지만 이제 N2는 독립형 노드이므로 동기화가 실패합니다. N1의 데이터는 T1 시간으로 재설정됩니다.
4. N1 관리 포털에 로그인하여 N2 노드를 삭제한 다음 다시 등록해야 합니다. N1 및 N2 노드 둘 다의 데이터가 T1 시간의 데이터로 재설정됩니다.

분산형구축에서 새 IP 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

분산형 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 새 위치에서 새 하드웨어를 재이미지화했으며 새 IP 주소와 호스트 이름이 필요합니다.

예를 들어 N1(기본 관리 노드/PAN) 및 N2(보조 정책 서비스 노드)의 두 개 ISE 노드가 있다고 가정해 보겠습니다. 시간 T1에 만든 N1 노드의 백업을 사용할 수 있습니다. 그런데 나중에 자연 재해로 인해 N1 및 N2 노드 둘 다에서 장애가 발생합니다. Cisco ISE 노드가 새 위치에서 대체되며, 새 호스트 이름은 N1A(PAN) 및 N2A(보조 정책 서비스 노드)입니다. 이 시점에서 N1A 및 N2A는 독립형 노드입니다.

가정

구축의 모든 Cisco ISE 노드가 제거되었습니다. 다른 위치에서 다른 호스트 이름과 IP 주소를 사용하여 새 하드웨어가 이미지화되었습니다.

해결 단계

1. N1 백업을 가져온 다음 N1A에서 복원합니다. 복원 스크립트는 호스트 이름 변경 및 도메인 이름 변경을 식별하여 현재 호스트 이름을 기반으로 구축 컨피그레이션에서 호스트 이름과 도메인 이름을 업데이트합니다.
2. 새 셀프 서명 인증서를 생성해야 합니다.

3. N1A에서 Cisco ISE 관리자 포털에 로그인해야합니다.Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** 에서 다음을 수행합니다.

   이전 N2 노드를 삭제합니다.

   새 N2A 노드를 보조 노드로 등록합니다. N1A 노드의 데이터가 N2A 노드로 복제됩니다.

독립형 구축에서 기존 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 N1 데이터베이스의 백업을 만들었습니다. N1 노드는 물리적 장애로 인해 다운되었으며 재이미지화해야 하거나 새 하드웨어를 사용해야 합니다. 같은 IP 주소와 호스트 이름을 사용하여 N1 노드를 다시 작동시켜야 합니다.

가정

이 구축은 독립형이며 새로 사용하거나 재이미지화되는 하드웨어의 IP 주소와 호스트 이름은 같습니다.

해결 단계

재이미지화 후에 N1 노드가 작동하거나 같은 IP 주소 및 호스트 이름을 사용하여 새 Cisco ISE 노드를 도입한 후에는 이전 N1 노드에서 만든 백업을 복구해야 합니다. 역할은 변경하지 않아도 됩니다.

독립형 구축에서 새 IP 주소 및 호스트 이름을 사용하여 노드 복구

시나리오

독립형 관리 노드가 다운되었습니다.

예를 들어 독립형 관리 노드가 N1이라고 가정해 보겠습니다. 시간 T1에 만든 N1 데이터베이스의 백업을 사용할 수 있습니다. N1 노드는 물리적 장애로 인해 다운되었으며, 다른 IP 주소와 호스트 이름을 사용하여 다른 위치에서 새 하드웨어로 해당 노드를 교체하려고 합니다.

가정

구축은 독립형이며 교체되는 하드웨어는 IP 주소와 호스트 이름이 다릅니다.

해결 단계

1. N1 노드를 새 하드웨어로 교체합니다. 이 노드는 독립형 상태가 되며 호스트 이름은 N1B입니다.
2. N1B 노드에서 백업을 복원할 수 있습니다. 역할은 변경하지 않아도 됩니다.

컨피그레이션 롤백

문제

실수로 컨피그레이션을 잘못 변경하는 경우가 있을 수 있습니다. 예를 들어 여러 NAD를 삭제하거나 일부 ADIUS 속성을 잘못 수정했지만, 몇 시간 후에야 이 문제를 깨달을 수 있습니다. 이 경우 변경하기 전에 작성한 백업을 복구하여 원래 컨피그레이션으로 되돌릴 수 있습니다.

가능한 원인

N1(기본 정책 관리 노드 또는 기본 PAN)과 N2(보조 정책 관리 노드 또는 보조 PAN)로 구성된 노드 2개와 N1 노드 백업이 지원됩니다. 일부 컨피그레이션을 잘못 변경하여 N1에서 변경 사항을 제거하고자 합니다.

해결책

잘못된 컨피그레이션 변경이 적용되기 전에 작성된 N1 노드 백업을 가져옵니다. N1 노드에서 이 백업을 복원합니다. 복원 스크립트는 N1의 데이터를 N2와 동기화합니다.

분산형 구축에서 장애 발생 시 기본 노드 복구

시나리오

다중 노드 구축에서 PAN에 장애가 발생했습니다.

예를 들어 N1(PAN) 및 N2(보조 관리 노드)라는 Cisco ISE 노드가 2개 있는데 하드웨어 문제로 인해 N1에 장애가 발생한다고 가정해 보겠습니다.

가정

분산형 구축의 기본 노드에만 장애가 발생했습니다.

해결 단계

1. N2 관리자 포털에 로그인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** 를 선택하고 기본 노드로 N2를 구성합니다.

   N1 노드가 새 하드웨어로 교체되고 재이미지화되며 독립형 상태가 됩니다.

2. N2 관리자 포털에서 새 N1 노드를 보조 노드로 등록합니다.

   이제 N2 노드가 기본 노드가 되고 N1 노드가 보조 노드가 됩니다.

N1 노드를 다시 기본 노드로 지정하려면 N1 관리자 포털에 로그인하여 N1 노드를 기본 노드로 지정합니다. 그러면 N2는 자동으로 보조 서버가 됩니다. 데이터는 손실되지 않습니다.

분산형 구축에서 장애 발생 시 보조 노드 복구

시나리오

다중 노드 구축에서 단일 보조 노드에 장애가 발생했습니다. 복원은 수행하지 않아도 됩니다.

예를 들어 N1(기본 PAN), N2(보조 PAN), N3(보조 정책 서비스 노드), N4(보조 정책 서비스 노드)라는 여러 노드가 있는데 보조 노드 중 하나인 N3에서 장애가 발생한다고 가정해 보겠습니다.

해결 단계

1. 새 N3A 노드를 기본 독립형 상태로 재이미지화합니다.
2. N1 관리 포털에 로그인하여 N3 노드를 삭제합니다.
3. N3A 노드를 다시 등록합니다.

   데이터는 N1에서 N3A로 복제됩니다. 복원은 수행하지 않아도 됩니다.

Cisco ISE 로깅 메커니즘

Cisco ISE는 감사, 결함 관리 및 문제 해결에 사용되는 로깅 메커니즘을 제공합니다. 로깅 메커니즘은 구축된 서비스에서 결함 조건을 식별하고 문제를 효율적으로 해결하는 데 도움이 됩니다. 또한 모니터링 및 문제 해결 기본 노드에서 일관된 방식으로 로깅 출력을 생성하기도 합니다.

가상 루프백 주소를 사용하여 로컬 시스템의 로그를 수집하도록 Cisco ISE 노드를 구성할 수 있습니다. 외부에서 로그를 수집하려면 호출 대상인 외부 시스템 로그 서버를 구성해 주십시오. 로그는 미리 정의된 여러 범주로 분류됩니다. 대상, 심각도 레벨 등과 관련된 범주를 편집하여 로깅 출력을 사용자 맞춤화할 수 있습니다.

Cisco ISE 모니터링 및 문제 해결(MnT) 노드에 syslog를 전송하도록 네트워크 디바이스를 구성하지 않는 것이 모범 사례입니다. 이 경우 Cisco NISE(Network Access Device) syslog가 손실되고 MnT 서버가 오버로드되어 로드 문제가 발생할 수 있기 때문입니다. NAD Syslog가 MnT로 직접 전송되도록 구성된 경우 세션 관리 기능이 중단됩니다. 문제 해결을 위해 NAD 시스템 로그를 외부 시스템 로그 서버로 전송할 수 있지만 MnT로 보내서는 안 됩니다.

노드에서 ISE 메시징 서비스에 장애가 발생할 때 프로세스 중단 경보가 더 이상 트리거되지 않습니다. 노드에서 ISE 메시징 서비스에 장애가 발생하면 해당 노드에서 메시징 서비스가 다시 작동할 때까지 모든 시스템 로그 및 프로세스 중단 경보가 손실됩니다.

이 경우 관리자는 Cisco ISE **Home(**홈**)** 창의 **Alarms(**경보**)** dashlet에 나열되는 **Queue Link Error(**대기열 링크 오류**)** 경보를 찾아야 합니다. 경보를 클릭하면 **Suggested Actions(**추천 작업**)** 섹션이 포함된 새 창이 열립니다. 다음 지침에 따라 문제를 해결합니다.

참고 모니터링 노드가 네트워크 디바이스에 대한 시스템 로그 서버로 구성된 경우 로깅 소스가 올바른 NAS(Network Access Server) IP 주소를 다음 형식으로 전송하는지 확인합니다.

<message_number>sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

그렇지 않으면 NAS IP 주소에 의존하는 기능에 영향을 미칠 수 있습니다.

시스템 로그 제거 설정 구성

다음 프로세스를 사용하여 로컬 로그 저장 기간을 설정하고 특정 기간이 지난 후 로컬 로그를 삭제합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Local Log Settings(**로컬 로그 설정**)**를 선택합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Local Log Settings(**로컬 로그 설정**)**.

단계 **3** **Local Log Storage Period(**로컬 로그 저장 기간**)** 필드에 로그 엔트리를 컨피그레이션 소스에 보관할 최대 기간을 일 단위로 입력합니다.

localStore 폴더의 크기가 97GB에 도달하면 구성된 **Local Log Storage Period(**로컬 로그 저장 기간**)**가 끝나기 전에 일찍 로그가 삭제될 수 있습니다.

단계 **4** 저장 기간이 만료되기 전에 언제든지 기존 로그 파일을 삭제하려면 **Delete Logs Now(**지금 로그 삭제**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE 시스템 로그

Cisco ISE에서 시스템 로그는 호출되는 로깅 대상이라고 하는 위치에서 수집됩니다. 대상이란 로그를 수집하고 저장하는 서버의 IP 주소를 나타냅니다. 로그는 로컬에서 생성하여 저장할 수도 있고, FTP 기능을 사용하여 외부 서버로 전송할 수도 있습니다. Cisco ISE에는 로컬 시스템의 루프백 주소에서 동적으로 구성되는 다음과 같은 기본 대상이 있습니다.

- LogCollector - 로그 컬렉터의 기본 시스템 로그 대상
- ProfilerRadiusProbe - 프로파일러 RADIUS 프로브의 기본 시스템 로그 대상

기본적으로 AAA Diagnostics(AAA 진단) 하위 범주 및 System Diagnostics(시스템 진단) 하위 범주 로깅 대상은 디스크 공간을 줄일 수 있도록 새로운 Cisco ISE 설치 또는 업그레이드 중에 비활성화됩니다. 이러한 하위 범주에 대해 수동으로 로깅 대상을 구성할 수 있지만 이러한 하위 범주의 로컬 로깅은 항상 활성화되어 있습니다.

Cisco ISE 설치 측에서 로컬로 구성한 기본 로깅 대상을 사용할 수 있습니다. 또는 외부 대상을 생성하여 로그를 저장할 수도 있습니다.

참고 시스템 로그 서버가 분산형 구축으로 구성된 경우 시스템 로그 메시지는 MnT 노드가 아닌 인증 PSN에서 직접 시스템 로그 서버로 전송됩니다.

관련 항목

Cisco ISE 메시지 코드, 35 페이지

원격 시스템 로그 컬렉션 위치 구성

웹 인터페이스를 사용하여 시스템 로그 메시지가 전송되는 원격 시스템 로그 서버 대상을 생성할 수 있습니다. 로그 메시지는 시스템 로그 프로토콜 표준에 따라 원격 시스템 로그 서버 타깃으로 전송됩니다(RFC-3164 참고). 시스템 로그 프로토콜은 비보안 UDP입니다.

이벤트가 발생하면 메시지가 생성됩니다. 이벤트는 프로그램 종료 시 표시되는 메시지와 같이 상태를 표시하는 항목 또는 경보일 수 있습니다. 커널, 메일, 사용자 레벨 등의 여러 기능에서 다양한 유형의 이벤트 메시지가 생성됩니다. 이벤트 메시지는 심각도 레벨과 연결되므로 관리자는 메시지를 필터링하고 우선순위를 설정할 수 있습니다. 기능과 심각도 레벨에는 숫자 코드가 할당됩니다. 시스템 로그 서버는 이벤트 메시지 컬렉터이며 이러한 기능에서 이벤트 메시지를 수집합니다. 관리자는 심각도 레벨에 따라 메시지를 전달할 이벤트 메시지 컬렉터를 선택할 수 있습니다.

기본 원격 로깅 대상은 UDP 시스템 로그(로그 컬렉터)입니다. 이 로깅 대상은 비활성화하는 경우 더 이상 로그 컬렉터로 작동하지 않으며 **Logging Categories(**로깅 범주**)** 창에서 제거되고, 활성화하는 경우 **Logging Categories(**로깅 범주**)** 창에서 로그 컬렉터로 지정됩니다.

참고 기본 원격 로깅 대상 **SecureSyslogCollector**를 변경하면 Cisco ISE 모니터링 및 문제 해결 로그 프로세서 서비스가 재시작됩니다.

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

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 필요한 세부정보를 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 원격 로깅 대상 페이지로 이동하여 새 대상이 생성되었는지 확인합니다.

그런 다음 로깅 대상을 아래의 각 로깅 범주에 매핑할 수 있습니다. PSN 노드는 해당 노드에서 활성화된 서비스에 따라 관련 로그를 원격 로깅 대상으로 전송합니다.

- AAA 감사
- AAA 진단

- 어카운팅
- 외부 MDM
- 패시브 ID
- Posture and Client Provisioning Audit(포스처 및 클라이언트 프로비저닝 감사)
- 포스처 및 클라이언트 프로비저닝 진단
- 프로파일러

다음 범주의 로그는 구축 환경의 모든 노드에서 로깅 대상으로 전송됩니다.

- Administrative and Operational Audit(관리 및 운영 감사)
- 시스템 진단
- 시스템 통계

Cisco ISE 메시지 코드

로깅 범주는 기능, 흐름 또는 활용 사례를 설명하는 메시지 코드 번들입니다. Cisco ISE에서 각 로그는 로그 메시지 콘텐츠에 따라 로깅 범주와 함께 제공되는 메시지 코드와 연결되어 있습니다. 로깅 범주는 그 안에 포함된 메시지 콘텐츠를 설명하는 데 도움이 됩니다.

로깅 범주에서 로깅 컨피그레이션을 승격할 수 있습니다. 각 범주에는 애플리케이션 요건에 따라 설정할 수 있는 이름, 대상 및 심각도 레벨이 있습니다.

Cisco ISE는 포스처, 프로파일러, 게스트, AAA(Authentication, Authorization, and Accounting) 등과 같이 서비스에 대해 미리 정의된 로깅 범주를 제공하므로 여기에 로그 대상을 할당할 수 있습니다.

로깅 범주 **Passed Authentications(**통과된 인증**)**의 경우 로컬 로깅을 허용하는 옵션은 기본적으로 비활성화되어 있습니다. 이 범주에 대한 로컬 로깅을 활성화하면 운영 공간의 사용률이 높아지며 prrt-server.log와 iseLocalStore.log가 입력집니다.

Passed Authentications(통과된 인증**)**에 대해 로컬 로깅을 활성화하려면 범주 섹션에서 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**로 이동하여 **Passed Authentications(**통과된 인증**)**을 클릭한 다음 **Local Logging(**로컬 로깅**)**에 대한 확인란을 선택합니다.

관련 항목

메시지 코드에 대한 심각도 레벨 설정, 35 페이지

메시지 코드에 대한 심각도 레벨 설정

로그 심각도 레벨을 설정하고 선택한 범주의 로그를 저장할 로깅 대상을 선택할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**.

단계 **2** 편집할 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 필수 필드 값을 수정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 로깅 범주 페이지로 이동하여 특정 범주에 대해 수행된 컨피그레이션 변경사항을 확인합니다.

Cisco ISE 메시지 카탈로그

메시지 카탈로그 페이지를 사용하여 모든 가능한 로그 메시지와 설명을 볼 수 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Message Catalog(**메시지 카탈로그**)**를 선택합니다.

Log Message Catalog(로그 메시지 카탈로그) 페이지가 나타나면 로그 파일에 표시될 수 있는 잠재적인 로그 메시지를 모두 볼 수 있습니다. **Export(**내보내기**)**를 선택하여 모든 시스템 로그 메시지를 CSV 파일 형식으로 내보냅니다.

Cisco ISE에서 전송한 시스템 로그 메시지의 전체 목록, 의미 및 로컬 및 원격 대상에서 메시지가 기록되는 방식은 Cisco ISE 시스템 로그를 참조하십시오.

엔드포인트 디버그 로그 컬렉터

특정 엔드포인트 관련 문제를 해결하려면 IP 주소 또는 MAC 주소를 기준으로 특정 엔드포인트의 디버그 로그를 다운로드할 수 있습니다. 특정 엔드포인트 관련 구축 환경에 있는 다양한 노드의 로그는 단일 파일로 수집되므로 문제를 신속하고 효율적으로 해결하는 데 도움이 됩니다. 이 문제 해결 도구는 한 번에 하나의 엔드포인트에 대해서만 실행할 수 있습니다. 로그 파일은 GUI에 나열됩니다. 엔드포인트 로그는 단일 노드에서 다운로드할 수도 있고, 구축 환경의 모든 노드에서 다운로드할 수도 있습니다.

특정 엔드포인트에 대한 디버그 로그 다운로드

네트워크에서 특정 엔드포인트 관련 문제를 해결하려는 경우 관리 포털에서 엔드포인트 디버그 도구를 사용할 수 있습니다. 인증 페이지에서 이 도구를 실행할 수도 있습니다. 이렇게 하려면 인증 페이지에서 엔드포인트 ID를 마우스 오른쪽 버튼으로 클릭하고 **Endpoint Debug(**엔드포인트 디버그**)**를 클릭합니다. 이 도구는 특정 엔드포인트와 관련된 모든 서비스에 대한 모든 디버그 정보를 단일 파일에서 제공합니다.

시작하기 전에

디버그 로그를 수집하려는 엔드포인트의 IP 주소 또는 MAC 주소가 필요합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Endpoint Debug(**엔드포인트 디버그**)**.

단계 **2** **MAC Address(MAC** 주소**)** 또는 **IP** 라디오 버튼을 클릭하고 엔드포인트의 MAC 또는 IP 주소를 입력합니다.

단계 **3** 지정된 시간 후에 로그 수집을 중지하려면 **Automatic disable after *n* Minutes(n**분 후 자동 비활성화**)** 확인란을 선택합니다. 이 확인란을 선택하는 경우 1~60분 사이의 시간을 입력해야 합니다.

"엔드포인트 디버그를 사용하는 경우 구축 성능이 저하됩니다. 계속하시겠습니까?"라는 메시지가 표시됩니다.

단계 **4** 로그를 수집하려면 **Continue(**계속**)**를 클릭합니다.

단계 **5** 로그 수집을 수동으로 중지하려면 **Stop(**중지**)**을 클릭합니다.

관련 항목

엔드포인트 디버그 로그 컬렉터, 36 페이지

수집 필터

모니터링 및 외부 서버로 전송되는 시스템 로그 메시지를 표시하지 않도록 수집 필터를 구성할 수 있습니다. 표시 안 함은 다양한 속성 유형에 따라 정책 서비스 노드 수준에서 수행될 수 있습니다. 특정 속성 유형 및 해당 값을 사용하여 여러 필터를 정의할 수 있습니다.

Cisco ISE는 시스템 로그 메시지를 모니터링 노드 또는 외부 서버로 보내기 전에 먼저 이러한 값을 전송 대상 시스템 로그 메시지의 필드와 비교합니다. 일치하는 항목이 있는 경우 해당 메시지가 전송되지 않습니다.

수집 필터 구성

다양한 속성 유형을 기준으로 여러 수집 필터를 구성할 수 있습니다. 필터 수는 20개로 제한하는 것이 좋습니다. 수집 필터를 추가, 편집 또는 삭제할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Collection Filters(**수집 필터**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 다음 목록에서 **Filter Type(**필터 유형**)**을 선택합니다.

- 사용자 이름
- MAC 주소
- 정책 집합 이름
- NAS IP 주소
- 디바이스 IP 주소

단계 **4** 선택한 필터 유형에 해당하는 **Value(**값**)**를 입력합니다.

단계 **5** 드롭다운 목록에서 **Result(**결과**)**를 선택합니다. 결과는 모두, 통과 또는 실패일 수 있습니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

관련 항목

수집 필터, 37 페이지
이벤트 억제 무시 필터, 38 페이지

이벤트 억제 무시 필터

Cisco ISE에서는 수집 필터를 사용하여 시스템 로그 메시지가 모니터링 노드 및 다른 외부 서버로 전송되지 않도록 억제하는 필터를 설정할 수 있습니다. 때로는 이와 같이 숨겨진 로그 메시지에 액세스해야 하는 경우가 있습니다. Cisco ISE는 이제 구성 가능한 기간 동안 사용자 이름과 같은 특정 속성에 따라 이벤트 억제를 무시할 수 있는 옵션을 제공합니다. 기본값은 50분이지만 5분부터 480분(8시간)까지 기간을 구성할 수 있습니다. 이벤트 억제 무시를 구성하고 나면 효과가 즉시 적용됩니다. 설정한 기간이 경과되면 억제 무시 필터가 만료됩니다.

Cisco ISE 사용자 인터페이스의 수집 필터 페이지에서 억제 무시 필터를 구성할 수 있습니다. 이제 이 기능을 사용하여 특정 ID(사용자)의 모든 로그를 볼 수 있으며 해당 ID에 대한 문제를 실시간으로 해결할 수 있습니다.

필터는 활성화하거나 비활성화할 수 있습니다. 이벤트 무시 필터에 구성한 기간이 경과되면 관리자가 다시 활성화할 때까지 필터가 자동으로 비활성화됩니다.

Cisco ISE는 컨피그레이션 변경 감사 보고서에서 이러한 컨피그레이션 변경 사항을 캡처합니다. 이 보고서에서는 이벤트 억제 또는 억제 무시를 구성한 사용자 및 이벤트가 억제되었거나 억제가 무시된 기간에 대한 정보를 제공합니다.

Cisco ISE 보고서

Cisco ISE(Identity Services Engine) 보고서는 모니터링 및 문제 해결 기능과 함께 중앙 위치에서 트렌드를 분석하고 시스템 성능과 네트워크 활동을 모니터링하는 데 사용됩니다.

Cisco ISE는 네트워크에서 로그 및 컨피그레이션 데이터를 수집합니다. 그런 다음 보고 분석할 수 있도록 데이터를 보고서로 집계합니다. Cisco ISE는 미리 정의된 표준 보고서 집합을 제공하므로 사용자 요구 사항에 맞게 사용하고 사용자 맞춤화할 수 있습니다.

Cisco ISE 보고서는 미리 구성되어 있으며 인증, 세션 트래픽, 디바이스 관리 , 컨피그레이션 및 관리, 문제 해결과 관련된 정보를 사용하여 논리 범주로 그룹화됩니다.

관련 항목

보고서 실행 및 보기, 40 페이지
보고서 내보내기, 41 페이지
사용 가능한 보고서, 45 페이지

보고서 필터

단일 섹션 및 다중 섹션이라는 2가지 보고서 유형이 있습니다. 단일 섹션 보고서는 단일 그리드(Radius 인증 보고서)를 포함하고, 다중 섹션 보고서는 다수의 그리드(인증 요약 보고서)로 구성되며 차트 및 표 형식으로 데이터를 표시합니다. 단일 섹션 보고서의 Filter(필터) 드롭다운 메뉴는 **Quick Filter(**빠른 필터**)**와 **Advanced Filter(**고급 필터**)**로 구성되어 있습니다. 다중 섹션 보고서에서는 고급 필터만 지정할 수 있습니다.

다중 섹션 보고서에는 입력이 필요한 하나 이상의 필수 고급 필터가 포함될 수 있습니다. 예를 들어 상태 요약 보고서 클릭하면(**Operations(**운영**) > Reports(**보고서**) > Diagnostics(**진단**)** 페이지), Server(서버) 및 Time Range(시간 범위)라는 2가지 필수 고급 필터가 나타납니다. 연산자 명령, 서버 이름, 이 두 필터에 대한 필수 값을 지정하고 **Go(**이동**)**를 클릭하여 보고서를 생성해야 합니다. 더하기(+) 특수문자를 클릭하여 새 고급 필터를 추가할 수 있습니다. 다중 섹션 보고서는 PDF 형식으로만 내보낼 수 있습니다. Cisco ISE 다중 섹션 보고서가 특정 시간에 또는 일정 시간 간격으로 실행 및 재실행되도록 예약할 수는 없습니다.

참고 보고서를 클릭하면 현재 날짜의 데이터가 기본적으로 생성됩니다. 그러나 일부 다중 섹션 보고서에서는 시간 범위를 제외하고 사용자가 필수적으로 입력해야 하는 항목이 있습니다.

기본적으로 Quick Filter(빠른 필터)는 단일 섹션 보고서의 첫 번째 행으로 표시됩니다. 이 필드에는 검색 조건을 선택할 수 있는 드롭다운 목록이 포함되어 있거나 텍스트 상자일 수 있습니다.

Advanced Filter(고급 필터)에는 하나 이상의 내부 기준이 속한 외부 기준이 포함되어 있습니다. 외부 기준은 검색이 All(모두) 또는 Any(일부)로 지정된 내부 기준을 충족해야 하는지를 지정하는 데 사용됩니다. 내부 기준에는 조건에 대한 범주(엔드포인트 ID, ID 그룹), 방법(Contains(포함), Does Not Contain(포함하지 않음) 연산자 명령) 및 시간 범위를 지정하는 데 사용되는 하나 이상의 조건이 포함되어 있습니다.

빠른 필터를 사용하는 경우 **Logged At(**기록된 시간**)** 드롭다운 목록에서 날짜 또는 시간을 선택하여 지난 30일 이내에 기록된 데이터 집합에 대한 보고서를 생성할 수 있습니다. 30일 이전의 날짜 또는 시간에 대한 보고서를 생성하려면 고급 필터를 사용하여 드롭다운 목록의 **Custom(**맞춤 설정**)** 옵션의 **From(**시작**)** 및 **To(**종료**)** 필드에 원하는 기간을 설정하십시오.

빠른 필터 기준 생성

이 섹션에서는 빠른 필터 기준을 생성하는 방법을 설명합니다. 단일 섹션 보고서에 대해서만 빠른 필터 기준을 생성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**) > Reports(**보고서**)**를 선택하고 원하는 보고서를 클릭합니다.

단계 **2** **Settings(**설정**)** 드롭다운 목록에서 필수 필드를 선택합니다.

단계 **3** 필수 필드의 드롭다운 목록에서 선택하거나 특정 문자를 입력하여 데이터를 필터링할 수 있습니다. 검색에서는 Contains(포함) 연산자 명령을 사용합니다. 예를 들어 "K"로 시작하는 텍스트를 기준으로 필터링하려면 K를 입력하거나 텍스트에 "geo"가 있는 텍스트를 필터링하려면 geo를 입력합니다. *abc로 시작하고 *def로 끝나는 regex와 같이 별표(*)를 사용할 수도 있습니다.

빠른 필터는 포함, 다음으로 시작, 다음으로 종료, 다음으로 시작 또는 종료, OR 연산자를 사용한 다중 값 조건을 사용합니다.

단계 **4** **Enter** 키를 누릅니다.

고급 필터 기준 생성

이 섹션에서는 고급 필터 기준을 생성하는 방법을 설명합니다. 단일 섹션 및 다중 섹션 보고서에 대해 고급 필터를 생성할 수 있습니다. 단일 섹션 보고서의 Filter(필터) 드롭다운 메뉴는 **Quick Filter(**빠른 필터**)**와 **Advanced Filter(**고급 필터**)**로 구성되어 있습니다. 다중 섹션 보고서에서는 고급 필터만 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)**를 선택하고 원하는 보고서를 클릭합니다.

단계 **2** **Filters(**필터**)** 섹션의 **Match(**일치**)** 드롭다운 목록에서 옵션 중 하나를 선택합니다.

a) **All(**모두**)**을 선택하여 지정된 모든 조건과 일치시킵니다.

b) **Any(**일부**)**를 선택하여 지정된 조건 중 하나와 일치시킵니다.

단계 **3** **Time Range(**시간 범위**)** 드롭다운 목록에서 원하는 범주를 선택합니다.

단계 **4** **Operator Commands(**운영자 명령**)** 드롭다운 목록에서 원하는 명령을 선택합니다. 예를 들어 특정 문자로 시작하는 텍스트(Begin With 사용) 또는 텍스트에 있는 특정 문자(Contains 사용)를 필터링할 수 있습니다. 또는 Logged Time(기록된 시간) 및 해당 Custom(맞춤 설정) 옵션을 선택하고 일정표에서 시작 및 종료 날짜와 시간을 지정하여 데이터를 필터링할 수 있습니다.

단계 **5** **Time Range(**시간 범위**)** 드롭다운 목록에서 원하는 옵션을 선택합니다.

단계 **6** **Go(**이동**)**를 클릭합니다.

필터링된 보고서를 저장하고 **Filter(**필터**)** 드롭다운 목록에서 검색하여 나중에 참조할 수 있습니다.

보고서 실행 및 보기

이 섹션에서는 보고서 보기를 사용하여 보고서를 실행, 확인 및 탐색하는 방법을 설명합니다. 보고서를 클릭하면 기본적으로 지난 7일 동안의 데이터가 생성됩니다. 각 보고서에는 페이지당 500개의 데이터 행이 표시됩니다. 보고서에서 데이터를 표시할 시간 단위를 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **ISE Reports(ISE** 보고서**)**.

각 작업 센터 아래의 **Reports(**보고서**)** 링크로 이동하여 해당 작업 센터와 관련된 보고서 세트를 볼 수도 있습니다.

단계 **2** 사용 가능한 **report(**보고서**)** 범주에서 보고서를 클릭합니다.

단계 **3** 보고서를 실행하기 위한 필터를 하나 이상 선택합니다. 각 보고서에서는 서로 다른 필터를 사용할 수 있으며, 그 중에는 필수 필터도 있고 선택적 필터도 있습니다.

단계 **4** 필터에 해당하는 값을 입력합니다.

단계 **5** **Go(**이동**)**를 클릭합니다.

관련 항목

보고서 내보내기, 41 페이지
사용 가능한 보고서, 45 페이지

보고서 탐색

보고서 출력에서 자세한 정보를 얻을 수 있습니다. 예를 들어 5개월 동안의 보고서를 생성한 경우 그래프 및 표에는 수 개월 기간의 보고서에 대한 집계 데이터가 나열됩니다.

표에서 특정 값을 클릭하여 이 특정 필드와 관련된 다른 보고서를 볼 수 있습니다. 예를 들어 인증 요약(Authentication Summary) 보고서에는 사용자 또는 사용자 그룹에 대한 실패 횟수가 표시됩니다. 실패 횟수를 클릭하면 특정 실패 횟수에 해당하는 인증 요약(Authentication Summary) 보고서가 열립니다.

보고서 내보내기

다음 보고서는 PDF 파일 형식으로만 내보낼 수 있습니다.

- 인증 요약(Authentication Summary)
- 상태 요약
- RBACL 삭제 요약

참고 RBACL 삭제 패킷에 대한 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.

- 게스트 스폰서 요약
- 엔드포인트 프로파일 변경
- 네트워크 디바이스 세션 상태

단계 **1** 보고서 실행 및 보기 섹션의 설명에 따라 보고서를 실행합니다.

단계 **2** 보고서 요약 페이지의 오른쪽 위에 있는 **Export To(**다음으로 내보내기**)**를 클릭합니다.

단계 **3** 다음 옵션 중 하나를 선택합니다.

- 저장소(CSV) : CSV 파일 형식으로 보고서를 저장소에 내보내려는 경우
- 로컬(CSV) : CSV 파일 형식으로 보고서를 로컬 디스크에 내보내려는 경우
- 로컬(PDF) : 보고서를 pdf 파일 형식으로 로컬 디스크에 내보내려는 경우

참고 로컬 CSV 또는 pdf 옵션을 선택하면 처음 500개 기록만 내보냅니다. Repository CSV(저장소 CSV) 옵션을 사용하여 모든 기록을 내보낼 수 있습니다.

Cisco ISE 보고서 예약 및 저장

보고서를 사용자 맞춤화하고 변경사항을 새 보고서로 저장하거나 Report Summary(보고서 개요) 페이지의 오른쪽 상단 모서리에 있는 **My Reports(**내 보고서**)**에서 기본 보고서 설정을 복구할 수 있습니다.

ISE 보고서를 맞춤화하여 특정 시간에 또는 특정 시간 간격으로 실행 및 다시 실행되도록 예약할 수도 있습니다. 보고서가 생성되면 이메일 알림을 보내고 받을 수도 있습니다.

시간별 빈도로 보고서를 예약할 경우 보고서를 여러 날에 걸쳐 실행할 수 있지만, 이틀에 걸쳐 기간을 설정할 수 없습니다.

예를 들어 2019년 5월 4일부터 5월 8일까지 시간별 보고서를 예약할 경우 시간 간격을 매일 오전 6시에서 오후 11시 사이로 설정할 수 있지만, 당일 오후 6시부터 익일 오전 11시까지로 설정할 수 없습니다. 후자의 경우 Cisco ISE에서 시간 범위가 유효하지 않다는 오류 메시지를 표시합니다.

참고 외부 관리자(예: Active Directory 관리자)가 email-id 필드를 채우지 않고 예약된 보고서를 생성하는 경우 이메일 알림이 전송되지 않습니다.

다음 보고서는 예약할 수 없습니다.

- 인증 요약(Authentication Summary)
- 상태 요약
- RBACL 삭제 요약
- 게스트 스폰서 요약
- Endpoint Profile Changes(엔드포인트 프로파일 변경)
- 네트워크 디바이스 세션 상태

참고 PAN에서만 Cisco ISE 보고서를 저장하거나 예약(맞춤화)할 수 있습니다.

참고 iI 기본 MnT가 다운되면 보조 MnT에서 예약된 보고서 작업을 실행합니다. 예약된 보고서 작업은 기본 MnT 및 보조 MnT에서 모두 실행됩니다. 보조 MnT에서는 내보내기 작업을 실행하기 전에 기본 MnT에 대해 ping을 시도합니다. ping이 실패할 경우 내보내기 작업만 실행되며, 그렇지 않으면 내보내기 작업을 건너뜁니다.

단계 **1** Running and Viewing Reports(보고서 실행 및 보기) 섹션의 설명에 따라 보고서를 실행합니다.

단계 **2** Report Summary(보고서 요약) 페이지의 오른쪽 상단에 있는 **My Reports(**내 보고서**)**를 클릭합니다.

단계 **3** 대화 상자에서 필요한 세부정보를 입력합니다.

단계 **4** **Save as New(**새 이름으로 저장**)**를 클릭합니다.

저장된 보고서로 돌아오면 모든 필터 옵션이 기본적으로 선택되어 있습니다. 사용하지 않으려는 필터는 선택을 취소하십시오.

My Reports(내 보고서**)** 범주에서 저장된 보고서를 제거할 수도 있습니다.

Cisco ISE 활성 RADIUS 세션

Cisco ISE는 라이브 세션을 위해 활성 RADIUS 세션을 동적으로 제어하는 데 사용할 수 있는 동적 CoA(Change of Authorization) 기능을 제공합니다. 다음 작업을 수행하도록 다시 인증 또는 연결 끊기 요청을 NAD(Network Access Device)로 보낼 수 있습니다.

- 인증과 관련된 문제 해결 - Session reauthentication(세션 재인증) 옵션을 사용하여 다시 재인증하려는 시도에 대한 후속 조치를 취할 수 있습니다. 그러나 이 옵션을 사용하여 액세스를 제한해서는 안 됩니다. 액세스를 제한하려면 종료 옵션을 사용해 주십시오.
- 문제가 있는 호스트 차단 - 네트워크를 통해 대량의 트래픽을 보내는 감염된 호스트를 차단하는 포트 종료 옵션과 함께 세션 종료를 사용할 수 있습니다. 그러나 RADIUS 프로토콜은 현재 종료된 포트를 다시 활성화하는 방법을 지원하지 않습니다.
- 엔드포인트가 IP 주소를 다시 가져오도록 강제 실행 - 신청자 또는 클라이언트가 없는 엔드포인트가 VLAN 변경 후 DHCP 요청을 생성하도록 포트 바운스 옵션과 함께 세션 종료를 사용할 수 있습니다.
- 업데이트된 권한 부여 정책을 엔드포인트에 푸시 - 세션 재인증 옵션을 사용하여 기존 세션에서 관리자 재량에 따른 권한 부여 정책의 변경과 같이 업데이트된 정책 컨피그레이션을 시행할 수 있습니다. 예를 들어 포스처 검증이 활성화된 경우 엔드포인트가 처음에 액세스 권한을 얻을 때 일반적으로 격리됩니다. 엔드포인트의 ID 및 포스처가 알려진 경우 엔드포인트가 해당 포스처

를 기준으로 실제 권한 부여 정책을 얻을 수 있도록 세션 재인증 명령을 엔드포인트로 보낼 수 있습니다.

CoA 명령이 디바이스에 인식되려면 옵션을 적절히 구성해야 합니다.

CoA가 제대로 작동하려면 동적 CoA(Change of Authorization)가 필요한 각 디바이스의 공유 암호를 구성해야 합니다. Cisco ISE는 공유 암호 컨피그레이션을 사용하여 디바이스에서 액세스를 요청하고 CoA 명령을 실행합니다.

참고 이 Cisco ISE 릴리스에서 표시될 수 있는 활성 인증 엔드포인트 세션의 최대 수는 100,000으로 제한됩니다.

관련 항목

RADIUS 세션에 대한 권한 부여 변경, 44 페이지

RADIUS 세션에 대한 권한 부여 변경

네트워크의 일부 네트워크 액세스 디바이스는 다시 로드한 후 계정 중지 또는 계정 끄기 패킷을 전송하지 않을 수도 있습니다. 이로 인해 세션 디렉토리 보고서에 세션이 두 개 표시될 수 있습니다. 두 세션 중 하나는 만료된 세션입니다.

활성 RADIUS 세션의 권한 부여를 동적으로 변경하거나 활성 RADIUS 세션의 연결을 끊으려면 가장 최근 세션을 선택해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **RADIUS Livelog(RADIUS** 라이브 로그**)**.

단계 **2** 보기를 **Show Live Session(**라이브 세션 표시**)**으로 전환합니다.

단계 **3** CoA를 실행할 RADIUS 세션의 CoA 링크를 클릭하고 다음 옵션 중 하나를 선택합니다.

- **SAnet Session Query(SAnet** 세션 쿼리**)** - SAnet 지원 디바이스에서 세션에 대한 정보를 쿼리하려면 이 옵션을 사용합니다.
- **Session reauthentication(**세션 재인증**)** - 세션을 재인증합니다. CoA를 지원하는 ASA 디바이스에서 설정된 세션에 대해 이 옵션을 선택하면 세션 정책 푸시 CoA가 호출됩니다.
- **Session reauthentication with last(**마지막 방법으로 세션 재인증**)** - 이 세션에 대해 마지막으로 성공한 인증 방법을 사용합니다.
- **Session reauthentication with rerun(**다시 실행하여 세션 재인증**)** - 구성된 인증 방법을 처음부터 실행합니다.

  참고 **Session reauthentication with last(**마지막 방법으로 세션 재인증**)** 및 **Session reauthentication with rerun(**다시 실행하여 세션 재인증**)** 옵션은 현재 Cisco iOS 소프트웨어에서 지원되지 않습니다.

- **Session termination(**세션 종료**)** - 세션을 종료합니다. 이 스위치를 선택하면 다른 세션에서 클라이언트가 재인증됩니다.
- **Session termination with port bounce(**포트를 반송하고 세션 종료**)** - 세션을 종료하고 포트를 다시 시작합니다.

- **Session termination with port shutdown(**포트를 종료하고 세션 종료**)** - 세션과 포트를 종료합니다.

단계 **4** **Run(**실행**)**을 클릭하여 선택한 재인증 또는 종료 옵션으로 CoA를 실행합니다.

CoA가 실패하는 경우 다음 원인 중 하나 때문일 수 있습니다.

- 디바이스가 CoA를 지원하지 않습니다.
- ID 또는 권한 부여 정책이 변경되었습니다.
- 공유 암호가 일치하지 않습니다.

사용 가능한 보고서

다음 표에는 미리 구성된 보고서가 범주에 따라 그룹화되어 있습니다. 보고서 기능 및 로깅 범주에 대한 설명도 제공됩니다.

로깅 범주에 대한 시스템 로그를 생성하려면 해당 **Log Severity Level(**로그 심각도 레벨**)**을 **Info(**정보**)**로 설정합니다.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**.
- 시스템 로그를 생성해야 하는 로깅 범주를 클릭합니다.
- **Log Severity Level(**로그 심각도 레벨**)** 필드의 드롭다운 메뉴에서 **Info(**정보**)**를 선택합니다.
- **Save(**저장**)**를 클릭합니다.

참고 Cisco ISE 릴리스 2.6 이상에서는 IPv6 주소를 사용하는 사용자의 감사 보고서에 로그인/로그아웃, 비밀번호 변경, 운영 변경 사항과 같은 이벤트가 기록됩니다. Administrator Logins(관리자 로그인), User Change Password Audit(사용자 비밀번호 변경 감사) 및 Operations Audit(작업 감사) 보고서에서 이제 IPv4 및 IPv6 기록을 기준으로 로그를 필터링할 수 있습니다.

보고서 이름	설명	로깅 범주
감사		

보고서 이름	설명	로깅 범주
적응형 네트워크 제어 감사	적응형 네트워크 제어 감사 보고서는 RADIUS 계정 관리를 기반으로 합니다. 각 엔드포인트에 대한 모든 네트워크 세션의 기록 보고 정보를 표시합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증) 및 RADIUS Accounting(RADIUS 계정 관리)을 선택합니다.
관리자 로그인	관리자 로그인 보고서는 모든 GUI 기반 관리자 로그인 이벤트와 성공한 CLI 로그인 이벤트에 대한 정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Administrative and Operational audit(관리 및 운영 감사).
컨피그레이션 변경 감사	컨피그레이션 변경 감사 보고서에서는 지정된 기간 내의 컨피그레이션 변경 사항에 대한 세부정보를 제공합니다. 특정 기능 문제를 해결해야 하는 경우 이 보고서를 통해 최근의 컨피그레이션 변경이 문제에 영향을 미쳤는지 확인할 수 있습니다.	

보고서 이름	설명	로깅 범주
데이터 비우기 감사	데이터 비우기 감사 보고서에서는 로깅 데이터가 비우기될 때 이를 기록합니다. 이 보고서에는 두 개의 데이터 비우기 소스가 반영됩니다. 매일 오전 4시에 Cisco ISE는 Administration(관리) > Maintenance(유지 관리) > Data Purging(데이터 비우기) 페이지에 설정한 기준을 충족하는 로깅 파일이 있는지 확인합니다. 있는 경우 파일이 삭제되고 이 보고서에 기록됩니다. 또한 Cisco ISE는 지속적으로 로그 파일의 저장 공간 중 사용된 공간을 최대 80%로 유지합니다. Cisco ISE는 매시간마다 이 비율을 확인하고 80% 임계값에 다시 도달할 때까지 가장 오래된 데이터를 삭제합니다. 이 정보도 이 보고서에 기록됩니다. 디스크 공간 사용률이 높은 경우 80% 임계값에 도달할 때 `ISE Monitor node(s) is about to exceed the maximum amount allocated`라는 알림 메시지가 표시됩니다. 그런 다음 90% 임계값에 도달할 때 `ISE Monitor node(s) has exceeded the maximum amount allocated`라는 알림 메시지가 표시됩니다.	—
엔드포인트 제거 활동	엔드포인트 제거 활동 보고서에서는 엔드포인트 제거 활동 기록을 검토할 수 있습니다. 이 보고서를 사용하려면 Profiler(프로파일러) 로깅 범주를 활성화해야 합니다. 이 범주는 기본적으로 활성화되어 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Profiler(프로파일러)를 선택합니다.

보고서 이름	설명	로깅 범주
내부 관리자 요약	내부 관리자 요약 보고서에서는 관리자 사용자의 자격을 확인할 수 있습니다. 이 보고서에서는 관리자 로그인 및 컨피그레이션 변경 감사 보고서에도 액세스할 수 있습니다. 이러한 보고서에서는 각 관리자에 대한 세부정보를 볼 수 있습니다.	—
운영 감사	운영 감사 보고서에서는 백업 실행, Cisco ISE 노드 등록 또는 애플리케이션 다시 시작 등 작동 변경에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Administrative and Operational audit(관리 및 운영 감사).
pxGrid 관리자 감사	pxGrid 관리자 감사 보고서에서는 클라이언트 등록, 클라이언트 등록 취소, 클라이언트 승인, 항목 생성, 항목 삭제, 기본 PAN에서의 게시자-구독자 추가 및 게시자-구독자 삭제 등의 pxGrid 관리 작업에 대한 세부정보를 제공합니다. 각 기록에는 노드에 대한 작업을 수행한 관리자 이름이 있습니다. 관리자 및 메시지 기준에 따라 pxGrid 관리자 감사 보고서를 필터링할 수 있습니다.	—
보안 통신 감사	보안 통신 감사 보고서는 Cisco ISE 관리 CLI의 보안 관련 이벤트에 대한 감사 세부정보를 제공합니다. 여기에는 인증 장애, 침입 시도 가능성, SSH 로그인, 장애가 발생한 비밀번호, SSH 로그아웃, 잘못된 사용자 계정 등이 포함됩니다.	—
사용자 변경 비밀번호 감사	사용자 변경 비밀번호 감사 보고서에서는 직원의 비밀번호 변경에 대한 확인을 표시합니다.	Administrative and Operational audit(관리 및 운영 감사)

보고서 이름	설명	로깅 범주
Trustsec 감사	Trustsec 감사 로그에는 다음이 포함됩니다. • Trustsec 구성 요소의 관리(생성, 이름 변경, 업데이트 및 삭제) • Trustsec이 활성화된 NAD에 SGACL 및 SGT 구축 • Trustsec 세션. Cisco ISE가 Cisco DNA Center와 통합되어 있고 SD Access가 Cisco DNA Center에서 관리되는 경우 이 로그는 비어 있습니다.	—
디바이스 관리		
인증 요약(Authentication Summary)	TACACS Authentication Summary(TACACS 인증 요약) 보고서는 가장 일반적인 인증 및 인증 실패 이유에 대한 세부정보를 제공합니다.	—
TACACS 계정 관리	TACACS 계정 관리 보고서는 디바이스 세션에 대한 계정 관리 세부정보를 제공합니다. 사용자와 디바이스의 생성된 시간 및 기록된 시간 관련 정보가 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 TACACS Accounting(TACACS 계정 관리)을 선택합니다.
Top N Authentication by Failure Reason(실패 이유별 상위 N 인증)	Top N Authentication by Failure Reason(실패 이유별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 실패 이유별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증)	Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 네트워크 디바이스별 통과 및 실패한 인증 수가 표시됩니다.	—

보고서 이름	설명	로깅 범주
Top N Authentication by User(사용자별 상위 N 인증)	Top N Authentication by User(사용자별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 사용자 이름별 통과 및 실패한 인증 수가 표시됩니다.	—
Diagnostics(진단**)**		
AAA 진단	AAA 진단 보고서에서는 Cisco ISE와 사용자 간의 모든 네트워크 세션에 대한 세부정보를 제공합니다. 사용자가 네트워크에 액세스할 수 없는 경우 이 보고서를 검토하여 트렌드를 파악하고 문제를 특정 사용자와 격리할 수 있는지, 아니면 좀 더 광범위한 문제로 나타낼 수 있는지 식별할 수 있습니다. 참고 때때로 ISE는 사용자 인증이 진행 중인 경우에 엔드포인트의 계정 관리 중지 요청을 자동으로 취소합니다. 그러나 ISE는 사용자 인증이 완료되고 나면 모든 계정 관리 요청을 승인합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Policy Diagnostics(정책 진단), Identity Stores Diagnostics(ID 저장소 진단), Authentication Flow Diagnostics(인증 플로우 진단) 및 RADIUS Diagnostics(RADIUS 진단) 로깅 범주를 선택합니다.
AD Connector 운영	AD Connector 운영 보고서에서는 Cisco ISE 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 관리 관리 등 AD Connector에서 수행된 작업 로그를 제공합니다. 일부 AD 장애가 발생하면 이 보고서의 세부정보를 검토하여 가능한 원인을 식별할 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 AD Connector를 선택합니다.

보고서 이름	설명	로깅 범주
Endpoint Profile Changes(엔드포인트 프로파일 변경)	엔드포인트별 상위 권한 부여(MAC 주소) 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 엔드포인트 MAC 주소에 대한 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
상태 요약	상태 요약 보고서에서는 대시보드와 유사한 세부정보를 제공합니다. 그러나 대시보드에는 지난 24시간 동안의 데이터만 표시되지만 이 보고서에서는 더 자세한 기록 데이터를 검토할 수 있습니다. 이 데이터를 평가하여 데이터의 일관된 패턴을 확인할 수 있습니다. 예를 들어 대부분의 직원이 하루 일과를 시작하는 시점에 CPU 사용량이 증가할 것을 예측할 수 있습니다. 이러한 트렌드의 불일치가 발견되는 경우 잠재적 문제를 식별할 수 있습니다. CPU Usage(CPU 사용량) 표에는 다양한 Cisco ISE 기능의 CPU 사용량 백분율이 나열됩니다. **show cpu usage** CLI 명령의 출력이 이 표에 나와 있으며, 이러한 값을 구축 내 문제와 연결하여 문제 원인을 식별할 수 있습니다.	—

보고서 이름	설명	로깅 범주
ISE 카운터	ISE Counters(ISE 카운터) 보고서에는 다양한 속성에 대한 임계값이 나열됩니다. 이러한 다양한 속성의 값은 서로 다른 간격으로 수집되며 데이터는 표 형식으로 표시됩니다. 하나는 5분 간격이고 다른 하나는 5분 초과 간격입니다. 이 데이터를 평가하여 추세를 확인할 수 있으며, 임계값보다 높은 값이 있는 경우 이 정보를 구축의 문제와 연관시켜 가능한 원인을 파악할 수 있습니다. Cisco ISE는 기본적으로 이러한 속성의 값을 수집합니다. Cisco ISE CLI에서 **application configure ise** 명령을 사용하여 이 데이터 수집을 비활성화하도록 선택할 수 있습니다. 옵션 14를 선택하여 카운터 속성 수집을 활성화하거나 비활성화하십시오.	—
핵심 성능 메트릭	Key Performance Metrics(핵심 성능 메트릭) 보고서는 구축에 연결되는 엔드포인트 수 및 각 PSN에서 시간 단위로 처리되는 RADIUS 요청 수에 대한 통계 정보를 제공합니다. 이 보고서는 서버의 평균 로드, 요청당 평균 레이턴시 및 초당 평균 트랜잭션을 나열합니다.	—

보고서 이름	설명	로깅 범주
잘못 구성된 NAS	잘못 구성된 NAS 보고서에서는 일반적으로 계정 관리 정보를 빈번하게 전송하는 경우 계정 관리 빈도가 부정확한 NAD에 대한 정보를 제공합니다. 정정 작업을 수행하고 잘못 구성된 NAD를 수정한 경우 보고서에는 수정 승인이 표시됩니다. 참고 이 보고서를 실행하려면 RADIUS 억제를 활성화해야 합니다.	—
잘못 구성된 신청자	잘못 구성된 신청자 보고서에서는 특정 신청자가 수행한 실패한 시도에 따른 통계와 함께 잘못 구성된 신청자 목록을 제공합니다. 정정 작업을 수행하고 잘못 구성된 신청자를 수정한 경우 보고서에는 수정 승인이 표시됩니다. 참고 이 보고서를 실행하려면 RADIUS 억제를 활성화해야 합니다.	—
네트워크 디바이스 세션 상태	네트워크 디바이스 세션 상태 요약 보고서를 사용하면 스위치에 직접 로그인하지 않고도 스위치 컨피그레이션을 표시할 수 있습니다. Cisco ISE는 SNMP 쿼리를 사용하여 이러한 세부정보에 액세스하므로 SNMP v1/v2c를 사용하여 네트워크 디바이스를 구성해야 합니다. 사용자에게 네트워크 문제가 발생하는 경우 이 보고서를 사용하면 해당 문제가 Cisco ISE가 아니라 스위치 컨피그레이션과 관련된 문제인지 쉽게 파악할 수 있습니다.	—

보고서 이름	설명	로깅 범주
OCSP 모니터링	OCSP 모니터링 보고서에서는 OCSP(Online Certificate Status Protocol) 서비스의 상태를 지정합니다. Cisco ISE가 성공적으로 인증서 서버에 연결하고 인증서 상태 감사를 제공할수 있는지 여부를 나타냅니다. Cisco ISE에서 수행하는 모든 OCSP 인증서 검증 작업에 대한 요약정보를 제공합니다. OCSP 서버에서 정상 상태 및 취소된 기본/보조 인증서와 관련된 정보를 검색합니다. Cisco ISE는 응답을 캐시하고 이를 이후의 OCSP 모니터링 보고서를 활용하는 데 활용합니다. 캐시가 지워지면 OCSP 서버에서 정보를 검색합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 System Diagnostics(시스템 진단).
RADIUS 오류	RADIUS Errors(RADIUS 오류) 보고서에서는 RADIUS 요청 삭제됨(알 수 없는 네트워크 액세스 디바이스에서 버려진 인증/계정 관리 요청), EAP 연결 시간 초과 및 알 수 없는 NAD를 확인할 수 있습니다. 참고 지난 5일 동안의 보고서만 볼 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Failed Attempts(실패한 시도)를 선택합니다.

보고서 이름	설명	로깅 범주
시스템 진단	시스템 진단 보고서에서는 Cisco ISE 노드의 상태에 대한 세부정보를 제공합니다. Cisco ISE 노드를 등록할 수 없는 경우 이 보고서를 검토하여 문제를 해결할 수 있습니다. 이 보고서를 사용하려면 먼저 여러 진단 로깅 범주를 활성화해야 합니다. 이러한 로그를 수집하는 경우 Cisco ISE 성능에 부정적 영향을 줄 수 있습니다. 그러므로 이러한 범주는 기본적으로 활성화되어 있지 않으므로 데이터를 수집하는 기간 동안만 활성화해야 합니다. 그렇지 않으면, 30분 후에 자동으로 비활성화됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택한 후에 Internal Operations Diagnostics(내부 운영 진단), Distributed Management(분산형 관리), Administrator Authentication and Authorization(관리자 인증 및 권한 부여) 로깅 범주를 선택합니다.
엔드포인트 및 사용자		
인증 요약(Authentication Summary)	인증 요약(Authentication Summary) 보고서는 RADIUS 인증을 기반으로 합니다. 가장 일반적인 인증과 함께 인증 실패에 대한 이유를 확인할 수 있습니다. 예를 들어 한 Cisco ISE 서버가 다른 서버에 비해 훨씬 많은 인증을 처리하고 있는 경우 향상된 로드 밸런싱을 위해 사용자를 다른 Cisco ISE 서버에 다시 할당해야 할 수 있습니다. 참고 인증 요약(Authentication Summary) 보고서 또는 대시보드에는 실패했거나 성공한 인증에 해당하는 최신 데이터가 수집되어 표시되므로, 보고서 내용이 표시될 때까지는 몇 분 정도 걸립니다.	—
에이전트리스 포스처	에이전트리스 포스처를 실행한 모든 엔드포인트를 나열합니다.	

보고서 이름	설명	로깅 범주
클라이언트 프로비저닝	클라이언트 프로비저닝 보고서에는 특정 엔드포인트에 적용된 클라이언트 프로비저닝 에이전트가 표시됩니다. 이 보고서를 사용하여 각 엔드포인트에 적용된 정책을 검토하여 엔드포인트가 올바르게 프로비저닝되었는지 여부를 확인할 수 있습니다. 참고 엔드포인트가 ISE와 연결되지 않거나(세션이 설정되지 않음) NAT(Network Address Translation) 주소가 세션에 사용되는 경우 엔드포인트의 MAC 주소가 엔드포인트 ID 열에 표시되지 않습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Client Provisioning Audit and Posture(포스처 및 클라이언트 프로비저닝 감사 및 포스처) 및 Client Provisioning Diagnostics(클라이언트 프로비저닝 진단)를 선택합니다.
현재 활성 세션	현재 활성 세션 보고서를 사용하면 지정된 기간 내에 현재 네트워크에 있는 사용자에 대한 세부정보가 포함된 보고서를 내보낼 수 있습니다. 사용자가 네트워크에 액세스하지 않은 경우에는 세션이 인증 또는 종료되었는지 확인하거나 세션에 다른 문제가 있는지 확인할 수 있습니다.	—
엔드포인트 스크립트 프로비저닝 요약	**Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)** 창에는 지난 30일간 엔드포인트 스크립트 마법사를 통해 실행된 작업의 세부정보가 표시됩니다.	—

보고서 이름	설명	로깅 범주
외부 모바일 디바이스 관리	외부 모바일 디바이스 관리 보고서에서는 Cisco ISE와 외부 MDM(Mobile Device Management) 서버 간 통합에 대한 세부정보를 제공합니다. 이 보고서를 사용하면 MDM 서버에 직접 로그인하지 않고도 MDM 서버에서 프로비저닝된 엔드포인트를 확인할 수 있습니다. 등록 및 MDM 규정 준수 상태 등에 대한 정보도 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 MDM을 선택합니다.
패시브 ID	Passive ID(패시브 ID) 보고서에서는 도메인 컨트롤러에 대한 WMI 연결의 상태를 모니터링하고 그와 관련된 통계(예: 수신된 알림 개수, 초당 사용자 로그인/로그아웃 수 등)를 수집할 수 있습니다. 참고 이 방법으로 인증된 세션의 보고서에는 인증 세부정보가 없습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Identity Mapping(ID 매핑)을 선택합니다.
수동 인증서 프로비저닝	수동 인증서 프로비저닝 보고서에는 인증서 프로비저닝 포털을 통해 수동으로 프로비저닝한 모든 인증서가 나열됩니다.	—
조건별 Posture Assessment	조건별 Posture Assessment 보고서를 사용하면 ISE에 구성되어 있는 포스처 정책 조건을 기준으로 기록을 확인하여 클라이언트 머신에서 최신 보안 설정 또는 애플리케이션을 사용할 수 있는지를 검증할 수 있습니다.	—

보고서 이름	설명	로깅 범주
엔드포인트별 Posture Assessment	Posture Assessment by Endpoint(엔드포인트별 포스처 평가) 보고서는 엔드포인트의 시간, 상태, PRA 작업 등의 자세한 정보를 제공합니다. **Details(**세부정보**)**를 클릭하여 엔드포인트에 대한 자세한 정보를 볼 수 있습니다. 참고 Posture Assessment by Endpoint(엔드포인트별 포스처 평가) 보고서는 엔드포인트의 애플리케이션 및 하드웨어 속성에 대한 포스처 정책 세부정보는 제공하지 않습니다. 이 정보는 Context Visibility(상황 가시성) 페이지에서만 볼 수 있습니다.	—
프로파일링된 엔드포인트 요약	프로파일링된 엔드포인트 요약 보고서는 네트워크에 액세스하는 엔드포인트에 대한 프로파일링 세부정보를 제공합니다. 참고 Cisco IP-Phone과 같이 세션 시간을 등록하지 않는 엔드포인트의 경우 Not Applicable(해당 없음)이 Endpoint session time(엔드포인트 세션 시간) 필드에 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Profiler(프로파일러)를 선택합니다.

보고서 이름	설명	로깅 범주
RADIUS 계정 관리	RADIUS Accounting Report에서는 네트워크에서 사용자가 유지된 기간을 식별합니다. 사용자의 네트워크 액세스가 손실되면 이 보고서를 사용하여 Cisco ISE가 네트워크 연결 문제의 원인인지 확인할 수 있습니다. 참고 임시 업데이트에 지정된 세션의 IPv4 또는 IPv6 주소 변경 사항 정보가 포함되어 있는 경우 RADIUS 계정 관리 임시 업데이트가 RADIUS 계정 관리 보고서에 포함됩니다.	
RADIUS 인증	RADIUS 인증 보고서에서는 인증 실패 및 성공 기록을 검토할 수 있습니다. 사용자가 네트워크에 액세스할 수 없는 경우 이 보고서의 세부정보를 검토하여 가능한 원인을 식별할 수 있습니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증) 및 Failed Attempts(실패한 시도) 로깅 범주를 선택합니다.
등록된 엔드포인트	등록된 엔드포인트 보고서에는 직원이 등록한 모든 개인 디바이스를 표시합니다.	—
거부된 엔드포인트	Rejected Endpoints(거부된 엔드포인트) 보고서에는 직원이 등록하고 거부되거나 릴리스된 모든 개인 디바이스가 나열됩니다.	—
신청자 프로비저닝	신청자 프로비저닝 보고서에서는 직원의 개인 디바이스에 프로비저닝된 신청자에 대한 세부정보를 제공합니다.	Posture and Client Provisioning Audit(포스처 및 클라이언트 프로비저닝 감사)

보고서 이름	설명	로깅 범주
엔드포인트별 상위 권한 부여	엔드포인트별 상위 권한 부여(MAC 주소) 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 엔드포인트 MAC 주소에 대한 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
사용자별 상위 권한 부여	사용자별 상위 권한 부여 보고서에서는 네트워크에 액세스할 수 있도록 Cisco ISE가 각 사용자에게 권한을 부여한 횟수를 표시합니다.	Passed authentications(통과한 인증), Failed Attempts(실패한 시도)
액세스 서비스별 상위 N 인증	Top N Authentication by Access Service(액세스 서비스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 액세스 서비스 유형별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Failure Reason(실패 이유별 상위 N 인증)	Top N Authentication by Failure Reason(실패 이유별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 실패 이유별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증)	Top N Authentication by Network Device(네트워크 디바이스별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 네트워크 디바이스별 통과 및 실패한 인증 수가 표시됩니다.	—
Top N Authentication by User(사용자별 상위 N 인증)	Top N Authentication by User(사용자별 상위 N 인증) 보고서에는 선택한 매개변수를 기준으로 특정 기간 동안 사용자 이름별 통과 및 실패한 인증 수가 표시됩니다.	—
게스트		

보고서 이름	설명	로깅 범주
AUP 수락 상태	AUP 수락 상태 보고서에서는 모든 게스트 포털의 AUP 수락에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Guest(게스트)를 선택합니다.
게스트 계정 관리	게스트 계정 보고서는 RADIUS 계정 보고서의 하위 집합입니다. 활성화된 게스트 또는 게스트 ID 그룹에 할당된 모든 사용자는 이 보고서에 표시됩니다.	—

보고서 이름	설명	로깅 범주
기본 게스트 보고서	Primary(기본) Guest(게스트) 보고서에는 다양한 게스트 액세스 보고서의 데이터가 결합되어 있으며 다양한 보고 소스의 데이터를 내보낼 수 있습니다. Primary(기본) Guest(게스트) 보고서에서는 게스트 사용자가 방문하는 웹사이트에 대한 세부정보도 제공합니다. 보안 감사용으로 이 보고서를 사용하여 게스트 사용자가 네트워크에 액세스한 시기, 그리고 어떤 작업을 수행했는지 살펴볼 수 있습니다. 또한 게스트 트래픽에 사용된 NAD(Network Access Device)에 대한 HTTP 검사도 활성화해야 합니다. 이 정보는 NAD에 의해 Cisco ISE로 다시 보내집니다. 클라이언트가 최대 동시 세션 제한에 도달하는 시기를 확인하려면 관리 포털에서 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**를 선택하고 다음을 수행합니다. **1.** "Authentication Flow Diagnostics(인증 플로우 진단)" 로깅 범주의 로그 레벨을 WARN에서 INFO로 높입니다. **2.** AAA Diagnostics(AAA 진단)의 "Logging Category(로깅 범주)"에서 LogCollector Target(LocCollector 타깃)을 Available(사용 가능한 항목)에서 Selected(선택한 항목)로 변경합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Logging(**로깅**) > Logging Categories(**로깅 범주**)**를 선택하고 Passed Authentications(통과한 인증)를 선택합니다.

보고서 이름	설명	로깅 범주
내 디바이스 로그인 및 감사	내 디바이스 로그인 및 감사 보고서에서는 내 디바이스 포털에서 디바이스에 대해 사용자가 수행한 로그인 활동 및 작업에 대한 세부정보를 제공합니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 My Devices(내 디바이스)를 선택합니다.
스폰서 로그인 및 감사	스폰서 로그인 및 감사 보고서에서는 게스트 사용자의 로그인, 추가, 삭제, 활성화, 일시 중지 및 업데이트 작업과 함께 스폰서 포털에서의 스폰서의 로그인 활동에 대한 세부정보를 제공합니다. 게스트 사용자가 대량으로 추가된 경우 '게스트 사용자' 열 아래 표시됩니다. 이 열은 기본적으로 숨겨져 있습니다. 내보내기 시에 이러한 대량 사용자는 내보내는 파일에도 표시됩니다.	Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 선택하고 Guest(게스트)를 선택합니다.
SXP		
SXP 바인딩	SXP 바인딩 보고서는 SXP 연결을 통해 교환되는 IP-SGT 바인딩에 대한 정보를 제공합니다.	—
SXP 연결	이 보고서를 사용하여 SXP 연결의 상태를 모니터링하고 피어 IP, SXP 노드 IP, VPN 이름, SXP 모드 등 해당 연결과 관련된 정보를 수집할 수 있습니다.	—
TrustSec		

보고서 이름	설명	로깅 범주
RBACL 삭제 요약	RBACL 삭제 요약 보고서는 고급 Cisco ISE 라이선스가 있는 경우에만 사용할 수 있는 TrustSec 기능과 관련된 보고서입니다. 또한 이 보고서를 사용하려면 삭제된 이벤트에 해당하는 NetFlow 이벤트를 Cisco ISE로 보내도록 네트워크 디바이스를 구성해야 합니다. 사용자가 특정 정책 또는 액세스를 위반하는 경우 패킷이 삭제되고 이 보고서에 표시됩니다. 참고 RBACL 삭제 패킷 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.	—
사용자별 상위 N개 RBACL 삭제	사용자별 상위 N개 RBACL 삭제 보고서는 고급 Cisco ISE 라이선스가 있는 경우에만 사용할 수 있는 TrustSec 기능과 관련된 보고서입니다. 또한 이 보고서를 사용하려면 삭제된 이벤트에 해당하는 NetFlow 이벤트를 Cisco ISE로 보내도록 네트워크 디바이스를 구성해야 합니다. 이 보고서에는 특정 사용자에 의한 정책 위반(패킷 삭제 기준)이 표시됩니다. 참고 RBACL 삭제 패킷 플로우는 Cisco Catalyst 6500 시리즈 스위치에서만 사용할 수 있습니다.	—

보고서 이름	설명	로깅 범주
TrustSec ACI	이 보고서에는 APIC의 IEPG, EEPG, 엔드포인트 및 서브넷 컨피그레이션과 동기화된 SGT 및 SXP 매핑이 나열됩니다. 이러한 세부정보는 TrustSec APIC 통합 기능이 활성화되어 있어야 표시됩니다.	—

보고서 이름	설명	로깅 범주
TrustSec 구축 확인		—

보고서 이름	설명	로깅 범주
	이 보고서를 사용하여 최신 TrustSec 정책이 모든 네트워크 디바이스에 구축되었는지 또는 Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치 사항이 있는지 확인할 수 있습니다. **Details(**세부정보**)** 아이콘을 클릭하여 확인 프로세스의 결과를 확인합니다. 다음과 같은 세부정보를 확인할 수 있습니다. • 확인 프로세스가 시작 및 완료된 시점 • 최신 TrustSec 정책이 네트워크 디바이스에 성공적으로 구축되었는지 여부. 최신 TrustSec 정책이 구축된 네트워크 디바이스의 이름 및 IP 주소도 볼 수 있습니다. • Cisco ISE와 네트워크 디바이스에 구성된 정책 간에 불일치 사항이 있는지 여부. 각 정책 차이에 대해 디바이스 이름, IP 주소, 해당 오류 메시지가 표시됩니다. **Alarms(**경보**)** dashlet(**Work Centers(**작업 센터**) > TrustSec > Dashboard(**대시보드**)** 및 **Home(**홈**) > Summary(**요약**)**에 있음)에서 TrustSec Deployment Verification(TrustSec 구축 확인) 경보를 볼 수 있습니다. 참고 • 보고에 소요되는 시간은 구축에 포함된 네트워크 디바이스 및 TrustSec 그룹 수에 따라 달라집니다. • TrustSec Deployment	

보고서 이름	설명	로깅 범주
	Verification(TrustSec 구축 확인) 보고서의 오류 메시지 길이는 현재 480자로 제한됩니다. 480자를 초과하는 오류 메시지는 잘리고 처음 480자만 보고서에 표시됩니다.	
TrustSec 정책 다운로드	이 보고서에는 정책(SGT/SGACL) 다운로드를 위해 네트워크 디바이스에서 전송한 요청과 ISE에서 전송한 세부정보가 나열됩니다. 워크플로우 모드가 활성화되어 있으면 프로덕션 또는 스테이징 매트릭스에 대한 요청을 필터링할 수 있습니다.	이 보고서를 보려면 다음을 수행해야 합니다. **1.** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**. **2.** **AAA Diagnostics(AAA** 진단**)** > **RADIUS Diagnostics(RADIUS** 진단**)**를 선택합니다. **3.** RADIUS 진단의 경우 Log Severity Level(로그 심각도 레벨)을 DEBUG로 설정합니다.
Threat Centric NAC 서비스		
어댑터 상태	어댑터 상태 보고서에는 위협 및 취약점 어댑터의 상태가 표시됩니다.	—
COA 이벤트	엔드포인트에 대한 취약점 이벤트가 수신되면 Cisco ISE는 해당 엔드포인트에 대해 CoA를 트리거합니다. CoA 이벤트 보고서에는 이러한 CoA 이벤트의 상태가 표시됩니다. 또한 이전 권한 부여 규칙 및 새 권한 부여 규칙과 이러한 엔드포인트에 대한 프로파일 세부정보도 표시됩니다.	—

보고서 이름	설명	로깅 범주
위협 이벤트	Threat Events(위협 이벤트) 보고서는 Cisco ISE가 사용자가 구성한 다양한 어댑터에서 수신하는 모든 위협 이벤트의 목록을 제공합니다.	—
취약점 평가	취약점 평가 보고서는 엔드포인트에 대해 수행되는 평가와 관련된 정보를 제공합니다. 이 보고서를 보고 구성된 정책을 기준으로 평가가 수행되는지를 확인할 수 있습니다.	—

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 ***6: 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.

인증 레이턴시

인증 레이턴시는 인증 프로세스가 시작된 시점부터 RADIUS 인증 프로세스의 평균 응답 시간입니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Dashboard(**대시보드**)** > **System Summary(**시스템 요약**)** dashlet(대시릿).에서 Cisco ISE 인증 레이턴시를 확인할 수 있습니다.

드롭 다운 목록에서 다음 인증 레이턴시 기간을 선택할 수 있습니다.

- **60mins(60**분**)** :이 옵션은 지난 60분 동안 시작된 인증에 대한 인증 레이턴시를 제공합니다.
- **12hrs(12**시간**)** :이 옵션은 지난 24시간 동안 시작된 인증 프로세스에 대한 인증 레이턴시를 제공합니다.

표시되는 응답 시간은 밀리초(ms)입니다. 인증 레이턴시에 대한 자세한 보고서를 보려면 **Live Logs(**라이브 로그**)** 창에서 최신 로그를 클릭합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **RADIUS**.

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 ***7: 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.

필드 이름	설명
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.
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.

필드 이름	설명
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.
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).

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 ***8: 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.

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 ***9:*** 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.

필드 이름	설명
Filter Parameters(필터 파라미터**)**	보고서를 내보내는 동안 선택한 필터 파라미터를 표시합니다.
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.