구축

Cisco ISE 구축 용어

Cisco ISE 구축 시나리오에 대해 설명할 때 일반적으로 사용되는 용어는 다음과 같습니다.

- 서비스: 서비스는 네트워크 액세스, 프로파일러, 포스처, 보안 그룹 액세스, 모니터링, 문제 해결 등 페르소나가 제공하는 특정 기능입니다.
- 노드: 노드는 Cisco ISE 소프트웨어를 실행하는 개별 인스턴스입니다. Cisco ISE는 어플라이언스는 물론 VMware에서 실행될 수 있는 소프트웨어로도 사용 가능합니다. Cisco ISE 소프트웨어를 실행하는 각 인스턴스(어플라이언스 또는 VMware)를 노드라고 합니다.
- 페르소나: 노드 페르소나는 노드에서 제공하는 서비스를 결정합니다. Cisco ISE 노드는 관리, 정책 서비스, 모니터링 및 pxGrid 페르소나 중 하나를 취할 수 있습니다. 관리 포털을 통해 사용할 수 있는 메뉴 옵션은 Cisco ISE 노드에서 맡는 역할 및 페르소나에 따라 달라집니다.
- 구축 모델: 분산형 구축인지, 독립형 구축인지, 아니면 기본 2노드 구축에 해당하는 독립형 모드의 고가용성 구축인지 결정합니다.

분산형 Cisco ISE 구축의 페르소나

Cisco ISE 노드는 관리, 정책 서비스 또는 모니터링 페르소나를 취할 수 있습니다.

Cisco ISE 노드는 그 페르소나에 따라 다양한 서비스를 제공할 수 있습니다. 구축의 각 노드는 관리, 정책 서비스 및 모니터링 페르소나를 취할 수 있습니다. 분산형 구축에서는 네트워크에 다음과 같은 노드 조합이 있을 수 있습니다.

- 고가용성을 위한 기본 PAN(Policy Administration Node) 및 보조 PAN(Policy Administration Node)
- 고가용성을 위한 기본 MnT 노드(Monitoring Node) 및 보조 MnT 노드(Monitoring Node)
- 기본 PAN 자동 페일오버를 위한 상태 확인 노드 쌍 또는 단일 상태 확인 노드
- 세션 페일오버를 위한 하나 이상의 PSN(Policy Service Node)

환경 다운로드에 성공했으며, 결과에는 가동 및 실행 중인 Cisco ISE 노드만 포함됩니다.

Cisco ISE 노드 구성

Cisco ISE 노드를 설치하고 나면 관리, 정책 서비스 및 모니터링 페르소나가 제공하는 모든 기본 서비스가 해당 노드에서 실행됩니다. 이 노드는 독립형 상태가 됩니다. Cisco ISE 노드를 구성하려면 해당 노드의 관리 포털에 로그인해야 합니다. 독립형 Cisco ISE 노드의 페르소나 또는 서비스는 편집할 수 없습니다. 그러나 기본/보조 Cisco ISE 노드의 페르소나 및 서비스는 편집할 수 있습니다. 먼저 기본 ISE 노드를 구성한 후 기본 ISE 노드에 보조 ISE 노드를 등록해야 합니다.

노드에 처음 로그인하는 경우에는 기본 관리자 비밀번호를 변경하고 유효한 라이선스를 설치해야 합니다.

운영 환경에서 Cisco ISE에 구성된 호스트 이름 및 도메인 이름은 변경하지 않는 것이 좋습니다. 이러한 이름을 변경해야 하는 경우에는 어플라이언스를 재이미지화하고 변경한 다음, 초기 구축 중에 세부정보를 구성합니다.

시작하기 전에

Cisco ISE에서 분산형 구축이 설정되는 방식을 기본적으로 파악해야 합니다. 분산형 구축을 설정하기 위한 지침을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **2** 구성할 Cisco ISE 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** 필요한 대로 값을 입력하고 **Save(**저장**)**를 클릭합니다.

기본 PAN(Policy Administration Node) 구성

분산형 구축을 설정하려면 먼저 Cisco ISE 노드를 기본 PAN으로 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

처음에는 Register(등록) 버튼이 비활성화되어 있습니다. 이 버튼을 활성화하려면 기본 PAN을 구성해야 합니다.

단계 **2** 현재 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Make Primary(**기본으로 설정**)**를 클릭하여 기본 PAN을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭하여 노드 컨피그레이션을 저장합니다.

다음에 수행할 작업

1. 구축에 보조 노드를 추가합니다.
2. 필요한 경우 프로파일러 서비스를 활성화하고 프로브를 구성합니다.

보조 Cisco ISE 노드 등록

Cisco ISE 노드를 기본 PAN에 등록하여 멀티 노드 구축을 구성할 수 있습니다. 구축에서 기본 PAN이 아닌 노드들은 보조 노드라고 합니다. 노드를 등록하는 동안 노드에서 활성화해야하는 페르소나 및 서비스를 선택할 수 있습니다. 등록된 노드는 기본 PAN에서 관리할 수 있습니다(예: 노드 페르소나, 서비스, 인증서, 라이선스 관리, 패치 적용 등 관리).

노드를 등록할 때 기본 PAN이 보조 노드로 컨피그레이션 데이터를 전달하며 보조 노드의 애플리케이션 서버가 재시작됩니다. 전체 데이터가 전달되고 나면 기본 PAN에 적용한 추가 컨피그레이션 변

경 사항이 보조 노드에 복제됩니다. 보조 노드에 변경 사항을 복제하는 데 걸리는 시간은 네트워크 지연, 시스템의 로드 등 다양한 요인에 따라 달라집니다.

시작하기 전에

기본 PAN과 등록 대상 노드가 서로 DNS로 확인 가능한지 확인합니다. 등록 대상 노드에서 신뢰할 수 없는 자체 서명 인증서를 사용하는 경우 인증서 세부정보가 포함된 인증서 경고가 표시됩니다. 인증서를 수락하면 노드와의 TLS 통신을 활성화하기 위해 기본 PAN의 신뢰할 수 있는 인증서 저장소에 인증서가 추가됩니다.

노드가 자체 서명되지 않은 인증서(예: 외부 CA에서 서명하는 경우)를 사용하는 경우 해당 노드의 관련 인증서 체인을 기본 PAN의 신뢰할 수 있는 인증서 저장소에 수동으로 가져와야 합니다. 보조 노드의 인증서를 신뢰할 수 있는 인증서 저장소로 가져올 때는 PAN이 보조 노드의 인증서를 검증하도록 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 창에서 **Trust for Authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.

네트워크 액세스, 게스트, 포스처 등의 세션 서비스가 활성화된 노드를 등록하는 동안에는 이를 노드 그룹에 추가 할 수 있습니다. 자세한 내용은 정책 서비스 노드 그룹 생성, 58 페이지를 참조하십시오.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 보조 노드 등록을 시작하려면 **Register(**등록**)**를 클릭합니다.

단계 **4** 등록하려는 독립형 노드의 DNS 확인 가능 FQDN(Fully Qualified Domain Name)을 입력합니다(abc.xyz.com과 같이 호스트 이름.도메인 이름의 형식). 기본 PAN과 등록 대상 노드가 서로 확인 가능한지 확인합니다.

단계 **5** **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 보조 노드의 GUI 기반 관리자 자격 증명을 입력합니다.

단계 **6** **Next(**다음**)**를 클릭합니다.

기본 PAN이 등록 대상 노드와의 (최초) TLS 통신 설정을 시도합니다.

- 노드가 신뢰할 수 있는 인증서를 사용하는 경우 7단계를 진행할 수 있습니다.
- 노드에서 신뢰할 수 없는 자체 서명 인증서를 사용하는 경우 인증서 경고 메시지에는 인증서에 대한 세부정보(예: 발급 대상, 발급자, 일련번호 등)가 표시되며 이 정보를 노드의 실제 인증서와 비교하여 확인할 수 있습니다. **Import Certificate and Proceed(**인증서 가져 오기 및 진행**)** 옵션을 선택하여 이 인증서를 신뢰하고 등록을 계속할 수 있습니다. Cisco ISE는 해당 노드의 기본 자체 서명 인증서를 기본 PAN의 신뢰할 수 있는 인증서 저장소로 가져옵니다. 기본 자체 서명 인증서를 사용하지 않으려면 **Cancel Registration(**등록 취소**)**을 클릭하고 해당 노드의 관련 인증서 체인을 기본 PAN의 신뢰할 수 있는 인증서 저장소에 수동으로 가져옵니다. 보조 노드의 인증서를 신뢰할 수 있는 인증서 저장소로 가져올 때는 PAN이 보조 노드의 인증서를 검증하도록 **Trust for Authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.
- 노드가 CA 서명 인증서를 사용하는 경우, 인증서 신뢰가 설정될 때까지 등록을 진행할 수 없다는 오류 메시지가 표시됩니다.

단계 **7** 노드에서 활성화할 페르소나 및 서비스를 선택하고 **Save(**저장**)**를 클릭합니다.

노드가 등록되면 노드 구축에 노드가 추가되었음을 확인하는 경보가 기본 PAN에 생성됩니다. Cisco ISE GUI **Dashboard(**대시보드**)**의 **Alarms(**경보**)** 대시릿에서 이 경보를 볼 수 있습니다. 등록된 노드가 동기화되고 재시작된 후, 기본 PAN에 사용된 동일한 자격 증명을 사용하여 보조 노드 GUI에 로그인할 수 있습니다.

다음에 수행할 작업

- 게스트 사용자, 액세스/권한 부여, 로깅 등 시간이 중요한 작업의 경우에는 노드의 시스템 시간이 동기화되는지 확인합니다.
- 보조 PAN을 등록했으며 내부 Cisco ISE CA 서비스를 사용하려는 경우에는 기본 PAN에서 Cisco ISE CA 인증서와 키를 백업한 다음 보조 PAN에서 이를 복원해야 합니다.

  기본 설정 장의 *Cisco ISE CA* 인증서 및 키 백업 및 복원 섹션을 참조하십시오.

여러 구축 시나리오 지원

Cisco ISE는 802.1X 유선, 무선 및 VPN(Virtual Private Network)을 지원하는 엔터프라이즈 인프라 전반에 구축될 수 있습니다.

Cisco ISE 아키텍처는 독립형 및 분산형(고가용성 또는 리던던시*(redundancy)*라고도 함) 구축을 모두 지원합니다. 여기서 한 머신은 기본 역할을 맡고 다른 백업 머신은 보조 역할을 맡습니다. Cisco ISE는 구성 가능한 고유한 페르소나, 서비스 및 역할을 제공하며, 관리자는 이를 통해 네트워크에서 필요한 Cisco ISE 서비스를 생성하고 적용할 수 있습니다. 그 결과 완전한 기능을 갖춘 통합 시스템으로 작동하는 포괄적인 Cisco ISE 구축을 실현할 수 있습니다.

Cisco ISE 노드는 하나 이상의 관리, 모니터링 및 정책 서비스 페르소나를 사용하여 구축할 수 있습니다. 각 페르소나는 전반적인 네트워크 정책 관리 토폴로지에서 서로 다른 중요한 부분을 수행합니다. 관리 페르소나 역할의 Cisco ISE를 설치하면 중앙 집중식 포털에서 네트워크를 구성 및 관리하여 효율성과 사용 편의성을 높일 수 있습니다.

Cisco ISE 분산형 구축

여러 Cisco ISE 노드가 있는 구축을 분산형 구축이라고 합니다. 페일오버를 지원하고 성능을 개선하기 위해 분산된 형태로 여러 Cisco ISE 노드가 포함된 구축을 설정할 수 있습니다. Cisco ISE 분산 구축에서는 관리 및 모니터링 활동이 중앙 집중식으로 이루어지며 처리 작업은 PSN에 분산됩니다. 성능 요구 사항에 따라 구축을 확장할 수 있습니다. 구축의 각 Cisco ISE 노드는 관리, 정책 서비스 및 모니터링 페르소나를 취할 수 있습니다.

Cisco ISE 구축 설정

Cisco Identity Services Engine 하드웨어 설치 설명서에 설명된 것처럼 모든 노드에 Cisco ISE를 설치하고 나면 노드가 독립형 상태로 표시됩니다. 그러면 하나의 노드를 기본 PAN으로 정의해야 합니다. 기본 PAN을 정의하면서 해당 노드에서 관리 및 모니터링 페르소나를 활성화해야 합니다. 기본 PAN에서 선택적으로 정책 서비스 페르소나를 활성화할 수 있습니다. 기본 PAN에서 페르소나를 정의하

는 작업을 완료한 후에는 다른 보조 노드를 기본 PAN에 등록하고 보조 노드에 대한 페르소나를 정의할 수 있습니다.

모든 Cisco ISE 시스템 및 기능 관련 컨피그레이션은 기본 PAN에서만 수행되어야 합니다. 기본 PAN에서 수행한 컨피그레이션 변경 사항은 구축 환경의 모든 보조 노드로 복제됩니다.

분산형 구축에는 MnT 노드가 하나 이상 있어야 합니다. 기본 PAN을 구성할 때 모니터링 페르소나를 활성화해야 합니다. 구축에서 MnT 노드를 등록한 후 필요에 따라 기본 PAN을 편집하여 모니터링 페르소나를 비활성화할 수 있습니다.

기본 ISE 노드에서 보조 ISE 노드로의 데이터 복제

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

전체 복제는 일반적으로 Cisco ISE 노드를 처음 보조 노드로 등록하는 경우에 발생합니다. 증분 복제는 전체 복제 후에 발생하고, PAN 컨피그레이션 데이터의 추가, 수정 또는 삭제와 같이 새롭게 변경된 내용이 보조 노드에 반영되도록 합니다. 복제 프로세스를 사용하면 구축의 모든 Cisco ISE 노드를 동기화할 수 있습니다. Cisco ISE 관리 포털의 **Deployment(**구축**)** 창에 있는 **Node Status(**노드 상태**)** 열에서 복제 상태를 확인할 수 있습니다. Cisco ISE 노드를 보조 노드로 등록하거나 PAN과의 수동 동기화를 수행하는 경우 노드 상태에는 요청한 작업이 진행 중임을 의미하는 주황색 아이콘이 표시됩니다. 동기화 작업이 완료되면 노드 상태는 보조 노드가 PAN과 동기화되었음을 나타내는 녹색으로 바뀝니다.

Cisco ISE 노드 등록 취소

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

PSN의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. PSN이 독립형 노드가 된 후 엔드포인트 데이터를 유지하도록 하려는 경우 다음 중 하나를 수행할 수 있습니다.

- 기본 PAN에서 백업을 가져온 다음 PSN이 독립형 노드가 되면 해당 노드에서 이 데이터 백업을 복구합니다.
- PSN의 페르소나를 관리(보조 PAN)로 변경하고 관리 포털의 **Deployment(**구축**)** 창에서 데이터를 동기화한 다음 노드 등록을 취소합니다. 이제 이 노드에 모든 데이터가 포함됩니다. 그런 다음 보조 PAN을 기존 구축에 추가할 수 있습니다.

참고 기본 PAN은 등록 취소할 수 없습니다.

분산형 구축을 설정하기 위한 지침

분산형 환경에서 Cisco ISE를 설정하기 전에 다음 정보를 신중히 읽어보십시오.

- Cisco ISE 서버에 대한 노드 유형을 선택합니다. 관리, 정책 서비스 및 모니터링 기능을 사용하려면 Cisco ISE 노드를 선택해야 합니다.
- 모든 노드에 대해 동일한 NTP(Network Time Protocol) 서버를 선택합니다. 노드 사이의 시간대 문제를 방지하려면 각 노드 설정 시 동일한 NTP 서버 이름을 제공해야 합니다. 이 설정을 사용하면 구축의 다양한 노드에서 제공하는 보고서 및 로그가 항상 타임스탬프와 동기화될 수 있습니다.
- Cisco ISE 설치 시 Cisco ISE 관리자 비밀번호를 구성합니다. 이전의 Cisco ISE 관리자 기본 로그인 자격 증명(admin/cisco)은 더 이상 유효하지 않습니다. 초기 설정 중에 생성된 사용자 이름 및 비밀번호나 현재 비밀번호(나중에 변경된 경우)를 사용합니다.
- DNS 서버 구성 DNS 서버에서 분산형 구축에 포함되는 모든 Cisco ISE 노드의 IP 주소 및 FQDN(Fully Qualified Domain Name)을 입력합니다. 그렇지 않으면 노드 등록이 실패합니다.
- DNS 서버의 분산형 구축에 있는 모든 Cisco ISE 노드에 대한 정방향 및 역방향 DNS 조회를 구성합니다. 그렇지 않으면 Cisco ISE 노드를 등록하고 다시 시작할 때 구축 관련 문제가 발생할 수 있습니다. 모든 노드에 대해 역방향 DNS 조회가 구성되지 않은 경우 성능이 저하될 수 있습니다.
- (선택 사항) Cisco ISE를 기본 PAN에서 제거하려면 보조 Cisco ISE 노드를 PAN에서 등록 취소합니다.
- 기본 MnT를 백업하고 데이터를 새 보조 MnT로 복구합니다. 이렇게 하면 새 변경 사항이 복제될 때 기본 MnT의 기록이 새 MnT와 동기화됩니다.
- 기본 PAN 및 보조 노드로 등록하려는 독립형 노드에서 동일한 버전의 Cisco ISE를 실행하고 있는지 확인합니다.
- 구축에 새 노드를 추가하는 동안 와일드카드 인증서의 발급자 인증서 체인이 새 노드에 대한 신뢰할 수 있는 인증서의 일부인지 확인합니다. 새 노드가 구축에 추가되면 와일드카드 인증서가 새 노드에 복제됩니다.
- Cisco TrustSec을 지원하도록 Cisco ISE 구축을 구성하거나 Cisco ISE가 Cisco DNA 센터와 통합된 경우 PSN을 SXP 전용으로 구성하지 마십시오. SXP는 Cisco TrustSec과 비 Cisco TrustSec 디바이스 간의 인터페이스입니다. SXP는 Cisco TrustSec 지원 네트워크 디바이스와 통신하지 않습니다.

기본 및 보조 노드에서 사용할 수 있는 메뉴 옵션

분산형 구축의 일부인 Cisco ISE 노드에서 사용할 수 있는 메뉴 옵션은 활성화되어 있는 페르소나에 따라 달라집니다. 모든 관리 및 모니터링 활동은 PAN(Primary Administration Node)을 통해 수행해야 합니다. 다른 작업은 보조 노드를 사용해야 합니다. 그러므로 보조 노드의 사용자 인터페이스는 해당 노드에 활성화되어 있는 페르소나에 따라 제한된 메뉴 옵션을 제공합니다.

한 노드에서 여러 페르소나를 맡고 있는 경우(예: 정책 서비스 페르소나 및 활성 역할이 있는 모니터링 페르소나) PSN 및 기본 Mnt에 대해서 나열된 메뉴 옵션을 해당 노드에서 사용할 수 있습니다.

다음 표에는 여러 페르소나를 맡고 있는 Cisco ISE 노드에서 사용할 수 있는 메뉴 옵션이 나와 있습니다.

표 ***1: Cisco ISE*** 노드 및 사용 가능한 메뉴 옵션

Cisco ISE 노드	사용 가능한 메뉴 옵션
모든 노드	• 시스템 시간 및 NTP 서버 설정을 보고 구성합니다. • 서버 인증서를 설치하고 인증서 서명 요청을 관리합니다. 모든 서버 인증서를 중앙에서 관리하는 기본 PAN을 통해 구축의 모든 노드에 대해 서버 인증서 작업을 수행할 수 있습니다. 참고 개인 키는 로컬 데이터베이스에 저장되지 않으며 관련 노드에서 복사되지도 않습니다. 개인 키는 로컬 파일 시스템에 저장됩니다.
기본 PAN(Policy Administration Node)	모든 메뉴 및 하위 메뉴
기본 모니터링 노드(기본 MnT 노드)	• 모니터링 데이터에 대한 액세스 제공 참고 **Operations(**운영**)** 메뉴는 기본 PAN에서만 볼 수 있습니다. Cisco ISE 2.1 이상의 모니터링 노드에는 **Operations(**운영**)** 메뉴가 표시되지 않습니다.
PSN(Policy Service Node)	Active Directory 도메인에 가입하거나 나가고 Active Directory 연결을 테스트할 수 있는 옵션이 있습니다. 각 PSN은 Active Directory 도메인에 개별적으로 가입해야 합니다. 먼저 도메인 정보를 정의하고 PAN을 Active Directory 도메인에 가입시킬 수 있습니다. 그런 다음 다른 PSN을 개별적으로 Active Directory 도메인에 가입시킬 수 있습니다.

Cisco ISE 노드	사용 가능한 메뉴 옵션
보조 PAN(Policy Administration Node)	보조 PAN을 기본 PAN으로 승격하는 옵션 참고 보조 노드를 기본 PAN으로 등록한 후에 보조 노드의 관리 포털에 로그인하는 동안 기본 PAN의 로그인 자격 증명을 사용해야 합니다.

구축 및 노드 설정

Deployment Nodes(구축 노드**)** 창에서는 Cisco ISE(PAN, PSN, MnT) 노드를 구성하고 구축을 설정할 수 있습니다.

구축 노드 목록 창

다음 표에서는 구축 환경에서 Cisco ISE 를 구성하는 데 사용할 수 있는 **Deployment Nodes List(**구축 노드 목록**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**입니다.

표 ***2:*** 구축 노드 목록

필드 이름	사용 지침
Hostname(호스트 이름**)**	노드의 호스트 이름을 표시합니다.
Personas(역할 분담**)**	(노드 유형이 Cisco ISE인 경우에만 나타남) Cisco ISE 노드가 맡은 페르소나를 나열합니다. 예: Administration(관리), Policy Service(정책 서비스), Monitoring(모니터링) 또는 pxGrid 예: **Administration(**관리**)**, **Policy Service(**정책 서비스**)**, **Monitoring(**모니터링**)** 또는 **pxGrid**
역할	현재 노드에서 이러한 페르소나가 활성화된 경우 관리 및 모니터링 페르소나가 맡은 역할 (기본, 보조 또는 독립형)을 나타냅니다. 역할은 다음 중 하나 이상일 수 있습니다. • **PRI(A)**: 기본 PAN을 나타냅니다. • **SEC(A)**: 보조 PAN을 나타냅니다. • **PRI(M)**: 기본 MnT를 나타냅니다. • **SEC(M)**: 보조 MnT를 나타냅니다.

필드 이름	사용 지침
서비스	(정책 서비스 페르소나가 활성화된 경우에만 나타남) 이 Cisco ISE 노드에서 실행되는 서비스를 나열합니다. 포함되는 서비스는 다음과 같습니다. • **ID** 매핑 • 세션 • 프로파일링 • 모두
Node Status(노드 상태**)**	구축 환경에서 데이터 복제에 대한 각 Cisco ISE 노드의 상태를 나타냅니다. • 녹색(연결됨): 구축 환경에 이미 등록되어 있는 Cisco ISE 노드가 기본 PAN과 동기화되어 있음을 표시합니다. • 빨간색(연결 끊김): Cisco ISE 노드가 연결할 수 없거나 작동 중지되었거나 데이터 복제가 발생하지 않음을 나타냅니다. • 주황색(진행 중): Cisco ISE 노드가 기본 PAN에 새로 등록되었거나 수동 동기화 작업을 수행했거나 Cisco ISE 노드가 기본 PAN과 동기화되지 않았음(동기화 중단)을 나타냅니다. 자세한 내용을 보려면 각 Cisco ISE 노드의 **Node Status(**노드 상태**)** 열에서 간단히 보기 아이콘을 클릭해 주십시오.

관련 항목

Cisco ISE 분산형 구축, 5 페이지
Cisco ISE 구축 용어, 2 페이지
Cisco ISE 노드 구성, 2 페이지
보조 Cisco ISE 노드 등록, 3 페이지

일반 노드 설정

다음 표에서는 Cisco ISE 노드의 **General Settings(**일반 설정**)** 창에 있는 필드에 대해 설명합니다. 이 창에서 노드에 페르소나를 할당하고 노드에서 실행할 서비스를 구성할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Deployment Node(**구축 노드**)** > **Edit(**편집**)** > **General Settings(**일반 설정**)**입니다.

표 *3:* 일반 노드 설정

필드 이름	사용 지침
Hostname(호스트 이름**)**	Cisco ISE 노드의 호스트 이름을 표시합니다.
FQDN	Cisco ISE 노드의 인증된 도메인 이름(예: ise1.cisco.com)을 표시합니다.
IP Address(IP 주소**)**	Cisco ISE 노드의 IP 주소를 표시합니다.
Node Type(노드 유형**)**	노드 유형을 표시합니다.
Personas(역할 분담**)**	
Administration(관리**)**	Cisco ISE 노드가 관리 페르소나 역할을 하도록 지정하려면 이 토클 버큰을 활성화합니다. 관리 서비스 제공 라이선스가 있는 노드에서만 관리 페르소나를 활성화할 수 있습니다. **Role(**역할**)**: 구축에서 관리 페르소나에 대해 지정된 역할을 표시합니다. 페르소나는 **Standalone(**독립형**)**, **Primary(**기본**)**, **Secondary(**보조**)** 중 하나의 값을 가질 수 있습니다. **Make Primary(**기본으로 지정**)**: 이 노드를 기본 Cisco ISE 노드로 지정하려면 이 버튼을 클릭합니다. 기본 Cisco ISE 노드는 구축당 하나만 포함할 수 있습니다. 이 창의 다른 옵션은 이 노드를 기본으로 지정해야 활성화됩니다. 관리 노드는 구축당 두 개만 포함할 수 있습니다. 노드가 **Standalone(**독립형**)** 역할을 갖는 경우 노드 옆에 **Make Primary(**기본으로 지정**)** 버튼이 표시됩니다. 노드가 **Secondary(**보조**)** 역할을 갖는 경우 노드 옆에 **Promote to Primary(**기본으로 승격**)** 버튼이 표시됩니다. 노드가 **Primary(**기본**)** 역할을 갖고 등록된 다른 노드가 없는 경우 노드 옆에 **Make Standalone(**독립형으로 지정**)** 버튼이 표시됩니다. **Make Standalone(**독립형으로 지정**)** 버튼을 클릭하여 기본 노드를 독립형 노드로 지정할 수 있습니다.

필드 이름	사용 지침
Monitoring(모니터링**)**	

필드 이름	사용 지침
	Cisco ISE 노드가 모니터링 페르소나 역할을 하고 로그 컬렉터로 작동하도록 지정하려면 이 토글 버튼을 활성화합니다. 분산형 구축에는 모니터링 노드가 하나 이상 있어야 합니다. 기본 PAN을 구성할 때 모니터링 페르소나를 활성화해야 합니다. 구축에서 보조 모니터링 노드를 등록한 후 필요에 따라 기본 PAN을 편집하여 모니터링 페르소나를 비활성화할 수 있습니다. VMware 플랫폼에서 Cisco ISE 노드를 로그 컬렉터로 구성하려면 다음 지침을 참조하여 필요한 최소 디스크 공간(네트워크의 엔드포인트당 180KB, 네트워크의 Cisco ISE 노드당 매일 2.5MB)을 결정해 주십시오. 모니터링 노드에 포함할 데이터의 양(월 단위)을 기준으로 하여 필요한 최대 디스크 공간을 계산할 수 있습니다. 구축에 모니터링 노드가 하나뿐이면 독립형 역할이 지정됩니다. 구축에 모니터링 노드가 두 개인 경우 Cisco ISE에는 기본-보조 역할을 구성할 수 있도록 다른 모니터링 노드의 이름이 표시됩니다. 이러한 역할을 구성하려면 다음 중 하나를 선택합니다. • **Primary(**기본**)**: 현재 노드를 기본 모니터링 노드로 지정합니다. • **Secondary(**보조**)**: 현재 노드를 보조 모니터링 노드로 지정합니다. • **None(**없음**)**: 모니터링 노드에 기본-보조 역할을 지정하지 않으려는 경우에 선택합니다. 모니터링 노드 중 하나를 기본 또는 보조로 구성하는 경우 다른 모니터링 노드는 그에 따라 각각 보조 또는 기본 노드로 자동 지정됩니다. 기본 및 보조 모니터링 노드는 모두 관리 및 정책 서비스 로그를 수신합니다. 노드를 모니터링 노드로 지정한 후 모니터링 노드 하나의 역할을 **None(**없음**)**으로 변경하면 다른 모니터링 노드의 역할도 **None(**없음**)**이 되어 고가용성 페어가 취소됩니다. 이 노드는 **Remote Logging Targets(**원격 로깅 대상**)** 창에서 시스템 로그 대상으로 나열됩니다.. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로

필드 이름	사용 지침
	깅 대상**)**.

필드 이름	사용 지침
Policy Service(정책 서비스**)**	

필드 이름	사용 지침
	다음과 같은 서비스 중 하나 또는 전체를 활성화하려면 이 토글 버튼을 활성화합니다. • **Enable Session Services(**세션 서비스 활성화**)**: 네트워크 액세스, 포스처, 게스트 및 클라이언트 프로비저닝 서비스를 활성화하려면 이 확인란을 선택합니다. **Include Node in Node Group(**노드 그룹의 노드 포함**)** 드롭다운 목록에서 이 정책 서비스 노드가 속하는 그룹을 선택합니다. CA(Certificate Authority) 및 EST(Enrollment over Secure Transport) 서비스는 세션 서비스가 활성화된 정책 서비스 노드에서만 실행할 수 있습니다. **Include Node in Node Group(**노드 그룹의 노드 포함**)**에서 이 정책 서비스 노드를 그룹에 포함하지 않으려는 경우에는 **None(**없음**)**을 선택합니다. 동일한 노드 그룹 내의 모든 노드는 NAD(Network Access Device)에서 RADIUS 클라이언트로 구성되어야 하며 CoA에 대해 권한이 부여되어야 합니다. 이러한 노드 중 하나가 노드 그룹의 노드를 통해 설정된 세션에 대해 CoA 요청을 발급할 수 있기 때문입니다. 로드 밸런서를 사용하지 않는 경우 노드 그룹의 노드는 NAD에서 구성한 RADIUS 서버 및 클라이언트와 동일하거나 해당 서버 및 클라이언트의 하위 집합이어야 합니다. 이러한 노드는 RADIUS 서버로도 구성됩니다. 여러 Cisco ISE 노드를 사용하여 단일 NAD 노드를 RADIUS 서버 및 동적 권한 부여 클라이언트로 구성할 수는 있지만 모든 노드가 동일한 노드 그룹에 있을 필요는 없습니다. 노드 그룹의 멤버는 기가비트 이더넷과 같은 고속 LAN 연결을 사용하여 서로 연결되어야 합니다. 노드 그룹 멤버가 L2에 인접해 있을 필요는 없지만 충분한 대역폭과 연결 가능성을 보장하려면 L2에 인접하는 것이 좋습니다. 섹션을 참고하십시오. • **Enable Profiling Service(**프로파일링 서비스 활성화**)**: 프로파일링 서비스를 활성화하려면 이 확인란을 선택합니다. 프로파일링 서비스를 활성화하는 경우 **Profiling**

필드 이름	사용 지침
	Configuration(프로파일링 구성**)** 탭을 클릭하고 필요한 세부정보를 입력해야 합니다. 정책 서비스 노드에서 실행되는 서비스를 활성화/비활성화하거나 이 노드를 변경하는 경우에는 해당 서비스가 실행되는 애플리케이션 서버 프로세스가 재시작됩니다. 이러한 서비스가 다시 시작되는 동안에는 작업이 지연됩니다. CLI에서 **show application status ise** 명령을 사용하여 노드에서 애플리케이션 서버가 재시작된 시간을 확인할 수 있습니다. • **Enable Threat-Centric NAC Service(Threat Centric NAC** 서비스 활성화**)**: TC-NAC(Threat-Centric Network Access Control) 기능을 활성화하려면 이 체크 박스를 선택합니다. 이 기능을 사용하면 위협 및 취약점 어댑터에서 수신되는 위협 및 취약점 속성을 기준으로 권한 부여 정책을 생성할 수 있습니다. 위협 심각도 레벨 및 취약점 평가 결과를 사용하여 엔드포인트나 사용자의 액세스 레벨을 동적으로 제어할 수 있습니다. • **Enable SXP Service(SXP** 서비스 활성화**)**: 노드에서 SXP 서비스를 활성화하려면 이 확인란을 선택합니다. SXP 서비스에 사용할 인터페이스도 지정해야 합니다. NIC 결합 또는 팀을 구성한 경우 결합된 인터페이스도 **Use Interface(**인터페이스 사용**)** 드롭다운 목록에 물리적 인터페이스와 함께 나열됩니다. • **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)**: 네트워크 디바이스 구성을 제어하고 감사하기 위해 TACACS 정책 집합, 정책 결과 등을 생성하려면 이 확인란을 선택합니다.

필드 이름	사용 지침
	• **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)**: ID 매핑 기능을 활성화하려면 이 확인란을 선택합니다. 이 기능을 사용하면 Cisco ISE가 아닌 도메인 컨트롤러에 의해 인증되는 사용자를 모니터링할 수 있습니다. Cisco ISE가 네트워크 액세스를 위해 사용자를 능동적으로 인증하지 않는 네트워크에서 ID 매핑 기능을 사용하여 Active Directory 도메인 컨트롤러에서 사용자 인증 정보를 수집할 수 있습니다.
pxGrid	pxGrid 페르소나를 활성화하려면 이 확인란을 선택합니다. Cisco pxGrid는 Cisco ISE 세션 디렉토리에서 Cisco ASA(Adaptive Security Appliance) 등의 다른 정책 네트워크 시스템으로 상황 민감 정보를 공유하는 데 사용됩니다. 또한 pxGrid 프레임워크를 사용하여 노드 간에 정책 및 구성 데이터를 교환하고(예: Cisco ISE와 서드파티 벤더 간에 태그 및 정책 개체 공유) 위협 정보와 같은 ISE와 관련이 없는 정보도 교환할 수 있습니다.

관련 항목

분산형 Cisco ISE 구축의 페르소나, 2 페이지
관리 노드, 28 페이지
정책 서비스 노드, 37 페이지
모니터링 노드, 41 페이지
Cisco pxGrid 노드, 49 페이지
기본 및 보조 Cisco ISE 노드 동기화, 56 페이지
정책 서비스 노드 그룹 생성, 58 페이지
Cisco pxGrid 노드 구축, 50 페이지
노드 페르소나 및 서비스 변경, 57 페이지
자동 페일오버용 MnT 노드 구성, 48 페이지

프로파일링 노드 설정

다음 표에서는 프로파일러 서비스용으로 프로브를 구성하는 데 사용할 수 있는 **Profiling Configuration(**프로파일링 컨피그레이션**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **ISE Node(ISE** 노드**)** > **Edit(**편집**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)**을 클릭합니다.

표 *4:* 프로파일링 노드 설정

필드 이름	사용 지침
NetFlow	이 토글 버튼을 활성화하여 라우터에서 전송된 NetFlow 패킷을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 NetFlow를 사용하도록 설정합니다. 다음 옵션에 필요한 값을 입력합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(**포트**)**: NetFlow에서 내보낸 패킷이 라우터에서 수신되는 NetFlow 리스너 포트 번호를 입력합니다. 기본 포트는 9996입니다.
DHCP	이 토글 버튼을 활성화하여 IP 도우미에서 DHCP 패킷을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DHCP를 사용하도록 설정합니다. 다음 옵션에 필요한 값을 입력합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(**포트**)**: DHCP 서버 UDP 포트 번호를 입력합니다. 기본 포트는 67입니다.
DHCP SPAN	이 토글 버튼을 활성화하여 DHCP 패킷을 수집하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DHCP SPAN을 사용하도록 설정합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다.
HTTP	이 토글 버튼을 활성화하여 HTTP 패킷을 수신하고 구문 분석하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 HTTP를 사용하도록 설정합니다. • **Interface(**인터페이스**)**: Cisco ISE 노드의 인터페이스를 선택합니다.
RADIUS	정책 서비스 페르소나가 지정된 ISE 노드 당 RADIUS가 Cisco ISO 센서 활성화 디바이스에서 RADIUS 세션 특성 및 CDP, LLDP 특성을 수집하도록 하려면 이 토글 버튼을 활성화합니다.

필드 이름	사용 지침
NMAP(Network Scan)	이 토글 버튼을 활성화하여 NMAP 프로브를 사용하도록 설정합니다.
DNS	이 토글 버튼을 활성화하여 FQDN에 대한 DNS 조회를 수행하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 DNS를 사용하도록 설정합니다. 시간 초과 기간을 초 단위로 입력합니다. 참고 분산형 구축의 특정 Cisco ISE 노드에서 DNS 프로브가 작동하도록 하려면 DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브 중 하나를 활성화해야 합니다. DNS 조회의 경우에는 이러한 프로브 중 하나를 DNS 프로브와 함께 시작해야 합니다.
SNMP Query(SNMP 쿼리**)**	이 토글 버튼을 활성화하여 지정된 간격으로 네트워크 디바이스를 폴링하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 SNMP 쿼리를 사용하도록 설정합니다. **Retries(**재시도**)**, **Timeout(**시간 초과**)**, **Event Timeout(**이벤트 시간 초과**)** (필수) 및 **Description**(설명) (선택 사항)에 값을 입력합니다. 참고 이처럼 SNMP 쿼리 프로브를 구성해야 할 뿐 아니라**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 위치에서 다른 SNMP 설정도 구성해야 합니다. 네트워크 디바이스에서 SNMP 설정을 구성할 때는 네트워크 디바이스에서 CDP 및 LLDP를 전역적으로 활성화해야 합니다.

필드 이름	사용 지침
SNMP Trap(SNMP 트랩)	이 토글 버튼을 활성화하여 네트워크 디바이스에서 linkUp, linkDown 및 MAC 알림 트랩을 수신하도록 정책 서비스 페르소나를 지정한 Cisco ISE 노드당 SNMP 트랩 프로브를 사용하도록 설정합니다. 다음 정보를 제공하거나 활성화합니다. • **Link Trap Query(링크 트랩 쿼리)**: 이 토글 버튼을 활성화하여 SNMP 트랩을 통해 수신된 알림을 수신하고 해석합니다. • **MAC Trap Query(MAC 트랩 쿼리)**: 이 토글 버튼을 활성화하여 SNMP 트랩을 통해 수신된 MAC 알림을 수신하고 해석합니다. • **Interface(인터페이스)**: Cisco ISE 노드의 인터페이스를 선택합니다. • **Port(포트)**: 사용할 호스트의 UDP 포트를 입력합니다. 기본 포트는 162입니다.
Active Directory	이 토글 버튼을 활성화하여 정의된 Active Directory 서버에서 Windows 사용자에 대한 정보를 스캔합니다. • **Days before rescan(다시 스캔할 때까지의 기간(일))**: 스캔을 다시 실행할 날짜를 선택합니다.
pxGrid	이 토글 버튼을 활성화하여 Cisco ISE가 pxGrid를 통해 엔드포인트 속성을 수집(프로파일)할 수 있도록 허용합니다.

관련 항목

Cisco ISE 프로파일링 서비스
프로파일링 서비스에 사용되는 네트워크 프로브
Cisco ISE 노드에서 프로파일링 서비스 구성

로깅 설정

다음 섹션에서는 디버그 로그의 심각도를 구성하고, 외부 로그 대상을 생성하고, Cisco ISE가 이러한 외부 로그 대상에 로그 메시지를 보낼 수 있도록 설정하는 방법에 대해 설명합니다.

원격 로깅 대상 설정

다음 표에서는 로깅 메시지를 저장하기 위한 외부 위치(시스템 로그 서버)를 생성하는 데 사용할 수 있는 **Remote Logging Targets(**원격 로깅 대상**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Remote Logging Targets(**원격 로깅 대상**)** 에서 **Add(**추가**)**를 클릭합니다.

표 ***5:*** 원격 로깅 대상 설정

필드 이름	사용 지침
Name(이름**)**	새 시스템 로그 대상의 이름을 입력합니다.
Target Type(대상 유형**)**	드롭다운 목록에서 대상 유형을 선택합니다. 기본값은 **UDP** 시스템 로그입니다.
Description(설명**)**	새 대상의 간략한 설명을 입력합니다.
IP Address(IP 주소**)**	로그를 저장할 대상 머신의 IP 주소 또는 호스트 이름을 입력합니다. Cisco ISE는 로깅에 IPv4 및 IPv6 형식을 지원합니다.
Port(포트**)**	대상 머신의 포트 번호를 입력합니다.
Facility Code(시설 코드**)**	드롭다운 목록에서 로깅에 사용할 시스템 로그 시설 코드를 선택합니다. 유효한 옵션은 Local0~Local7입니다.
Maximum Length(최대 길이**)**	원격 로그 대상 메시지의 최대 길이를 입력합니다. 유효한 값은 200~1024바이트입니다.
Buffer Message When Server Down(서버 다운 시 메시지 버퍼링**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **TCP** 시스템 로그 또는 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. TCP 시스템 로그 대상 및 보안 시스템 로그 대상을 사용할 수 없을 때 Cisco ISE가 시스템 로그 메시지를 버퍼링하도록 하려면 이 확인란을 선택합니다. Cisco ISE는 대상에 연결을 재개할 때 대상에 대한 메시지 전송을 다시 시도합니다. 연결이 재개되면 메시지는 가장 오래된 것부터 시작하여 최신순으로 전송됩니다. 버퍼링된 메시지는 항상 새 메시지보다 먼저 전송됩니다. 버퍼가 가득 차면 오래된 메시지는 폐기됩니다.
Buffer Size (MB)(버퍼 크기**(MB))**	각 대상의 버퍼 크기를 설정합니다. 기본적으로 버퍼 크기는 100MB로 설정됩니다. 버퍼 크기를 변경하면 버퍼가 지워지며 특정 대상에 대해 기존에 버퍼링된 모든 메시지는 손실됩니다.

필드 이름	사용 지침
Reconnect Timeout (Sec)(다시 연결 시간 초과**(**초**))**	서버가 다운되었을 때 TCP 및 보안 시스템 로그를 폐기할 때까지 저장할 시간을 초 단위로 입력합니다.
Select CA Certificate(CA 인증서 선택**)**	이 드롭다운 목록은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. 드롭다운 목록에서 클라이언트 인증서를 선택합니다.
Ignore Server Certificate Validation(서버 인증서 검증 무시**)**	이 확인란은 **Target Type(**대상 유형**)** 드롭다운 목록에서 **Secure Syslog(**보안 시스템 로그**)**를 선택할 때 표시됩니다. Cisco ISE가 서버 인증서 인증을 무시하고 모든 시스템 로그 서버를 수락하도록 하려면 이 확인란을 선택합니다.

로깅 범주 구성

다음 표에서는 로깅 범주를 구성하는 데 사용할 수 있는 필드에 대해 설명합니다. 로그 심각도 레벨을 설정하고 로깅 범주의 로그에 대한 로깅 대상을 선택합니다. **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**입니다.이 창에 액세스하려면 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Logging Categories(**로깅 범주**)**를 클릭합니다.

보고자 하는 범주 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 다음 표에서는 로깅 범주의 편집 창에 표시되는 필드에 대해 설명합니다.

표 ***6:*** 로깅 범주 설정

필드 이름	사용 지침
Name(이름**)**	로깅 범주의 이름을 표시합니다.

필드 이름	사용 지침
Log Severity Level(로그 심각도 레벨**)**	일부 로깅 범주의 경우이 값은 기본적으로 설정되며 수정할 수 없습니다. 일부 로깅 범주의 경우 드롭다운 목록에서 다음 심각도 레벨 중 하나를 선택할 수 있습니다. • **FATAL**: 긴급 범주입니다. 이 레벨은 Cisco ISE를 사용할 수 없으며 필요한 조치를 즉시 수행해야 함을 의미합니다. • **ERROR**: 이 레벨은 심각한 오류 상태를 나타냅니다. • **WARN**: 이 레벨은 정상적이기는 하지만 중요한 상태를 나타냅니다. 이 레벨은 여러 로깅 범주에 대해 설정되는 기본 수준입니다. • **INFO**: 이 레벨은 정보 메시지를 나타냅니다. • **DEBUG**: 이 레벨은 진단 버그 메시지를 나타냅니다.
Local Logging(로컬 로깅**)**	로컬 노드의 범주에 대한 이벤트 로깅을 활성화하려면 이 확인란을 선택합니다.
Targets(대상**)**	이 영역에서는 왼쪽 및 오른쪽 화살표 아이콘을 사용하여 **Available(**사용 가능**)** 영역과 **Selected(**선택됨 **)** 영역 간에 대상을 전송하는 방식으로 로깅 범주에 대한 대상을 변경할 수 있습니다. **Available(**사용 가능**)** 상자에는 기존 로깅 대상이 포함되어 있습니다. 여기에는 미리 정의된 로컬 대상과 사용자가 정의한 외부 대상이 모두 포함됩니다. **Selected(**선택됨**)** 영역은 처음에는 비어 있으며, 이후에 이 범주에 대해 선택된 대상을 표시됩니다.

관리자 액세스 설정

이 섹션에서는 관리자용 액세스 설정을 구성할 수 있습니다.

관리자 비밀번호 정책 설정

다음 표에서는 **Password Policy(**비밀번호 정책**)** 탭의 필드에 대해 설명합니다. 이 탭을 사용하여 관리자 비밀번호가 충족해야 하는 기준을 정의할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Password Policy(**비밀번호 정책**)** .

표 *7:* 관리자 비밀번호 정책 설정

필드 이름	사용 지침
최소 길이	최소 비밀번호 길이를 문자 단위로 지정합니다. 기본값은 6자입니다.

필드 이름	사용 지침
비밀번호는 다음을 포함할 수 없습니다.	관리자 이름 또는 그 문자를 역순으로 배열한 단어: 관리자 이름 또는 그 문자를 역순으로 배열한 단어의 사용을 제한하려면 이 확인란을 선택합니다.
	Cisco 또는 그 문자를 역순으로 배열한 단어: Cisco 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	이 단어 또는 그 문자를 역순으로 배열한 단어: 사용자가 정의한 특정 단어 또는 그 문자를 비밀번호의 역순으로 배열한 단어의 사용을 제한하려면 이 체크 박스를 선택합니다.
	4번 이상 반복되는 문자: 비밀번호에 4번 이상 반복되는 문자를 연속으로 사용하는 것을 제한하려면 이 체크 박스를 선택합니다.
	사전 단어**,** 반대 순서의 문자 또는 다른 문자로 교체 된 문자: 사전 단어의 비밀번호 사용을 제한하거나 반대 순서로 문자를 교체하거나 문자를 다른 문자로 교체하려면 이 확인란을 선택합니다. s를 $, a를 @, o를 0, l를 1, i를 !, e를 3으로 대체할 수 없습니다. 예를 들어 Pa$$w0rd는 허용되지 않습니다. • **Default Dictionary(**기본 사전**)**: Cisco ISE에서 기본 Linux 사전을 사용하려면 이 옵션을 선택합니다. 기본 사전에는 약 480,000개의 영어 단어가 포함되어 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. • **Custom Dictionary(**맞춤형 사전**)**: 맞춤 설정한 사전을 사용하려면 이 옵션을 선택합니다. **Choose File(**파일 선택**)**을 클릭하여 맞춤형 사전 파일을 선택합니다. 텍스트 파일은 새 줄 구분된 단어, .dic 확장자여야 하며 크기가 20MB 미만이어야 합니다.

필드 이름	사용 지침
Password must contain at least one character of each of the selected types(비밀번호는 선택한 유형별로 하나 이상의 문자를 포함해야 함**)**	관리자 비밀번호에 포함해야 하는 문자 유형에 대한 확인란을 선택합니다. 다음 옵션 중 하나 이상을 선택합니다. • 소문자 알파벳 문자 • 대문자 알파벳 문자 • 숫자 • 영숫자 이외의 문자
Password History(비밀번호 기록**)**	같은 비밀번호를 반복적으로 사용하지 못하도록 하기 위해, 새로 입력하는 비밀번호와 달라야 하는 이전 비밀번호의 수를 지정합니다. **Password must be different from the previous *n*versions(**비밀번호는 이전 **n** 버전과 달라야 함**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다. 비밀번호를 재사용할 수 있을 때까지의 기간을 일 단위로 입력합니다. **Cannot reuse password within *n* days(n**일 이내에 비밀번호를 재사용 할 수 없음**)** 확인란을 선택하고 해당 필드에 번호를 입력합니다.
Password Lifetime(비밀번호 수명**)**	사용자가 지정된 기간 이후 비밀번호를 변경해야 하도록 강제 지정하려면 확인란을 선택합니다. • 관리자 비밀번호는 생성 또는 마지막 변경 이후 ***n***일 후에 만료: 비밀번호를 변경하지 않으면 관리자 계정을 비활성화할 때까지의 시간(일))입니다. 유효한 범위는 1일~3650일입니다. • 비밀번호 만료 ***n***일 전에 관리자에게 이메일 알림 보내기: 비밀번호가 만료 될 것임을 관리자에게 알리기 전까지의 시간(일)입니다. 유효한 범위는 1일~3650일입니다.
네트워크 디바이스 민감한 데이터 표시	
Require Admin Password(관리자 비밀번호 필요**)**	공유 암호 및 비밀번호와 같은 네트워크 디바이스의 민감한 데이터를 확인하기 위해 관리 사용자가 로그인 비밀번호를 입력해야 하도록 지정하려면 이 체크 박스를 선택합니다.

필드 이름	사용 지침
Password cached for *n* Minutes(n분 동안 비밀번호 캐시**)**	관리 사용자가 입력한 비밀번호가 이 기간 동안 캐시됩니다. 이 기간 동안에는 관리 사용자가 네트워크 디바이스의 민감한 데이터를 볼 때 비밀번호를 다시 입력하라는 메시지가 표시되지 않습니다. 유효 범위는 1분~60분입니다.

관련 항목

Cisco ISE 관리자
새 관리자 생성

세션 시간 초과 및 세션 정보 설정

다음 표에서는 세션 시간 초과를 정의하고 활성 관리 세션을 종료하는 데 사용할 수 있는 **Session(**세션**)** 창의 필드에 대해 설명합니다. 이 창에 액세스하려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리 액세스**)** > **Settings(**설정**)** > **Session(**세션**)**을 선택합니다.

표 ***8:*** 세션 시간 초과 및 세션 정보 설정

필드 이름	사용 지침
세션 시간 초과	
Session Idle Timeout(세션 유휴 시간 초과**)**	작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효 범위는 6분~100분입니다.
세션 정보	
Invalidate(무효화**)**	종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관련 항목

관리자 액세스 설정
관리자에 대한 세션 시간 초과 구성
활성 관리 세션 종료

관리 노드

관리 페르소나의 Cisco ISE 노드에서는 Cisco ISE에 대한 모든 관리 작업을 수행할 수 있습니다. 인증, 권한 부여, 감사 등과 같은 기능과 관련된 모든 시스템 관련 컨피그레이션을 처리합니다. 분산형 환경에서는 최대 두 개의 노드에서 관리 페르소나를 실행할 수 있습니다. 관리 페르소나는 독립형, 기본 또는 보조 역할 중 하나를 맡을 수 있습니다.

관리 노드의 고가용성

고가용성 구성에서 기본 PAN(Policy Administration Node)은 활성 상태입니다. 보조 PAN은 대기 상태입니다. 즉, 기본 PAN에서 모든 구성 업데이트를 수신하지만 Cisco ISE 네트워크에서는 활성 상태가 아닙니다.

Cisco ISE는 수동 및 자동 페일오버를 지원합니다. 자동 페일오버를 사용하는 경우 기본 PAN이 다운되면 보조 PAN의 자동 승격이 시작됩니다. 자동 페일오버에는 비관리 보조 노드(상태 확인 노드라고 함)가 필요합니다. 상태 확인 노드는 기본 PAN의 상태를 확인합니다. 기본 PAN이 작동 중지되거나 연결 불가능한 상태로 탐지될 경우 상태 확인 노드는 보조 PAN을 승격하여 기본 역할을 인계하도록 합니다.

자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나이고 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. 기본 PAN과 보조 PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN에 대해 상태 확인 노드가 있어야 합니다.

다음 표에는 PAN이 작동 중지될 경우 보조 PAN에서 인계해야 하는 영향을 받는 기능이 나와 있습니다.

기능 이름	기본 **PAN**이 작동 중지된 경우 사용 가능한지 여부 **(**예**/**아니요**)**
기존 내부 사용자 RADIUS 인증	예
기존 또는 신규 AD 사용자 RADIUS 인증	예
프로파일이 변경되지 않은 기존 엔드포인트	예
프로파일이 변경된 기존 엔드포인트	아니요
프로파일링을 통해 학습된 신규 엔드포인트	No(아니요)
기존 게스트: LWA(Local Web Authentication)	예
기존 게스트: CWA(Central Web Authentication)	예(자동 디바이스 등록 기능이 있는 핫스팟, BYOD 및 CWA와 같이 디바이스 등록용으로 활성화된 플로우는 제외)
게스트 변경 비밀번호	아니요
게스트: AUP	No(아니요)
게스트: 실패한 최대 로그인 횟수	아니요
새 게스트(스폰서 또는 셀프 등록)	아니요
포스처	예
내부 CA가 있는 BYOD	아니요

기능 이름	기본 **PAN**이 작동 중지된 경우 사용 가능한지 여부 **(**예**/**아니요**)**
기존에 등록된 디바이스	예
MDM 온보딩	아니요
pxGrid 서비스	아니요
보조 노드의 GUI 로그인	예(마지막 로그인 세부정보를 업데이트하기 위해 PAN에 대한 차단 호출이 시도되어 로그인 프로세스가 지연되며, 이 호출이 시간 초과되면 로그인이 진행됨)

내부 CA(Certificate Authority)를 사용하는 인증서 프로비저닝을 지원하기 위해 승격 후 원래 기본 PAN 및 해당 키가 포함된 루트 인증서를 새 기본 노드로 가져와야 합니다. 보조 노드가 기본 PAN으로 승격된 이후에 추가된 PSN 노드가 자동으로 페일오버될 경우 인증서 프로비저닝이 작동하지 않습니다.

고가용성 상태 확인 노드

기본 PAN의 상태 확인 노드를 활성 상태 확인 노드라고 합니다. 보조 PAN의 상태 확인 노드를 비활성 상태 확인 노드라고 합니다. 활성 상태 확인 노드는 기본 PAN의 상태를 확인하고 관리 노드의 자동 페일오버를 관리합니다. 2 개의 비-관리 ISE 노드를 상태 확인 노드로 사용하는 것이 좋습니다. 하나는 기본, 다른 하나는 보조 PAN용입니다. 상태 확인 노드를 하나만 사용하는 경우 해당 노드가 다운되면 자동 페일오버가 수행되지 않습니다.

두 PAN이 동일한 데이터 센터에 있는 경우, 단일 비-관리 ISE 노드를 기본 PAN 및 보조 PAN 모두에 대한 상태 확인 노드로 사용할 수 있습니다. 단일 상태 확인 노드가 기본 및 보조 PAN의 상태를 모두 확인하는 경우 활성 역할과 비활성 역할을 동시에 수행합니다.

상태 확인 노드는 비관리 노드이며 정책 서비스, 모니터링 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. 관리 노드와 같은 데이터 센터에 있는 PSN 노드를 상태 확인 노드로 지정하는 것이 좋습니다. 그러나 관리 노드 두 개가 같은 위치(LAN 또는 데이터 센터)에 있는 소규모 또는 중앙 집중식 구축의 경우에는 관리 페르소나를 포함하지 않는 모든 노드(PSN/pxGrid/MnT)를 상태 확인 노드로 사용할 수 있습니다.

자동 페일오버를 활성화하지 않기로 하고 기본 PAN에 장애가 발생했을 때 보조 노드의 수동 승격에 의존하는 경우에는 확인 노드가 필요하지 않습니다.

보조 **PAN**의 상태 확인 노드

보조 PAN의 상태 확인 노드는 비활성 모니터입니다. 이 노드는 보조 PAN이 기본 PAN으로 승격될 때까지 아무 조치도 수행하지 않습니다. 보조 PAN이 기본 PAN으로 승격되면 관련 상태 확인 노드가 관리 노드의 자동 페일오버를 관리하는 활성 역할을 하게 됩니다. 그러면 이전 기본 PAN의 상태 확인 노드는 이제 보조 PAN의 상태 확인 노드로서 비활성 모니터링을 수행하게 됩니다.

상태 확인 비활성화 및 재시작

상태 확인 역할에서 노드가 제거되거나 자동 페일오버 컨피그레이션이 비활성화되면 해당 노드에서 상태 확인 서비스가 중지됩니다. 지정된 고가용성 상태 확인 노드에서 자동 페일오버 컨피그레이션을 활성화하면 노드가 관리 노드의 상태 확인을 다시 시작합니다. 노드에서 고가용성 상태 확인 역할을 지정하거나 제거할 때는 해당 노드에서 애플리케이션이 다시 시작되지 않으며 상태 확인 작업만 시작되거나 중지됩니다.

고가용성 상태 확인 노드는 다시 시작되는 경우 기본 PAN의 이전 다운타임을 무시하고 상태 확인을 새로 시작합니다.

상태 확인 노드

활성 상태 확인 노드는 구성된 폴링 간격으로 기본 PAN의 상태를 확인합니다. 상태 확인 노드는 기본 PAN에 요청을 보내며, 수신되는 응답이 컨피그레이션과 일치하면 기본 PAN을 정상 상태로 간주하고 그렇지 않은 경우에는 기본 PAN을 비정상 상태로 간주합니다. 기본 PAN의 상태가 구성된 페일오버 기간을 초과해서 계속 비정상인 경우 상태 확인 노드가 보조 PAN에 대한 페일오버를 시작합니다.

상태 확인 중에 언제든지 이전에 페일오버 기간 내에 비정상으로 보고된 상태가 정상으로 확인된 경우 상태 확인 노드는 기본 PAN 상태를 정상으로 표시하고 상태 확인 주기를 재설정합니다.

기본 PAN의 상태 확인 응답은 상태 확인 노드에서 사용할 수 있는 컨피그레이션 값을 기준으로 검증됩니다. 응답이 해당 값과 일치하지 않으면 경보가 발생됩니다. 단, 승격 요청은 보조 PAN으로 전송됩니다.

상태 노드 변경

상태 확인에 사용 중인 Cisco ISE 노드를 변경할 수 있지만, 몇 가지 사항을 고려해야 합니다.

상태 확인 노드(H1)가 동기화되지 않은 상태에서 다른 노드(H2)가 기본 PAN의 상태 확인 노드로 지정되는 경우를 예로 들어 보겠습니다. 이러한 경우 기본 PAN이 다운되면 H1은 다른 노드(H2)가 같은 기본 PAN을 확인 중인지 알 수 없습니다. 이후 H2도 다운되거나 네트워크에서 연결이 끊기면 실제로 페일오버를 수행해야 합니다. 그러나 보조 PAN에는 승격 요청을 거부할 권한이 있습니다. 따라서 보조 PAN이 기본 역할로 승격되면 H2의 승격 요청이 오류와 함께 거부됩니다. 기본 PAN의 상태 확인 노드는 동기화되지 않은 상태이더라도 기본 PAN의 상태를 계속 확인합니다.

보조 **PAN**에 대한 자동 페일오버

기본 PAN을 사용할 수 없을 때 보조 PAN을 자동으로 승격하도록 Cisco ISE를 구성할 수 있습니다. 컨피그레이션은 **Deployment(**구축**)** 창의 기본 정책 관리 노드(기본 PAN)에서 수행됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다. 페일오버 기간은 **Number of Failure Polls Before Failover(**페일오버 전의 오류 폴링 횟수**)**에서 구성된 횟수에 **Polling Interval(**폴링 간격**)**에 설정된 시간(초)으로 정의됩니다. 기본 컨피그레이션의 경우 10분입니다. 보조 PAN을 기본 PAN으로 승격하는 데 10분이 더 소요됩니다. 따라서 기본 PAN 오류에서 보조 PAN 작동까지 걸리는 총 시간은 대개 20분입니다.

보조 PAN이 페일오버 호출을 받으면 실제 페일오버를 진행하기 전에 먼저 다음과 같은 검증을 수행합니다.

- 기본 PAN은 네트워크에서 사용할 수 없습니다.
- 페일오버 요청이 유효한 상태 확인 노드에서 발생했습니다.
- 이 PAN에 대한 페일오버 요청입니다.

모든 검증을 통과한 경우 보조 PAN은 자신을 기본 역할로 승격시킵니다.

다음은 보조 PAN의 자동 페일오버가 시도되는 몇 가지 샘플 시나리오입니다(이에 국한되지 않음).

- 기본 PAN의 상태는 폴링 기간 동안 **Number of failure polls before failover(**페일오버 전의 오류 폴링 횟수**)** 값에 대해 지속적으로 양호하지 않습니다.
- 기본 PAN의 Cisco ISE 서비스는 수동으로 중지되며 페일오버 기간 동안 중지된 상태로 유지됩니다.
- 기본 PAN은 소프트 중지 또는 재부팅 옵션을 통해 종료되며 구성된 페일오버 기간 동안 종료된 상태로 유지됩니다.
- 기본 PAN이 갑작스레 다운(전원 꺼짐)되고 페일오버 기간 동안 다운된 상태로 유지됩니다.
- 기본 PAN의 네트워크 인터페이스가 다운(네트워크 포트 종료 또는 네트워크 서비스 다운)되거나 다른 이유로 상태 확인 노드에서 연결할 수 없으며, 설정된 페일오버 기간 동안 다운된 상태로 유지됩니다.

상태 확인 노드 재시작

다시 시작하면 고가용성 상태 확인 노드가 기본 PAN의 이전 다운타임을 무시하고 상태 확인을 새로 시작합니다.

보조 **PAN**에 대한 자동 페일오버가 수행된 경우의 **BYOD(Bring Your Own Device)**

기본 PAN이 다운되더라도 기본 PAN 루트 CA 체인에서 이미 발급한 인증서가 있는 엔드포인트에 대한 인증은 중단되지 않습니다. 이는 구축의 모든 노드가 신뢰 및 검증을 위해 전체 인증서 체인을 가지고 있기 때문입니다.

그러나 보조 PAN이 기본으로 승격될 때까지 새 BYOD 디바이스는 온보딩되지 않습니다. BYOD 온보딩에는 활성 기본 PAN이 필요합니다.

원래의 기본 PAN이 복구되거나 보조 PAN이 승격되면 새 BYOD 엔드포인트가 문제없이 온보딩됩니다.

장애가 발생한 기본 PAN을 기본 PAN으로 재참가시킬 수 없는 경우 새로 승격된 기본 PAN(원래 보조 PAN)에서 루트 CA 인증서를 다시 생성합니다.

기존 인증서 체인의 경우 새 루트 CA 인증서를 트리거하면 하위 CA 인증서가 자동으로 생성됩니다. 새 하위 인증서가 생성되는 경우에도 이전 체인에서 생성된 엔드포인트 인증서는 계속 유효합니다.

자동 페일오버가 차단되는 샘플 시나리오

아래에서는 상태 확인 노드에 의한 자동 페일오버가 차단되거나 보조 노드로의 승격 요청이 거부되는 사례를 나타내는 몇 가지 샘플 시나리오가 나와 있습니다.

- 승격 요청을 수신하는 노드가 보조 노드가 아님
- 보조 PAN에서 수신한 승격 요청에 올바른 기본 PAN 정보가 포함되어 있지 않음
- 승격 요청이 잘못된 상태 확인 노드에서 수신됨
- 승격 요청이 수신되었지만 기본 PAN이 작동 중이며 정상 상태임
- 승격 요청을 수신하는 노드가 동기화되지 않은 상태임

PAN 자동 페일오버 기능의 영향을 받는 기능

다음 표에는 구축에서 PAN 자동 페일오버 구성이 활성화되어 있는 경우 차단되거나 구성을 추가로 변경해야 하는 기능이 나와 있습니다.

기능	영향 세부정보
차단되는 작업	
업그레이드	CLI를 통한 업그레이드가 차단됩니다. 이전 버전의 Cisco ISE에서 릴리스 1.4로 업그레이드하고 나면 PAN 자동 페일오버 기능의 구성이 가능해집니다. 이 기능은 기본적으로 비활성화됩니다. 자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나로 지정되며 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN의 상태 확인 노드가 있어야 합니다.
백업의 복원	CLI 및 사용자 인터페이스를 통한 복원이 차단됩니다. 복구 전에 PAN 자동 페일오버 구성을 활성화한 경우에는 정상적인 복구 이후에 PAN 자동 페일오버를 재구성해야 합니다.

기능	영향 세부정보
노드 페르소나 변경	사용자 인터페이스를 통한 다음 노드 페르소나 변경이 차단됩니다. • 기본 및 보조 PAN의 관리 페르소나 • PAN의 페르소나 • PAN 자동 페일오버 기능 활성화 이후의 상태 확인 노드 등록 취소
기타 CLI 작업	CLI를 통한 다음 관리 작업이 차단됩니다. • 패치 설치 및 롤백 • DNS 서버 변경 • eth1, eth2 및 eth3 인터페이스의 IP 주소 변경 • eth1, eth2 및 eth3 인터페이스의 호스트 별칭 변경 • 표준 시간대 변경
기타 관리 포털 작업	사용자 인터페이스를 통한 다음 관리 작업이 차단됩니다. • 패치 설치 및 롤백 • HTTPS 인증서 변경 • 비밀번호 기반 인증과 인증서 기반 인증 간의 관리 인증 유형 변경
최대 수의 디바이스가 연결된 사용자는 연결할 수 없음	일부 세션 데이터가 장애가 발생한 PAN에 저장되며 PSN에서 업데이트될 수 없습니다.
PAN 자동 페일오버를 비활성화해야 하는 작업	

기능	영향 세부정보
CLI 작업	PAN 자동 페일오버 구성이 활성화되어 있는 경우 CLI를 통해 다음 관리 작업을 수행할 때 경고 메시지가 표시됩니다. 이러한 작업을 수행할 때 페일오버 기간 이내에 서비스 또는 시스템을 다시 시작하지 않으면 자동 페일오버가 트리거될 수 있습니다. 따라서 다음 작업을 수행하는 동안에는 PAN 자동 페일오버 구성을 비활성화하는 것이 좋습니다. • Cisco ISE 서비스 수동 중지 • 관리 CLI를 사용한 Cisco ISE 소프트 재로드(재부팅)

자동 페일오버를 위한 기본 PAN 구성

시작하기 전에

자동 페일오버 기능을 구축하려면 노드가 3개 이상 있어야 합니다. 여기서 노드 2개는 관리 페르소나로 지정되며 노드 1개는 상태 확인 노드로 작동합니다. 상태 확인 노드는 비관리 노드이며 PSN, MnT 또는 pxGrid 노드이거나 이러한 노드의 조합일 수 있습니다. PAN이 서로 다른 데이터 센터에 있는 경우 각 PAN의 상태 확인 노드가 있어야 합니다.

단계 **1** 기본 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **PAN Failover(PAN** 페일오버**)**를 선택합니다.

단계 **3** **Enable PAN Auto Failover(PAN** 자동 페일오버 활성화**)** 확인란을 선택하여 기본 PAN의 자동 페일오버를 활성화합니다.

보조 PAN만 기본 PAN으로 승격할 수 있습니다. PSN, MnT, pxGrid 노드 또는 이러한 노드의 조합으로만 지정된 Cisco ISE 노드는 기본 PAN으로 승격할 수 없습니다.

단계 **4** 사용 가능한 모든 보조 노드가 포함되어 있는 **Primary Health Check Node(**기본 상태 확인 노드**)** 드롭다운 목록에서 기본 PAN의 상태 확인 노드를 선택합니다.

이 노드는 기본 PAN과 동일한 위치 또는 데이터 센터에 있는 것이 좋습니다.

단계 **5** 사용 가능한 모든 보조 노드가 포함되어 있는 **Secondary Health Check Node(**보조 상태 확인 노드**)** 드롭다운 목록에서 보조 PAN용 상태 확인 노드를 선택합니다.

이 노드는 보조 PAN과 동일한 위치 또는 데이터 센터에 있는 것이 좋습니다.

단계 **6** **Polling Interval(**폴링 간격**)** 시간을 입력합니다. 이 시간이 지나면 PAN 상태를 확인합니다. 유효 범위는 30~300초입니다.

단계 **7** **Number of Failure Polls before Failover(**페일오버 전의 오류 폴링 횟수**)**에 대한 횟수를 입력합니다.

지정한 오류 폴링 횟수 동안 PAN의 상태가 정상이 아닌 경우 페일오버가 수행됩니다. 유효 범위는 2~60개입니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

보조 PAN을 기본 PAN으로 승격한 후 다음을 수행합니다.

- 이전 기본 PAN을 수동으로 동기화하여 구축으로 다시 가져옵니다.
- 동기화 상태가 아닌 다른 보조 노드를 수동으로 동기화하여 구축으로 다시 가져옵니다.

보조 PAN을 기본으로 수동 승격

PAN 자동 페일오버를 구성하지 않은 상태에서 기본 PAN에 오류가 발생하는 경우 보조 PAN을 수동으로 승격하여 새 기본 PAN으로 지정해야 합니다.

시작하기 전에

기본 PAN으로 승격하려는 관리 페르소나가 지정된 두 번째 Cisco ISE 노드를 구성했는지 확인해 주십시오.

단계 **1** 보조 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **3** **Edit Node(**노드 편집**)** 창에서 **Promote to Primary(**기본으로 승격**)**를 클릭합니다.

보조 PAN만 기본 PAN으로 승격할 수 있습니다. 정책 서비스 또는 모니터링 페르소나 중 하나 또는 두 가지가 모두 지정된 Cisco ISE 노드는 기본 PAN으로 승격할 수 없습니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

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

보조 노드의 노드 편집 창에서는 옵션이 비활성화되어 있으므로 페르소나 또는 서비스를 수정할 수 없습니다. 변경을 수행하려면 관리 포털에 로그인해야 합니다.

기존 Cisco ISE 구축 노드를 새 Cisco ISE 구축을 위한 기본 PAN으로 재사용

기존 Cisco ISE 구축의 노드를 새 Cisco ISE 구축의 기본 PAN으로 재사용하려는 경우 다음 단계를 수행해야 합니다.

단계 **1** 먼저 사용중인 Cisco ISE 버전에 대한 Cisco ISE 설치 가이드에 설명된 대로 Cisco ISE 유틸리티 "Perform System Erase"를 실행합니다. https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-guides-list.html

단계 **2** Cisco ISE 설치 가이드에 설명된 대로 Cisco ISE를 새로 설치합니다.

단계 **3** 기본 PAN(Policy Administration Node) 구성, 3 페이지를 참조하여 독립형 노드를 기본 정책 관리 노드로 구성합니다.

기본 PAN에 서비스 복원

Cisco ISE에서는 원래 기본 PAN으로의 자동 대체를 지원하지 않습니다. 보조 PAN에 대한 자동 페일오버가 시작된 후 원래의 기본 PAN을 네트워크로 다시 가져오는 경우에는 보조 PAN으로 구성해야 합니다.

관리 노드에 대한 자동 페일오버 지원

Cisco ISE는 관리 페르소나에 대한 자동 페일오버를 지원합니다. 자동 페일오버 기능을 활성화하려면 분산 설정에서 적어도 2개의 노드를 관리 페르소나로 지정하고 한 노드를 비관리 페르소나로 지정해야 합니다. 기본 PAN이 다운되면 보조 PAN의 자동 승격이 시작됩니다. 이런 이유로 비관리 보조 노드가 각 PAN에 대한 상태 확인 노드로 지정됩니다. 상태 확인 노드가 구성한 간격으로 기본 PAN의 상태를 확인합니다. 디바이스가 다운되었거나 연결할 수 없는 등의 이유로 기본 PAN에 대해 수신된 상태 확인 응답이 정상 상태가 아닌 경우 상태 확인 노드는 구성한 임계치만큼 기다렸다가 기본 역할을 인계받을 수 있도록 보조 PAN의 승격을 시작합니다. 보조 PAN의 자동 페일오버 이후에 사용할 수 없는 몇 가지 기능이 있습니다. Cisco ISE는 원래 기본 PAN으로의 대체를 지원하지 않습니다. 자세한 내용은 관리 노드의 고가용성 섹션을 참고하십시오.

정책 서비스 노드

PSN(Policy Service Node)은 정책 서비스 페르소나의 Cisco ISE 노드이며 네트워크 액세스, 포스처, 포스처, 게스트 액세스, 클라이언트 프로비저닝, 프로파일링 서비스를 제공합니다.

분산 설정에서 하나 이상의 노드가 정책 서비스 페르소나를 맡아야 합니다. 이 페르소나는 정책을 평가하고 모든 결정을 내립니다. 일반적으로 분산형 구축에는 두 개 이상의 PSN이 있습니다.

같은 고속 LAN(Local Area Network)이나 로드 밸런서 뒤에 있는 모든 PSN은 함께 그룹화하여 하나의 노드 그룹을 만들 수 있습니다. 노드 그룹의 노드 중 하나에 장애가 발생하면 다른 노드가 장애를 탐지하고 URL로 리디렉션된 세션을 재설정합니다.

정책 서비스 노드의 고가용성

노드 장애를 탐지하고 장애가 발생한 노드에서 URL이 리디렉션된 모든 세션을 재설정하려는 경우에는 같은 노드 그룹에 둘 이상의 PSN을 배치할 수 있습니다. 노드 그룹에 속한 노드에 장애가 발생하면 동일한 노드 그룹의 다른 노드가 장애 발생 노드의 URL이 리디렉션된 모든 세션에 대해 CoA(Change of Authorization)를 실행합니다.

동일한 노드 그룹 내의 모든 노드는 NAD(Network Access Device)에서 RADIUS 클라이언트로 구성되어야 하며 CoA에 대해 권한이 부여되어야 합니다. 이러한 노드 중 하나가 노드 그룹의 노드를 통해 설정된 세션에 대해 CoA 요청을 발급할 수 있기 때문입니다. 로드 밸런서를 사용하지 않는 경우 노드 그룹의 노드는 NAD에서 구성한 RADIUS 서버 및 클라이언트와 동일하거나 해당 서버 및 클라이언트의 하위 집합이어야 합니다. 이러한 노드는 RADIUS 서버로도 구성됩니다.

여러 Cisco ISE 노드를 사용하여 단일 NAD 노드를 RADIUS 서버 및 동적 권한 부여 클라이언트로 구성할 수는 있지만 모든 노드가 동일한 노드 그룹에 있을 필요는 없습니다.

노드 그룹의 멤버는 기가비트 이더넷과 같은 고속 LAN 연결을 사용하여 서로 연결되어야 합니다. 노드 그룹 멤버가 L2에 인접해 있을 필요는 없지만 충분한 대역폭과 연결 가능성을 보장하려면 L2에 인접하는 것이 좋습니다. 자세한 내용은 정책 서비스 노드 그룹 생성, 58 페이지 섹션을 참고하십시오.

PSN 간에 요청을 균일하게 분산시키는 로드 밸런서

구축에 여러 PSN이 있을 때는 로드 밸런서를 사용하여 요청을 균일하게 분산시킬 수 있습니다. 로드 밸런서는 요청을 작동하는 여러 노드로 분산시킵니다. 로드 밸런서 뒤에서 PSN을 구축하는 방법에 대한 자세한 내용과 모범 사례는 Cisco 및 F5 구축 설명서: BIG-IP를 사용한 ISE 로드 밸런싱을 참고하십시오.

정책 서비스 노드의 세션 페일오버

노드 그룹의 PSN은 세션 정보를 공유합니다. 노드는 하트 비트 메시지를 교환하여 노드 장애를 탐지합니다. 노드에 장애가 발생하면 노드 그룹의 피어 중 하나가 장애가 발생한 PSN의 세션을 인식하고 CoA를 실행하여 그러한 세션의 연결을 끊습니다. 대부분의 클라이언트는 자동으로 다시 연결되고 새 세션을 설정합니다.

일부 클라이언트는 자동으로 다시 연결되지 않습니다. 예를 들어 클라이언트가 VPN을 통해 연결되는 경우 해당 클라이언트가 CoA를 인식하지 못할 수 있습니다. IP 폰, 멀티 호스트 802.1X 포트 또는 가상 머신인 클라이언트도 CoA를 인식하거나 CoA에 응답하지 않을 수 있습니다. URL 리디렉션 클라이언트(webauth)도 자동으로 연결할 수 없습니다. 이러한 클라이언트는 수동으로 다시 연결해야 합니다.

타이밍 문제로 재연결이 안 될 수도 있습니다. PSN 페일오버 시 포스처 상태가 보류 중인 경우를 예로 들 수 있습니다.

PSN 세션 공유에 대한 자세한 내용은 라이트 데이터 배포, 39 페이지를 참고하십시오.

정책 서비스 노드 그룹의 노드 수

노드 그룹에 포함될 수 있는 노드 수는 구축 요건에 따라 다릅니다. 노드 그룹은 노드 장애가 탐지되고 피어가 권한 부여되었지만 아직 포스처되지는 않은 세션에 CoA를 실행하도록 합니다. 노드 그룹 크기는 그리 크지 않아도 됩니다.

노드 그룹 크기가 커지면 노드 간에 교환되는 메시지 및 하트비트의 수가 크게 증가합니다. 결과적으로 트래픽도 증가하게 됩니다. 노드 그룹의 노드 수가 적을수록 트래픽도 줄어들며, 그와 동시에 PSN 장애를 탐지하기 위한 이중화를 충분히 제공할 수 있습니다.

노드 그룹 클러스터에서 가질 수 있는 PSN의 수에는 제한이 없습니다.

라이트 데이터 배포

라이트 데이터 배포는 사용자 세션 정보를 저장하여 구축의 모든 PSN 전반에 복제하는 데 사용되므로, 사용자 세션 세부정보를 위해 PAN 또는 MnT 노드에 의존할 필요가 없습니다.

라이트 데이터 배포는 다음 두 디렉토리로 구성됩니다.

- Radius 세션 디렉토리
- 엔드포인트 소유자 디렉토리

또한 **Advanced Settings(**고급 설정**)**에서 다음 옵션을 구성 할 수 있습니다.

- **Batch Size(**배치 크기**)**: 세션 업데이트를 일괄 적으로 전송할 수 있습니다. 이 값은 라이트 데이터 배포 인스턴스에서 구축의 다른 PSN으로 각 배치에서 전송되는 기록 수를 지정합니다. 이 필드를 1로 설정하면 세션 업데이트가 일괄적으로 전송되지 않습니다. 기본값은 기록 10개입니다.
- **TTL**: 이 값은 라이트 데이터 배포를 업데이트하기 전에 세션이 배치가 완료될 때까지 기다리는 최대 시간을 지정합니다. 기본값은 1000밀리초입니다.

PSN간에 연결 문제가 발생하는 경우(예: PSN이 다운된 경우) 세션 세부정보는 MnT 세션 디렉토리에서 검색되며, 나중에 사용할 수 있도록 저장됩니다.

대규모 구축에서는 최대 2,000,000개의 세션 기록을 저장할 수 있습니다. 소규모 구축에서는 1,000,000개의 세션 기록을 저장할 수 있습니다. 세션에 대한 계정 관리 중지 요청이 수신되면 모든 라이트 데이터 배포 인스턴스에서 해당 세션 데이터가 삭제됩니다. 저장된 기록의 수가 최대 한도를 초과하면 타임스탬프를 기준으로 가장 오래된 세션이 삭제됩니다.

참고

- 세션의 IPv6 접두사 길이가 128 비트보다 작고 인터페이스 ID가 지정되지 않은 경우 IPv6 접두사가 거부되어 여러 세션이 동일한 키를 가질 수 없습니다.
- 라이트 데이터 배포는 노드 간 통신에 ISE 메시징 서비스를 사용합니다. Cisco ISE 메시징 서비스는 다른 인증서 (내부 CA 체인에서 서명)를 사용합니다. Cisco ISE 메시징 서비스에 문제가 있는 경우 ISE 메시징 서비스 인증서를 다시 생성해야 합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. **Certificate(s) will be used for(**사용될 인증서**)** 섹션에서 **ISE Messaging service(ISE** 메시징 서비스**)**를 선택합니다. **Generate ISE messaging service certificate(ISE** 메시징 서비스 인증서 생성**)**을 클릭합니다.

Radius 세션 디렉토리

RADIUS 세션 디렉토리는 사용자 세션 정보를 저장하고 이를 구축의 PSN 전체에 복제하는 데 사용됩니다. **RADIUS** 세션 디렉토리는 CoA(Change of Authorization)에 필요한 세션 속성만 저장합니다.

이 기능은 Cisco ISE 릴리스 2.7에서 기본적으로 활성화됩니다. **Light Data Distribution(**라이트 데이터 배포**)** 창에서 **RADIUS Session Directory (RADIUS** 세션 디렉토리**)** 확인란을 선택하거나 선택 취소하여 이 기능을 활성화하거나 비활성화 할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Light Data Distribution(**라이트 데이터 배포**)**입니다.

엔드포인트 소유자 디렉토리

Cisco ISE 릴리스 2.6까지는 특정 엔드포인트에 대한 요청을 원래 처리한 것과 다른 PSN(Policy Service Node)에서 엔드포인트 프로브가 수신되면 엔드포인트 소유자가 새 PSN으로 변경됩니다. 이로 인해 엔드포인트 소유권이 플래핑됩니다.

Cisco ISE 릴리스 2.7부터는 **Endpoint Owner Directory(**엔드포인트 소유자 디렉토리를 사용하여 Cisco ISE에 연결하는 각 MAC 주소의 PSN FQDN을 저장하고 구축에서 PSN 전체에 걸쳐 이 데이터를 복제합니다. 이렇게 하면 모든 PSN이 이제 엔드포인트 소유자를 전부 인식하므로 엔드포인트 소유권 플래핑을 방지할 수 있습니다. 엔드포인트 소유권은 다른 PSN에서 해당 엔드포인트의 RADIUS 인증에 성공한 경우에만 변경됩니다.

또한 정적 엔드포인트 할당은 동일한 엔드포인트에 대해 수신 프로브가 받게 되는 속성에 우선되므로, 속성 재정의 문제가 발생하지 않습니다.

이 기능은 Cisco ISE 릴리스 2.7에서 기본적으로 활성화됩니다. 필요한 경우 비활성화하여 엔드포인트 소유자 디렉토리를 사용하지 않는 이전 메커니즘으로 되돌릴 수 있습니다. 엔드포인트 소유자 디렉토리는 프로파일링에도 사용되며, 이 옵션을 비활성화하면 레거시 프로파일러 소유자의 디렉토리가 사용됩니다. **Light Data Distribution(**라이트 데이터 배포**)** 창에서 **Enable Endpoint Owner Directory(**엔드포인트 소유자 디렉토리 활성화**)** 확인란을 선택하거나 선택 취소하여 해당 기능을 활

성화하거나 비활성화할 수 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Light Data Distribution(**라이트 데이터 배포**)**입니다.

모니터링 노드

모니터링 페르소나를 사용하는 Cisco ISE 노드는 로그 컬렉터로 작동하며, 네트워크에 있는 PAN 및 PSN의 로그 메시지를 저장합니다. 이 페르소나는 네트워크 및 리소스를 효율적으로 관리하는 데 사용할 수 있는 고급 모니터링 및 문제 해결 도구를 제공합니다. 이 페르소나를 사용하는 노드는 관리자가 수집하여 보고서 형식으로 의미 있는 정보를 제공하는 데이터를 집계하고 상관관계를 지정합니다.

Cisco ISE에서는 이 페르소나를 사용하는 노드를 두 개까지 가질 수 있으며, 그러한 노드는 고가용성을 위해 기본 또는 보조 역할을 맡을 수 있습니다. 기본 및 보조 MnT 노드 모두 로그 메시지를 수집합니다. 기본 MnT가 다운되면 기본 PAN이 보조 노드를 가리키며 모니터링 데이터를 수집합니다. 그러나 보조 노드는 기본 노드로 자동 승격되지 않습니다. 이 작업은 수동으로 MnT 역할 수정.

분산 설정에서 하나 이상의 노드가 모니터링 페르소나를 맡아야 합니다. 동일한 Cisco ISE 노드에서 모니터링 페르소나와 정책 서비스 페르소나를 함께 활성화하지 않는 것이 좋습니다. 최적의 성능을 위해서는 모니터링 전용 노드를 사용하는 것이 좋습니다.

구축의 기본 모니터링 노드

참고 pxGrid를 활성화한 경우 pxGrid 노드에 대한 새 인증서를 생성해야 합니다. 디지털 서명을 사용하여 인증서 템플릿을 생성하고 새 pxGrid 인증서를 생성합니다.

수동으로 MnT 역할 수정

기본 PAN에서 MnT 역할을 수동으로 수정(기본에서 보조로, 보조에서 기본으로)할 수 있습니다.

단계 **1** 기본 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 노드 목록에서 역할을 변경할 MnT 노드 옆의 확인란을 선택합니다.

단계 **4** **Edit(**편집**)**를 클릭합니다.

단계 **5** **Monitoring(**모니터링**)** 섹션에서 역할을 **Primary(**기본**)** 또는 **Secondary(**보조**)**로 변경합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

참고 해당 노드에서 활성화된 다른 모든 페르소나 및 서비스를 비활성화하려는 경우 **Dedicated MnT(**전용 **MnT)** 옵션을 활성화할 수 있습니다. 이 옵션을 활성화하면 해당 노드에서 컨피그레이션 데이터 복제 프로세스가 중지됩니다. 이는 MnT 노드의 성능을 개선하는 데 도움이 됩니다. 해당 옵션을 비활성화하면 수동 동기화가 트리거됩니다.

Cisco ISE 메시징 서비스의 시스템 로그

Cisco ISE 릴리스 2.6에서는 기본 내장 UDP 시스템 로그 수집 대상인 LogCollector 및 LogCollector2에 대한 MnT WAN 지속 가능성을 제공합니다. 이 지속 가능성은 **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT**로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)**(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Logging(**로깅**)** > **Log Settings(**로그 설정**)**) 옵션을 통해 활성화됩니다. 이 옵션을 활성화하면 UDP 시스템 로그가 TLS(Transport Layer Security)로 보호됩니다.

Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)** 옵션은 Cisco ISE 릴리스 2.6, FCS(First Customer Ship)에서 기본적으로 비활성화되어 있습니다. 이 옵션은 Cisco ISE 릴리스 2.6 누적 패치 2 이상 릴리스에서 기본적으로 활성화되어 있습니다.

UDP 시스템 로그에 Cisco ISE 메시징 서비스를 사용하면 MnT 노드에 연결할 수 없는 경우에도 제한된 기간 동안 운영 데이터가 유지됩니다. MnT WAN 지속 가능성 기간은 약 2시간 30분입니다.

이 서비스는 TCP 포트 8671을 사용합니다. 이에 따라 네트워크를 구성하고, 구축에서 다른 모든 Cisco ISE 노드의 각 Cisco ISE 노드에서 TCP 포트 8671로의 연결을 허용합니다. Light Session Directory(*Cisco ID* 서비스 엔진 관리자 가이드에서 "배포된 환경에서의 Cisco ISE 설정" 장의 "Light Session Directory" 섹션 참조)와 Profiler Persistence Queue 기능도 Cisco ISE 메시징 서비스를 사용합니다. .

참고 구축에서 Cisco ISE 구축에 TCP 또는 보안 시스템 로그를 사용하는 경우 기능은 이전 릴리스와 동일하게 유지됩니다.

대기열 링크 경보

Cisco ISE 메시징 서비스는 내부 CA 체인에서 서명한 다른 인증서를 사용합니다. Cisco ISE GUI 대시보드의 **Alarms(**경보**)** 대시릿에서 대기열 링크 경보를 가져올 수 있습니다. 이 경보는 구축에 노드를 등록하거나, 기본 PAN에서 노드를 수동으로 동기화하거나, 노드가 동기화되지 않은 상태이거나, 노드에서 애플리케이션 서비스가 다시 시작되는 등의 구축 작업을 수행하는 경우에 발생합니다. 다음을 확인하여 경보를 해결합니다.

- 모든 노드가 연결되어 있고 동기화됩니다.
- 모든 노드 및 Cisco ISE 메시징 서비스가 제대로 기능합니다.
- Cisco ISE 메시징 서비스 포트는 방화벽과 같은 외부 엔티티에 의해 차단되지 않습니다.
- 각 노드의 Cisco ISE 메시징 인증서 체인이 손상되지 않았으며 인증서 상태가 양호합니다.

위에 나열된 전제 조건이 충족되면 다음 작업으로 인해 대기열 링크 경보가 트리거됩니다.

- PAN 또는 PSN의 도메인 이름 또는 호스트 이름 변경
- 새 구축에서 백업 복원
- 업그레이드 후 이전 기본 PAN을 새 기본 PAN으로 승격

대기열 링크 경보를 해결하려면 Cisco ISE 루트 CA 체인을 다시 생성합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**를 선택합니다. **Generate Certificate Signing Requests (CSR)(CSR(**인증서 서명 요청**)** 생성**)**를 클릭합니다. **Certificate(s) will be used for(**인증서 사용 대상**)** 드롭다운 목록에서 **ISE Root CA(ISE** 루트 **CA)**를 선택합니다. **Replace ISE Root CA Certificate Chain(ISE** 루트 **CA** 인증서 체인 교체**)**을 클릭합니다.

다음 시나리오로 인해 **Queue Link Error(**대기열 링크 오류**)** 경보가 생성 될 수 있습니다.

- 시간 초과 : Cisco ISE 구축에서 두 노드간에 네트워크 문제가있는 경우 **Timeout(**시간 초과**)** 원인이 있는 **Queue Link Error(**대기열 링크 오류**)** 경보가 발생합니다. 이 오류를 해결하려면 포트 8671에서 연결을 확인합니다.
- 알 수 없는 CA: **System Certificates(**시스템 인증서**)** 창(이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System Certificates(**시스템 인증서**))**창 손상된 Cisco ISE 메시징 인증서가 있는 경우 **Unknown CA(**알 수 없는 **CA** 원인**)**이 있는 **Queue Link Error(**대기열 링크 오류**)** 경보가 발생합니다. 이 문제는 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Certificate Signing Requests(**인증서 서명 요청**)**을 선택한 다음 Cisco ISE GUI에서 **Generate Certificate Signing Request (CSR)(CSR(**인증서 서명 요청**)** 생성**)**에서 생성을 클릭하여 Cisco ISE 메시징 인증서를 재생성하여 해결할 수 있습니다. Cisco ISE 루트 CA 인증서 체인을 이미 교체한 경우에는 재생성이 필요하지 않습니다.

Cisco ISE 루트 CA 체인을 교체하면 Cisco ISE 메시징 서비스 인증서도 교체됩니다. 그 후에는 약 2분의 다운타임이 지나고 Cisco ISE 메시징 서비스가 재시작됩니다. 따라서 이 다운타임 중에 시스템 로그가 손실됩니다. 다운타임 중에 시스템 로그가 손실되지 않도록 하려면 Cisco ISE 메시징 서비스를 잠시 비활성화할 수 있습니다.

MnT로의 UDP 시스템 로그 전달 시 Cisco ISE 메시징 서비스를 활성화하거나 비활성화하려면 다음을 따릅니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Logging(**로깅**)** > **Log Settings(**로그 설정**)**.

단계 **2** **Use "ISE Messaging Service" for UDP Syslogs delivery to MnT(MnT**로의 **UDP** 시스템 로그 전달 시 **"ISE** 메시징 서비스**"** 사용**)** 확인란을 선택하거나 선택 취소하여 ISE 메시징 서비스 사용을 활성화 또는 비활성화합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

MnT 노드의 자동 페일오버

MnT 노드는 고가용성을 제공하지 않지만 활성-대기 구성을 지원합니다. PSN은 운영 감사 데이터를 기본 및 보조 MnT 노드에 복사합니다.

자동 페일오버 프로세스

기본 MnT 노드의 작동이 중지되면 보조 MnT 노드가 모든 모니터링 및 문제 해결 정보를 인계받습니다.

보조 노드를 기본 노드로 수동 전환하려면 수동으로 MnT 역할 수정을 참고하십시오. 보조 노드가 승격된 후에 기본 노드가 복구되면 보조 역할을 맡습니다. 보조 노드가 승격되지 않은 경우에는 기본 MnT 노드가 복구되고 나면 기본 역할을 다시 수행합니다.

⚠

주의 페일오버 이후에 기본 노드가 복구되면 보조 노드의 백업을 확보하고 데이터를 복구하여 기본 노드를 업데이트합니다.

MnT 노드의 활성-대기 페어를 설정하기 위한 지침

Cisco ISE 네트워크에서 MnT 노드 2개를 지정하고 활성-대기 페어로 구성할 수 있습니다. 기본 MnT 노드를 백업하고 데이터를 새 보조 MnT 노드로 복구하는 것이 좋습니다. 이렇게 하면 기본 노드에서 새 데이터를 복제할 때 기본 MnT 노드의 기록이 새 보조 노드와 동기화됩니다. 활성-대기 페어에 적용되는 규칙은 다음과 같습니다.

- 모든 변경 사항이 기본 MnT 노드에 기록됩니다. 보조 노드는 읽기 전용입니다.
- 기본 노드에 적용된 변경 사항은 자동으로 보조 노드에 복제됩니다.
- 기본 노드와 보조 노드는 다른 모든 노드가 로그를 전송하는 로그 컬렉터로 나열됩니다.
- Cisco ISE 대시보드는 모니터링 및 문제 해결을 위한 기본 시작점입니다. 모니터링 정보는 PAN의 대시보드에 표시됩니다. 기본 노드가 작동 중지되면 보조 노드에서 모니터링 정보가 제공됩니다.
- MnT 데이터를 백업하고 비우기하는 작업은 표준 Cisco ISE 노드 백업 프로세스에 포함되지 않습니다. 기본 및 보조 MnT 노드에서 백업 및 데이터 비우기를 위한 저장소를 구성하고 각각에 동일한 저장소를 사용해야 합니다.

MnT 노드 페일오버 시나리오

다음 시나리오는 MnT 노드에 해당하는 활성-대기 또는 단일 노드 구성에 적용됩니다.

- MnT 노드의 활성-대기 구성에서 기본 PAN은 항상 모니터링 데이터를 수집하기 위해 기본 MnT 노드를 가리킵니다. 기본 MnT 노드에 장애가 발생한 경우 PAN은 대기 MnT 노드를 가리킵니다. 기본 노드에서 보조 노드로의 페일오버는 5분 이상 작동이 중지된 후에 이루어집니다.

  그러나 기본 노드에서 장애가 발생한 후에는 보조 노드가 기본 노드가 되지 않습니다. 기본 노드가 복구되면 PAN은 재개된 기본 노드에서 다시 모니터링 데이터 수집을 시작합니다.

- 기본 MnT 노드가 작동 중지된 상태에서 대기 MnT 노드를 활성 상태로 승격하려는 경우 수동으로 MnT 역할 수정하거나 기존 기본 MnT 노드를 등록 취소하면 됩니다. 기존의 기본 MnT 노드를 등록 취소하면 대기 노드가 기본 MnT 노드가 되고, PAN은 자동으로 새로 승격된 기본 노드를 가리키게 됩니다.
- 활성-대기 페어에서 보조 MnT 노드를 등록 취소하거나 보조 MnT 노드가 작동 중지되면 기존의 기본 MnT 노드는 기본 노드로 유지됩니다.
- Cisco ISE 구축 환경에 MnT 노드가 하나만 있는 경우 이 노드는 PAN에 모니터링 데이터를 제공하는 기본 MnT 노드로 작동합니다. 그러나 새 MnT 노드를 등록하고 구축 환경에서 이를 기본 노드로 전환하면 기존의 기본 MnT 노드는 자동으로 대기 노드가 됩니다. PAN은 모니터링 데이터를 수집하기 위해 새로 등록된 기본 MnT 노드를 가리킵니다.

모니터링 데이터베이스

모니터링 기능에 사용되는 데이터 비율과 양에 따라 전용 노드에서 이러한 용도로 사용할 별도의 데이터베이스가 필요합니다.

PSN처럼 MnT 노드에는 이 섹션에서 설명하는 항목과 같이 유지 관리 작업을 수행해야 하는 전용 데이터베이스가 있습니다.

모니터링 데이터베이스 백업 및 복구

모니터링 데이터베이스는 대량의 데이터를 처리합니다. 시간의 경과할수록 MnT 노드의 성능과 효율성은 해당 데이터를 얼마나 잘 관리하느냐에 따라 달라집니다. 효율성을 높이기 위해서는 데이터를 백업하여 정기적으로 원격 저장소로 전송하는 것이 좋습니다. 자동 백업을 예약하여 이 작업을 자동화할 수 있습니다.

참고 제거 작업이 진행 중인 경우 백업을 수행해서는 안 됩니다. 제거 작업 중에 백업을 시작하면 제거 작업이 중단되거나 실패합니다.

보조 MnT 노드를 등록하는 경우에는 먼저 기본 MnT 노드를 백업한 다음, 데이터를 새 보조 MnT 노드에 복구하는 것이 좋습니다. 이렇게 하면 새 변경 사항이 복제될 때 기본 MnT 노드의 기록이 새 보조 노드와 동기화됩니다.

Monitoring(모니터링) Database Purge(데이터베이스 비우기)

비우기 프로세스를 사용하면 비우기하는 동안 데이터를 유지할 개월 수를 지정하여 모니터링 데이터베이스의 크기를 관리할 수 있습니다. 기본값은 3개월입니다. 이 값은 비우기를 위한 디스크 공간 사용 임계값(디스크 공간의 백분율)을 충족할 때 사용됩니다. 이 옵션에서 각 달은 30일로 구성됩니다. 3개월의 기본값은 90일입니다.

모니터링 데이터베이스 비우기를 위한 지침

다음은 모니터링 데이터베이스 디스크 사용량과 관련하여 따라야 하는 지침입니다.

- 모니터링 데이터베이스 디스크 사용량이 임계값 설정의 80%를 초과하는 경우에는 데이터베이스 크기가 할당된 디스크 크기를 초과했음을 나타내는 중요 경보가 생성됩니다. 디스크 사용량이 90%를 초과하면 또 다른 경보가 생성됩니다.

  비우기 프로세스가 실행되면 **Data Purging Audit(**데이터 비우기 감사**)** 창에서 볼 수 있는 상태 기록 보고서가 생성됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Data Purging Audit(**데이터 비우기 감사**)**입니다. 비우기가 완료되면 정보(INFO) 경보가 생성됩니다.

- 비우기는 데이터베이스의 사용된 디스크 공간 백분율도 기반으로 합니다. 모니터링 데이터베이스의 사용된 디스크 공간이 임계값(기본값: 80%) 이상이면 비우기 프로세스가 시작됩니다. 이 프로세스에서는 관리 포털에서 구성된 값에 관계없이 모니터링 데이터의 가장 오래된 7일 분량만 삭제합니다. 사용된 디스크 공간이 80% 미만이 될 때까지 루프에서 이 프로세스가 계속 진행됩니다. 비우기를 계속하기 전에 항상 모니터링 데이터베이스 디스크 공간을 확인합니다.

운영 데이터 비우기

Cisco ISE 모니터링 운영 데이터베이스에는 Cisco ISE 보고서로 생성되는 정보가 포함되어 있습니다. 최신 Cisco ISE 릴리스에는 Cisco ISE 관리 CLI 명령 **application configure ise**를 실행한 후 모니터링 운영 데이터를 제거하고 모니터링 데이터베이스를 재설정하는 옵션이 있습니다.

제거 옵션은 데이터를 정리하는 데 사용되며 보존 기간(일)을 지정하라는 메시지를 표시합니다. 재설정 옵션은 데이터베이스를 출고 시 기본값으로 재설정하는 데 사용되며 백업된 모든 데이터를 영구적으로 삭제합니다. 파일이 너무 많은 파일 시스템 공간을 사용하는 경우 데이터베이스를 재설정할 수 있습니다.

참고 재설정 옵션을 사용하면 재시작 전까지 Cisco ISE 서비스를 일시적으로 사용할 수 없게 됩니다.

Operational Data Purging(운영 데이터 비우기**)** 창에는 **Database Utilization(**데이터베이스 사용률**)** 및 **Purge Data Now(**지금 데이터 비우기**)** 영역이 포함되어 있습니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 비우기**)**입니다. **Database Utilization(**데이터베이스 사용률**)** 영역에 저장된 RADIUS 및 TACACS 데이터 및 총 가용 데이터베이스 공간을 볼 수 있습니다. 상태 표시줄 위에 마우스를 올려 놓으면 사용 가능한 디스크 공간과 기존 데이터가 데이터베이스에 저장된 일수가 표시됩니다. **Data Retention Period(**데이터 보존 기간**)** 영역에서 RADIUS 및 TACACS 데이터를 보존할 기간을 지정할 수 있습니다. 데이터는 매일 오전 4시에 제거되며, 보존 기간(일)을 지정하여 제거하기 전에 저장소에 데이터를 내보내도록 구성할 수 있습니다. **Enable Export Repository(**내보내기 저장소 활성화**)** 확인란을 선택하여 저장소를 선택 및 생성하고 **Encryption Key(**암호화 키**)**를 지정할 수 있습니다.

Purge Data Now(지금 데이터 제거**)** 영역에서 모든 RADIUS 및 TACACS 데이터를 제거하거나 특정 기간이 경과되면 데이터를 제거하도록 일수를 지정할 수 있습니다.

참고 비우기하기 전에 RADIUS 인증 및 계정 관리, TACACS 권한 부여 및 계정 관리, RADIUS 오류 및 잘못 구성된 supplicant 표을 저장소로 내보낼 수 있습니다.

관련 항목

이전 운영 데이터 비우기, 47 페이지

이전 운영 데이터 비우기

운영 데이터는 일정 기간 동안 서버에 수집되며, 즉시 또는 정기적으로 비울 수 있습니다. **Data Purging Audit(**데이터 비우기 감사**)** 보고서를 확인하여 데이터 비우기 성공 여부를 확인할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 비우기**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 다음 중 하나를 수행합니다.

- **Data Retention Period(**데이터 보존 기간**)** 영역에서 다음을 수행합니다.
  1. RADIUS 및 TACACS 데이터를 보존할 기간을 일 단위로 지정합니다. 지정한 기간 이전의 모든 데이터는 저장소로 내보내집니다.
  2. **Repository(**저장소**)** 영역에서 **Enable Export Repository(**내보내기 저장소 활성화**)** 확인란을 선택하여 데이터를 저장할 저장소를 선택합니다.
  3. **Encryption Key(**암호화 키**)** 텍스트 상자에 필요한 비밀번호를 입력합니다.
  4. **Save(**저장**)**를 클릭합니다.

     참고 구성된 보존 기간이 진단 데이터에 해당하는 기존 보존 임계값보다 작으면 구성된 값이 기존 임계값을 재정의합니다. 예를 들어 보존 기간을 3일로 구성했는데 이 값이 진단 표의 기존 임계값(예: 기본값인 5일)보다 작은 경우에는 이 창에서 구성한 값(3일)에 따라 데이터를 제거합니다.

- **Purge Data Now(**지금 데이터 제거**)** 영역에서 다음을 수행합니다.
  1. 모든 데이터를 제거할지 아니면 지정된 기간(일)보다 오래된 데이터를 제거할지 선택합니다. 데이터는 어떤 저장소에도 저장되지 않습니다.
  2. **Purge(**제거**)**를 클릭합니다.

자동 페일오버용 **MnT** 노드 구성

구축에 MnT 노드가 두 개인 경우에는 Cisco ISE 모니터링 서비스 다운타임을 방지하기 위해 자동 페일오버용으로 기본-보조 쌍을 구성할 수 있습니다. 이처럼 기본-보조 쌍을 구성하면 기본 노드에서 오류가 발생하는 경우 보조 MnT 노드가 모니터링 기능을 자동으로 제공합니다.

시작하기 전에

- 자동 페일오버용 MnT 노드를 구성하려면 해당 노드를 Cisco ISE 노드로 등록해야 합니다.
- 두 노드에서 모두 모니터링 역할과 서비스를 구성한 다음 기본 및 보조 역할에 맞게 적절한 이름을 지정합니다.
- 기본 및 보조 MnT 노드 둘 다에서 백업 및 데이터 비우기용 저장소를 구성합니다. 백업 및 비우기 기능이 정상적으로 작동하도록 하려면 두 노드에 대해 동일한 저장소를 사용합니다. 비우기는 이중화 쌍의 기본 및 보조 노드 둘 다에서 수행됩니다. 예를 들어 기본 MnT 노드가 백업과 비우기용으로 두 개 저장소를 사용하는 경우 보조 노드에 대해서도 동일한 저장소를 지정해야 합니다.

  시스템 CLI에서 **repository** 명령을 사용하여 MnT 노드에 대해 데이터 저장소를 구성합니다.

  ⚠ 주의 모니터링 이중화 쌍의 노드에서 예약된 백업 및 비우기가 정상적으로 작동하도록 하려면 CLI를 사용하여 기본 노드와 보조 노드 둘 다에서 동일한 저장소를 하나 이상 구성합니다. 저장소는 두 노드 간에 자동으로 동기화되지 않습니다.

Cisco ISE 대시보드에서 MnT 노드가 준비되었는지 확인합니다. **System Summary(**시스템 요약**)** dashlet에서 서비스가 준비된 MnT 노드의 왼쪽에는 녹색 확인 표시가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **2** **Deployment Nodes(**구축 노드**)** 창에서 기본으로 지정할 MnT 노드 옆의 확인란을 선택하고 **Edit**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭하고 **Role(**역할**)** 드롭다운 목록에서 **Primary(**기본**)**를 선택합니다.

MnT 노드를 기본으로 선택하면 나머지 MnT 노드는 자동으로 보조가 됩니다. 독립형 구축의 경우에는 기본 및 보조 역할 컨피그레이션이 비활성화됩니다.

단계 **4** **Save** 버튼을 클릭합니다. 기본 노드와 보조 노드가 모두 재시작됩니다.

Cisco pxGrid 노드

Cisco pxGrid는 Cisco ISE 세션 디렉토리에서 다른 네트워크 시스템(예: Cisco ISE 에코시스템 파트너 시스템 및 기타 Cisco 플랫폼)과 상황 민감 정보를 공유하는 데 사용됩니다. 또한 pxGrid 프레임워크를 사용하여 노드 간에 정책 및 컨피그레이션 데이터를 교환하고(예: ISE와 서드파티 벤더 간에 태그 및 정책 객체 공유) 다른 정보도 교환할 수 있습니다. 또한 Cisco pxGrid에서는 서드파티 시스템이 네트워크 또는 보안 이벤트에 대한 응답으로 사용자나 장치 또는 둘 다를 격리하기 위해 EPS(적응형 네트워크 제어 작업)를 호출할 수 있습니다. 태그 정의, 값 및 설명과 같은 TrustSec 정보는 Cisco TrustSec 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. FQN(Fully Qualified Names)을 사용하는 엔드포인트 프로파일은 엔드포인트 프로파일 메타 토픽을 통해 Cisco ISE에서 다른 네트워크로 전달될 수 있습니다. Cisco pxGrid는 태그 및 엔드포인트 프로파일의 대량 다운로드도 지원합니다.

Cisco pxGrid를 통해 SXP 바인딩(IP-SGT 매핑)을 게시하고 구독할 수 있습니다. SXP 바인딩에 대한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 보안 그룹 태그 교환 프로토콜 섹션을 참조하십시오. 참조.

고가용성 컨피그레이션에서 Cisco pxGrid 서버는 PAN을 통해 노드 간에 정보를 복제합니다. PAN이 다운되면 Cisco pxGrid 서버는 클라이언트 등록 및 서브스크립션 처리를 중단합니다. Cisco pxGrid 서버가 활성화되도록 하려면 PAN을 수동으로 승격해야 합니다. Cisco pxGrid 서비스 창(Administration(관리) > pxGrid Services(pxGrid 서비스))에서 Cisco pxGrid 노드가 현재 활성 상태인지 아니면 대기 상태인지를 확인할 수 있습니다.

pxGrid 페르소나가 있는 활성 Cisco 노드에서 이러한 프로세스는 **Running(**실행 중**)**으로 표시됩니다. 대기 중인 Cisco pxGrid 노드에서는 **Standby(**대기**)**로 표시됩니다. 활성 pxGrid 노드가 다운되면 대기 중인 pxGrid 노드가 이를 탐지하고 4개의 pxGrid 프로세스를 시작합니다. 몇 분 내에 이러한 프로세스가 **Running(**실행 중**)**으로 표시되고 대기 노드는 활성 노드가 됩니다. CLI 명령 **show logging application pxgrid/pxgrid.state**를 실행하여 Cisco pxGrid 서비스가 해당 노드에서 대기 중인지 확인할 수 있습니다.

XMPP(Extensible Messaging and Presence Protocol) 클라이언트의 경우 Cisco pxGrid 노드는 활성 노드에서 활성-대기 고가용성 모드로 작동합니다. 즉, Cisco pxGrid Service는 활성 노드에서는 실행 중 상태이며 대기 모드에서는 비활성화됨 상태입니다.

참고 고가용성 Cisco ISE 구축에서 활성-대기 설정에서 작동하는 pxGrid 개인 설정 노드는 pxGrid 서비스가 활성 노드에서 실행 중 상태이며 대기 노드에서는 대기 상태임을 표시합니다.

Cisco ISE 노드에서 pxGrid 서비스의 상태를 확인하려면 다음 CLI 명령을 사용합니다.

```
show logging application pxgrid/pxgrid.state
```

보조 Cisco pxGrid 노드에 대한 자동 페일오버가 시작된 후 원래 기본 Cisco pxGrid 노드가 네트워크에 다시 연결되면, 원래 기본 Cicsco pxGrid 노드는 계속 보조 역할로 지정되며 현재 기본 노드가 강등되지 않는 한 기본 역할로 다시 승격되지 않습니다.

참고 간혹 원래 기본 Cisco pxGrid 노드가 자동으로 기본 역할로 다시 승격되기도 합니다.

고가용성 구축의 경우 기본 Cisco pxGrid 노드가 강등되면 보조 Cicsco pxGrid 노드로 전환하는 데 3~5분 정도 걸릴 수 있습니다. 기본 Cisco pxGrid 노드 장애가 발생하는 경우 클라이언트는 되도록 전환이 완료될 때까지 기다린 다음 캐시 데이터를 지워야 합니다.

Cisco pxGrid 노드에 사용할 수 있는 로그는 다음과 같습니다.

- pxgrid.log: 상태 변경 알림입니다.
- pxgrid-cm.log: 클라이언트와 서버 간의 게시자 또는 가입자 또는 둘 다에 대한 및 데이터 교환 활동에 대한 업데이트입니다.
- pxgrid-controller.log: 클라이언트 기능, 그룹 및 클라이언트 권한 부여 세부정보를 표시합니다.
- pxgrid-jabberd.log: 시스템 상태 및 인증 관련 전체 로그입니다.
- pxgrid-pubsub.log: 게시자 및 가입자 이벤트 관련 정보입니다.

참고 노드에서 pxGrid 서비스가 비활성화된 경우, 포트 5222는 작동하지 않지만 (Web Clients(웹 클라이언트)에서 사용하는) 포트 8910은 작동하며 요청에 계속 응답합니다.

참고 Cisco ISE Advantage 라이선스로 Cisco pxGrid 및 Cisco pxGrid 페르소나를 활성화 할 수 있습니다.

참고 Passive ID Work Center(패시브 ID 작업 센터)를 이용하려면 Cisco pxGrid를 정의해야 합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 자산 가시성의 PassiveID 작업 센터 섹션을 참조하십시오 .

Cisco pxGrid 노드 구축

독립형 노드와 분산형 구축 노드에서 모두 Cisco pxGrid 페르소나를 활성화할 수 있습니다.

시작하기 전에

- Cisco pxGrid 페르소나를 활성화하려면 Cisco ISE Advantage 라이선스가 있어야 합니다.
- 라이선싱 요건은 ISE 라이선싱/주문을 참조하십시오.
- 모든 노드는 Cisco pxGrid 서비스 사용 시 CA 인증서를 사용합니다. 업그레이드 전에 Cisco pxGrid 서비스에 기본 인증서를 사용한 경우에는 업그레이드 시 해당 인증서가 내부 CA 인증서로 대체됩니다.

- Websockets(pxGrid 2.0)에 대해서는 포트 8910이 열려 있고 XMPP(pxGrid V1.0)에 대해서는 포트 5222가 열려 있어야 합니다. 노드에서 pxGrid 서비스가 비활성화된 경우, 포트 5222는 작동하지 않지만 포트 8910은 작동하며 요청에 계속 응답합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **2** **Deployment Nodes(**구축 노드**)** 창에서 Cisco pxGrid 서비스를 활성화할 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭하고 **pxGrid** 토글 버튼을 활성화.

단계 **4** **Save(**저장**)**를 클릭합니다.

이전 버전에서 업그레이드하는 경우 **Save(**저장**)** 옵션이 비활성화되어 있을 수 있습니다. 브라우저 캐시가 이전 버전 Cisco ISE의 오래된 파일을 참고하는 경우 이러한 현상이 발생합니다. **Save(**저장**)** 옵션을 활성화하려면 브라우저 캐시를 지우십시오.

Cisco pxGrid 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- **Automatically approve new certificate-based accounts(**새 인증서 기반 계정 자동 승인**)**: 새 Cisco pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- **Allow password based account creation(**비밀번호 기반 계정 생성 허용**)**: Cisco pxGrid 클라이언트에 대해 사용자 이름 또는 비밀번호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 Cisco pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

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

단계 **3** **Save(**저장**)**를 클릭합니다.

Cisco pxGrid **Settings(**설정**)** 창의 **Test(**테스트**)** 옵션을 사용하여 Cisco pxGrid 노드에서 상태 확인을 실행할 수 있습니다. pxgrid 또는 pxgrid-test.log 파일에서 세부정보를 볼 수 있습니다.

Cisco pxGrid 인증서 생성

시작하기 전에

일부 Cisco ISE 버전에는 NetscapeCertType을 사용하는 Cisco pxGrid용 인증서가 있습니다. 새 인증서를 생성하는 것이 좋습니다.

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- 기본 PAN에서 Cisco pxGrid 인증서를 생성해야 합니다.
- Cisco pxGrid 인증서가 SAN(Subject Alternative Name) 확장을 사용하는 경우, 주체 ID의 FQDN을 DNS 이름 항목으로 포함해야 합니다.
- 디지털 서명을 사용하여 인증서 템플릿을 생성하고 이를 사용하여 새 Cisco pxGrid 인증서를 생성합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Client Management(**클라이언트 관리**)** > **Certificates(**인증서**)**.

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

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)**: 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다.
- **Generate a single certificate without a certificate signing request(**인증서 서명 요청을 이용해 단일 인증서 생성**)**: 이 옵션을 선택하면 Certificate Signing Request(인증서 서명 요청) 세부정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부정보를 포함하는 CSV 파일을 업로드할 수 있습니다.
- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: 루트 인증서를 다운로드하여 신뢰할 수 있는 인증서 저장소에 추가합니다. 호스트 이름 및 인증서 다운로드 형식을 지정해야 합니다.

단계 **3** **CN(Common Name)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. pxGrid 클라이언트의 FQDN을 입력합니다.

단계 **4** **Certificate Signing Request Details(**인증서 서명 요청 세부정보**)**: **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)** 옵션을 선택하는 경우에 필요합니다. 전체 인증서 서명 요청 세부정보를 입력합니다.

단계 **5** **Description(**설명**)**: (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **6** **Certificate Template(**인증서 템플릿**)**: **pxGrig_Certificate_Template** 링크를 클릭하여 인증서 템플릿을 다운로드하고 요구 사항에 따라 템플릿을 편집합니다.

단계 **7** **SAN(Subject Alternative Name)**: 여러 SAN을 추가할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 Cisco pxGrid 클라이언트의 IP 주소를 입력합니다.
- **FQDN**: pxGrid 클라이언트의 정규화된 도메인 이름을 입력합니다.

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

단계 **8** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.
- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **9** **Certificate Password(**인증서 비밀번호**)**: 인증서의 비밀번호를 입력하고 다음 필드에 비밀번호를 다시 입력하여 확인합니다.

단계 **10** **Create(**생성**)**를 클릭합니다.

생성한 인증서는 Cisco ISE의 **Issued Certificates(**발급된 인증서**)** 창에 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Issued Certificates(**발급된 인증서**)**입니다. 인증서는 브라우저의 다운로드 디렉터리에도 다운로드됩니다.

참고 Cisco ISE 2.4 패치 13부터는 pxGrid 서비스에 대한 인증서 요건이 더욱 엄격해졌습니다. Cisco ISE의 기본 SSC(Self-Signed Certificate, 자가서명 인증서)를 pxGrid 인증서로 사용하는 경우 Cisco ISE 2.4 패치 13 이상 버전을 적용한 후 Cisco ISE에서 해당 인증서를 거부할 수 있습니다. 해당 인증서의 이전 버전에서 **Netscape Cert Type(Netscape** 인증서 유형**)** 확장이 **SSL Server(SSL** 서버**)**로 지정되었기 때문에 실패하는 것입니다(이제 클라이언트 인증서도 필요함).

규정 미준수 인증서가 있는 클라이언트는 Cisco ISE와 통합되지 않습니다. 내부 CA에서 발급한 인증서를 사용하거나 적절한 사용 확장을 사용하여 새 인증서를 생성합니다.

- 인증서의 키 사용**(Key Usage)** 확장에는 **Digital Signature(**디지털 서명**)** 및 **Key Encipherment(**키 암호화**)** 필드가 포함되어야 합니다.
- 인증서의 **Extended Key Usage(**확장 키 사용**)** 확장에는 **Client Authentication(**클라이언트 인증**)** 및 **Server Authentication(**서버 인증**)** 필드가 포함되어야 합니다.
- **Netscape Certificate Type(Netscape** 인증서 유형**)** 확장은 필요하지 않습니다. 해당 확장을 포함하려면 확장에 **SSL Client(SSL** 클라이언트**)** 및 **SSL Server(SSL** 서버**)**를 모두 포함해야 합니다.
- 자가서명 인증서를 사용하는 경우 **Basic Constraints CA** 기본 제약 조건 **CA)** 필드를 True로 설정하고 **Key Usage(**키 사용**)** 확장에 **Key Cert Sign(**키 인증서 서명**)** 필드를 포함해야 합니다.

Cisco pxGrid 클라이언트에 대한 권한 제어

Cisco pxGrid 클라이언트에 대한 권한을 제어하기 위한 Cisco pxGrid 권한 부여 규칙을 생성할 수 있습니다. Cisco pxGrid 클라이언트에 제공되는 서비스를 제어하려면 이 규칙을 사용합니다.

서로 다른 유형의 그룹을 생성하고 Cisco pxGrid 클라이언트에 제공된 서비스를 이러한 그룹에 매핑할 수 있습니다. **Client Management(**클라이언트 관리**)** 창에서 **Groups(**그룹**)** 옵션을 사용하여 새 그룹을 추가합니다. **Client Management(**클라이언트 관리**)** > **Policies(**정책**)** 창에서 사전 정의된 그룹(예: EPS 및 ANC)을 사용하는 사전 정의된 권한 부여 규칙을 확인할 수 있습니다. 사전 정의된 규칙에 대해 **Custom Operations(**사용자 맞춤화 작업**)** 필드만 업데이트할 수 있습니다.

pxGrid 클라이언트에 대한 권한 부여 규칙을 생성하려면

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Client Management(**클라이언트 관리**)** > **Policy(**정책**)**.

단계 **2** **Service(**서비스**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **com.cisco.ise.pubsub**
- **com.cisco.ise.config.anc**
- **com.cisco.ise.config.profiler**
- **com.cisco.ise.config.trustsec**
- **com.cisco.ise.service**
- **com.cisco.ise.system**
- **com.cisco.ise.radius**
- **com.cisco.ise.sxp**
- **com.cisco.ise.trustsec**
- **com.cisco.ise.mdm**

단계 **3** **Operation(**운영**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **<ANY>**
- **publish**
- **publish /topic/com.cisco.ise.session**
- **publish /topic/com.cisco.ise.session.group**
- **publish /topic/com.cisco.ise.anc**
- **<CUSTOM>**

  참고 이 옵션을 선택하면 사용자 맞춤화 작업을 지정할 수 있습니다.

단계 **4** **Groups(**그룹**)** 드롭다운 목록에서 이 서비스에 매핑할 그룹을 선택합니다.

사전 정의된 그룹(예: EPS 및 ANC) 및 수동으로 추가한 그룹이 이 드롭다운 목록에 나열됩니다.

구축 노드 확인

Deployment Nodes(구축 노드**)** 창에서는 구축에 포함된 모든 Cisco ISE 노드(기본 및 보조 노드)를 확인할 수 있습니다.

단계 **1** 기본 Cisco ISE 관리 포털에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **3** 왼쪽 탐색창에서 **Deployment(**구축**)**를 클릭합니다.

구축에 속하는 모든 Cisco ISE 노드가 나열됩니다.

MnT 노드에서 엔드포인트 통계 데이터 다운로드

MnT 노드에서 네트워크에 연결하는 엔드포인트에 대한 통계 데이터를 다운로드할 수 있습니다. 로드, CPU 사용량, 인증 트래픽 데이터가 포함되어 있는 KPM(Key Performance Metrics)는 네트워크의 문제를 모니터링하고 해결하는 데 사용할 수 있습니다. Cisco ISE CLI(Command Line Interface)에서 **application configure ise** 명령을 사용하여 옵션 12 또는 13을 선택하여 일일 KPM 통계 또는 최근 8주 동안의 KPM 통계를 각각 다운로드할 수 있습니다.

이 명령의 출력은 엔드포인트에 대한 다음 데이터를 제공합니다.

- 네트워크의 총 엔드포인트 수
- 성공적인 연결을 설정한 엔드포인트 수
- 인증에 실패한 엔드포인트 수
- 매일 연결된 새로운 총 엔드포인트 수
- 매일 온보드된 총 엔드포인트 수

출력에는 타임스탬프 세부정보, 구축에서 각 PSN(Policy Service Node)을 통해 연결된 총 엔드포인트 수, 총 엔드포인트 수, 활성 엔드포인트, 로드 및 인증 트래픽 세부정보도 포함됩니다.

이 명령에 대한 자세한 내용은 *Cisco Identity Services Engine CLI Reference Guide*를 참고해 주십시오.

데이터베이스 충돌 또는 파일 손상 문제

정전이 발생하거나 그 외에 데이터가 손실되는 이유로 인해 Oracle 데이터베이스 파일이 손상된 경우 Cisco ISE가 충돌할 수 있습니다. 사고 유형에 따라 아래 단계를 수행하여 데이터 손실을 복구합니다.

- 구축 시 PAN이 손상된 경우에는 보조 PAN을 기본 PAN으로 승격해야 합니다.
- 소규모 구축 또는 기타 이유로 인해 보조 PAN의 승격이 불가능한 경우 사용 가능한 최신 백업을 복원합니다.
- PSN이 손상된 경우, 등록을 취소하고 컨피그레이션을 재설정한 다음 노드를 다시 등록하는 단계를 수행합니다.
- 독립형 디바이스의 경우 사용 가능한 최신 백업을 복원합니다.

참고 최신 컨피그레이션 변경 사항이 손실되지 않도록 독립형 상자에서 정기적으로 백업을 가져옵니다.

모니터링을 위한 디바이스 컨피그레이션

MnT 노드는 대시보드 화면을 채우기 위해 네트워크의 디바이스에서 데이터를 수신하여 사용합니다. MnT 노드와 네트워크 디바이스 간 통신을 위해서는 스위치 및 NAD를 올바르게 구성해야 합니다.

기본 및 보조 Cisco ISE 노드 동기화

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

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

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

노드 페르소나 및 서비스 변경

Cisco ISE 노드 컨피그레이션을 편집하여 노드에서 실행되는 페르소나 및 서비스를 변경할 수 있습니다.

시작하기 전에

- PSN에서 실행되는 서비스를 활성화/비활성화하거나 PSN을 변경하는 경우에는 해당 서비스가 실행되는 애플리케이션 서버 프로세스가 다시 시작됩니다. 이러한 서비스가 다시 시작되는 동안에는 작업이 지연됩니다.
- 서비스가 다시 시작될 때의 이러한 지연으로 인해 구축에서 활성화된 경우 자동 페일오버가 시작될 수 있습니다. 이를 방지하려면 자동 페일오버 컨피그레이션이 꺼져 있는지 확인합니다.

단계 **1** 기본 PAN에 로그인합니다.

단계 **2** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**.

단계 **3** 페르소나 또는 서비스를 변경하려는 노드 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **4** 원하는 페르소나 및 서비스를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 기본 PAN에서 경보가 수신되는지 확인하여 페르소나 또는 서비스 변경을 확인합니다. 페르소나 또는 서비스 변경 사항이 정상적으로 저장되지 않으면 경보가 생성되지 않습니다.

Cisco ISE에서 노드 수정의 효과

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

- 노드 등록(독립형에서 보조로)
- 노드 등록 취소(보조에서 독립형으로)
- 기본 노드를 독립형으로 변경(다른 노드가 등록되지 않은 경우, 기본에서 독립형으로)
- 관리 노드 승격(보조에서 기본으로)
- 페르소나 변경(정책 서비스 또는 모니터링 페르소나를 노드에서 할당하거나 제거하는 경우)
- 정책 서비스 노드에서 서비스 수정(세션 및 프로파일러 서비스 활성화 또는 비활성화)
- 기본 노드에서 백업을 복원하면 동기화 작업이 트리거되어 기본 노드에서 보조 노드로 데이터 복제

정책 서비스 노드 그룹 생성

둘 이상의 PSN(Policy Service Node)이 같은 고속 LAN(Local Area Network)에 연결되어 있을 때 해당 노드를 같은 노드 그룹에 배치하는 것이 좋습니다. 이 설계를 사용하는 경우 중요도가 낮은 속성을 그룹에 로컬로 유지하고 네트워크에서 원격 노드로 복제되는 정보를 줄여 엔드포인트 프로파일링 데이터 복제를 최적화할 수 있습니다. 노드 그룹 멤버는 피어 그룹 멤버의 가용성도 확인합니다. 그룹은 멤버에 장애가 발생했음을 탐지하면 장애가 발생한 노드에서 URL로 리디렉션된 모든 세션의 재설정 및 복구를 시도합니다.

참고 모든 PSN을 같은 노드 그룹의 동일 로컬 네트워크 부분에서 만드는 것이 좋습니다. PSN이 같은 노드 그룹에 가입하기 위해 로드 밸런싱된 클러스터의 일부분일 필요는 없습니다. 그러나 로드 밸런싱된 클러스터의 각 로컬 PSN은 일반적으로 같은 노드 그룹의 일부분이어야 합니다.

참고 노드 그룹은 URL 리디렉션(포스처 서비스, 게스트 서비스 및 MDM)이 적용된 세션의 PSN 페일오버에 사용됩니다.

PSN을 노드 그룹에 멤버로 추가하기 전에 노드 그룹을 먼저 생성해야 합니다. 관리 포털의 **Depolyment(**구축**)** 창에서 PSN 그룹을 생성, 편집 및 삭제할 수 있습니다.

시작하기 전에

노드 그룹 멤버는 TCP/7800을 통해 통신할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** 왼쪽 탐색창 상단에서 **Settings(**설정**)** 아이콘을 클릭합니다.

단계 **3** **Create Node Group(**노드 그룹 생성**)**을 클릭합니다.

단계 **4** 노드 그룹의 고유한 이름을 입력합니다.

참고 노드 등록에서 바람직하지 않은 문제가 발생할 수 있으므로 이름이 **None**인 노드 그룹을 구성하지 않는 것이 좋습니다.

단계 **5** (선택 사항) 노드 그룹에 대한 설명을 입력합니다.

단계 **6** (선택 사항) **Enable MAR Cache Distribution(MAR** 캐시 배포 활성화**)** 확인란을 선택하고 다른 옵션을 입력합니다. 이 옵션을 활성화하기 전에 **Active Directory** 창에서 MAR이 활성화되어 있는지 확인하십시오.

단계 **7** **Submit(**제출**)**을 클릭하여 노드 그룹을 저장합니다.

저장한 노드 그룹은 왼쪽 탐색 창에 표시됩니다. 왼쪽 창에 노드 그룹이 표시되지 않는 경우 해당 그룹이 숨겨져 있는 것일 수 있습니다. 숨겨진 개체를 보려면 탐색창에서 **Expand(**확장**)** 버튼을 클릭합니다.

다음에 수행할 작업

노드 그룹에 노드를 추가합니다. **Policy Service(**정책 서비스**)**에 있는 **Include node in node group(**노드 그룹의 노드 포함**)** 드롭다운 목록에서 노드 그룹을 선택하여 노드를 편집합니다.

구축에서 노드 제거

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

이 노드는 기본 PAN에서 받은 마지막 컨피그레이션을 유지하며 독립형 노드의 기본 페르소나(관리, 정책 서비스, 모니터링)로 지정됩니다. MnT 노드는 등록 취소하는 경우 더 이상 시스템 로그 대상으로 사용되지 않습니다.

기본 PSN의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. PSN이 독립형 노드가 된 후 엔드포인트 데이터를 유지하도록 하려는 경우 다음 중 하나를 수행할 수 있습니다.

- 기본 PAN에서 백업을 가져온 다음 PSN이 독립형 노드가 되면 해당 노드에서 이 데이터 백업을 복구합니다.
- PSN의 페르소나를 관리(보조 PAN)로 변경하고 관리 포털의 **Deployment(**구축**)** 창에서 데이터를 동기화한 다음 노드 등록을 취소합니다. 이제 이 노드에 모든 데이터가 포함됩니다. 그런 다음 보조 PAN을 기존 구축에 추가할 수 있습니다.

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

시작하기 전에

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

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** 제거할 보조 노드 옆의 확인란을 선택하고 **Deregister(**등록 취소**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

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

Cisco ISE 노드 종료

Cisco ISE CLI(Command Line Interface)에서 `halt` 명령을 실행하기 전에 Cisco ISE 애플리케이션 서비스를 중지하고 백업, 복구, 설치, 업그레이드 또는 제거 작업을 수행하지 않는 것이 좋습니다. Cisco ISE에서 이러한 작업 중 하나를 수행 중일 때 halt 명령을 실행하는 경우, 다음 경고 메시지 중 하나가 표시됩니다.

```
WARNING: A backup or restore is currently in progress! Continue with halt?
```

```
WARNING: An install/upgrade/remove is currently in progress! Continue with halt?
```

halt 명령을 사용 중일 때 프로세스를 실행하고 있지 않은 경우 또는 표시되는 경고 메시지에 대한 응답에 `Yes`를 입력하는 경우, 다음 질문에 응답해야 합니다.

```
Do you want to save the current configuration?
```

기존 Cisco ISE 구성을 저장하기 위해 `Yes`를 입력하는 경우 다음 메시지가 표시됩니다.

```
Saved the running configuration to startup successfully.
```

참고 어플라이언스를 재부팅하기 전에 애플리케이션 프로세스를 중지하는 것이 좋습니다.

이는 Cisco ISE 재부팅에도 적용됩니다. 자세한 내용은 Cisco Identity Services Engine CLI Reference Guide를 참고해 주십시오.

독립형 Cisco ISE 노드의 호스트 이름 또는 IP 주소 변경

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

시작하기 전에

Cisco ISE 노드가 분산형 구축의 일부분인 경우에는 구축에서 해당 노드를 제거하고 독립형 노드인지를 확인해야 합니다.

단계 **1** Cisco ISE CLI에서 **hostname**, **ip address,** 또는 **ip domain-name** 명령을 사용하여 Cisco ISE 노드의 호스트 이름이나 IP 주소를 변경합니다.

단계 **2** 모든 서비스를 다시 시작하려면 Cisco ISE CLI에서 **application stop ise** 명령을 사용하여 Cisco ISE 애플리케이션 구성을 재설정합니다.

단계 **3** Cisco ISE 노드가 분산형 구축의 일부분인 경우에는 기존 PAN에 해당 노드를 등록합니다.

참고 Cisco ISE 노드를 등록하는 동안 호스트 이름을 사용하는 경우에는 *abc.xyz.com*과 같이 등록하려는 독립형 노드의 FQDN(Fully Qualified Domain Name)이 기본 PAN의 DNS 확인 가능 이름이어야 합니다. 그렇지 않으면 노드 등록이 실패합니다. DNS 서버에서 분산형 구축의 일부분인 Cisco ISE 노드의 IP 주소와 FQDN을 입력해야 합니다.

Cisco ISE 노드를 보조 노드로 등록하고 나면 기본 PAN이 IP 주소, 호스트 이름 또는 도메인 이름의 변경사항을 구축의 다른 Cisco ISE 노드로 복제합니다.