관리 ISE-PIC

ISE-PIC 노드 관리

보조 노드를 추가하거나 제거하고, 노드간에 데이터를 동기화하고, 보조 노드를 기본 노드로 승격하는 등의 작업을 수행합니다.

Cisco ISE-PIC 구축 설정

Cisco Identity Services Engine 하드웨어 설치 설명서에 설명된 것처럼 모든 노드에 Cisco ISE-PIC를 설치하고 나면 노드가 독립형 상태로 표시됩니다. 그러면 한 노드를 PAN(Primary Administration Node)으로 정의하고 보조 노드를 PAN에 등록해야 합니다.

모든 Cisco ISE-PIC 시스템 및 기능 관련 컨피그레이션은 PAN에서만 수행되어야 합니다. PAN에서 수행한 컨피그레이션 변경 사항은 구축 환경의 보조 노드로 복제됩니다. 보조 노드에서 수행할 수 있는 유일한 작업은 해당 보조 노드를 PAN으로 승격하는 것입니다.

보조 노드를 PAN으로 등록한 후에 보조 노드의 관리 포털에 로그인하는 동안 PAN의 로그인 자격 증명을 사용해야 합니다.

기본 노드에서 보조 ISE-PIC 노드로의 데이터 복제

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

전체 복제는 일반적으로 ISE-PIC 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-PIC 노드

를 동기화할 수 있습니다. Cisco ISE-PIC 관리 포털의 구축 페이지에 있는 노드 상태 열에서 복제 상태를 확인할 수 있습니다. Cisco ISE-PIC 노드를 보조 노드로 등록하거나 PAN과의 수동 동기화를 수행하는 경우 노드 상태에는 요청한 작업이 진행 중임을 의미하는 주황색 아이콘이 표시됩니다. 작업이 완료되면 노드 상태는 보조 노드가 PAN과 동기화됨을 나타내는 녹색으로 바뀝니다.

Cisco ISE-PIC에서 노드 수정의 효과

Cisco ISE-PIC 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)
- 노드 승격(보조에서 기본으로)
- 기본 노드에서 백업을 복원하면 동기화 작업이 트리거되어 기본 노드에서 보조 노드로 데이터 복제

구축에서 2노드를 설정하기 위한 지침

Cisco ISE-PIC를 설정하기 전에 다음 정보를 신중히 읽어보십시오.

- 두 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-PIC 설치 시 Cisco ISE-PIC Admin 비밀번호를 구성합니다. 이전의 Cisco ISE-PIC Admin 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(Domain Name System) 서버를 구성합니다. DNS 서버에서 구축에 포함되는 두 Cisco ISE-PIC 노드의 IP 주소 및 FQDN(Fully Qualified Domain Name)을 입력합니다. 그렇지 않으면, 노드 등록이 실패합니다.
- DNS 서버의 고가용성 구축에 있는 두 Cisco ISE-PIC 노드에 대한 정방향 및 역방향 DNS 조회를 구성합니다. 그렇지 않으면 Cisco ISE-PIC 노드를 등록하고 다시 시작할 때 구축 관련 문제가 발생할 수 있습니다. 두 노드에 대해 역방향 DNS 조회가 구성되지 않은 경우 성능이 저하될 수 있습니다.
- (선택 사항) Cisco ISE-PIC를 PAN에서 제거하려면 보조 Cisco ISE-PIC 노드를 PAN에서 등록 취소합니다.
- PAN 및 보조 노드로 등록하려는 독립형 노드에서 동일한 버전의 Cisco ISE-PIC를 실행하고 있는지 확인합니다.

구축 노드 확인

Deployment Nodes(구축 노드**)** 창에서는 구축에 포함된 모든 ISE-PIC 노드를 확인할 수 있습니다.

단계 **1** 기본 Cisco ISE-PIC 관리 포털에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

구축에 속하는 모든 Cisco ISE 노드가 나열됩니다.

보조 **Cisco ISE-PIC** 노드 등록

보조 노드를 등록하고 나면 보조 노드의 컨피그레이션이 기본 노드의 데이터베이스에 추가되며 보조 노드의 애플리케이션 서버가 재시작됩니다. 재시작이 완료된 후 PAN의 구축 페이지에서 모든 컨피그레이션 변경사항을 확인할 수 있습니다. 그러나 변경사항이 적용되어 구축 페이지에 표시될 때까지는 5분 정도 걸릴 수 있습니다.

단계 **1** PAN에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.
구축에 보조 노드가 등록되지 않은 경우 **Add Secondary Node(**보조 노드 추가**)** 섹션이 페이지 하단에 나타납니다.

단계 **3** **Add Secondary Node(**보조 노드 추가**)** 섹션에서 보조 Cisco ISE 노드의 DNS 확인 가능 호스트 이름을 입력합니다.

Cisco ISE-PIC 노드를 등록하는 동안 호스트 이름을 사용하는 경우에는 *abc.xyz.com*과 같이 등록하려는 독립형 노드의 FQDN(Fully Qualified Domain Name)이 PAN의 DNS 확인 가능 이름이어야 합니다. 그렇지 않으면 노드 등록이 실패합니다. DNS 서버에서 보조 노드의 FQDN 및 IP 주소를 이전에 정의한 상태여야 합니다.

단계 **4** Username(사용자 이름) 및 Password(비밀번호) 필드에 독립형 노드의 UI 기반 관리자 자격 증명을 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE-PIC가 보조 노드에 연결하여 호스트 이름, 기본 게이트웨이 등의 몇 가지 기본 정보를 가져온 다음 표시합니다.

구축에 보조 노드가 등록되면 노드가 재시작되며, 구축 페이지에서 보조 노드 정보가 표시되기까지 최대 5분이 걸릴 수 있습니다.

보조 노드가 성공적으로 등록되면 구축 페이지의 **Secondary Node(**보조 노드**)** 섹션에 해당 노드에 대한 세부 사항이 표시됩니다.

보조 노드가 정상적으로 등록되면 노드 등록 성공을 확인하는 경보가 PAN에 수신됩니다. 보조 노드를 PAN에 등록할 수 없는 경우에는 경보가 생성되지 않습니다. 노드가 등록되면 해당 노드에서 애플리케이션 서버가 재시작됩니다. 등록 및 데이터베이스 동기화가 성공한 후 기본 관리 노드의 자격 증명을 입력하여 보조 노드의 사용자 인터페이스에 로그인합니다.

참고 구축의 기존 기본 노드 외에 새 노드를 정상적으로 등록하면 새로 등록된 노드에 해당하는 경보는 표시되지 않습니다. 컨피그레이션 변경됨 경보는 새로 등록된 노드에 해당하는 정보를 반영합니다. 이 정보를 통해 새 노드 등록 성공을 확인할 수 있습니다.

기본 및 보조 **Cisco ISE-PIC** 노드 동기화

기본 PAN을 통해서만 Cisco ISE-PIC의 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** 다음 메뉴를 선택합니다. .

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

보조 **PAN**을 기본으로 수동 승격

PAN 자동 장애 조치를 구성하지 않은 상태에서 기본 PAN에 오류가 보조 PAN을 수동으로 승격하여 새 기본 PAN으로 지정해야 합니다.

시작하기 전에

기본 PAN으로 승격하려는 두 번째 Cisco ISE-PIC 노드를 구성했는지 확인해 주십시오.

단계 **1** 보조 PAN의 사용자 인터페이스에 로그인합니다.

단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **3** **Promote to Primary(**기본으로 승격**)**를 클릭합니다.

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.

구축에서 노드 제거

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

노트의 등록을 취소하면 엔드포인트 데이터가 손실됩니다. 노드가 독립형 노드가 된 후 노드의 엔드포인트 데이터를 유지하려는 경우 기본 PAN에서 백업을 가져 와서 이 데이터 백업을 복원할 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 노드를 제거하려면 노드 등록을 취소해야 합니다. 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.

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

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **2** 보조 노드 세부 사항 옆에있는 **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-PIC 노드의 호스트 이름 또는 **IP** 주소 변경

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

시작하기 전에

Cisco ISE-PIC 노드가 2노드 구축의 일부분인 경우에는 구축에서 해당 노드를 제거하고 독립형 노드인지를 확인해야 합니다.

단계 **1** ISE-PIC 노드의 호스트 이름 또는 IP 주소는 **hostname**, **ip address,** 또는 **ip domain-name** 명령을 사용하여 변경할 수 있습니다.

단계 **2** Cisco ISE-PIC CLI에서 **application stop ise** 명령을 사용하여 Cisco ISE 애플리케이션 컨피그레이션을 재설정하여 모든 서비스를 재시작합니다.

단계 **3** Cisco ISE-PIC 노드가 2노드 구축의 일부분인 경우에는 기존 PAN에 해당 노드를 등록합니다.

참고 Cisco ISE-PIC 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 구축의 일부분인 Cisco ISE-PIC 노드의 IP 주소와 FQDN을 입력해야 합니다.

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

Cisco ISE-PIC 어플라이언스 하드웨어 교체

Cisco ISE-PIC 어플라이언스 하드웨어는 문제가 있는 경우에만 교체해야 합니다. 소프트웨어 문제의 경우에는 어플라이언스를 재이미지화하고 Cisco ISE-PIC 소프트웨어를 다시 설치할 수 있습니다.

단계 **1** 새 노드에서 Cisco ISE-PIC 소프트웨어를 재이미지화하거나 다시 설치합니다.

단계 **2** 기본 및 보조 PAN용 UDI가 포함된 라이센스를 얻어 기본 PAN에 설치합니다.

단계 **3** 교체한 기본 PAN에서 백업을 복원합니다.

복원 스크립트는 보조 PAN에서 데이터 동기화를 시도하지만 현재는 보조 PAN이 독립형 노드이므로 동기화가 실패합니다. 데이터는 기본 PAN에서 백업을 가져온 시간으로 설정됩니다.

단계 **4** 새 노드를 보조 노드로 기본 PAN에 등록합니다.

ISE-PIC 설치 관리

패치를 설치하거나, 백업을 실행하거나, 시스템 복원을 구현합니다.

소프트웨어 패치 설치

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)** 선택한 다음 설치를 클릭합니다.

단계 **2** **Browse(**찾아보기**)**를 클릭하여 Cisco.com에서 다운로드한 패치를 선택합니다.

단계 **3** **Install(**설치**)**을 클릭하여 패치를 설치합니다.

패치가 PAN에 설치되고 나면 Cisco ISE-PIC에서 로그아웃되고 다시 로그인하려면 몇 분 정도 기다려야 합니다.

참고 패치 설치가 진행 중일 때

Patch Management(패치 관리) 페이지에서 액세스할 수 있는 기능은 **Show Node Status(**노드 상태 표시**)**뿐입니다.

단계 4 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)** 그런 다음 패치 설치 페이지로 돌아갑니다.

단계 5 보조 노드에 설치한 패치 옆의 라디오 버튼을 클릭하고 **Show Node Status(**노드 상태 표시**)**를 클릭하여 설치가 완료되었는지 확인합니다.

다음에 수행할 작업

보조 노드에 패치를 설치해야 하는 경우에는 노드가 작동 중인지 확인한 다음 이 프로세스를 반복하여 나머지 노드에 패치를 설치합니다.

Cisco ISE-PIC 소프트웨어 패치

Cisco ISE-PIC 소프트웨어 패치는 일반적으로 누적됩니다. Cisco ISE-PIC를 사용하면 CLI 또는 GUI에서 패치 설치 및 롤백을 수행할 수 있습니다.

기본 PAN에서 구축 내 Cisco ISE-PIC 서버에 패치를 설치할 수 있습니다. 기본 PAN에서 패치를 설치하려면 Cisco.com에서 클라이언트 브라우저를 실행하는 시스템에 패치를 다운로드해야 합니다.

GUI에서 패치를 설치하는 경우에는 패치가 먼저 기본 PAN에 자동으로 설치됩니다. 그런 다음 GUI에 나열된 순서대로 구축의 다른 노드에 패치를 설치합니다. 노드가 업데이트되는 순서는 제어할 수 없습니다. 패치 버전을 수동으로 설치, 롤백, 확인할 수도 있습니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > System(**시스템**) > Maintenance(**유지 보수**) > Patch Management(**패치 관리**)**.

CLI에서 패치를 설치하는 경우 노드가 업데이트되는 순서를 제어할 수 있습니다. 그러나 기본 PAN에 패치를 먼저 설치하는 것이 좋습니다.

전체 구축을 업그레이드하기 전에 일부 노드에서 패치를 검증하려면 CLI를 사용하여 선택한 노드에 패치를 설치하면 됩니다. 다음 CLI 명령을 사용하여 패치를 설치합니다.

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

자세한 내용은 Cisco Identity Services Engine CLI 참조 설명서의 'EXEC 모드의 Cisco ISE CLI 명령' 장에서 '패치 설치' 섹션을 참조하십시오.

필요한 패치 버전을 직접 설치할 수 있습니다. 예를 들어 현재 Cisco ISE 2.x를 사용 중이고 Cisco ISE 2.x 패치 5를 설치하려는 경우 이전 패치(이 예에서는 ISE 2.x 패치 1~4)를 설치하지 않고 Cisco ISE 2.x 패치 5를 직접 설치할 수 있습니다. 패치 버전을 CLI에서 보려면 다음 CLI 명령을 사용합니다.

```
show version
```

소프트웨어 패치 설치 지침

ISE 노드에 패치를 설치하면 설치가 완료된 후 노드가 재부팅됩니다. 다시 로그인하려면 몇 분 동안 기다려야 할 수 있습니다. 패치 설치를 유지 보수 기간으로 예약하면 일시적인 중단을 방지할 수 있습니다.

네트워크에 구축된 Cisco ISE-PIC 버전에 적용할 수 있는 패치를 설치해야 합니다. Cisco ISE-PIC는 모든 버전 불일치와 패치 파일의 오류를 보고합니다.

참고 Cisco ISE 패치는 ISE-PIC에도 설치할 수 있습니다.

Cisco ISE-PIC에 현재 설치되어 있는 패치보다 낮은 버전의 패치는 설치할 수 없습니다. 마찬가지로, 상위 버전이 현재 Cisco ISE-PIC에 설치되어 있는 경우 하위 버전의 패치 변경 사항을 롤백할 수 없습니다. 예를 들어 Cisco ISE-PIC 서버에 패치 3이 설치된 경우 1 또는 2 패치를 설치하거나 롤백할 수 없습니다.

2노드 구축의 일부인 기본 PAN에서 패치를 설치하는 경우 Cisco ISE-PIC는 기본 노드에 패치를 설치한 다음 보조 노드에 설치합니다. 패치가 기본 PAN에 성공적으로 설치되면 Cisco ISE-PIC가 보조 노드에서 패치 설치를 계속합니다. 기본 PAN에서 패치 설치가 실패하면 보조 노드에서 설치가 진행되지 않습니다.

소프트웨어 패치 롤백

다중 노드 구축에 속한 PAN에서 패치를 롤백하면 Cisco ISE-PIC는 기본 노드에서 패치를 롤백한 다음 구축의 보조 노드에서 패치를 롤백합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 보수**)** > **Patch Management(**패치 관리**)**.

단계 **2** 변경사항을 롤백하려는 패치 버전의 라디오 버튼을 클릭하고 **Rollback(**롤백**)**을 클릭합니다.

참고 패치 롤백이 진행 중일 때 패치 관리 페이지에서 액세스할 수 있는 기능은 **Show Node Status(**노드 상태 표시**)**뿐입니다.

패치가 PAN에서 롤백되고 나면 Cisco ISE에서 로그아웃되며, 몇 분 동안 기다려야 다시 로그인할 수 있습니다.

단계 **3** 로그인한 후 페이지 맨 아래의 **Alarms(**경보**)** 링크를 클릭하면 롤백 작업의 상태를 확인할 수 있습니다.

단계 **4** 패치 롤백의 진행률을 확인하려면 패치 관리 페이지에서 패치를 선택하고 **Show Node Status(**노드 상태 표시**)**를 클릭합니다.

단계 **5** 보조 노드에서 패치의 라디오 버튼을 클릭하고 **Show Node Status(**노드 상태 표시**)**를 클릭하면 구축의 모든 노드에서 패치가 롤백되었는지를 확인할 수 있습니다.

보조 노드에서 패치가 롤백되지 않은 경우에는 해당 노드가 작동 중인지 확인한 다음 이 프로세스를 반복하여 나머지 노드에서 변경사항을 롤백합니다. Cisco ISE-PIC는 해당 버전의 패치가 아직 설치되어 있는 노드에서만 패치를 롤백합니다.

소프트웨어 패치 롤백 지침

구축의 Cisco ISE-PIC 노드에서 패치를 롤백하려면 먼저 PAN에서 변경 사항을 롤백해야 합니다. 작업이 성공한 경우 패치가 보조 노드에서 롤백됩니다. PAN에서 롤백 프로세스가 실패하면 패치가 보조 노드에서 롤백되지 않습니다.

Cisco ISE-PIC가 보조 노드에서 패치를 롤백하는 동안 PAN GUI에서 다른 작업을 계속 수행할 수 있습니다. 롤백 후에는 보조 노드가 다시 시작됩니다.

백업 및 복원

참고 Cisco ISE-PIC는 대부분의 경우 Cisco ISE 백업 및 복원 절차와 동일하게 작동하므로 Cisco ISE라는 용어는 경우에 따라 Cisco ISE-PIC와 관련된 작업 및 기능을 나타내는 의미로 사용됩니다.

Cisco ISE-PIC에서는 기본 또는 독립형 노드의 데이터를 백업할 수 있습니다. 백업은 CLI 또는 사용자 인터페이스에서 수행할 수 있습니다.

Cisco ISE-PIC에서는 다음 데이터 유형을 백업할 수 있습니다.

- 컨피그레이션 데이터 - 애플리케이션별 데이터와 Cisco ADE 운영 체제 컨피그레이션 데이터를 모두 포함합니다.
- 작업 데이터 - 모니터링 및 문제 해결 데이터를 포함합니다.

리포지토리 백업 및 복원

Cisco ISE-PIC에서는 리포지토리를 생성하거나 삭제할 수 있습니다. 다음과 같은 리포지토리 유형을 생성할 수 있습니다.

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

KVM을 사용하여 생성한 가상 CD-ROM의 리포지토리 유형으로 CD-ROM을 생성할 수 있습니다.

참고 리포지토리는 각 디바이스에 대해 로컬입니다.

참고 리포지토리 크기는 소규모 구축(100개 엔드포인트 이하)인 경우 10GB, 중간 규모 구축인 경우 100GB, 대규모 구축인 경우 200GB를 사용하는 것이 좋습니다.

리포지토리 생성

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

- CLI를 통해 생성하는 리포지토리는 로컬에 저장되며 다른 구축 노드로 복제되지 않습니다. 이러한 리포지토리는 GUI의 리포지토리 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 ISE-PIC에서 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.

시작하기 전에

- 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** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Repository(**저장소**)**를 선택합니다.

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

단계 **3** 새 리포지토리를 설정하는 데 필요한 값을 입력합니다. 필드에 대한 설명은 리포지토리 설정, 11 페이지를 참고하십시오.

단계 **4** 리포지토리를 생성하려면 **Submit(**제출**)**을 클릭합니다.

단계 **5** 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 리포지토리를 생성할 때 입력한 경로가 없으면

  ```
  %Invalid Directory
  ```

  오류가 표시됩니다.

- 온디맨드 백업을 실행하거나 백업을 예약합니다.

리포지토리 설정

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

표 *1:* 리포지토리 설정

필드	사용 지침
Repository(리포지토리)	리포지토리의 이름을 입력합니다. 영숫자 문자를 입력할 수 있으며 최대 길이는 80자입니다.
Protocol(프로토콜)	사용 가능한 프로토콜 중에서 사용하려는 프로토콜 하나를 선택합니다.
호스트	(TFTP, HTTP, HTTPS, FTP, SFTP 및 NFS의 경우 필수) 리포지토리를 생성할 서버의 호스트 이름 또는 IPv4 주소(IPv4 또는 IPv6)를 입력합니다. 참고 IPv6 주소를 사용해 리포지토리를 추가하는 경우 ISE eth0 인터페이스가 IPv6 주소로 구성되어야 합니다.

필드	사용 지침
Path(경로)	리포지토리의 경로를 입력합니다. 경로는 유효해야 하며 리포지토리를 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.

관련 항목

리포지토리 백업 및 복원

리포지토리 생성, 10 페이지

SFTP 리포지토리에서 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 운영 체제 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 PAN에 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.

온디맨드 백업 수행

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

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

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

- 옵션 **1:**

  CLI를 통해 소스 ISE-PIC 노드에서 CA 인증서를 내보내고 CLI를 통해 대상 시스템으로 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발행한 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 ISE-PIC의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 백업 파일을 저장할 저장소를 생성했는지 확인합니다.
- 로컬 리포지토리를 사용하여 백업해서는 안 됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Backup and Restore(**백업 및 복구**)**.

단계 **2** 백업 유형을 Configuration(구성) 또는 Operational(운영) 중에서 선택합니다.

단계 **3** **Backup Now(**지금 백업**)**를 클릭합니다.

단계 **4** 필요한 값을 입력하여 백업을 수행합니다.

단계 **5** **Backup(**백업**)**을 클릭합니다.

단계 **6** 백업이 정상적으로 완료되었는지 확인합니다.

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

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 알람이 표시될 수 있습니다. 백업이 완료되면 CPU 사용률이 정상으로 돌아옵니다.

백업 예약

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

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

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

- 옵션 **1:**

  CLI를 통해 소스 ISE-PIC 노드에서 CA 인증서를 내보내고 CLI를 통해 대상 시스템으로 가져옵니다.

  장점**:** 소스 시스템에서 엔드포인트에 발행한 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.

  동의**:** 원래 소스 인증서 또는 원래 대상 인증서가 사용되므로 안정하기 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 ISE-PIC의 백업 데이터 유형에 대해 기본적으로 파악해야 합니다.
- 리포지토리를 구성했는지 확인합니다.
- 로컬 리포지토리를 사용하여 백업해서는 안 됩니다.

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

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 복원) 페이지의 History(기록) 테이블에서 사용할 수 있습니다.

실패한 백업의 경우 Cisco ISE-PIC가 경보를 트리거합니다. 백업 기록 페이지에 실패 이유가 제공됩니다. 실패 이유는 운영 감사 보고서에서도 확인할 수 있습니다. 장애 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 운영 체제 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 알람을 생성합니다. Cisco ISE가 구성된 모든 NTP 서버와 동기화할 수 없는 경우 Cisco ISE에서 NTP 동기화 실패 알람을 생성합니다. NTP 서비스가 중지되었거나 동기화 문제가 있는 경우 Cisco ISE 백업이 실패할 수 있습니다. Alarms(알람) dashlet을 확인하고 NTP 동기화 또는 서비스 문제를 해결한 후에 백업 작업을 다시 시도하십시오.
- 다른 백업이 동시에 실행되고 있지 않은지 확인합니다.
- 구성한 리포지토리에 대해 사용 가능한 디스크 공간을 확인합니다.
  - 모니터링 데이터가 할당된 모니터링 데이터베이스 크기의 75%를 사용한 경우 모니터링(운영) 백업이 실패합니다. 예를 들어 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 복원 작업이 수행되지 않습니다.
- 리포지토리가 올바르게 구성되었는지 확인합니다.

Cisco ISE 복원 작업

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

참고 Cisco ISE-PIC의 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-PIC 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-PIC 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-PIC 노드에 해당 백업을 복원하려는 경우 복원 프로세스가 실패할 수 있습니다. 백업 파일의 타임스탬프가 백업을 복원하는 Cisco ISE-PIC 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-PIC 노드에서 컨피그레이션을 재설정하려면 Cisco ISE CLI에서 다음 명령을 입력합니다.
  - **application reset-config ise**
- 초기 Cisco ISE-PIC 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-PIC 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 PAN에서 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 ISE-PIC가 백업 파일을 저장하는 위치인 데이터 리포지토리가 필요합니다. 온디맨드 또는 예약 백업을 실행하려면 리포지토리를 생성해야 합니다.
- 독립형 노드에 오류가 발생하는 경우에는 컨피그레이션 백업을 실행하여 해당 노드를 복원해야 합니다. 기본 PAN에 오류가 발생하는 경우에는 보조 관리 노드를 기본 노드로 승격할 수 있습니다. 기본 PAN이 작동하면 기본 PAN에서 데이터를 복원할 수 있습니다.

참고 Cisco ISE-PIC는 트러블슈팅용으로 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.

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

구문 설명

restore	컨피그레이션 또는 운영 백업에서 데이터를 복원하려면 이 명령을 입력합니다.
filename	리포지토리에 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 리포지토리를 지정합니다.
repository-name	복원할 백업이 있는 리포지토리의 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 ISE-PIC에서 restore 명령을 사용하는 경우 Cisco ISE-PIC 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#
```

Related Commands

	설명
backup	백업을 수행하고(Cisco ISE-PIC 및 Cisco ADE OS) 리포지토리에 백업을 저장합니다.
backup-logs	시스템 로그를 백업합니다.
repository	백업 컨피그레이션을 위한 리포지토리 하위 모드로 진입합니다.
show repository	특정 리포지토리에 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.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Backup and Restore(**백업 및 복구**)**.

단계 **2** 컨피그레이션 백업 목록에서 백업 이름을 선택하고 **Restore(**복원**)**를 클릭합니다.

단계 **3** 백업 중에 사용한 암호화 키를 입력합니다.

단계 **4** **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 PAN에서 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.

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 얻으려면 Cisco ISE CLI에서 **backup-logs** 명령을 실행하고 ADE.log 파일을 확인해야 합니다.

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

기본 및 보조 노드 동기화

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

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Deployment(**구축**)**.

단계 **2** 복제 상태가 동기화되지 않은 경우 보조 노드 옆의 확인란을 선택합니다.

단계 **3** **Syncup**을 클릭하고 노드가 PAN과 동기화될 때까지 기다립니다. 이 프로세스가 완료될 때까지 기다려야 Cisco ISE-PIC 관리 포털에 다시 액세스할 수 있습니다.

2노드 구축에서 손실된 노드 복구

이 섹션에서는 2노드 구축에서 손실된 노드를 복구하는 데 사용할 수 있는 문제 해결 정보를 제공합니다. 다음 활용 사례 중 일부에서는 백업 및 복원 기능을, 다른 일부에서는 복제 기능을 사용하여 손실된 데이터를 복구합니다.

2노드 구축에서 기존 IP 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

2노드 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-PIC 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 라이센스를 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.

2노드 구축에서 새 IP 주소 및 호스트 이름을 사용하여 손실된 노드 복구

시나리오

2노드 구축에서 자연 재해로 인해 모든 노드가 손실되었습니다. 새 위치에서 새 하드웨어를 재이미지화했으며 새 IP 주소와 호스트 이름이 필요합니다.

예를 들어 N1(기본 정책 관리 노드/PAN) 및 N2(보조 노드)의 두 개 ISE-PIC 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-PIC 노드가 새 위치에서 대체되며, 새 호스트 이름은 N1A(PAN) 및 N2A(보조 노드)입니다. 이 시점에서 N1A 및 N2A는 독립형 노드입니다.

가정

구축의 모든 Cisco ISE-PIC 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. 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-PIC 노드를 도입한 후에는 이전 N1 노드에서 만든 백업을 복원해야 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. 이 경우 변경하기 전에 작성한 백업을 복원하여 원래 컨피그레이션으로 되돌릴 수 있습니다.

가능한 원인

N1(기본 정책 관리 노드 또는 기본 PAN)과 N2(보조 정책 관리 관리 노드)로 구성된 노드 2개와 N1 노드 백업 1개가 지원됩니다. 일부 컨피그레이션을 잘못 변경하여 N1에서 변경 사항을 제거하고자 합니다.

솔루션

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

2노드 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-PIC 노드가 2개 있는데 하드웨어 문제로 인해 N1에 장애가 발생한다고 가정해 보겠습니다.

가정

2노드 구축의 기본 노드에만 장애가 발생했습니다.

해결 단계

1. N2 관리자 포털에 로그인합니다. Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 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.

2노드 구축에서 장애 발생 시 보조 노드 복구

시나리오

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

해결 단계

1. 보조 노드를 기본 독립형 상태로 재이미지화합니다.
2. 기본 노드에서 관리 포털에 로그인하고 보조 노드를 삭제합니다.
3. 보조 노드를 다시 등록합니다.

   데이터가 기본 노드에서 보조 노드로 복제됩니다. 복원은 수행하지 않아도 됩니다.

Database Purge(데이터베이스 제거)

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

데이터베이스 비우기를 위한 지침

다음은 데이터베이스 디스크 사용량과 관련하여 따라야 하는 지침입니다.

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

운영 데이터 제거

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.

관련 항목

이전 운영 데이터 비우기, 25 페이지

이전 운영 데이터 비우기

운영 데이터는 일정 기간 동안 서버에 수집되며, 즉시 또는 정기적으로 비울 수 있습니다.

단계 **1** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Maintenance(**유지 관리**)** > **Operational Data Purging(**운영 데이터 제거**)**.

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. ISE-PIC에서는 RADIUS 또는 TACACS 기능을 제공하지는 않지만 일부 인프라가 Cisco ISE와 공유되므로 데이터베이스에서 이러한 정보를 주기적으로 제거해야 할 수 있습니다.
  2. **Repository(**저장소**)** 영역에서 **Enable Export Repository(**내보내기 저장소 활성화**)** 체크 박스를 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 테이블의 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.

전체 **ISE** 설치로 **ISE-PIC** 업그레이드

Cisco ISE-PIC는 전체 CISCO ISE GUI를 기반으로 단순하며 직관적인 GUI로 표시됩니다. 그래서 ISE-PIC를 설치하면 ISE로 쉽고 효율적으로 업그레이드할 수 있습니다. ISE-PIC에서 ISE 기본 라이센스로 업그레이드할 때 ISE는 업그레이드하기 전에 ISE-PIC에서 이용할 수 있었던 모든 기능을 계속 제공하며, 업그레이드한 ISE-PIC 노드를 기본 PAN으로 사용한다면 이전에 구성한 설정을 다시 구성하지 않아도 됩니다.

참고 업그레이드한 기존 ISE-PIC 노드를 기본 PAN으로 사용하지 않는다면, 노드에 있는 데이터는 업그레이드할 때 삭제되며 사용자는 새로 추가된 노드에서 기존 전체 ISE 구축의 데이터에 액세스할 수 있습니다.

먼저 노드에 ISE-PIC Upgrade License(업그레이드 라이센스)를 설치한 다음 아래 작업을 수행하면 전체 업그레이드 프로세스를 수행할 수 있습니다.

- 업그레이드한 ISE-PIC 노드를 기존 ISE 구축에 추가합니다.
- 또는 Base 라이센스를 하나 이상 설치합니다.

참고 전체 Cisco ISE 구축으로 업그레이드하면 이전 Cisco ISE-PIC 설치로 롤백할 수 없습니다.

ISE로의 업그레이드가 제공하는 이점에 관한 자세한 내용은 ISE-PIC와 ISE/CDA 비교 항목을 참고하십시오.

라이선스를 등록하여 **ISE**로 업그레이드

시작하기 전에

Cisco ISE-PIC 영구 라이선스를 설치했는지 확인합니다. 또한 다음 방법 중 하나로 노드를 업그레이드할 수 있습니다.

- 기존 전체 ISE 구축에 ISE-PIC 노드 추가 - 업그레이드된 ISE-PIC 노드가 기존 구축을 보조 노드로 조인합니다. 이렇게 하려면 Cisco ISE-PIC 업그레이드 라이센스를 사용하여 이 작업의 단계를 5단계까지만 수행합니다. ISE-PIC 노드를 보조 노드로 추가할 경우 기존 ISE 구축의 모든 데이터는 유지되며 새로 조인된(업그레이드된) ISE-PIC 노드에 동기화되지만 원래 ISE-PIC 노드 데이터는 유지되지 않습니다. 이 라이센스는 Cisco 담당자에게 문의하십시오.

- 특정 ISE-PIC 노드를 ISE 구축의 기본 또는 독립형 노드로 업그레이드 - 기존의 모든 데이터를 보존하면서 ISE-PIC 노드를 업그레이드합니다. Cisco ISE-PIC 업그레이드 라이센스 및 Cisco ISE 기본 라이센스에 대해서는 Cisco 담당자에게 문의하십시오.

라이선싱 모델에 대한 자세한 내용은 다음을 참조하십시오. Cisco ISE-PIC 라이센싱

단계 **1** 보조 노드가 설치되어있는 경우 Cisco ISE-PIC 기본 노드 설치에서 **Administration(**관리**)** > **Deployment(**구축**)** 을 선택하고 보조 노드의 등록을 해제합니다. 그러면 두 노드가 모두 기본 노드가 되며 둘 중 하나를 업그레이드할 수 있습니다.

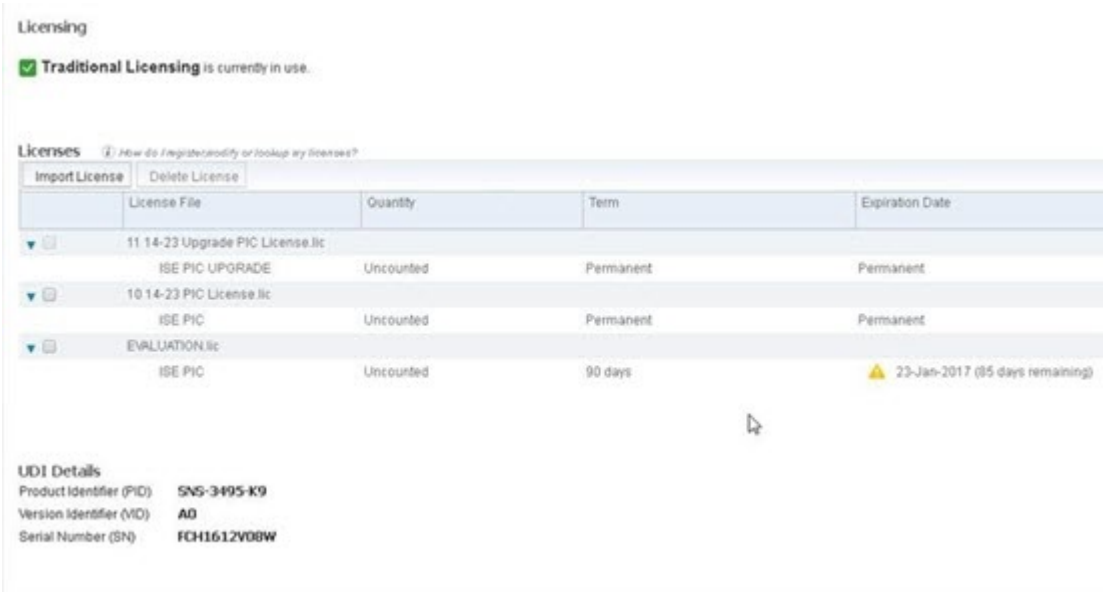
단계 **2** 다음 메뉴를 선택합니다. **Administration(**관리**)** > **Licensing(**라이센싱**)**.

단계 **3** **Import License(**라이센스 가져오기**)**를 클릭합니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭하고 업그레이드 라이센스 파일을 찾아 **OK(**확인**)**를 클릭합니다.

단계 **5** 참고 이 ISE-PIC 노드를 기존 ISE 구축에 추가하는 경우 이 단계를 완료하면 업그레이드를 완료한 것이므로 이제 해당 구축의 기본 노드에서 노드를 등록하여 노드를 추가할 수 있습니다. 자세한 내용은 *Cisco Identity Services Engine* 관리 설명서를 참조하십시오.

Import New License File(새 라이선스 파일 가져오기**)** 화면에서 **Import(**가져오기**)**를 클릭합니다.
다음과 같은 업그레이드 라이센스를 포함하여 업그레이드 테이블이 이제 새로 고쳐집니다.



단계 **6** 이 업그레이드된 노드를 전체 ISE 구축의 기본 노드로 만들려면 지금 기본 라이선스를 가져오십시오. **Import License(**라이선스 가져오기**)**를 다시 클릭합니다.

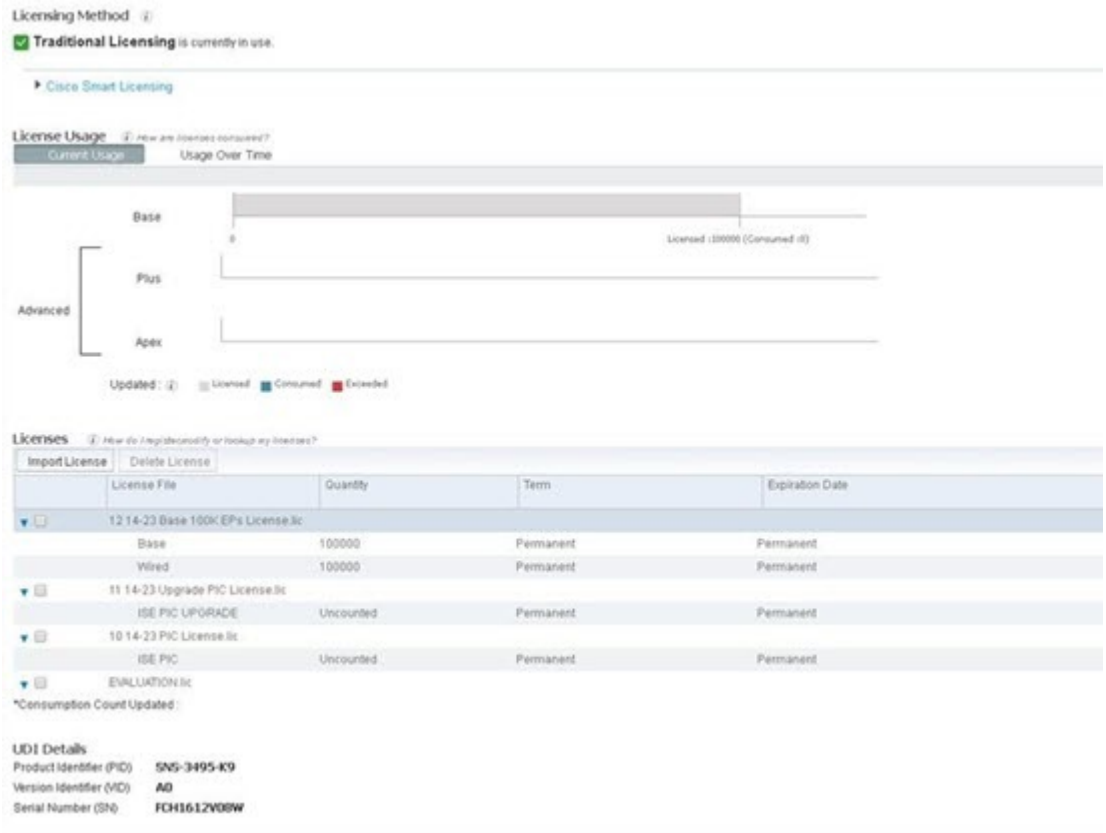
단계 **7** **Choose File(**파일 선택**)**을 클릭하고 Cisco 담당자로부터 받은 전체 ISE 기본 라이센스를 찾은 다음 **OK(**확인**)**를 클릭합니다.

단계 **8** **Import New License File(**새 라이선스 파일 가져오기**)** 화면에서 **Import(**가져오기**)**를 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.
ISE의 기본 노드로의 업그레이드가 시작되고 다음 메시지가 나타납니다. 이 노드는 현재 백그라운드에서 *ISE*로 업그레이드되고 있습니다. 몇 분 정도 기다렸다가 *ISE*에 로그인하십시오.

단계 **10** **OK(**확인**)**를 클릭합니다.

다음과 같은 기본 라이센스를 포함하여 업그레이드 테이블이 이제 새로 고쳐집니다.



몇 분 후에 로그인 화면이 나타납니다. 다시 로그인하여 전체 ISE 기본 라이센스 설치에서 제공하는 모든 메뉴에 액세스합니다.

이제 기본 ISE-PIC 노드를 전체 ISE 설치에서 기본 노드로 업그레이드했으며 이전 보조 노드는 이제 ISE-PIC 독립형 설치에서 기본이자 유일한 노드입니다. 이제 동일한 방식으로 마지막 ISE-PIC 노드를 개별적으로 업그레이드할 수 있습니다.

API 제공자에서 **ISE-PIC**

역할 기반 액세스 제어

Cisco ISE-PIC에서는 특정 시스템 작동 권한을 관리자에게 허용하거나 거부하는 RBAC(Role-based Access Control) 정책을 정의할 수 있습니다. 이러한 RBAC 정책은 개별 관리자 또는 관리자가 속하는 관리 그룹의 ID에 따라 정의됩니다.

보안을 강화하고 관리 포털에 액세스할 수 있는 사용자를 효과적으로 제어하려면 다음을 수행합니다.

- 원격 클라이언트의 IP 주소에 따라 관리 액세스 설정 구성
- 관리 계정을 위한 강력한 비밀번호 정책 정의
- 관리 GUI 세션에 대한 세션 시간 초과 구성

Cisco ISE-PIC 관리자

관리자는 관리 포털을 사용하여 다음을 수행할 수 있습니다.

- 구축 노드 모니터링, 문제 해결을 관리합니다.
- Cisco ISE-PIC 서비스관리자 계정 및 시스템 컨피그레이션 및 작업을 관리합니다.
- 관리자 및 사용자 비밀번호를 변경합니다.

CLI 관리자는 Cisco ISE 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

설치 중에 구성하는 사용자 이름 및 비밀번호는 CLI에 대한 관리 액세스 용도로만 사용됩니다. 이 역할은 CLI 관리자라고도 하는 CLI 관리 사용자로 간주됩니다. 기본적으로 CLI 관리 사용자의 사용자 이름은 admin이고 비밀번호는 설치 과정에서 정의됩니다. 비밀번호는 기본값이 없습니다. 이 CLI 관리 사용자는 기본 관리 사용자이며 이 사용자 계정은 삭제할 수 없습니다. 그러나 이 계정에 대한 비밀번호를 활성화, 비활성화 또는 변경하는 옵션을 포함하여 다른 관리자가 수정할 수 있습니다.

관리자를 만들 수도 있고 기존 사용자를 관리자 역할로 승격시킬 수도 있습니다. 또한 해당 관리 권한을 비활성화하여 관리자를 단순 네트워크 사용자 상태로 강등시킬 수도 있습니다.

관리자는 컨피그레이션에 대한 로컬 권한이 있으며 Cisco ISE-PIC 시스템을 운영하는 사용자입니다.

관리자는 하나 이상의 관리 그룹에 할당됩니다. 이러한 관리자 그룹은 다음 섹션에서 설명하는 것처럼 사용자 편의를 위해 시스템에 미리 정의되어 있습니다.

관련 항목

Cisco ISE-PIC 관리자 그룹, 29 페이지

Cisco ISE-PIC 관리자 그룹

관리자 그룹은 Cisco ISE-PIC의 RBAC(Role-based Access Control) 그룹입니다. 같은 그룹에 속하는 모든 관리자는 공통 ID를 공유하고 동일한 권한을 갖습니다. 특정 관리 그룹의 멤버인 관리자의 ID는 권한 부여 정책에서 조건으로 사용될 수 있습니다. 한 관리자는 여러 관리자 그룹에 속할 수 있습니다.

모든 액세스 수준을 가진 관리자 계정을 사용하여 액세스 권한이 있는 창에서 해당 개체를 수정하거나 삭제할 수 있습니다.

다음 테이블에는 Cisco ISE-PIC에 미리 정의된 관리자 그룹과 함께 해당 그룹의 멤버가 수행할 수 있는 작업이 나열되어 있습니다. 이러한 사전 정의된 그룹만 시스템에서 관리자 사용자를 정의하는 데 사용할 수 있습니다.

표 *2: Cisco ISE* 관리자 그룹, 액세스 레벨, 권한 및 제한 사항

관리자 그룹 역할	액세스 레벨	권한	제한 사항
슈퍼 관리자	모든 Cisco ISE-PIC 관리 기능. 기본 관리자 계정은 이 그룹에 속합니다.	모든 Cisco ISE-PIC 리소스에 대한 생성, 읽기, 업데이트, 삭제 및 실행(CRUDX) 권한	
ERS(External RESTful Services) 관리자	GET, POST, DELETE, PUT 등 모든 ERS API 요청에 대한 전체 액세스	• ERS API 요청 생성, 읽기, 업데이트 및 삭제	이 역할은 내부 사용자, ID 그룹 및 엔드포인트를 지원하는 ERS 권한 부여에만 사용됨

CLI 관리자와 웹 기반 관리자의 권한

CLI 관리자는 Cisco ISE-PIC 애플리케이션을 시작 및 중지하고, 소프트웨어 패치를 적용하고, Cisco ISE-PIC 어플라이언스를 업그레이드, 다시 로드 또는 종료하고, 모든 시스템 및 애플리케이션 로그를 볼 수 있습니다. CLI 관리자에게는 특수 권한이 부여되므로 Cisco ISE-PIC 구축을 구성하고 관리하기 위해서는 CLI 관리자 자격 증명을 보호하고 웹 기반 관리자를 생성하는 것이 좋습니다.

새 관리자 생성

Cisco ISE-PIC 관리자에게는 특정 관리 작업을 수행하기 위한 특정 역할이 할당된 계정이 있어야 합니다. 관리자 계정을 생성하고 이러한 관리자가 수행해야 하는 관리 작업을 기준으로 해당 관리자에게 하나 이상의 역할을 할당할 수 있습니다.

Admin Users(관리자 사용자**)** 창을 사용하여 Cisco ISE-PIC 관리자의 특성에 대해 확인/생성/수정/삭제/상태 변경/복제/검색을 수행할 수 있습니다.

참고 관리자 사용자의 도메인이 CLI와 GUI에서 모두 동일할 경우 GUI에 가입하기 전에 Active Directory 액세스를 먼저 구성하는 것이 좋습니다. 그러지 않을 경우, GUI에서 도메인에 다시 가입해야 해당 도메인에 대한 인증 실패를 방지할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Admin Users(**관리자 사용자**)** > **Add(**추가**)** > **Create an Admin User(**관리자 사용자 생성**)**.

단계 **2** 필드에 값을 입력합니다. **Name(**이름**)** 필드에 입력할 수 있는 문자는 # $ ' ( ) * + -입니다. / @ _입니다.

단계 **3** **Submit(**제출**)**을 클릭하여 Cisco ISE-PIC 내부 데이터베이스에 새 관리자를 생성합니다.

관련 항목

- 읽기 전용 관리 정책
- 내부 읽기 전용 관리자 생성
- 읽기 전용 관리자를 위한 메뉴 액세스 사용자 지정
- 읽기 전용 관리자 그룹에 외부 그룹 매핑

Cisco ISE-PIC에 대한 관리 액세스

Cisco ISE-PIC 관리자는 자신이 속해 있는 관리 그룹에 따라 다양한 관리 작업을 수행할 수 있습니다. 이러한 관리 작업은 매우 중요합니다. 네트워크에서 Cisco ISE-PIC를 관리할 권한이 있는 사용자에게만 관리 액세스 권한을 부여하십시오.

Cisco ISE-PIC에서는 다음 옵션을 통해 웹 인터페이스에 대한 관리 액세스를 제어할 수 있습니다.

참고 Cisco ISE 서버가 네트워크에 추가되는 경우 웹 인터페이스가 작동하면 실행 중인 상태로 표시됩니다. 그러나 포스처 서비스와 같은 일부 고급 서비스를 사용하려면 시간이 더 오래 걸릴 수 있으므로 모든 서비스가 완전히 작동하는 데 시간이 추가로 소요될 수 있습니다.

관리 액세스 방법

여러 방법으로 Cisco ISE 서버에 연결할 수 있습니다. PAN은 관리자 포털을 실행하며, 관리자 포털에 로그인하려면 관리자 암호가 필요합니다. 다른 ISE 페르소나 서버는 SSH 또는 CLI를 실행하는 콘솔을 통해 액세스할 수 있습니다. 이 섹션에서는 각 연결 유형에 사용 가능한 프로세스 및 암호 옵션에 대해 설명합니다.

- **Admin password(**관리자 암호**)**: 설치하는 동안 생성한 Cisco ISE 관리 사용자는 기본적으로 45일 후에 타임아웃됩니다. 다음에서 암호 수명 주기를 끄는 방식으로 이를 방지할 수 있습니다. **Administration(**관리**)** > **System(**시스템**)** > **Admin Settings(**관리자 설정**)**. **Password Policy(**암호 정책**)** 탭을 클릭하고 **Password Lifetime(**암호 수명 주기**)** 아래에서 **Administrative passwords expire(**관리자 비밀번호 만료**)**를 선택 취소합니다.

  아니면 암호가 만료되고 나서 **application reset-passwd** 명령을 실행하여 CLI에서 관리자 암호를 재설정할 수 있습니다. 콘솔에 연결하여 CLI에 액세스하거나 ISE 이미지 파일을 재부팅하고 부팅 옵션 메뉴에 액세스하여 관리자 암호를 재설정할 수 있습니다.

- **CLI password(CLI** 암호**)**: 설치 중에 CLI 암호를 입력해야 합니다 잘못된 암호로 인해 CLI에 로그인하는 데 문제가 있는 경우 CLI 암호를 재설정할 수 있습니다. 콘솔에 연결하고 **password** CLI 명령을 실행하여 암호를 재설정합니다. 자세한 내용은 *ISE CLI* 참조를 확인하십시오.

-

관리자 액세스 설정

Cisco ISE-PIC를 사용하면 관리자 계정에 대한 일부 규칙을 정의하여 보안을 개선할 수 있습니다. 관리 인터페이스에 대한 액세스를 제한하여 관리자가 강력한 비밀번호를 사용하거나 비밀번호를 정기

적으로 변경하는 등의 작업을 하도록 강제할 수 있습니다. Cisco ISE-PIC의 관리자 계정 설정에서 정의하는 비밀번호 정책은 모든 관리자 계정에 적용됩니다.

Cisco ISE-PIC는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

동시 관리 세션 및 로그인 배너의 최대 수 구성

관리자에게 관리 웹 또는 CLI 인터페이스에 액세스하는 사용자를 알려 주는 동시 관리 GUI 또는 CLI(SSH) 세션 및 로그인 배너의 최대 수를 구성할 수 있습니다. 관리자 로그인 전과 후에 표시되는 로그인 배너를 구성할 수 있습니다. 이러한 로그인 배너는 기본적으로 비활성화됩니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Access Settings(**액세스 설정**)** > **Session(**세션**)**.

단계 **2** GUI 및 CLI 인터페이스를 통해 허용하려는 동시 관리 세션의 최대 수를 입력합니다. 동시 관리 GUI 세션의 유효한 범위는 1~20입니다. 동시 관리 CLI 세션의 유효한 범위는 1~10입니다.

단계 **3** 관리자 로그인 전에 Cisco ISE-PIC가 메시지를 표시하도록 하려면 **Pre-login banner(**로그인 전 배너**)** 체크 박스를 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **4** 관리자 로그인 후에 Cisco ISE-PIC가 메시지를 표시하도록 하려면 **Post-login banner(**로그인 후 배너**)** 체크 박스를 선택하고 텍스트 상자에 메시지를 입력합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

선택한 **IP** 주소에서 **Cisco ISE-PIC**로의 관리 액세스 허용

Cisco ISE-PIC에서는 관리자가 Cisco ISE-PIC 관리 인터페이스에 액세스할 수 있는 IP 주소 목록을 구성할 수 있습니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Access Settings(**액세스 설정**)** > **IP Access(IP** 액세스**)**.

단계 **2** **Allow only listed IP addresses to connect(**목록에 나열된 **IP** 주소만 연결 허용**)**를 선택합니다.

참고 포트 161(SNMP)에 대한 연결은 관리 액세스에 사용됩니다. 그러나 IP 액세스 제한이 구성된 경우, snmpwalk가 수행되는 출처 노드를 관리 액세스용으로 구성하지 않으면 snmpwalk는 실패합니다.

단계 **3** 액세스 제한용 IP 목록 구성 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** IP address(IP 주소) 필드에 IP 주소를 CIDR(Classless Interdomain Routing) 형식으로 입력합니다.

참고 이 IP 주소의 범위는 IPv4~IPv6입니다. 이제 하나의 ISE 노드에 대해 여러 IPv6 주소를 구성할 수 있습니다.

단계 **5** Netmask in CIDR format(CIDR의 네트워크 마스크 형식) 필드에 서브넷 마스크를 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다. 위의 과정을 반복하여 이 목록에 IP 주소 범위를 더 추가합니다.

단계 **7** **Save(**저장**)**를 클릭하여 변경사항을 저장합니다.

단계 **8** **Reset(**재설정**)**을 클릭하여 **IP Access(IP** 액세스**)** 페이지를 새로 고칩니다.

관리자 계정의 비밀번호 정책 구성

Cisco ISE-PIC에서는 보안을 강화하기 위해 관리자 계정용 비밀번호 정책을 생성할 수도 있습니다. 여기에서 정의하는 비밀번호 정책은 Cisco ISE-PIC의 모든 관리자 계정에 적용됩니다.

참고

- 내부 관리자 사용자에 대한 이메일 알림은 root@host로 전송됩니다. 이메일 주소를 구성 할 수 없으며 많은 SMTP 서버가 이 이메일을 거부합니다.

  이메일 주소를 변경할 수 있는 개선된 오픈 결함 CSCui5583을 따를 수 있습니다.

- Cisco ISE-PIC는 UTF-8 문자를 포함하는 관리자 비밀번호를 지원합니다.

단계 **1** ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**.

단계 **2** **Password Policy(**비밀번호 정책**)** 탭을 클릭하고 값을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭하여 관리자 비밀번호 정책을 저장합니다.

참고 로그인 시 외부 ID 저장소를 사용하여 관리자를 인증하는 경우, 관리자 프로파일에 적용되는 비밀번호 정책에 대해 이 설정이 구성되어 있더라도 외부 ID 저장소는 관리자의 사용자 이름과 비밀번호를 계속 검증합니다.

관리자 계정의 계정 비활성화 정책 구성

Cisco ISE-PIC에서는 구성된 연속 기간(일) 동안 관리자 계정이 인증되지 않은 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Admin Access(**관리 액세스**)** > **Authentication(**인증**)** > **Account Disable Policy(**계정 비활성화 정책**)**를 선택합니다.

단계 **2** **Disable account after *n* days of inactivity(n**일 동안 비활성 상태였던 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다.

이 옵션을 사용하면 구성된 연속 기간(일) 동안 관리자 계정이 비활성 상태인 경우 해당 관리자 계정을 비활성화할 수 있습니다.

단계 **3** 관리자에 대한 전역 계정 비활성화 정책을 구성하려면 **Save(**저장**)**를 클릭합니다.

관리자에 대한 세션 시간 초과 구성

Cisco ISE-PIC에서는 관리 GUI 세션이 비활성 상태로 계속 연결되어 있을 수 있는 시간을 결정할 수 있습니다. Cisco ISE-PIC가 관리자를 로그아웃 처리할 때까지의 시간을 분 단위로 지정할 수 있습니다. 세션 시간이 초과되고 나면 관리자는 다시 로그인해야 Cisco ISE-PIC 관리 포털에 액세스할 수 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Session Settings(**세션 설정**)** > **Session Timeout(**세션 시간 초과**)**.

단계 2 작업을 수행하지 않는 경우 관리자가 로그아웃될 때까지 Cisco ISE-PIC가 대기하도록 할 시간을 분 단위로 입력합니다. 기본값은 60분입니다. 유효한 범위는 6분~100분입니다.

단계 3 **Save(**저장**)**를 클릭합니다.

활성 관리 세션 종료

Cisco ISE-PIC는 필요한 경우 언제든지 세션을 선택하여 종료할 수 있도록 모든 활성 관리 세션을 표시합니다. 동시 관리 GUI 세션의 최대 수는 20개입니다. GUI 세션의 최대 수에 도달하면 슈퍼 관리자 그룹에 속하는 관리자가 로그인하여 일부 세션을 종료할 수 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Admin Access(**관리자 액세스**)** > **Session Settings(**세션 설정**)** > **Session Info(**세션 정보**)**.

단계 2 종료할 세션 ID 옆의 확인란을 선택하고 **Invalidate(**무효화**)**를 클릭합니다.

관리 포털에서 사용되는 포트

관리 포털은 HTTP 포트 80 및 HTTPS 포트 443을 사용하도록 설정되어 있으며 이러한 설정은 변경할 수 없습니다. 또한 Cisco ISE-PIC에서는 최종 사용자 포털이 동일한 포트를 사용하도록 할당할 수 없습니다. 이 기능으로 인해 관리 포털에 대한 위험이 감소합니다.

알림을 지원하도록 **SMTP** 서버 구성

알람에 대한 이메일 알림을 보내려면 SMTP(Simple Mail Transfer Protocol) 서버를 구성합니다.

이메일을 전송할 ISE 노드

다음 목록에는 분산 ISE 환경에서 이메일을 전송하는 노드가 나와 있습니다.

이메일 용도	이메일을 전송하는 노드
게스트 만료	기본 PAN
경보	활성 MnT
게스트 및 스폰서 포털의 스폰서 및 게스트 알림	PSN
비밀번호 만료	기본 PAN

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **SMTP Server(SMTP** 서버**)**.

단계 2 **SMTP server(SMTP** 서버**)** 필드에 아웃바운드 SMTP 서버의 호스트 이름을 입력합니다. Cisco ISE-PIC 서버에서 이 SMTP 호스트 서버에 액세스할 수 있어야 합니다. 이 필드의 최대 길이는 60자입니다.

단계 3 **Save(**저장**)**를 클릭합니다.

알람 알림의 수신자는 **Include system alarms in emails(**이메일에 시스템 알람 포함**)** 옵션이 활성화된 모든 내부 관리 사용자가 될 수 있습니다. 경보 알림을 보내기 위한 보낸 사람의 이메일 주소는 ise@<호스트 이름>으로 하드 코드됩니다.

GUI—ERS 설정에서 외부 RESTful 서비스 API 활성화

시작하기 전에

Cisco ISE REST API용으로 개발된 애플리케이션에서 Cisco ISE에 액세스할 수 있도록 Cisco ISE REST API를 활성화해야 합니다. Cisco REST API는 기본적으로 HTTPS 포트 9060을 사용합니다. Cisco ISE REST API가 Cisco ISE 관리자 서버에서 활성화되지 않은 경우, 클라이언트 애플리케이션은 모든 게스트 REST API 요청에 대해 서버에서 시간 초과 오류를 수신합니다.

모든 유형의 외부 RESTful 서비스 요청은 기본 ISE 노드에만 유효합니다. 보조 노드에는 읽기-액세스 권한(GET 요청)이 있습니다.

단계 1 ISE-PIC GUI에서 메뉴 아이콘(☰)을 클릭하고 **Settings(**설정**)** > **ERS Settings(ERS** 설정**)**.

단계 2 **Enable ERS for Read/Write(**읽기/쓰기용 **ERS** 활성화**)**를 선택하고 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

API 호출 및 ISE-PIC에 대한 자세한 내용은 ISE API 참조 가이드를 참조하십시오.