ISE 복제 이해 및 문제 해결

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine®)의 복제 및 문제 해결에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco ISE(Identity Services Engine®)에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 이러한 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco Identity Services Engine 3.4 이상 버전.

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

Cisco ISE의 복제

ISE의 복제는 컨피그레이션 및 운영 데이터를 일관되게 유지하기 위해 구축의 여러 노드 간에 동기화하는 프로세스입니다.

기본 관리 노드는 구축에서 수행된 변경 사항을 구축의 다른(보조) 모든 노드에 복제합니다.

Cisco ISE는 JGroups, 안정적인 그룹 통신 프레임워크를 복제 아키텍처의 일부로 사용합니다. JGroups는 ISE 구축의 노드가 서로 통신하고 복제 데이터를 교환할 수 있도록 합니다. 구축 전반에 걸쳐 동기화를 유지하면서 노드 간에 컨피그레이션 및 데이터베이스 업데이트를 제공하는 데 도움이 되는 메시징 프레임워크를 제공합니다.

- JGroups는 복제를 위해 Cisco ISE에서 사용하는 통신 프레임워크입니다. 복제된 데이터 자체는 저장하지 않습니다.
- Cisco ISE 내의 모든 데이터가 JGroup을 통해 복제되는 것은 아닙니다. 서로 다른 서비스는 전송되는 데이터의 유형에 따라 서로 다른 통신 메커니즘을 사용한다.
- 복제가 일시적으로 중단되면 일부 Cisco ISE 서비스는 동기화가 복원될 때까지 로컬에서 사용 가능한 데이터를 사용하여 계속 작동할 수 있습니다.

데이터 전송 방법의 예

데이터	통신 방법
컨피그레이션 및 복제 메시지	JGroups
지원 번들 컬렉션	HTTPS API(TCP 포트 443)
디버그 컨피그레이션	HTTPS API(TCP 포트 443)
라이브 로그 및 보고서	구축 컨피그레이션에 따라 RabbitMQ 또는 UDP

Cisco ISE 복제에 대한 주요 사전 요구 사항 및 검증 확인

- DNS 확인: 정방향 및 역방향 DNS 조회는 구축에 참여하는 모든 Cisco ISE 노드를 성공적으로 확인해야 합니다. 노드 통신 및 복제 작업에 적절한 DNS 확인이 필요합니다.
- NTP 동기화: 모든 Cisco ISE 노드를 신뢰할 수 있는 NTP 소스에 동기화하여 구축 전반에 걸쳐 시스템 시간을 일관되게 유지해야 합니다. 시간 동기화는 복제 및 인증서 검증에 필수적입니다.
- 인증서: 각 Cisco ISE 노드에 설치된 관리자 인증서는 유효하고 신뢰할 수 있어야 합니다. 복제 프로세스는 노드 간의 안전한 통신을 위해 관리자 인증서를 사용합니다.
- 포트 요구 사항: 네트워크 연결은 복제 및 노드 간 서비스에 필요한 포트를 통한 통신을 허용해야 합니다.

서비스	프로토콜/포트
HTTPS(SOAP)	TCP/443
데이터 동기화 및 복제(JGroups)	TCP/12001
관리 액세스	TCP/8443
ISE 메시징 서비스(SSL)	TCP/8671
프로 파 일러 엔드 포인트 소유권 동기화	TCP/6379

- 네트워크 연결성: Cisco ISE 노드 간의 네트워크 연결은 안정적이어야 하며 레이턴시는 300ms를 초과해서는 안 됩니다. 노드 간 지연 시간 및 패킷 손실을 확인하면 안정적인 복제가 보장됩니다.
- 대기열 링크 상태: Cisco ISE 메시징 인증서는 TCP 포트 8671을 통한 노드 간 통신을 보호하는 데 사용됩니다. 유효하지 않거나 손상된 메시징 인증서는 큐 링크 오류 및 복제 실패로 이어질 수 있습니다. 이러한 시나리오에서는 ISE 루트 CA 인증서 또는 ISE 메시징 인증서를 적절하게 재생성해야 합니다.
- ISE Stunnel Service: Cisco ISE Stunnel Service는 분산형 구축에서 작동하며 노드 간의 안전한 통신을 지원합니다. 복제를 지원하려면 서비스가 적용 가능한 모든 노드에서 실행 중이어야 합니다. Cisco ISE CLI에서 다음 명령을 사용하여 서비스 상태를 확인할 수 있습니다.

show tech-support | 스턴넬 포함

- ISE 패치 및 버전: 기본 관리 노드와 조닝 노드(독립형 노드)는 노드 등록 및 동기화를 위해 동일한 버전 및 패치 레벨을 가져야 원활하게 작동합니다.

Cisco ISE의 복제 단계

Cisco ISE의 복제는 구축의 모든 노드에서 동기화를 설정하고 유지하기 위해 함께 작동하는 세 가지 서로 다른 단계로 구성됩니다. 각 단계는 노드 온보딩부터 시작하여 초기 데이터베이스 동기화, 마지막으로 모든 노드의 동기화를 유지하기 위한 증분 업데이트의 지속적인 교환으로 이어지는 특정 목적을 수행합니다.

- 노드 등록
- 전체 동기화
- 증분 동기화

Cisco ISE의 노드 등록 이해

노드 등록은 Cisco ISE 노드가 기존 구축에 가입하고 PAN(Primary Administration Node)과의 통신을 설정하는 프로세스입니다.

노드 등록 중:

1단계: 가입 노드(독립형 노드)는 기본 관리 노드와의 통신을 시작합니다.

2단계: 상호 인증서 검증은 Cisco ISE 관리자 인증서를 사용하여 수행됩니다.

3단계: DNS 확인, NTP 동기화, 네트워크 연결성 및 필수 포트 접근성은 통신 프로세스의 일부로 검증됩니다.

4단계: 기본 관리 노드는 독립 형 노드 / 가입 노드가 호환 가능 한 Cisco ISE 버전 및 패치 수준을 실행 하고 있는지 확인 합니다.

5단계: 구축 정보, 노드 역할 및 신뢰 관계가 교환됩니다.

6단계: 데이터베이스 복제 서비스가 초기화되고 동기화를 위해 준비됩니다.

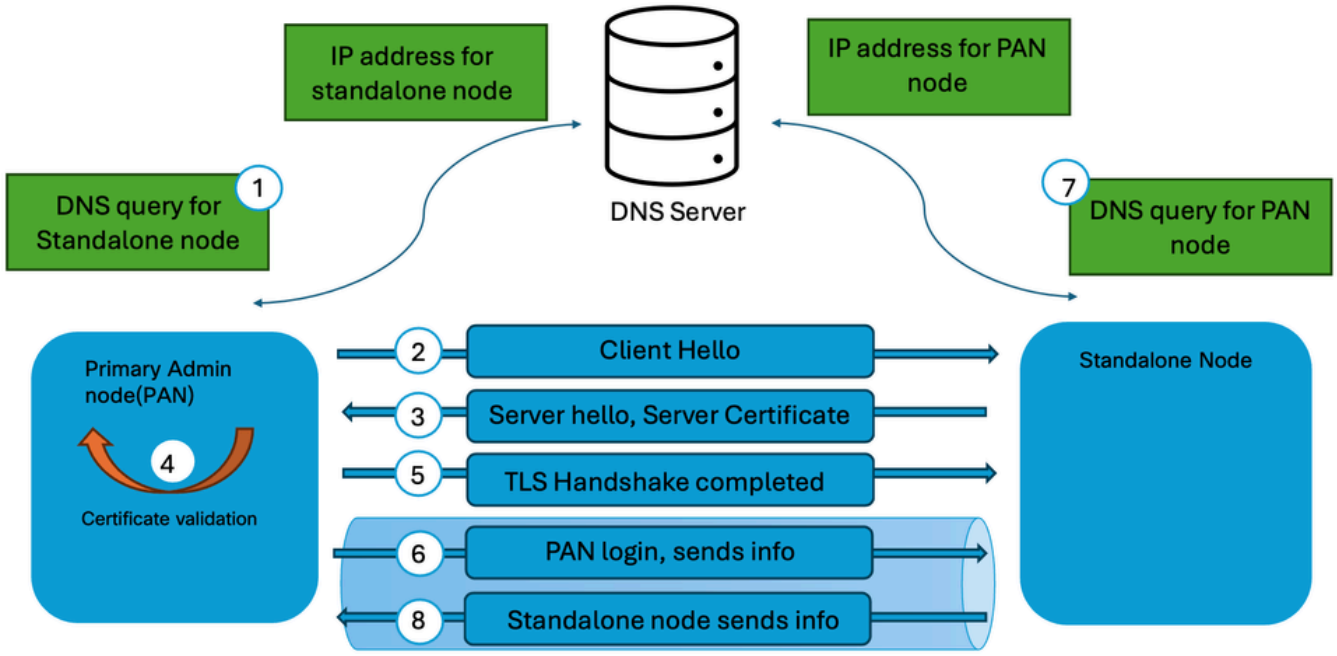
노드 등록이 성공적으로 완료되면 노드가 구축의 신뢰할 수 있는 구성원으로 설정되고 복제 프로세

스가 시작됩니다.

주요 특징

- 새 노드가 구축에 추가될 때 발생합니다.
- 신뢰 및 통신 채널을 설정합니다.
- 전체 컨피그레이션 데이터베이스를 즉시 전송하지 않습니다.
- 후속 동기화 작업을 위한 전제 조건 역할을 합니다.

노드 등록 프로세스에 대한 자세한 설명은 Cisco ISE의 노드 등록 프로세스 이해를 참조하십시오.



노드 등록 프로세스

참고: 구축에 추가되는 노드는 독립형 노드여야 합니다. 또한 PAN(Primary Administration Node)에서 Cisco ISE의 노드 등록을 허용하려면 구축에서 기본 관리 역할을 활성화해야 합니다.

Cisco ISE의 전체 동기화 이해

전체 동기화는 전체 컨피그레이션 데이터베이스가 기본 PAN에서 다른 노드로 전송되는 완전한 데

이터베이스 복제 프로세스입니다. 전체 동기화는 수정된 레코드만 전송하지 않습니다. 대신 전체 컨피그레이션 데이터 세트가 수신 노드에서 재구축됩니다.

전체 동기화는 다음과 같은 시나리오에서 발생할 수 있습니다.

- 노드 등록 후 초기 동기화
- 복제 실패 시 복구
- 데이터베이스 불일치가 심각합니다.
- 구축에 노드를 다시 참가 합니다.
- 수동 동기화는 Cisco TAC 문제 해결 절차를 통해 시작됩니다.
- 증분 동기화가 더 이상 데이터베이스 일관성을 복원할 수 없음을 결정하는 내부 복제 메커니즘.

전체 동기화 중:

1단계: 기본 관리 노드는 전체 데이터베이스 스냅샷을 준비합니다.

2단계: 컨피그레이션 데이터는 .dmp 파일에 패키지화되어 수신 노드로 전송됩니다.

3단계: 수신 노드의 기존 복제 데이터가 검증되고 업데이트됩니다.

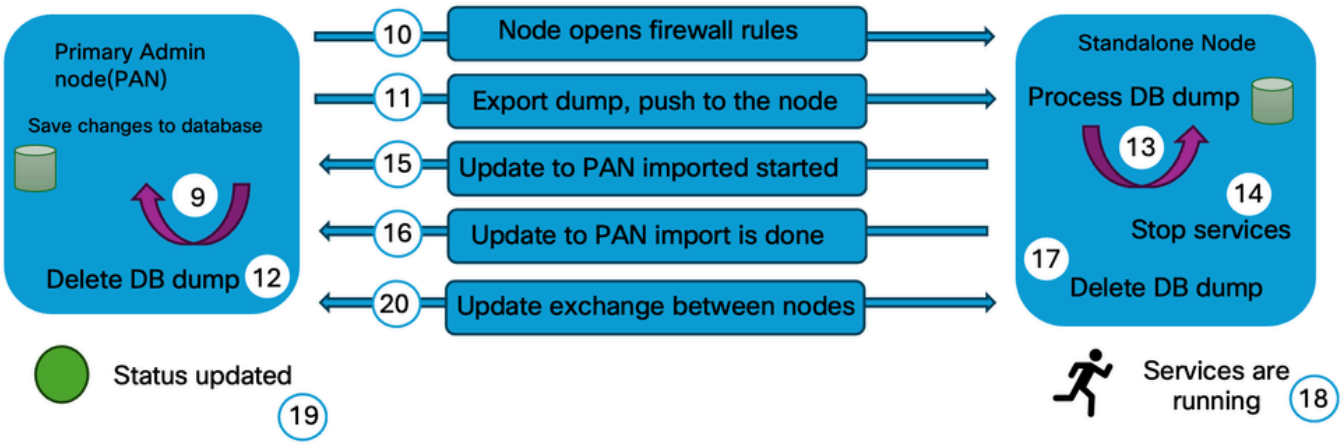
4단계: 전체 구성 데이터베이스는 1 기본 관리 노드에 일치 하도록 재작성 됩니다.

5단계: 복제 상태는 완료 시 확인됩니다.

전체 동기화는 증분 동기화보다 훨씬 많은 데이터를 포함하므로 추가 처리 시간과 네트워크 리소스가 필요합니다.

전체 동기화 특성

- 전체 구성 데이터베이스를 전송합니다.
- 더 많은 대역폭과 시스템 리소스를 소비합니다.
- 증분 동기화보다 시간이 더 오래 걸립니다.
- 불일치가 감지되면 데이터베이스 일관성을 복원합니다.
- 일반적으로 증분 동기화보다 덜 자주 발생합니다.



전체 동기화 프로세스

Cisco ISE의 증분 동기화 이해

증분 동기화는 노드가 성공적으로 구축에 참여한 후 컨피그레이션 변경 사항을 배포하기 위해 Cisco ISE에서 사용하는 지속적인 복제 메커니즘입니다. 관리자가 PAN에서 컨피그레이션을 변경할 경우 Cisco ISE는 전체 데이터베이스를 전송하지 않습니다. 대신 수정된 레코드만 가입자 노드에 복제됩니다.

증분 동기화를 통해 복제되는 변경 사항의 예는 다음과 같습니다.

- 정책 수정
- 네트워크 디바이스 추가 또는 업데이트
- 엔드포인트 그룹 변경
- 인증 프로파일 업데이트
- 인증서 관련 구성 변경
- ID 소스 구성 업데이트

변동분 동기화 프로세스는 지속적으로 작동하며 모든 노드에서 일관성을 유지하면서 대역폭 사용률 및 복제 오버헤드를 최소화하도록 설계되었습니다.

증분 동기화의 이점

- 복제 트래픽 감소.
- 동기화 시간 최소화.

- 컨피그레이션 변경 사항을 신속하게 전파할 수 있습니다.
- 구축 전반에 걸쳐 거의 실시간에 가까운 일관성을 유지합니다.

복제 워크플로

1단계: 기본 관리 노드에서 컨피그레이션이 변경됩니다.

2단계: 변경 사항은 1 기본 관리 노드 데이터베이스에 기록 됩니다.

3단계: 복제 서비스는 수정된 레코드를 식별합니다.

4단계: 기본 관리 노드는 트랜잭션 테이블에 새 이벤트 / 변경 사항을 기록합니다.

5단계: PAN에서 스레드를 분리하면 구축의 보조 노드에 정보/변경 사항이 게시됩니다.

6단계: 구축의 보조 노드는 1 기본 관리 노드에서 변경 사항을 수신 합니다.

7단계: 구축의 보조 노드는 1 기본 관리 노드에서 수신 한 변경 사항을 적용 합니다.

8단계: 복제 상태는 완료 시 업데이트됩니다.

정상 작동 조건에서 Cisco ISE의 대부분의 복제 활동은 증분 동기화를 통해 발생합니다.

참고: 보조 노드가 누락된 복제 메시지를 식별하면 PAN(Primary Administration Node)에 대한 요청을 시작하여 누락된 메시지를 검색하고 동기화를 유지합니다

복제 시퀀스 개요 및 동기화 상태

Cisco ISE 구축의 전체 복제 워크플로는 다음과 같이 요약할 수 있습니다.

1. 노드 등록 신뢰를 설정하고 구축에 노드를 추가합니다.

2. 초기 전체 동기화 전체 구성 데이터베이스를 새로 등록된 노드로 전송합니다.

3. 증분 동기화 구성 변경 사항을 정상 작업 전체에 지속적으로 전파합니다.

4. 전체 동기화(필요한 경우) 복제 문제 또는 데이터베이스 불일치가 탐지되면 데이터베이스 일관성을 재구축합니다.

이러한 단계별 접근 방식을 통해 Cisco ISE는 모든 노드에서 일관된 구성 데이터베이스를 유지하는 동시에 네트워크 사용률 및 복제 성능을 최적화할 수 있습니다.

동기화 상태

각 노드에 대해 표시되는 동기화 상태는 현재 복제 및 연결 상태를 나타냅니다.

- 녹색 - 노드가 구축과 동기화되었으며 복제가 정상적으로 작동하고 있습니다.
- 노란색 - 노드가 동기화되지 않았거나, 노드 등록에 실패했거나, 클러스터 연결이 끊어졌습니다(노드가 지난 5분 동안 클러스터에서 연결할 수 없음).
- 빨간색 - 노드가 물리적으로 연결할 수 없으며 네트워크 연결 확인(예: ICMP ping 및 HTTPS)을 통해 연결할 수 없습니다.

참고: 복제가 제대로 수행되지 않을 경우 기본 관리 노드에 로그인하여 기본 관리 노드를 사용하여 보조 노드에 수동 동기화를 수행하고, 관리 > 시스템 > 구축 > 노드를 선택한 다음 동기화를 누릅니다.

엔드포인트 복제

엔드포인트 복제는 ISE가 모든 PSN(Policy Service Node) 및 PAN(Primary Administration Node)에서 엔드포인트 데이터베이스 정보를 동기화하여 구축 전체에서 엔드포인트 ID의 일관된 보기를 유지하는 프로세스입니다.

- Cisco ISE는 네트워크에 연결 하는 장치에 대한 정보를 저장 하는 중앙 집중 형 엔드 포인트 데이터베이스를 유지 관리 합니다. 이 정보에는 인증, 프로파일링, 포스처 평가 또는 외부 ID 소스와의 통합을 통해 정적으로 구성된 엔드포인트와 동적으로 학습된 엔드포인트가 모두 포함됩니다.
- 엔드포인트 정보가 생성되거나 수정되면 Cisco ISE는 구축의 다른 노드에 변경 사항을 복제합니다. 이 동기화를 통해 모든 정책 서비스 노드는 요청을 처리하는 PSN에 관계없이 동일한 엔드포인트 정보를 사용하여 인증 및 권한 부여 요청을 평가할 수 있습니다.
- 엔드포인트 복제는 Cisco ISE에서 자동으로 처리되며 전체 데이터베이스 복제 메커니즘의 일부를 구성합니다. 관리자는 정상 작동 중에 수동으로 엔드포인트 동기화를 시작할 필요가 없습니다.

엔드포인트 복제 작동 방식

- 엔드포인트 업데이트: 엔드포인트는 인증, 프로파일링, 포스처 또는 수동 컨피그레이션을 통해 생성되거나 업데이트됩니다.
- 변경 감지: Cisco ISE는 엔드 포인트 변경을 감지 하고 복제를 위해 준비 합니다.
- 복제: 업데이트된 엔드포인트 정보는 ISE 복제 프레임워크를 사용하여 구축의 다른 노드에 복제됩니다.
- 데이터베이스 동기화: 보조 노드는 복제 된 정보로 로컬 엔드 포인트 데이터베이스를 업데이트 합니다.
- 일관된 정책 시행: 동기화가 완료되면 모든 정책 서비스 노드는 인증 및 권한 부여 결정에 동일한 엔드포인트 정보를 사용합니다.

Cisco ISE 릴리스 3.3에서 동적으로 검색된 엔드포인트는 모든 노드에 자동으로 복제되지 않습니다. 이 기능은 Endpoint Replication(엔드포인트 복제) 창에서 활성화 또는 비활성화할 수 있습니다. Administration > System > Settings > Endpoint Replication으로 이동하여 요구 사항에 따라 활성화 또는 비활성화합니다.

참고: 엔드포인트 복제와 세션 복제를 구분하는 것이 중요합니다. 엔드포인트 복제는 영구 엔드포인트 데이터베이스 레코드(예: MAC 주소, 엔드포인트 그룹 및 프로파일링 정보)를 동기화하는 반면, 세션 복제는 런타임 세션 정보를 동기화하여 정책 시행 및 운영 연속성을 지원합니다. 이러한 메커니즘은 독립적으로 작동하며 Cisco ISE 아키텍처 내에서 서로 다른 기능을 수행합니다.

공통 노드 복제 문제

시나리오 1: DNS 확인 실패로 인해 노드 등록 실패

"호스트 이름을 확인할 수 없습니다. DNS 구성을 확인하십시오."라는 오류 이유로 노드를 등록하지 못했습니다.

확인 단계

- 유효한 DNS 서버가 기본 관리 노드 및 독립형 노드에 구성되어 있는지 확인합니다. show running-config 명령을 사용하여 DNS 서버 컨피그레이션을 확인합니다 | 이름 서버 포함
- 정방향 DNS 조회를 위한 노드의 nslookup FQDN 명령과 역방향 DNS 조회를 위한 노드의 nslookup ip 주소를 사용하여 기본 관리 노드와 독립형 노드에서 정방향 및 역방향 DNS 확인을 검증합니다.
- ISE 노드의 CLI에서 ping DNS 서버 IP 명령을 사용하여 기본 관리 노드 및 독립형 노드에서

DNS 서버 연결성을 검증합니다.

시나리오 2: 관리자 인증서 만료로 인해 노드 등록 실패

노드 등록에 실패했습니다. "인증서를 로드하는 동안 오류가 발생했습니다. 현재 노드에 연결할 수 없습니다. 나중에 다시 시도하십시오."

확인 단계

- 1 기본 관리 노드 및 독립 형 노드의 관리자 인증서를 확인 하여 유효 하고 인증서 상태를 확인 합니다. Administration > System > Certificates로 이동하여 노드를 선택하고 Admin 인증서의 유효성 및 상태를 확인합니다.
- 관리자 인증서가 만료 된 경우 인증서를 대체 하거나 갱신 하고 관리자 사용 이 할당 되어 있는지 확인 하십시오.

시나리오 3: 버전이 일치하지 않아 노드를 등록하지 못했습니다.

"버전/패치 세부 정보가 일치하지 않음"과 같은 오류 이유로 인해 노드를 등록하지 못했습니다.

확인 단계

- 버전 세부사항이 일치하는지 확인하기 위해 show version 명령을 사용하여 기본 관리 노드 및 독립형 노드의 패치와 함께 소프트웨어 버전을 확인합니다.

디버그 로그의 구성 요소

Cisco ISE에서 복제를 격리하고 문제를 해결하기 위해 디버그 모드로 설정할 공통 구성 요소입니다 .

- Replication-Deployment(replication.log 및 ise-psc.log)
- Replication-JGroup(replication.log 및 ise-psc.log)
- 복제 추적기(tracking.log)
- 최대 절전 모드(hibernate.log)
- JMS(replication.log)
- ca-service(caservice.log)
- admin-ca(ise-psc.log)

참조

- ISE에서 디버깅 문제 해결 및 활성화
- ISE - 큐 링크 오류
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.4
- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.5

이 번역에 관하여

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