ISE 인증서 복제 경보 이해 및 문제 해결

목차

소개

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

사전 요구 사항

요구 사항

Cisco에서는 Cisco ISE(Identity Services Engine®)에 대한 지식이 있는 것을 권장합니다.

사용되는 구성 요소

이 문서의 정보는 이러한 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco ISE(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.

복제 경보

Cisco ISE의 복제 경보는 구축 전체에서 복제 프레임워크의 상태 및 동기화 상태에 대한 가시성을 제공합니다. 이러한 경보는 데이터 일관성, 노드 통신 또는 복제 프로세스에 영향을 줄 수 있는 조건을 식별하는 데 도움이 되므로 관리자는 시스템 운영에 영향을 주기 전에 문제를 탐지하고 해결할 수 있습니다. 복제 경보의 목적과 중요성을 이해하는 것은 건강한 ISE 구축을 유지하고 구성 및 운영 데이터가 모든 노드에서 동기화된 상태를 유지하도록 하는 데 필수적입니다.

ISE 인증서 복제 경보

인증서 복제 실패

인증서 복제 실패 경보는 Cisco ISE가 PAN(Primary Administration Node)에서 구축의 하나 이상의 노드로 인증서 관련 데이터를 복제하지 못할 때 생성됩니다. ISE는 모든 노드에서 일관성을 유지하기 위해 기본 PAN에서 인증서를 가져오거나 생성하고 갱신하거나 수정할 때마다 인증서 및 관련 컨피그레이션을 자동으로 복제합니다. 이 경보는 복제 프로세스가 실패하여 영향을 받는 노드에서 인증서 컨피그레이션이 일관되지 않음을 나타냅니다.

경보 이유

인증서 복제 실패 경보는 Cisco ISE가 하나 이상의 노드에서 인증서 관련 데이터를 성공적으로 전송, 검증 또는 설치할 수 없을 때 발생할 수 있습니다. 일반적인 원인은 다음과 같습니다

- 네트워크 통신 문제: 패킷 손실, 높은 네트워크 레이턴시, 방화벽 제한, 복제 트래픽 차단, ISE 노드 간 라우팅 문제, MTU 불일치로 인해 패킷 조각화 또는 삭제로 인해 인증서 복제가 중단될 수 있습니다.
- 복제 서비스 문제: RabbitMQ, JGroups 또는 기타 내부 복제 서비스를 사용할 수 없거나 다시 시작하거나 제대로 작동하지 않으면 인증서 복제가 실패할 수 있습니다.
- 인증서 유효성 검사 실패: 인증서 체인이 완전하지 않거나, CA 또는 중간 인증서가 없거나, 인증서가 만료되거나 손상되었거나, 지원되지 않는 키 사용 또는 잘못된 형식이 포함된 경우 복제가 실패할 수 있습니다.
- 노드 통신 문제: 대상 노드가 오프라인 상태이거나, 재시작, 등록 취소, 구축과의 연결이 끊겼거나, 연결할 수 없는 경우 인증서 복제를 완료할 수 없습니다.
- 디스크 공간 부족: 대상 노드에 사용 가능한 디스크 공간이 부족하여 복제된 인증서를 가져오

고 설치할 수 없습니다.
- 내부 데이터베이스 문제: ISE 컨피그레이션 데이터베이스가 인증서 메타데이터를 저장하거나 업데이트할 수 없는 경우 복제가 실패할 수 있습니다.

경보의 영향

이 경보의 영향은 복제되는 인증서의 유형 및 이 유형에 의존하는 서비스에 따라 달라집니다. 인증서 복제 실패 시 ISE 노드 전체에서 일관성 없는 인증서 컨피그레이션, HTTPS 인증서 불일치, EAP 인증 실패, pxGrid 신뢰 설정 문제, SCEP 등록 또는 인증서 프로비저닝 실패, 신뢰할 수 있는 인증서 저장소의 불일치, 외부 통합과의 TLS 검증 실패가 발생할 수 있습니다.

인증서 복제가 일시적으로 실패했습니다.

인증서 복제 일시적으로 실패 경보는 Cisco ISE가 일시적으로 PAN(Primary Administration Node)에서 구축의 하나 이상의 노드로 인증서 관련 데이터를 복제할 수 없을 때 생성됩니다. 인증서 복제 실패 경보와 달리 이 경보는 복제 실패가 일시적인 것으로 간주됨을 나타내며, 기본 조건이 해결되면 Cisco ISE가 자동으로 복제 작업을 재시도합니다.

경보 이유

경보는 일반적으로 인증서 복제를 일시적으로 방해하는 일시적인 조건으로 인해 생성됩니다. 일반적인 원인은 다음과 같습니다.

- 일시적인 네트워크 통신 문제: 간략한 네트워크 중단, 패킷 손실, 높은 레이턴시, 방화벽 지연 또는 ISE 노드 간의 일시적인 라우팅 문제
- 복제 서비스 초기화 또는 다시 시작: RabbitMQ, JGroups 또는 기타 내부 복제 서비스가 다시 시작되거나 일시적으로 사용할 수 없습니다.
- 임시 노드를 사용할 수 없습니다. 대상 노드가 부팅 중이거나, 응용 프로그램 서비스를 다시 시작하거나, 배포에 다시 참가 중이거나, 일시적으로 연결할 수 없습니다.
- 임시 시스템 리소스 제약: 높은 CPU 사용률, 메모리 압력 또는 디스크 I/O 경합이 복제 처리를 일시적으로 지연시킵니다.
- 동시 관리 작업: 다른 인증서 가져오기, 백업, 복원, 패치 설치 또는 배포 동기화가 진행되는 동안 인증서 복제가 지연될 수 있습니다.
- 임시 데이터베이스 또는 복제 큐 지연: 내부 데이터베이스 작업 또는 복제 큐가 다른 동기화 요청을 처리하는 동안 일시적으로 사용 중입니다.

경보의 영향

대부분의 경우 Cisco ISE가 복제 작업을 자동으로 재시도하기 때문에 이 경보는 운영 영향을 최소화합니다. 그러나 복제가 성공적으로 완료될 때까지 노드 간에 다음과 같은 일시적인 불일치가 발

생할 수 있습니다.

- 새로 가져오거나 갱신된 인증서의 전파 지연
- 구축 전체에서 임시 인증서 컨피그레이션이 일치하지 않습니다.
- 영향을 받는 노드에서 인증서 기반 서비스의 가용성 지연
- 복제된 인증서에 의존하는 경우 HTTPS, EAP, pxGrid 또는 SCEP 서비스의 일시적인 지연

경보가 지속되거나 반복적으로 발생하면 Certificate Replication Failed(인증서 복제 실패) 경보로 이어집니다.

ISE 인증서 복제 경보 문제 해결

이는 ISE에서 인증서 복제 경보를 트러블슈팅하거나 확인할 때 확인되어야 하는 일반적인 요인입니다.

1. 노드의 배포 상태 확인

인증서 복제가 성공하려면 보조 노드가 Cisco ISE 구축 내에서 연결됨 상태여야 합니다. Administration > System > Deployment로 이동하여 영향을 받는 노드의 상태를 확인합니다. 노드 상태 옆의 정보(i) 아이콘 위에 마우스 커서를 올려 놓으면 동기화 세부 정보 및 보류 중인 복제 메시지를 검토할 수 있습니다.

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

- 녹색 - 노드가 구축과 동기화되어 있으며 복제가 정상적으로 작동하고 있습니다.
- 노란색 - 노드가 동기화되지 않았거나, 노드 등록이 실패했거나, 클러스터 연결이 끊어졌습니다. 이 상태는 노드가 지난 5분 동안 클러스터에서 연결할 수 없음을 나타냅니다.
- 빨간색 - 노드에 연결할 수 없으며 ICMP ping 또는 HTTPS와 같은 네트워크 연결 확인을 통해 연결할 수 없습니다.

노드가 노란색 또는 빨간색 상태를 표시하는 경우 해당 노드에 영향을 미치는 복제 또는 연결 문제를 나타냅니다. 또한 노드 정보에 표시되는 복제 메시지 수를 확인합니다. 보류 중인 메시지 수는 5,000 이하여야 합니다. 보류 중인 메시지가 5,000개가 넘는 대기열은 복제 대기열이 누적되었음을 나타내며, 이는 복제를 지연시키거나 차단시킬 수 있습니다.

2. 구축에서 대기열 링크 경보 확인

Cisco ISE에서 성공적인 복제는 RabbitMQ 메시징 서비스 및 JGroups 클러스터 통신 프레임워크의 가용성과 통신에 따라 달라집니다. 두 구성 요소 중 하나에서 통신 문제가 발생하면 Cisco ISE는 대기열 링크 오류를 생성하여 구축 노드 간의 복제를 중단할 수 있습니다.

경보 상태를 확인하려면 Operations(운영) > Dashboard(대시보드) > Alarms(경보)로 이동하고 영향 받는 노드에서 Queue Link Errors(대기열 링크 오류)를 확인합니다.

대기열 링크 오류가 있는 경우, 인증서 관련 통신 오류로 인해 일반적으로 대기열 링크 오류가 발생하므로 Cisco ISE 루트 CA 인증서를 갱신합니다. 인증서 문제가 해결되면 추가 작업 없이 복제가 자동으로 재개됩니다.

참고: 대기열 링크 오류에 대한 자세한 내용은 ISE 대기열 링크 오류 설명서를 참조하십시오.

---

3. 네트워크 레이턴시 및 연결 확인

Cisco ISE 복제는 구축 노드 간의 안정적인 네트워크 연결에 의존합니다. 네트워크 지연 시간이 길거나 연결이 간헐적이면 복제가 지연되고 특히 지리적으로 분산된 구축에서 동기화 장애가 발생할 수 있습니다.

ping과 같은 연결 테스트를 사용하여 영향을 받는 노드 간의 네트워크 대기 시간을 확인합니다. 안정적인 복제를 위해서는 노드 간의 왕복 지연 시간이 약 300ms 이내여야 합니다. 이 임계값을 지속적으로 초과하는 레이턴시는 복제 성능 및 동기화에 부정적인 영향을 줄 수 있습니다. 또한 구축 노드 간 통신에 영향을 주는 간헐적인 네트워크 중단, 패킷 손실 또는 방화벽 제한이 없는지 확인합니다.

4. 인증서가 영향을 받는 노드에 이미 없는지 확인합니다.

복제 중인 인증서가 보조 노드에 이미 있는 경우 인증서 복제가 실패할 수 있습니다.

Administration > System > Certificates로 이동하고 영향을 받는 노드를 선택한 다음 인증서가 이미 설치되어 있는지 확인합니다. 인증서가 있는 경우 해당 속성을 검토하여 복제 중인 인증서와 일치하는지 확인하고 중복되거나 충돌하는 인증서가 있는지 확인합니다.

5. 시스템 리소스 사용률 확인

시스템 리소스 사용률이 높으면 Cisco ISE 성능에 영향을 미치고 복제 작업을 지연시킬 수 있습니다. CPU, 메모리 또는 디스크 사용률이 너무 높으면 복제 프로세스가 제대로 완료되지 않을 수 있습니다.

영향을 받는 노드에 사용 가능한 시스템 리소스가 충분한지, 리소스 사용률이 권장 운영 제한 내에 있는지 확인합니다. 리소스 사용률이 지속적으로 높은 경우, 추가 리소스를 할당하거나 노드의 워크로드를 줄여 정상적인 복제 성능을 복구합니다.

참고: Cisco ISE 구축에 권장되는 하드웨어 크기 조정 및 리소스 할당 지침은 성능 및 확장성 설명서를 참조하십시오.

6. 구축 및 네트워크에서 포트 가용성 확인

Cisco ISE 복제는 무중단 통신 및 성공적인 복제를 보장하기 위해 구축의 모든 노드 간에 열려 있는 특정 TCP 포트를 필요로 합니다. 이러한 포트 중 하나가 방화벽, 액세스 제어 정책 또는 네트워크 디바이스에 의해 차단된 경우 복제 실패 또는 동기화 문제가 발생할 수 있습니다.

다음 TCP 포트가 열려 있고 모든 Cisco ISE 노드 간에 연결할 수 있는지 확인합니다.

- TCP 443 - HTTPS 통신
- TCP 8443 - 관리 통신
- TCP 12001 - JGroups 클러스터 통신 및 복제
- TCP 6379 - 내부 메시징 서비스
- TCP 8671 - Cisco ISE 메시징(RabbitMQ)

Cisco ISE CLI에 로그인하고 show ports 명령을 실행하여 노드에서 허용되는 언급된 포트를 확인합니다.

필수 포트가 Cisco ISE 노드에서 활성화되어 있는지 확인하고 네트워크 경로 전체에서 허용되는지 확인합니다. 중간 방화벽, 보안 디바이스 또는 네트워크 정책이 구축 노드 간의 이러한 포트에서 통신을 차단하고 있지 않은지 확인합니다.

복제 경보에 대한 로그 수집

Cisco ISE에서 복제 경보를 격리하고 문제를 해결하기 위해 디버그 모드에서 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)

참조

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.5
- ISE에서 디버깅 문제 해결 및 활성화
- Identity Services Engine에서 지원 번들 수집

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.