ISE 노드 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.

ISE 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 노드 복제 경보

복제 실패

복제 실패 경보는 구축의 보조 노드가 구축의 기본 관리 노드에 의해 복제된 메시지를 사용할 수 없을 때 생성됩니다. 이 경보는 복제 프로세스가 실패했으며 영향을 받는 노드에 더 이상 최신 컨피그레이션 또는 운영 데이터가 없음을 나타냅니다.

인증서별 복제 알람과 달리 이 알람은 일반적인 복제 프레임워크의 장애를 나타내며 구축 전반의 여러 컨피그레이션 객체 및 서비스에 영향을 미칠 수 있습니다.

경보 이유

복제 실패 경보는 Cisco ISE가 복제 된 데이터를 성공적으로 전송 하거나 적용 할 수 없을 때 발생할 수 있습니다. 일반적인 원인은 다음과 같습니다.

- 네트워크 통신 문제: 패킷 손실, 높은 네트워크 레이턴시, 방화벽 제한, 라우팅 문제 또는 MTU 불일치로 인해 ISE 노드 간의 통신이 중단됩니다.
- 복제 서비스 문제: RabbitMQ, JGroups 또는 기타 내부 복제 서비스를 사용할 수 없거나 다시 시작하거나 제대로 작동하지 않습니다.

- 노드 통신 문제: 대상 노드가 오프라인 상태이거나, 다시 시작되거나, 등록 취소되거나, 구축과의 연결이 끊기거나, 그 밖의 경우 연결할 수 없습니다.
- 데이터베이스 동기화 문제: 데이터베이스 오류 또는 동기화 실패로 인해 대상 노드가 복제된 데이터를 커밋할 수 없습니다.
- 시스템 리소스 제약: 높은 CPU 사용률, 메모리 압력, 디스크 공간 부족 또는 과도한 디스크 I/O로 인해 복제 처리가 지연됩니다.
- DNS 또는 호스트 이름 확인 문제: 정방향 또는 역방향 DNS 확인이 잘못되어 노드 간 통신이 제대로 수행되지 않습니다.
- 버전 또는 구축 불일치: 노드가 지원되는 소프트웨어 버전에서 작동하지 않거나 업그레이드 또는 노드 등록 후 구축이 일관되지 않은 상태인 경우 복제가 실패합니다.
- 관리자 인증서 만료: ISE 노드에 대한 관리자 인증서는 만료/손상 / 잘못된 노드 간의 통신이 복제 실패로 이어질 수 있기 때문에.
- 큐 링크 오류: 포트 8671에서 ISE 메시징 인증서/ISE 루트 CA 체인이 손상되었거나 유효하지 않은 경우의 큐 링크 오류가 배포 또는 영향을 받는 노드에 표시됩니다.
- Stunnel 서비스가 비활성화됨/오프라인: Stunnel 서비스는 분산형 구축의 모든 노드에서 실행됩니다. Stunnel 서비스의 Disabled/not running 상태가 복제에 실패하는 경보가 발생합니다.
- 복제 포트가 차단됨: 12001, 8671,443 8443 및 6379 포트는 구축의 원활한 복제 절차를 위해 구축의 노드와 네트워크 간에 열려 있어야 합니다.

경보의 영향

그 영향은 복제되는 데이터의 유형에 따라 달라집니다. 복제 실패로 인해 ISE 노드 간의 컨피그레이션이 일관되지 않고, 관리 변경 사항의 전파가 지연되고, 오래된 정책, 네트워크 디바이스 또는 ID 정보가 누락되고, 인증서 동기화가 실패하고, 엔드포인트 데이터가 일관되지 않을 수 있습니다. 장기간 복제가 실패하면 구축 전반의 관리 작업 및 정책 일관성에 영향을 미칠 수 있습니다.

복제 중지됨

기본 관리 노드가 정보를 구축의 보조 노드에 복제할 수 없을 때 "복제 중지됨" 경보가 생성됩니다. 이 경보는 복제 프로세스가 실패했으며 영향을 받는 노드에 더 이상 최신 컨피그레이션 또는 운영 데이터가 없음을 나타냅니다.

경보 이유

"복제 중지" 경보는 기본 관리 노드가 복제 된 데이터를 성공적으로 전송 할 수 없는 경우 발생 할 수 있습니다. 일반적인 원인은 다음과 같습니다.

- 네트워크 통신 문제: 패킷 손실, 높은 네트워크 레이턴시, 방화벽 제한, 라우팅 문제 또는 MTU 불일치로 인해 ISE 노드 간의 통신이 중단됩니다.
- 복제 서비스 문제: RabbitMQ, JGroups 또는 기타 내부 복제 서비스를 사용할 수 없거나 다시 시작하거나 기본 관리 노드에서 제대로 작동하지 않습니다.
- 시스템 리소스 제약: 높은 CPU 사용률, 메모리 압박, 디스크 공간 부족 또는 디스크 I/O가 과중하여 기본 관리 노드에서 복제 처리가 지연됩니다.
- DNS 또는 호스트 이름 확인 문제: 정방향 또는 역방향 DNS 확인이 잘못되어 노드 간 통신이 제대로 수행되지 않습니다.
- 버전 또는 구축 불일치: 노드가 지원되는 소프트웨어 버전에서 작동하지 않거나 업그레이드 또는 노드 등록 후 구축이 일관되지 않은 상태인 경우 복제가 실패합니다.
- 관리자 인증서 만료: ISE 노드에 대한 관리자 인증서는 만료/손상 / 잘못된 노드 간의 통신이 복제 실패로 이어질 수 있기 때문에.
- 큐 링크 오류: 포트 8671에서 ISE 메시징 인증서/ISE 루트 CA 체인이 손상되었거나 유효하지 않은 경우의 큐 링크 오류가 배포 또는 영향을 받는 노드에 표시됩니다.
- Stunnel 서비스가 비활성화됨/오프라인: Stunnel 서비스는 분산형 구축의 모든 노드에서 실행됩니다. Stunnel 서비스의 Disabled/not running 상태가 복제에 실패하는 경보가 발생합니다.
- 복제 포트가 차단됨: 12001, 8671,443 8443 및 6379 포트는 구축의 원활한 복제 절차를 위해 구축의 노드와 네트워크 간에 열려 있어야 합니다.

경보의 영향

복제가 중지되면 구축의 노드는 더 이상 기본 관리 노드에서 컨피그레이션 업데이트를 수신하지 않습니다. 이로 인해 정책의 일관성이 떨어지고, 네트워크 디바이스 정의가 오래되고, 엔드포인트 정보가 누락되고, 인증서 동기화가 지연되고, 구축 전체에서 컨피그레이션이 불일치할 수 있습니다. 오랫동안 복제가 중지된 상태로 남아 있으면 동기화가 복원될 때까지 기본 PAN에 대한 관리 변경 사항이 영향을 받는 노드에 적용되지 않습니다.

복제 실패 및 복제 중지 경보 문제 해결

느린 복제 경보

기본 PAN에서 컨피그레이션이 변경될 때마다 Cisco ISE는 복제 대기열에 변경 사항을 넣고 보조 노드와 동기화합니다. 정상적인 조건에서는 짧은 기간 내에 복제가 완료됩니다. 그러나 복제 대기열이 구축되기 시작하거나 대상 노드가 복제 요청을 처리하는 데 예상보다 오래 걸리는 경우 Cisco ISE는 느린 복제 경보를 생성합니다.

Cisco ISE는 이러한 경보를 세 가지 심각도 레벨로 분류합니다.

- 느린 복제 정보
- 느린 복제 경고
- 느린 복제 오류

경보 이유

"느린 복제" 경보는 일반적으로 복제 처리를 지연시키는 일시적인 조건으로 인해 생성됩니다. 일반적인 원인은 다음과 같습니다.

- 임시 시스템 리소스 사용률: CPU 사용률이 높거나 메모리 사용량이 많거나 디스크 I/O가 증가하면 복제 처리가 지연될 수 있습니다.
- 네트워크 레이턴시: ISE 노드 간의 네트워크 지연 시간이 짧거나 패킷 손실이 적을 경우 데이터 전송 속도가 느려질 수 있습니다.
- 대규모 컨피그레이션 변경: 대량 엔드포인트 가져오기, 정책 업데이트, 인증서 가져오기 또는 기타 대규모 관리 변경은 복제할 데이터의 양을 늘립니다.
- 백그라운드 시스템 작업: 백업, 복원, 제거, 패치 설치 또는 업그레이드 작업으로 인해 시스템 로드가 일시적으로 증가합니다.
- 복제 큐 백로그: 짧은 기간 내에 여러 컨피그레이션을 변경하면 일시적으로 복제 대기열이 증가할 수 있습니다.
- 임시 서비스 지연: RabbitMQ, JGroups 또는 데이터베이스 서비스는 계속 정상적으로 작동하는 동안 간단한 처리 지연을 경험합니다.

느린 복제 경보 - 정보

보류 중인 메시지 수가 10000을 초과하거나 메시지를 복제하는 데 걸린 시간이 1시간 이상인 경우 느린 복제 또는 중단된 복제가 감지됩니다.

확인: 보류 중인 동기화 메시지 수를 확인합니다. Administration > System > Deployment로 이동하고 영향을 받는 노드를 선택한 다음 Information (i) 아이콘을 클릭하여 보류 중인 복제 메시지의 수를 검토합니다.

느린 복제 경보 - 경고

보류 중인 메시지 수가 20000보다 크거나 메시지를 복제하는 데 걸린 시간이 3시간을 초과하면 느린 복제 또는 중단된 복제가 탐지됩니다.

확인: 보류 중인 동기화 메시지 수를 확인합니다. Administration > System > Deployment로 이동하고 영향을 받는 노드를 선택한 다음 Information (i) 아이콘을 클릭하여 보류 중인 복제 메시지의 수를 검토합니다.

느린 복제 경보 - 오류

보류 중인 메시지 수가 40000보다 크거나 메시지를 복제하는 데 걸린 시간이 5시간을 초과하면 느린 복제 또는 중단된 복제가 탐지됩니다.

확인: 보류 중인 동기화 메시지 수를 확인합니다. Administration > System > Deployment로 이동하고 영향을 받는 노드를 선택한 다음 Information (i) 아이콘을 클릭하여 보류 중인 복제 메시지의 수를 검토합니다.

노드 복제 경보 문제 해결

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 영향받는 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. 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.

5. 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.

6. DNS 확인 확인

Cisco ISE 복제는 구축의 모든 노드 간의 성공적인 통신에 의존합니다. 노드 간 통신이 제대로 작동하려면 노드에 연결할 수 있어야 하며, 정방향 및 역방향 DNS 확인이 모두 구성되어 제대로 작동해야 합니다. DNS 확인 문제로 인해 노드가 통신하지 못해 복제 오류가 발생할 수 있습니다.

ISE 노드에서 DNS 확인을 확인하려면 Cisco ISE CLI에 로그인하고 nslookup 명령을 사용하여 구축의 각 노드에 대한 정방향 및 역방향 DNS 확인을 모두 확인합니다.

예를 들면 다음과 같습니다.

- 정방향 DNS 조회: nslookup www.example.com 명령은 해당 Cisco ISE 노드의 IP 주소를 반환해야 합니다.

- 역방향 DNS 조회: nslookup 10.x.x.1 명령은 해당 Cisco ISE 노드의 FQDN(Fully Qualified Domain Name)을 반환해야 합니다.

7. 관리자 및 ISE 메시징 인증서 확인

Cisco ISE는 관리자 인증서 및 ISE 메시징 인증서를 사용하여 복제에 필요한 안전한 노드 간 통신을 설정합니다. 인증서 중 하나가 유효하지 않거나, 만료되었거나, 손상되었거나, 신뢰할 수 없는 경우 구축 노드 간 복제가 실패할 수 있습니다.

인증서 상태를 확인하려면 Administration > System > Certificates로 이동하고 영향을 받는 노드를 선택한 다음 Admin 및 ISE 메시징 인증서를 검토합니다. 인증서가 유효하고, 만료되지 않았으며, 신뢰할 수 있고, 정상 상태인지 확인합니다.

관리자 인증서 또는 ISE 메시징 인증서가 유효하지 않거나, 손상되었거나, 만료된 경우 인증서를 교체하거나 갱신합니다. 인증서 문제가 해결되면 노드 간의 보안 통신이 다시 설정된 후 복제가 다시 시작됩니다.

참고: 인증서의 갱신에 대한 자세한 내용은 ISE 대기열 링크 오류 및 ISE의 인증서 설치를 참조하십시오.

---

8. ISE Stunnel 서비스 상태 확인

Cisco ISE의 Stunnel 서비스는 ISE 구성 요소와 외부 서비스 간의 통신을 위해 보안 SSL/TLS 터널링을 제공하는 내부 서비스입니다. ISE는 모든 애플리케이션에서 독립적으로 TLS 암호화를 구현하는 대신 일반 TCP를 통해 통신하는 서비스에 SSL/TLS 암호화를 추가하는 래퍼로서 Stunnel을 사용합니다. 이렇게 하면 보안이 향상되는 동시에 보안 커뮤니케이션의 구현이 간소화됩니다.

복제가 올바르게 작동하려면 Stunnel 서비스가 Cisco ISE 구축의 모든 노드에서 Running 상태여야 합니다. 이 서비스는 복제 프로세스 동안 노드 간 보안 TLS 통신을 설정하기 위해 유효한 ISE 관리자 및 ISE 메시징 인증서에 따라 달라집니다. 서비스 상태는 Cisco ISE CLI에서 show tech-support 명령을 사용하여 확인할 수 있습니다 | 스턴넬 포함

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.