두부 인증서로 인한 PriME Infrastructure 3.5+ 통합 문제

목차

소개

이 문서에서는 Cisco Prime Infrastructure(기본/보조)에서 새로운 CSR(Certificate Signing Request)이 생성된 후 두부(Trust-on-first-use) 인증서가 일치하지 않아 발생하는 통합 문제, 트러블슈팅 및 해결 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Prime Infrastructure
- 고가용성

사용되는 구성 요소

이 문서의 정보는 Cisco Prime Infrastructure 버전 3.5 이상을 기반으로 합니다.

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

배경 정보

Cisco Prime Infrastructure의 고가용성 및 인증서 생성에 대한 정보를 제공하는 참조 문서입니다.

고가용성 가이드:https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide_chapter_01011.html

관리자 가이드:https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-6/admin/guide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide/bk_CiscoPrimeInfrastructure_3_6_AdminGuide_chapter_0100.html

문제

두부 - 원격 호스트에서 받은 인증서는 처음 연결할 때 신뢰됩니다.

Prime 인프라 또는 Prime이 연결된 원격 호스트의 두부 인증서는 새 인증서가 생성되거나 서버가 VM 호스트에 다시 구축된 경우 변경될 수 있습니다.

Prime Infrastructure Server(기본/보조)에서 새 CSR을 생성하고 가져오면 서비스가 다시 시작된 후 연결이 다시 시작되면 새 두부 인증서 정보를 원격 서버로 보냅니다.

원격 호스트가 첫 번째 이후 후속 연결에 대해 다른 인증서를 전송하면 연결이 거부됩니다.

원격 호스트는 이전 두부가 여전히 있는 (HA 구축의 기본 또는 보조 서버, ISE(Integrated Service Engine) 서버) 일 수 있습니다.

이렇게 하면 기본 서버와 보조 서버, Prime 및 ISE 서버 간에 등록 오류가 발생합니다.

문제 해결 섹션에서는 이러한 시나리오의 상태 모니터 로그에서 찾을 수 있는 오류 메시지에 대해 설명합니다.

문제 해결

기본 상태 모니터 로그에서 보조 인증서의 불일치를 가리키는 이러한 오류 메시지를 찾을 수 있습니다.

```
[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-sec, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US

javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-sec
```

이러한 오류 메시지는 ISE 서버 인증서의 불일치를 가리키는 기본 인프라 로그에서 찾을 수 있습니다.

```
[system] [seqtaskexecutor-3069] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=ISE-server

javax.net.ssl.SSLHandshakeException: java.security.cert.
CertificateException: Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=ISE-server
```

보조 상태 모니터 로그에서 기본 인증서의 불일치를 가리키는 이러한 오류 메시지를 찾을 수 있습니다.

```
[system] [HealthMonitorThread] TOFU failed.
Check local trust Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-pri, OU=Prime Infra, O=Cisco Systems, L=SJ, ST=CA, C=US



javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException:
Trust-on-first-use is configure for this connection.
Current certificate of the remote host is different from what was used earlier
- CN=prime-pri
```

솔루션

prime의 통합을 다시 시도하기 전에 해당 원격 호스트에 대한 이전 인증서 항목을 식별하여 제거해야 하는 prime의 현재 두부 인증서를 나열해야 합니다.

구성

인증서 검증 목록 보기

ncs certvalidation **dover-certs listcerts 명령을** 사용하여 인증서 검증 목록을 볼 수 있습니다.

이 출력은 Cisco Prime Infrastructure 기본 서버 [IP=1XX.XX.XX.XX]에서 가져옵니다.

```
prime-pri/admin# ncs certvalidation tofu-certs listcerts

Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...

host=1X.XX.XX.XX_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-pri
host=1Z.ZZ.ZZ.ZZ_443;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=ISE-server
host=1YY.YY.YY.YY_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec

prime-pri/admin#
```

이 출력은 Cisco Prime Infrastructure 보조 서버 [IP=1YY.YY.YY.YY]에서 가져옵니다.

```
prime-sec/admin# ncs certvalidation tofu-certs listcerts

Host certificate are automatically added to this list on first connection,
if trust-on-first-use is configured - ncs certvalidation certificate-check ...
```

```
host=1YY.YY.YY.YY_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec
host=127.0.0.1_8082;  subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-sec
host=1X.XX.XX.XX_8082; subject= /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=prime-pri

prime-sec/admin#
```

인증서 삭제

ncs certvalidation **dofurts deleteert host <host> 명령을 사용하여** 인증서 유효성 검사를 삭제합니다 .

기본 서버에서 ISE 및 보조 서버의 두부 인증서에 대한 이전 항목을 각각 확인하고 삭제합니다.

- **ncs certvalidation budoum-certs deleteert host** 1YY.YY.YY.YY_8082
- **ncs certvalidation budoum-certs deleteert host** 1Z.ZZ.ZZ.ZZ_443

보조 서버에서 ncs certvalidation **dofcerts deleteert host 1X.XX.XX.XX**_8082 명령을 사용하여 기본 서버의 두부 인증서**에 대한 이전 항목을 확인하고 삭제합니다**.

HA를 기본에서 보조로 다시 초기화

1단계. 관리자 권한이 있는 사용자 ID와 비밀번호로 Cisco Prime Infrastructure에 로그인합니다.

2단계. 메뉴에서 Administration(관리) **> Settings(설정) > High Availability(고가용성)로 이동합니다** .Cisco Prime Infrastructure에 HA 상태 페이지가 표시됩니다.

3단계. HA Configuration(HA 컨피그레이션)을 선택한 다음 다음과 같이 필드를 완료합니다.

1. 보조 서버:보조 서버의 IP 주소 또는 호스트 이름을 입력합니다.
2. 인증 키:보조 서버를 설치하는 동안 설정한 인증 키 비밀번호를 입력합니다.
3. 이메일 주소:HA 상태 변경에 대한 알림을 보낼 주소(또는 쉼표로 구분된 주소 목록)를 입력합니다.Mail Server Configuration(메일 서버 구성) 페이지("이메일 서버 설정 구성" 참조)를 사용하여 이메일 알림을 이미 구성한 경우 여기에 입력한 이메일 주소가 메일 서버에 대해 이미 구성된 주소 목록에 추가됩니다.
4. 장애 조치 유형:수동 또는 자동을 선택합니다.수동 을 선택하는 것이 좋습니다.

호스트 이름을 IP 주소로 확인하려면 DNS 서버를 사용하는 것이 좋습니다.DNS 서버 대신 **/etc/hosts** 파일을 사용하는 경우 호스트 이름 대신 보조 IP 주소를 입력해야 합니다.

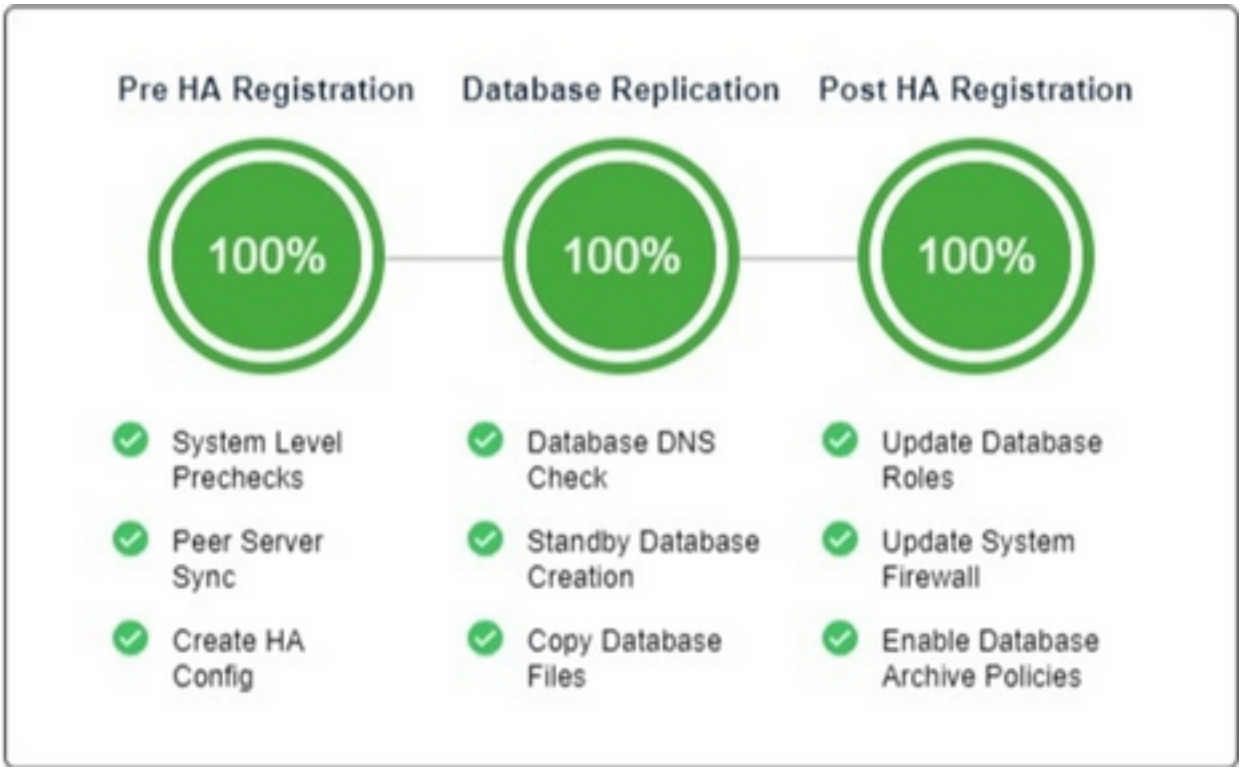
4단계. 가상 IP 기능을 사용하는 경우 **Enable Virtual IP(가상 IP 활성화)** 확인란을 선택한 다음 다음과 같이 추가 필드를 완료합니다.

1. IPV4 가상 IP:두 HA 서버에서 모두 사용할 가상 IPv4 주소를 입력합니다.
2. IPV6 가상 IP:(선택 사항) 두 HA 서버에서 모두 사용할 IPv6 주소를 입력합니다.

두 서버가 동일한 서브넷에 있지 않으면 가상 IP 주소 지정이 작동하지 않습니다.IPV6 주소 블록 fe80은 링크-로컬 유니캐스트 주소 지정을 위해 예약되어 있으므로 사용하지 마십시오.

5단계. **Check Readiness(준비** 확인)를 클릭하여 HA 관련 환경 매개변수가 컨피그레이션에 대해 준비되었는지 확인합니다.

6단계. 이정표 진행 표시줄을 보려면 **등록**을 클릭하여 여기에 표시된 대로 HA 전 등록, 데이터베이스 복제 및 HA 등록 후 100% 완료를 확인합니다.Cisco Prime Infrastructure는 HA 등록 프로세스를 시작합니다.등록이 성공적으로 완료되면 **Configuration Mode(컨피그레이션 모드)**에 Primary Active(기본 활성)의 값이 표시됩니다.



ISE 서버 다시 구성

1단계. Administration(관리) **> Servers(서버) > ISE Servers(ISE 서버)로 이동합니다.**

2단계. Select a **command(명령 선택) > Add ISE Server(ISE 서버 추가)**로 이동한 다음 **이동**
3단계. ISE 서버의 IP 주소, 사용자 이름 및 비밀번호를 입력합니다.

4단계. ISE 서버 비밀번호를 확인합니다.

5단계. **저장**을 클릭합니다.

다음을 확인합니다.

ncs certvalidation **dover-certs listcerts 명령을** 사용하여 새 인증서를 확인할 수 있습니다.

관련 정보

- Cisco Prime Infrastructure 릴리스 정보:http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html
- Cisco Prime Infrastructure 빠른 시작 가이드:http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-installation-guides-list.html
- Cisco Prime Infrastructure 명령 참조 설명서: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-command-reference-list.html
- Cisco Prime Infrastructure 사용 설명서:http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html
- Cisco Prime Infrastructure 관리자 가이드:http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-maintenance-guides-list.html
- **기술 지원 및 문서 – Cisco Systems**