

Expressway 15.5.20용 업그레이드 체크리스트

목차

[소개](#)

[사용되는 구성 요소](#)

[업그레이드 전](#)

[인증서를 읽는 방법](#)

[유지 관리 창 이전에 해야 할 작업](#)

[업그레이드가 실패할 경우](#)

[준비 상태 검사에서 업그레이드를 중지했습니다.](#)

[노드 발생 후 경보](#)

[관리자가 로그인할 수 없음](#)

[인증서 또는 피어 ID 실패](#)

[업그레이드 중 또는 업그레이드 직후 클러스터 경보](#)

[노드가 작동 후 로그인 문제](#)

[TAC 케이스가 필요한 경우 수집할 수 있는 증거](#)

[업그레이드 후](#)

[모든 노드에서](#)

[클러스터 전용](#)

[사용 중인 항목에 따라 서비스 확인](#)

소개

이 문서에서는 X15.5.20 보안 강화 업그레이드를 위해 Expressway를 준비하는 방법에 대해 설명합니다. 여기에는 각 전제조건과 이를 수정하는 방법이 나열되어 있다.

사용되는 구성 요소

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.

업그레이드 전



주의: 모든 피어가 준비도 검사를 통과할 때까지 클러스터 업그레이드를 시작하지 마십시오. TLS 확인을 Enforcement(시행)로 설정하고 클러스터가 정상인지 확인합니다. IP 주소와 FQDN을 혼합하지 않고 하나의 피어 ID 형식을 사용합니다. 각 서버 인증서는 SAN에 해당 노드의 FQDN을 포함하거나 SAN이 비어 있을 때만 CN에 있어야 합니다. OpenSSL을 사용하여 CSR을 생성하면 빈 SAN이 발생할 수 있습니다. 확인이 실패하면 기존 클러스터

컨피그레이션을 변경하지 않고 업그레이드가 중지됩니다.

수표	독립형	클러스터	사실이 아닌 경우
업그레이드 경로가 부록 3과 일치함	필수	필수	X8.11.4 이전에는 X8.11.4에서 먼저 중지합니다. X12 PAK 라이선스를 X15.x 이전 Smart Licensing으로 변환합니다.
현재 백업 및 테스트된 롤백 계획	필수	모든 노드에 필요	창 앞에 백업을 수행합니다. 공장 초기화 이후 설정은 지워집니다.
클러스터 정상, 설명되지 않은 경보 없음, 동기화 중 복제	해당 없음	필수	업그레이드하기 전에 클러스터를 수정하십시오. 롤링 업그레이드는 여전히 일반적인 클러스터 분할 동작을 사용합니다.
TLS 확인은 시행 중이며 클러스터는 정상 상태입니다.	해당 없음	업그레이드 전에 필요	Permissive를 Enforcement로 변경하고, 인증서를 수정하고, 복제를 확인합니다. 창에서 이 항목을 발견하지 마십시오.
모든 피어는 동일한 ID 형식을 사용하며 피어 목록은 비어 있지 않습니다	피어 ID 검사 통과	필수. 혼합 IP 및 FQDN이 재부팅되기 전에 차단됨	모든 FQDN 또는 모든 IP 주소를 표준화하고 변경 사항을 복제하며 클러스터가 정상인지 확인합니다. 롤링 업그레이드 중에는 형식을 변경하지 마십시오.
서버 인증서는 SAN에 시스템 FQDN을 포함하거나 SAN이 비어 있는 경우에만 CN에 포함됩니다	업그레이드가 인증서를 확인하는 경우 필수	필수. 업그레이드가 중지되고 클러스터 컨피그레이션이 변경되지 않은 상태로 남음	인증서를 다시 발급합니다. SAN이 있는 경우 CN에 의존하지 마십시오. 포함된 NUL이 포함된 이름을 거부합니다.
인증서가 최신 상태이고 피어에서 신뢰함, RSA 2048+ 또는 P-256+, SHA-2 서명	권장	필수	SHA-1 시그니처가 X15.2에서 이미 지원되지 않습니다. 인증서를 다시 발급하십시오. 자체 서명 인증서는 모든 피어가 인증서를 신뢰하도록 명시적으로 구성된 경우에만 허용됩니다.
알려진 피어에서만 허용되는 TCP 4371	권장	필수	방화벽을 제한합니다. 이는 ClusterDB에 대한 심층 방어 업그레이드를 대체할 수 없습니다.
관리자 API 클라이언트 검토됨	API를 사용하는 경우 필수	API를 사용하는 경우 필수	더 엄격한 이름 및 비밀번호 검증이 필요하며 CSRF는 FormPutXML 쓰기에 대해 검사하며 옵션 키 API는 없습니다.
유지 보수 윈도우에는 롤링 업그레이드 및 가능한 짧은 클러스터 경보가 포함됩니다.	일반 창	필수	쿠키 재암호화는 클러스터 통신 경보를 발생시킬 수 있습니다. 그것은 저절로 막아질 것으로 예상됩니다.

인증서를 읽는 방법

서버 인증서를 내보내고 검사합니다.

- SAN의 FQDN. 릴리스 [노트에는](#) SAN에서 시스템 FQDN이 필요합니다. SAN 확장이 비어 있는 경우에만 CN이 선택됩니다.
- CN 폴백이 없습니다. SAN이 있고 일치하지 않으면 [CN이 올바른더라도 확인이 실패합니다.](#) 모든 필수 DNS 이름 또는 IP 주소를 올바른 SAN 유형에 입력합니다.
- NUL 문자 포함된 NUL을 포함하는 인증서 이름은 거부됩니다.
- 날짜. notBefore는 과거여야 하고 notAfter는 미래여야 합니다.
- 키. RSA 2048비트 이상 또는 P-256 이상의 EC 키
- 서명. SHA-2 가족. X15.2부터는 [sha1WithRSAEncryption](#) 및 [ecdsa-with-SHA101](#) 지원되지 않습니다.
- 발급자. Subject(주체)와 Issuer(발급자)가 동일한 경우 자체 서명됩니다. 피어가 이미 이를 신뢰해야 합니다.

유지 관리 창 이전에 해야 할 작업

- 창 전에 클러스터 TLS 확인을 Enforcement로 설정하고, [클러스터](#)를 다시 시작하고(게시자 우선 부터 시작), 클러스터가 정상인지 확인합니다. 허용 모드는 지원되지 않습니다. 레거시 허용 값은 계속 표시될 수 있지만 ClusterDB 인증서 신뢰 또는 피어 ID 검증을 우회하지는 않습니다.
- 피어 ID는 모두 FQDN이거나 모두 IP 주소여야 합니다. 롤링 업그레이드가 진행되는 동안에는 해당 형식을 변경하지 마십시오.
- 별칭이 두 개 이상인 인증된 H.323 엔드포인트에는 모든 별칭에 대한 [자격 증명 별칭 맵](#)이 필요하거나 하위 영역에서 자격 증명 별칭 바인딩이 해제되어 있을 수 있습니다. 바인딩을 해제하면 보안 상태가 악화됩니다.
- 로컬 관리자 비밀번호 만료는 PasswordExpiryDays가 0일 때 꺼진 상태로 유지됩니다. 로컬 자정이 아닌 00:00 UTC에서 만료가 계산됩니다.
- [비밀번호 기록 깊이의 기본값은 12입니다.](#) 교육 범위는 3~24입니다. 빈 관리자 비밀번호는 거부되고 최근에 사용한 비밀번호는 거부될 수 있습니다.
- [LDAP 관리자-역할 매핑에는](#) 정확한 그룹-이름 일치가 필요합니다. 구성된 이름만 포함된 그룹 이름은 더 이상 역할을 부여하지 않습니다.
- 새 설치, 공장 초기화 또는 무인 배포는 공장 기본 [루트 암호](#)를 다시 사용할 수 [없습니다.](#) 업그레이드로 인해 현재 관리자 비밀번호가 지워지지 않습니다.
- 읽기 전용 관리자는 더 이상 SAML IdP 트러스트를 변경할 수 없습니다.
- STARTTLS를 완료할 수 없는 이메일은 암호화되지 않은 상태로 전송되지 않습니다.
- [스마트 라이선싱](#)은 유일한 라이선싱 모드입니다. PAK 옵션 키가 X14.2에서 제거되었습니다. 표준 Expressway 이미지는 [2,500개의 암호화된 신호 세션](#)을 허용합니다. Expressway Select는 달하지 않은 이미지입니다.

업그레이드가 실패할 경우

클러스터를 그대로 둡니다. 준비 검사를 실패해도 기존 클러스터 컨피그레이션은 변경되지 않습니다. 장애를 극복하기 위해 노드를 공장 초기화 하지 마십시오.

준비 상태 검사에서 업그레이드를 중지했습니다.

설치 프로그램은 인증서, TLS 확인 또는 피어 ID 요구 사항이 실패하는 경우 재부팅 전에 중지합니다. 독립형 노드는 피어 ID 검사를 통과합니다.

노드 발생 후 정보

클러스터 데이터베이스 재암호화의 버스트는 클러스터 통신 실패 경보를 발생시킬 수 있습니다. 끝낼 시간을 주세요. 정상 상태로 유지되면 에스컬레이션합니다.

관리자가 로그인할 수 없음

설치 실패와 별도로 처리합니다. 만료되거나 재사용되거나 첫 번째 로그인 비밀번호가 세션을 차단합니다. 이미지가 실패했다는 의미는 아닙니다.

인증서 또는 피어 ID 실패

1. 중지된 노드에서 전체 시스템 스냅샷을 다운로드합니다. 해당 스냅샷의 tmp 디렉토리에서 install-error를 엽니다.
2. 메시지가 피어 ID에 대한 것일 경우 IP 주소와 FQDN의 조합 또는 빈 피어 목록을 확인합니다. 모든 피어가 하나의 형식을 사용하도록 하고 복제를 기다린 다음 클러스터가 정상인지 확인하고 다시 시도하십시오. 롤링 업그레이드 중간에 ID 형식을 변경하지 마십시오.
3. 메시지가 인증서에 대한 것일 경우 릴리스 노트 규칙과 비교합니다. 시스템 FQDN은 SAN에 있거나 SAN이 비어 있을 때만 CN에 있어야 합니다. 현재 SAN은 CN으로 폴백할 수 없습니다.
4. 올바른 SAN 유형에서 필요한 모든 DNS 이름 또는 IP 주소로 인증서를 다시 발급합니다. 포함된 NUL이 포함된 이름을 거부합니다.
5. 새 인증서가 최신 상태이고 신뢰할 수 있는 RSA 2048+ 또는 P-256+이며 SHA-2로 서명되었는지 확인합니다. 케이스에 개인 키를 연결하지 마십시오.
6. TLS 확인을 Enforcement(적용)로 설정하고 클러스터가 정상인지 확인한 다음 중지된 노드에서 업그레이드를 다시 시도하십시오.
7. 해당 노드가 정상인 후에만 롤링 업그레이드를 계속합니다. 이 확인에서 한 노드가 중지된 동안에는 나머지 노드를 업그레이드하지 마십시오.

업그레이드 중 또는 업그레이드 직후 클러스터 정보

1. 업그레이드 자체가 완료되었으며 노드가 X15.5.20에 있는지 확인합니다.
2. 이벤트 로그에서 developer.upgrade 메시지를 확인합니다. ClusterDB 필드 재암호화, "마이그레이션된 데이터를 CDB에 저장"에 대한 메시지입니다.
3. 경보가 해제될 때까지 기다리세요. 교육 자료에 따르면 재암호화가 완료되면 지워집니다.
4. 남아 있는 경우 각 피어에서 클러스터 상태, 경보 및 스냅샷을 수집합니다. 클러스터 쿠키 또는 주요 자료를 케이스 노트에 복사하지 마십시오.
5. TCP 4371 및 4372가 피어 사이에서만 열려 있고 상호 TLS가 성공하는지 확인합니다. 어디서

든 4371을 허용하는 방화벽은 해결책이 아닙니다.

노드가 작동 후 로그인 문제

- 웹 UI가 암호 변경으로 리디렉션됩니다. 현재 암호를 입력해야 하며 새 암호는 달라야 합니다. 이는 설치 또는 공장 재설정 후 첫 번째 GUI 로그인 시, 그리고 로컬 비밀번호가 만료된 경우에 필요합니다.
- SSH에서 키보드 인터랙티브/PAM이 실패했으며 셸을 열지 않았다고 합니다. 만료된 로컬 비밀번호를 변경해야 합니다. 이전 세션이 허용되지 않습니다.
- REST는 401을 반환합니다. 만료된 로컬 관리자여야 합니다. 이벤트 로그에 API 영역에 대한 비밀번호 불일치 또는 `taa-chkpasswd` 오류가 표시될 수 있습니다. 암호를 변경한 다음 다시 시도하십시오.
- 새 비밀번호가 거부되었습니다. 기록(기본값 마지막 12)에 있거나 현재 복잡성 규칙에 실패했습니다.
- LDAP 관리자가 필요한 역할을 상실했습니다. 구성된 그룹을 LDAP에서 반환된 정확한 그룹 이름과 비교합니다. 부분 또는 부분 문자열 일치는 더 이상 역할을 부여하지 않습니다. 읽기 전용 관리자는 SAML IdP 트러스트를 편집할 수 없습니다.
- 새 설치 또는 공장 초기화에 공장 기본 루트 비밀번호가 없습니다. 기본 자격 증명을 검색하거나 배포하지 마십시오. 업그레이드로 인해 현재 관리자 비밀번호가 지워지지 않습니다.



주의: 공장 초기화는 업그레이드-복구 단계가 아닙니다. 클러스터 ID 및 클러스터 쿠키를 삭제합니다. 클러스터링을 해제하거나 일관되지 않은 클러스터 데이터베이스가 IP 주소와 관리자 및 루트 비밀번호를 유지하고, 다른 컨피그레이션과 로그를 지우고, 노드를 임시 인증서로 되돌립니다. 릴리스 노트에서 호출하는 경우에만 사용하고 백업이 있는 경우에만 사용합니다.

TAC 케이스가 필요한 경우 수집할 수 있는 증거

1. 모든 노드의 소프트웨어 버전 및 역할, 그리고 중지된 노드.
2. `tmp/install-error`를 포함하여 장애가 발생한 노드의 전체 시스템 스냅샷입니다.
3. 서버 인증서 텍스트(`openssl x509 -text -noout`). 개인 키가 없습니다.
4. 클러스터 상태, 경보 및 `xConfiguration` 클러스터 `TlsVerify`에 허용 또는 적용 여부가 표시됩니다.
5. 업그레이드에 대한 이벤트 로그 줄 및 관련 있는 경우 `sshd` 또는 `httpd` 인증 실패 비밀번호와 쿠키를 수정합니다.
6. 로컬, LDAP 또는 SAML 관리자, Smart Licensing 및 모든 API 자동화 사용 여부

업그레이드 후

모든 노드에서

1. 버전은 X15.5.20 빌드로 사용할 예정입니다.
2. 관리 주소에서 노드에 연결할 수 있으며 웹 UI가 로드됩니다.

3. 새 하드웨어, 디스크 또는 애플리케이션 경보가 발생하지 않습니다. (클러스터 통신 경보는 다시 암호화한 후에 지워집니다.)
4. 클러스터가 안정되면 새 백업을 수행합니다.

클러스터 전용

1. 모든 피어가 클러스터 내에서 가동 중이며 복제는 정상입니다.
2. 피어는 TCP 4371 및 4372에서 상호 TLS와 통신합니다. 유효한 클라이언트 인증서가 없는 연결은 실패해야 합니다.
3. 클러스터 TlsVerify를 적용하는 중입니다.

허용은 지원되지 않습니다. 레거시 허용 값은 계속 표시될 수 있지만 검증을 우회하지는 않습니다. Enforcement(적용)를 설정하고 클러스터가 정상적으로 유지되고 있는지 확인합니다.

4. 방화벽은 피어 주소에서만 TCP 4371을 계속 허용합니다.
5. 업로드한 로그 또는 스냅샷 노트에 클러스터 쿠키 또는 진단 암호가 표시되지 않습니다.

사용 중인 항목에 따라 서비스 확인

사용하는 경우	어떤 게 좋아 보이나요	장애 발생 시
로컬 관리자	GUI, SSH 및 API는 현재 비밀번호를 수락합니다. 만료된 어카운트는 비밀번호 변경 또는 HTTP 401 수신에 푸시됩니다.	만료가 00:00 UTC이고 새 암호가 기록 창 외부에 있는지 확인합니다.
LDAP 관리자	관리자는 LDAP 그룹 이름이 구성된 그룹과 정확히 일치하는 경우에만 로그인합니다.	디렉토리 그룹을 Expressway 그룹과 비교합니다. 강제로 로그인하려면 일치 항목을 확장하지 마십시오.
SIP 또는 B2B 통화	테스트 통화는 양방향으로 연결됩니다.	통화 기록 및 스냅샷을 수집합니다.
인증된 H.323 등록	엔드포인트는 H.323 ID 및 E.164 번호를 포함하여 사용하는 모든 별칭에 등록됩니다.	각 별칭에 대한 자격 증명 별칭 맵을 추가합니다. 릴리스 노트에서는 패턴 유형이 Exact인 xConfiguration 등록 CredentialAliasMap을 사용합니다. 하위 영역에서 CredentialAliasBinding을 해제하면 등록이 복원되고 보안 상태가 악화됩니다. H.323 자체는 제거되지 않습니다.
MRA 또는 디바이스 등록	알려진 엔드포인트가 등록되고 통화가 발신됩니다. UC 클라이언트 인증서 SAN은 특정 DNS 이름 또는 IP 주소이며, 지나치게 광범위하거나 형식이 잘못된 값은 아닙니다.	인증서, 접근 자격 증명 및 DNS를 업그레이드 전 백업과 비교합니다. SAN이 너무 넓은 인증서를 다시 발급합니다.
이메일 알림	테스트 메시지는 STARTTLS를 사용하여 노드를 떠납니다.	STARTTLS를 완료할 수 없는 경우 전달이 달하지 않습니다. 메일 서버 트러스트 또는 TLS를 수정합니다. 일반 텍스트 폴백을 기대하지 마십시오.

사용하는 경우	어떤 게 좋아 보이나요	장애 발생 시
스마트 라이선싱	등록 및 권한 부여가 웹 UI와 일치합니다. 표준 이미지는 2500개 의 암호화된 시그널링 세션 내에 있거나 노드가 Expressway Select입니다.	전송 및 CSSM을 확인합니다. CSSM "Allow export-controlled functionality(내보내기 제어 기능 허용)" 확인란은 Expressway에 적용되지 않습니다. 토큰을 해지하고 제품 인스턴스를 삭제하면 노드가 Deregistered로 설정됩니다. 옵션 키는 해결 방법이 아닙니다.
REST 또는 컨피그레이션 스크립트	계정 이름이 새 길이 및 문자 제한과 일치합니다. 컨피그레이션 쓰기에는 GUI에서 사용하는 CSRF 보호가 포함됩니다.	배송 API 스키마에 대해 클라이언트를 업데이트합니다. 제거된/프로비저닝/optionkey 호출이 실패합니다.

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.