

Upgrade Checklist voor Expressway 15.5.20

Inhoud

[Inleiding](#)

[Gebruikte componenten](#)

[Voordat u de upgrade uitvoert](#)

[Hoe het certificaat te lezen](#)

[Wat te doen voor het onderhoudsvenster](#)

[Als de upgrade mislukt](#)

[Gereedheidscontrole heeft de upgrade gestopt](#)

[Alarm nadat een knooppunt opkomt](#)

[Beheerder kan zich niet aanmelden](#)

[Falen van certificaat of peer-identiteit](#)

[Clusteralarm tijdens of net na de upgrade](#)

[Aanmeldingsproblemen nadat de node is opgestart](#)

[Bewijs dat moet worden verzameld in het geval dat TAC nodig is](#)

[Na de upgrade](#)

[Op elk knooppunt](#)

[Alleen voor clusters](#)

[Servicecontroles, door wat het apparaat gebruikt](#)

Inleiding

In dit document wordt beschreven hoe u Expressway kunt voorbereiden op de X15.5.20-upgrade voor beveiligingshardening. Het geeft een overzicht van elke vereiste en hoe deze te corrigeren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Voordat u de upgrade uitvoert



Waarschuwing: start geen clusterupgrade totdat elke peer de gereedheidscontroles heeft doorstaan. Stel TLS-verificatie in op Handhaving en bevestig dat het cluster gezond is. Gebruik één peer-identity-indeling, geen mix van IP-adressen en FQDN's. Elk servercertificaat moet de FQDN van die node in het SAN bevatten, of alleen in de CN wanneer het SAN leeg is. Een leeg SAN kan optreden als OpenSSL is gebruikt om de

CSR te maken. Als een controle mislukt, stopt de upgrade zonder de bestaande clusterconfiguratie te wijzigen.

controleren	op zichzelf staand	Cluster	Als het niet waar is
Upgradepad komt overeen met aanhangsel 3	verplicht	verplicht	Voor X8.11.4, stop eerst bij X8.11.4. Converteer X12 PAK-licenties naar Smart Licensing vóór X15.x .
Huidige back-up en een getest terugdraaiplan	verplicht	Vereist op elk knooppunt	Neem de back-up voor het venster. Een latere fabrieksreset maakt de configuratie vrij.
Cluster gezond, geen onverklaarbare alarmen, replicatie in sync	Niet van toepassing	verplicht	Repareer het cluster voordat u een upgrade uitvoert. Een rollende upgrade maakt nog steeds gebruik van het normale split-clustergedrag.
TLS-verificatie wordt gehandhaafd en het cluster is gezond	Niet van toepassing	Vereist vóór de upgrade	Wijzig Permissive in Enforcing, repareer het certificaat en bevestig de replicatie. Ontdek dit niet tijdens het raam.
Elke peer gebruikt hetzelfde identiteitsformaat en de peer-lijst is niet leeg	Peer-identity check passes	vereist. Gemengde IP en FQDN worden geblokkeerd voordat opnieuw wordt opgestart	Standaardiseer op alle FQDN's of alle IP-adressen, laat de wijziging repliceren en bevestig dat het cluster gezond is. Wijzig het formaat niet tijdens een voortschrijdende upgrade.
Servercertificaat bevat het systeem-FQDN in het SAN of alleen in de CN wanneer het SAN leeg is	Vereist als de upgrade het certificaat controleert	vereist. Upgrade stopt en laat de clusterconfiguratie ongewijzigd	Geef het certificaat opnieuw af. Als een SAN bestaat, moet u niet vertrouwen op de CN. Namen weigeren die een ingesloten NUL bevatten.
Certificaat is in datum, vertrouwd door peers, RSA 2048 + of P-256 +, SHA-2 handtekening	aanbevolen	verplicht	SHA-1-handtekeningen worden al niet ondersteund door X15.2 . Geef het certificaat opnieuw af. Een zelfondertekend certificaat is alleen acceptabel als elke peer expliciet is geconfigureerd om het te vertrouwen.
TCP 4371 alleen toegestaan van bekende leeftijdsgenoten	aanbevolen	verplicht	Beperk de firewall. Dit is een grondige verdediging voor ClusterDB; het is geen vervanging voor de upgrade.
Beheer API-clients	Vereist als	Vereist als API's	Verwacht strakkere naam- en

controleren	op zichzelf staand	Cluster	Als het niet waar is
beoordeeld	API's worden gebruikt	worden gebruikt	wachtwoordvalidatie, CSRF-controles op FormPutXML-schrijfbewerkingen en geen API met optiesleutel.
Onderhoudsvenster dekt een rollende upgrade plus een mogelijk kort clusteralarm	Normaal venster	verplicht	Her codering van cookies kan een clustercommunicatiealarm doen rinkelen. Verwacht wordt dat het vanzelf verdwijnt.

Hoe het certificaat te lezen

Exporteer het servercertificaat en inspecteer het.

- FQDN in het SAN. Voor de [releasenota's is](#) het systeem FQDN in een SAN vereist. De CN wordt alleen gecontroleerd als de SAN-extensie leeg is.
- Geen CN-fallback. Als een SAN aanwezig is en niet overeenkomt, [mislukt de verificatie, zelfs als de GN juist is](#). Zet elke vereiste DNS-naam of IP-adres in het juiste SAN-type.
- NUL-teken. Een certificaatnaam die een ingesloten NUL bevat, wordt afgewezen.
- Datus. Niet voor moet in het verleden zijn en niet in de toekomst.
- Sleutel. RSA ten minste 2048 bits, of een EC-sleutel op P-256 of sterker.
- Handtekening. SHA-2 familie. Vanaf X15.2 worden [sha1WithRSAEncryption en ecDSA-with-SHA1](#) niet ondersteund.
- Emittent. Als Onderwerp en Uitgever hetzelfde zijn, is het zelfondertekend. Gelijken moeten het al vertrouwen.

Wat te doen voor het onderhoudsvenster

- Stel voor het venster TLS-verificatie van het cluster in op [Handhaving](#), start het cluster opnieuw op (vanaf de eerste uitgever) en bevestig dat het cluster gezond is. De modus Permissive wordt niet ondersteund. Een bestaande waarde voor Permissive kan zichtbaar blijven, maar deze gaat niet voorbij aan het vertrouwenscertificaat van ClusterDB of de validatie van de peer identity.
- Peer identiteiten moeten allemaal FQDN's of alle IP-adressen zijn. Wijzig dat formaat niet terwijl een voortschrijdende upgrade wordt uitgevoerd.
- Een geverifieerd H.323-eindpunt met meer dan één alias kan een [referentiële aliaskaart](#) nodig hebben voor elke alias, of een inlogaliasbinding die op de subzone is uitgeschakeld. Het uitschakelen van de binding verzwakt de beveiligingspositie.
- Het verstrijken van het lokale beheerderswachtwoord blijft uit wanneer PasswordExpiryDays 0 is. Wanneer het is ingeschakeld, wordt de vervaldatum berekend om 00:00 UTC, niet om middernacht.
- [De diepte van de wachtwoordgeschiedenis is standaard 12](#). Het trainingsbereik is 3 tot 24. Lege beheerderswachtwoorden worden geweigerd en een recent gebruikt wachtwoord kan

worden geweigerd.

- [Voor het toewijzen van LDAP-beheerdersrollen is](#) een exacte overeenkomst tussen de groepsnamen vereist. Een groepsnaam die alleen de geconfigureerde naam bevat, verleent de rol niet langer.
- Een nieuwe installatie, fabrieksreset of implementatie zonder toezicht kan een [fabrieksstandaard hoofdwachtwoord](#) niet opnieuw gebruiken. Bij een upgrade wordt het huidige beheerderswachtwoord niet gewist.
- Een alleen-lezen beheerder kan de SAML IdP-trust niet meer wijzigen.
- E-mail die STARTTLS niet kan voltooien, wordt niet verzonden in de clear.
- [Smart Licensing](#) is de enige licentiemodus. PAK-optietoetsen zijn verwijderd in X14.2. De standaard Expressway-afbeelding maakt [2500 gecodeerde signaalsessies](#) mogelijk; Expressway Select is de niet-gecodeerde afbeelding.

Als de upgrade mislukt

Laat het cluster zoals het is. Een mislukte gereedheidscontrole wijzigt de bestaande clusterconfiguratie niet. Stel een knooppunt niet opnieuw in de fabriek in om voorbij de storing te komen.

Gereedheidscontrole heeft de upgrade gestopt

Het installatieprogramma stopt voordat het opnieuw wordt opgestart wanneer het certificaat, de TLS-verificatie of de peer-identity-vereiste mislukt. Standalone knooppunten slagen voor de peer-identity check.

Alarm nadat een knooppunt opkomt

Een uitbarsting van hercodering van de clusterdatabase kan een noodsignaal voor clustercommunicatie doen rinkelen. Geef het de tijd om te eindigen. Escaleren als het blijft staan.

Beheerder kan zich niet aanmelden

Behandel dit apart van een installatiefout. Verlopen, opnieuw gebruikt of wachtwoorden voor de eerste aanmelding blokkeren de sessie. Dat wil niet zeggen dat het beeld is mislukt.

Falen van certificaat of peer-identiteit

1. Download een volledige systeemmomentopname van het knooppunt dat is gestopt. Open de installatiefout in de tmp-directory van die momentopname.
2. Als het bericht over peer identity gaat, controleer dan op een combinatie van IP-adressen en FQDN's of een lege peer list. Zorg ervoor dat elke peer één formaat gebruikt, wacht op replicatie, bevestig dat het cluster gezond is en probeer het opnieuw. Wijzig het identiteitsformaat niet in het midden van een voortschrijdende upgrade.
3. Als het bericht over het certificaat gaat, vergelijkt u het met de regel voor de release-note:

het systeem-FQDN moet zich in het SAN bevinden, of alleen in de CN wanneer het SAN leeg is. Een aanwezig SAN mag niet terugvallen op de CN.

4. Geef het certificaat opnieuw uit met elke vereiste DNS-naam of IP-adres in het juiste SAN-type. Verwerp een naam die een ingesloten NUL bevat.
5. Bevestig dat het nieuwe certificaat op datum, vertrouwd, RSA 2048+ of P-256+ is en is ondertekend met SHA-2. Bevestig de privésleutel niet aan de zaak.
6. Stel TLS-verificatie in op Enforcing (Afdwingen), bevestig dat het cluster gezond is en probeer de upgrade opnieuw uit op het knooppunt dat is gestopt.
7. Ga pas door met de rollende upgrade nadat die node gezond is. Upgrade de resterende knooppunten niet terwijl één knooppunt bij deze controle wordt gestopt.

Clusteralarm tijdens of net na de upgrade

1. Bevestig dat de upgrade zelf is voltooid en dat de node op X15.5.20 staat.
2. Kijk in het gebeurtenislogboek voor developer.upgrade-berichten over het opnieuw coderen van ClusterDB-velden en vervolgens "Gemigreerde gegevens opslaan in CDB."
3. Wacht tot het alarm is gewist. Het trainingsmateriaal zegt dat het wordt gewist wanneer re-encryptie is voltooid.
4. Als dit het geval is, verzamelt u de clusterstatus, alarmen en een momentopname van elke peer. Kopieer geen clustercookies of belangrijk materiaal naar de casusnotities.
5. Bevestig dat TCP 4371 en 4372 alleen open zijn tussen de peers en dat wederzijds TLS slaagt. Een firewall die 4371 vanaf elke locatie toestaat, is niet de oplossing.

Aanmeldingsproblemen nadat de node is opgestart

- Web UI verwijst naar een wachtwoordwijziging. Het huidige wachtwoord moet worden ingevoerd en het nieuwe wachtwoord moet anders zijn. Dit wordt verwacht bij de eerste GUI-aanmelding na een installatie of fabrieksreset en wanneer een lokaal wachtwoord is verlopen.
- SSH zegt dat toetsenbord-interactief / PAM is mislukt en nooit een shell opent. Een verlopen lokaal wachtwoord moet worden gewijzigd. De oude sessie wordt niet toegekend.
- REST geeft 401 terug. Verwacht voor een verlopen lokale beheerder. Het gebeurtenislogboek kan Password Mismatch of taa-chkpasswd failure voor het API-rijk weergeven. Wijzig het wachtwoord en probeer het opnieuw.
- Nieuw wachtwoord afgewezen. Het bevindt zich in de geschiedenis (standaard laatste 12), of het heeft de huidige complexiteitsregels niet gehaald.
- De LDAP-beheerder heeft de verwachte rol verloren. Vergelijk de geconfigureerde groep met de exacte groepsnaam die door LDAP wordt geretourneerd. Een gedeeltelijke of substring match geeft de rol niet meer. Een alleen-lezen beheerder kan SAML IdP trust niet bewerken.
- Er is geen fabrieksstandaard hoofdwachtwoord bij een nieuwe installatie of fabrieksreset. Zoek of distribueer geen standaardreferenties. Bij een upgrade wordt het huidige beheerderswachtwoord niet gewist.



Let op: Factory reset is niet de upgrade-herstelstap. Het verwijdert clusteridentiteit en clustercookies. Een door het systeem geactiveerde reset na het declusteren of een inconsistente clusterdatabase houdt het IP-adres en de admin- en root-wachtwoorden bij, ruimt andere configuratie en logs op en retourneert de node naar zijn tijdelijke certificaat. Gebruik het alleen wanneer de release notes hiervoor oproepen, en alleen nadat er een back-up is gemaakt.

Bewijs dat moet worden verzameld in het geval dat TAC nodig is

1. Softwareversie en rol van elk knooppunt, plus welk knooppunt stopte.
2. Volledige systeemmomentopname van de mislukte node, inclusief tmp/install-error.
3. Servercertificaattekst (openssl x509 -text -noout). Geen privé sleutel.
4. Clusterstatus, alarmen en of xConfiguration Cluster TlsVerify Permissive of Enforce weergeeft.
5. Logregels voor gebeurtenissen voor de upgrade en, indien van toepassing, fouten in de sshd- of httpd-verificatie. Reageer wachtwoorden en cookies.
6. Of het nu gaat om lokale, LDAP- of SAML-beheerders, Smart Licensing en API-automatisering.

Na de upgrade

Op elk knooppunt

1. Versie is de beoogde X15.5.20-build.
2. Node is bereikbaar op het beheeradres en de web-UI wordt geladen.
3. Er is geen nieuw hardware-, schijf- of toepassingsalarm meer opgeheven. (Een clustercommunicatiealarm wordt gewist na hercodering.)
4. Er wordt een nieuwe back-up gemaakt nadat het cluster stabiel is.

Alleen voor clusters

1. Elke peer is boven, in de cluster, en replicatie is gezond.
2. Gelijken communiceren met wederzijdse TLS op TCP 4371 en 4372. (Een verbinding zonder geldig clientcertificaat moet mislukken.)
3. Cluster TlsVerify wordt gehandhaafd.

Permissive wordt niet ondersteund. Een waarde voor nalatenschap kan nog steeds zichtbaar zijn, maar de validatie wordt niet omzeild. Stel Enforcing in en bevestig dat het cluster gezond blijft.

4. Firewall staat nog steeds TCP 4371 alleen toe vanaf de peer-adressen.
5. Er wordt geen clustercookie of diagnostisch geheim weergegeven in logboeken of de snapshot-notities die u uploadt.

Servicecontroles, door wat het apparaat gebruikt

Indien het gebruik van	Hoe ziet goed eruit	Als het mislukt
Lokale beheerders	GUI, SSH en API accepteren het huidige wachtwoord. Verlopen accounts worden doorgestuurd om een wachtwoord te wijzigen of HTTP 401 te ontvangen.	Bevestig dat de vervaldatum om 00:00 UTC is en dat het nieuwe wachtwoord zich buiten het geschiedenisvenster bevindt.
LDAP-beheerders	Een beheerder meldt zich alleen aan wanneer de naam van de LDAP-groep exact overeenkomt met de geconfigureerde groep.	Vergelijk de directorygroep met de Expressway-groep. Verbreed de wedstrijd niet om een login te forceren.
SIP- of B2B-gesprekken	Een testrit verbindt in beide richtingen.	Verzamel gespreksgeschiedenis en een momentopname.
Geverifieerde H.323-registratie	Het eindpunt registreert met elk alias dat het gebruikt, inclusief een H.323-ID en een E.164-nummer.	Voeg voor elke alias een kaart met een alias toe. De releasenota's gebruiken xConfiguration Registration CredentialAliasMap met patroontype Exact. Als u CredentialAliasBinding uitschakelt op de subzone, wordt ook de registratie hersteld en wordt de beveiligingspositie verzwakt. H.323 zelf is niet verwijderd.
MRA of registratie van medisch hulpmiddel	Een bekend eindpunt registreert en plaatst een oproep. UC-clientcertificaatSAN's zijn specifieke DNS-namen of IP-adressen, niet te brede of misvormde waarden.	Vergelijk certificaten, verplaatsingsreferenties en DNS met de back-up vóór de upgrade. Geef een certificaat waarvan het SAN te breed is, opnieuw uit.
E-mailberichten	Een testbericht verlaat de node met behulp van STARTTLS.	Als STARTTLS niet kan worden voltooid, mislukt de levering. Herstel het vertrouwen in de e-mailserver of TLS. Verwacht geen duidelijke tekstterugval.
Smart Licensing	Registratie en autorisatie komen overeen met de Web UI. De standaardafbeelding blijft binnen 2500 gecodeerde signaalsessies , of de node is Expressway Select.	Controleer transport en CSSM. Het selectievakje CSSM "allow export-controlled function" is niet van toepassing op Expressway. Door het token in te trekken en de productinstantie te verwijderen, wordt de node uitgeschreven. Optiesleutels zijn geen workaround.
REST- of configuratiescripts	Accountnamen komen overeen met de nieuwe lengte- en	Update de client volgens het API-schema voor verzending. Een verwijderde /provisioning/optionele sleutel

Indien het gebruik van	Hoe ziet goed eruit	Als het mislukt
	tekenlimieten. Configuratieschrijven bevatten de CSRF-beveiliging die de GUI gebruikt.	oproep zal naar verwachting mislukken.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.