Liste de contrôle de mise à niveau pour Expressway 15.5.20 et versions ultérieures

Table des matières

- Introduction
- Composants utilisés
- Avant la mise à niveau
  - Comment lire le certificat
  - Que faire avant la fenêtre de maintenance
- Si la mise à niveau échoue
  - Vérification du niveau de préparation a arrêté la mise à niveau
  - Alarme lorsqu'un noeud apparaît
  - L'administrateur ne peut pas se connecter
  - Échec du certificat ou de l'identité homologue
  - Alarme de cluster pendant ou juste après la mise à niveau
  - Problèmes de connexion une fois le noeud actif
  - Preuves à collecter au cas où un cas TAC serait nécessaire
- Après la mise à niveau
  - Sur chaque noeud
  - Cluster uniquement
  - Vérifications de service, en fonction de l'utilisation du

Introduction

Ce document décrit comment préparer Expressway pour une mise à niveau vers X15.5.20 ou X15.5.21. Il répertorie chaque prérequis et comment le corriger.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Remarque : X15.5.21 peut être téléchargé. Il contient le correctif pour la vulnérabilité PHP d'octobre 2026, également appelée PHP2shell (CVE-2026-109618 et CVE-2026-109619, ID de bogue Cisco CSCwx37062.
X15.5.20 est la version de sécurisation renforcée et n'inclut pas ce correctif PHP. Utilisez

---

les vérifications de préparation de ce document pour une mise à niveau vers X15.5.20 ou vers X15.5.21. Les vérifications sont les mêmes pour les deux versions. Téléchargez X15.5.21 depuis Cisco.com. Expressway Series, ou Expressway Select pour l'image non coiffée, puis Expressway Core et Edge, version X15.5.21. L'avis de sécurité peut toujours indiquer 15.5.21 comme étant à déterminer. L'image est déjà publiée sur la page de téléchargement du logiciel ci-dessus.

Avant la mise à niveau

⚠ Mise en garde : Ne démarrez pas une mise à niveau de cluster tant que chaque homologue n'a pas passé les vérifications de préparation. Définissez la vérification TLS sur Application et confirmez que le cluster est sain. Utilisez le nom de domaine complet pour chaque identité homologue. Chaque certificat de serveur doit contenir le nom de domaine complet de ce noeud dans le SAN ou dans le CN uniquement lorsque le SAN est vide. Un SAN vide peut se produire si OpenSSL a été utilisé pour créer le CSR. Si une vérification échoue, la mise à niveau s'arrête sans modifier la configuration de cluster existante.

Chèque	Autonome	Grappe	Si ce n'est pas vrai
Le chemin de mise à niveau correspond à Annexe 3	Requis	Requis	Avant X8.11.4, arrêtez-vous à X8.11.4. Convertissez les licences PAK X12 en licences Smart avant X15.x.
Sauvegarde actuelle et plan de restauration testé	Requis	Requis sur chaque noeud	Effectuez la sauvegarde avant la fenêtre. Une réinitialisation d'usine ultérieure efface la configuration.
Cluster sain, pas d'alarmes inexpliquées, réplication synchronisée	Sans objet	Requis	Corrigez le cluster avant la mise à niveau. Une mise à niveau progressive utilise toujours le comportement normal du cluster divisé.
La vérification TLS est en cours d'application et le cluster est sain	Sans objet	Requis avant la mise à niveau	Remplacez Permissive par Enenforcement, corrigez le certificat et confirmez la réplication. Ne le découvrez pas pendant la fenêtre.
Chaque homologue utilise le nom de domaine complet et la liste d'homologues n'est pas vide	Réussites du contrôle d'identité homologue	Obligatoire. IP et FQDN mixtes bloqués avant le redémarrage	Standardisez tous les noms de domaine complets, laissez les modifications se répliquer et confirmez que le cluster est sain. Voir Modifier le cluster pour utiliser les FQDN . Ne modifiez pas le format lors d'une mise à

Chèque	Autonome	Grappe	Si ce n'est pas vrai
			niveau progressive.
Le certificat de serveur contient le nom de domaine complet du système dans le SAN ou dans le CN uniquement lorsque le SAN est vide	Obligatoire si la mise à niveau vérifie le certificat	Obligatoire. La mise à niveau s'arrête et laisse la configuration de cluster inchangée	Réémettez le certificat. S'il existe un SAN, ne vous fiez pas au CN. Rejeter les noms contenant une valeur NUL incorporée.
Le certificat est en date, approuvé par les homologues, signature RSA 2048+ ou P-256+, SHA-2	Recommandé	Requis	Les signatures SHA-1 ne sont déjà pas prises en charge par X15.2. Réémettez le certificat. Un certificat auto-signé n'est acceptable que lorsque chaque homologue est explicitement configuré pour l'approuver.
TCP 4371 autorisé uniquement à partir d'homologues connus	Recommandé	Requis	Restreignez le pare-feu. Il s'agit de la défense en profondeur pour ClusterDB ; il ne remplace pas la mise à niveau.
Clients API d'administration examinés	Requis si des API sont utilisées	Requis si des API sont utilisées	Attendez-vous à une validation plus stricte du nom et du mot de passe, à des contrôles CSRF sur les écritures FormPutXML et à aucune API de clé d'option.
La fenêtre de maintenance couvre une mise à niveau progressive ainsi qu'une alarme de cluster courte éventuelle	Fenêtre normale	Requis	Le re-cryptage des cookies peut déclencher une alarme de communication de cluster. Elle devrait s'éclaircir toute seule.

Comment lire le certificat

Exportez le certificat du serveur et inspectez-le.

- FQDN dans le SAN. Les notes de version nécessitent le nom de domaine complet du système dans un SAN. Le CN est vérifié uniquement lorsque l'extension SAN est vide.
- Pas de secours CN. Si un SAN est présent et ne correspond pas, la vérification échoue même si le CN est correct. Placez chaque nom DNS requis dans le type de SAN approprié.
- Caractères NUL. Un nom de certificat qui contient un NUL incorporé est rejeté.
- Dates. `notBefore` doit être dans le passé et `notAfter` doit être dans le futur.
- Clé. RSA au moins 2 048 bits, ou une clé EC sur P-256 ou supérieure.
- Signature. Famille SHA-2. À partir de X15.2, `sha1WithRSAEncryption` et `ecdsa-with-SHA1` ne sont pas pris en charge.
- Émetteur . Si l'objet et l'émetteur sont identiques, il est auto-signé. Les pairs doivent déjà y

faire confiance.

Que faire avant la fenêtre de maintenance

- Avant la fenêtre, définissez la vérification TLS du cluster sur Application, redémarrez le cluster (en commençant par l'éditeur) et vérifiez que le cluster est sain. Le mode permissif n'est pas pris en charge. Une valeur Permissive héritée peut rester visible, mais elle ne contourne pas l'approbation de certificat ClusterDB ou la validation d'identité d'homologue.
- Les identités des homologues doivent toutes être des noms de domaine complets. Ne modifiez pas ce format pendant qu'une mise à niveau progressive est en cours.
- Un point de terminaison H.323 authentifié avec plusieurs alias peut nécessiter une carte d'alias d'informations d'identification pour chaque alias, ou la liaison d'alias d'informations d'identification peut être désactivée sur la sous-zone. Désactiver la liaison affaiblit la position de sécurité.
- L'expiration du mot de passe d'administrateur local reste désactivée lorsque `PasswordExpiryDays` est 0. Lorsqu'elle est activée, l'expiration est calculée à 00:00 UTC, et non à minuit locale.
- La profondeur de l'historique des mots de passe est définie par défaut sur 12. La plage de formation est comprise entre 3 et 24. Les mots de passe administrateur vides sont rejetés et un mot de passe récemment utilisé peut être rejeté.
- Le mappage des rôles d'administrateur LDAP nécessite une correspondance exacte de nom de groupe. Un nom de groupe qui contient uniquement le nom configuré n'accorde plus le rôle.
- Une nouvelle installation, une réinitialisation en usine ou un déploiement sans assistance ne peuvent pas réutiliser un mot de passe racine par défaut. Une mise à niveau n'efface pas le mot de passe administrateur actuel.
- Un administrateur en lecture seule ne peut plus modifier l'approbation du fournisseur d'identité SAML.
- Les e-mails qui ne peuvent pas terminer STARTTLS ne sont pas envoyés en clair.
- Smart Licensing est le seul mode de licence. Les clés d'option PAK ont été supprimées dans X14.2. L'image Expressway standard autorise 2 500 sessions de signalisation chiffrées ; Expressway Select est l'image non coiffée.

Si la mise à niveau échoue

Laissez le cluster tel quel. Un contrôle de préparation en échec ne modifie pas la configuration de cluster existante. Ne réinitialisez pas en usine un noeud pour dépasser l'échec.

Vérification du niveau de préparation a arrêté la mise à niveau

Le programme d'installation s'arrête avant le redémarrage lorsque le certificat, la vérification TLS ou l'exigence d'identité homologue échoue. Les noeuds autonomes réussissent le contrôle

d’identité des homologues.

Alarme lorsqu'un noeud apparaît

Une rafale de re-cryptage de base de données de cluster peut déclencher une alarme d'échec de communication de cluster. Laisse-lui le temps de finir. Escalade si ça reste en place.

L'administrateur ne peut pas se connecter

Traitez ce problème séparément d'un échec d'installation. Les mots de passe expirés, réutilisés ou de première connexion bloquent la session. Elles ne signifient pas que l'image a échoué.

Échec du certificat ou de l'identité homologue

1. Téléchargez un snapshot système complet à partir du noeud qui s'est arrêté. Ouvrez installlimage.log dans le répertoire tmp de ce snapshot.
2. Si le message concerne l'identité d'homologue, recherchez une combinaison d'adresses IP et de FQDN, ou une liste d'homologues vide. Faites en sorte que chaque homologue utilise un format unique, attendez la réplication, confirmez que le cluster est sain et réessayez. Ne modifiez pas le format d'identité au milieu d'une mise à niveau progressive.
3. Si le message concerne le certificat, comparez-le à la règle de la note de version : le nom de domaine complet du système doit se trouver dans le SAN ou dans le CN uniquement lorsque le SAN est vide. Un SAN actuel n'est pas autorisé à revenir au CN.
4. Réémettez le certificat avec chaque nom DNS requis dans le type SAN correct. Rejeter un nom qui contient un NUL incorporé.
5. Vérifiez que le nouveau certificat est en date, approuvé, RSA 2048+ ou P-256+ et signé avec SHA-2. N'attachez pas la clé privée au boîtier.
6. Définissez la vérification TLS sur Enenforcement, confirmez que le cluster est sain et réessayez la mise à niveau sur le noeud qui s'est arrêté.
7. Poursuivez la mise à niveau progressive uniquement une fois que ce noeud est sain. Ne mettez pas à niveau les noeuds restants tant qu'un noeud est arrêté lors de cette vérification.

Alarme de cluster pendant ou juste après la mise à niveau

1. Vérifiez que la mise à niveau est terminée et que le noeud se trouve sur la version prévue, X15.5.20 ou X15.5.21.
2. Recherchez dans le journal des événements des messages developer.upgrade sur le re-chiffrement des champs ClusterDB, puis « Saving migrated data to CDB ».
3. Attendez que l'alarme se désactive. Le matériel de formation indique qu'il est effacé lorsque le réencodage est terminé.
4. S'il reste, collectez l'état du cluster, les alarmes et un instantané de chaque homologue. Ne copiez pas les cookies de cluster ou les éléments clés dans les notes de cas.

Problèmes de connexion une fois le noeud actif

- L'interface utilisateur Web redirige vers un changement de mot de passe. Le mot de passe actuel doit être entré et le nouveau mot de passe doit être différent. Cela est prévu lors de la première connexion à l'interface graphique utilisateur après une installation ou une réinitialisation d'usine, et lorsqu'un mot de passe local a expiré.
- SSH dit clavier-interactif / PAM a échoué et n'ouvre jamais un shell. Un mot de passe local expiré doit être modifié. L'ancienne session n'est pas accordée.
- REST renvoie 401. Attendu pour un administrateur local arrivé à expiration. Le journal des événements peut afficher `Password Mismatch` ou `taa-chkpasswd` failure pour le domaine API. Modifiez le mot de passe, puis réessayez.
- Nouveau mot de passe rejeté. Il est dans l'historique (par défaut 12 derniers), ou il a échoué les règles de complexité actuelles.
- L'administrateur LDAP a perdu le rôle attendu. Comparez le groupe configuré avec le nom de groupe exact renvoyé par LDAP. Une correspondance partielle ou de sous-chaîne n'accorde plus le rôle. Un administrateur en lecture seule ne peut pas modifier l'approbation du fournisseur d'identité SAML.
- Il n'existe aucun mot de passe racine par défaut sur une nouvelle installation ou réinitialisation d'usine. Ne recherchez pas et ne distribuez pas d'informations d'identification par défaut. Une mise à niveau n'efface pas le mot de passe administrateur actuel.

⚠ Mise en garde : La réinitialisation en usine n'est pas l'étape de mise à niveau/récupération. Il supprime l'identité et les cookies de cluster. Une réinitialisation déclenchée par le système après la désagrégation ou une base de données de cluster incohérente conserve l'adresse IP et les mots de passe admin et root, efface d'autres configurations et journaux et renvoie le noeud à son certificat temporaire. Utilisez-la uniquement lorsque les notes de version l'appellent et uniquement après l'existence d'une sauvegarde.

Preuves à collecter au cas où un cas TAC serait nécessaire

1. Version logicielle et rôle de chaque noeud, plus le noeud arrêté.
2. Instantané système complet à partir du noeud défaillant, y compris tmp/installimage.log.
3. Texte du certificat du serveur (openssl x509 -text -noout). Pas de clé privée.
4. État du cluster, alarmes et indication si xConfiguration Cluster TlsVerify indique Permissive ou Enforce.
5. Lignes du journal des événements pour la mise à niveau et, le cas échéant, échecs d'authentification sshd ou httpd. Supprimer les mots de passe et les cookies.
6. Qu'il s'agisse d'administrateurs locaux, LDAP ou SAML, de licences Smart et de toute automatisation d'API.

Après la mise à niveau

Sur chaque noeud

1. Version est la version prévue. Utilisez X15.5.21 lorsque la mise à niveau concerne la vulnérabilité PHP d'octobre 2026. X15.5.20 n'inclut pas ce correctif.
2. Le noeud est accessible sur son adresse de gestion et l'interface utilisateur Web se charge.
3. Aucune nouvelle alarme matérielle, disque ou application n'est déclenchée. (Une alarme de communication de cluster disparaît après un nouveau cryptage.)
4. Une nouvelle sauvegarde est effectuée une fois que le cluster est stable.

Cluster uniquement

1. Chaque homologue est actif, dans le cluster, et la réplication est saine.
2. Les homologues communiquent avec TLS mutuel sur TCP 4371 et 4372. (Une connexion sans certificat client valide doit échouer.)
3. Cluster TlsVerify est en cours d'application.

Les autorisations ne sont pas prises en charge. Une valeur Permissive héritée peut toujours être visible, mais elle ne contourne pas la validation. Définissez Application et confirmez que le cluster reste sain.

4. Le pare-feu autorise toujours le protocole TCP 4371 uniquement à partir des adresses homologues.

5. Aucun cookie de cluster ou secret de diagnostic n'apparaît dans les journaux ou les notes de capture instantanée que vous téléchargez.

Vérifications de service, en fonction de l'utilisation du

Si vous utilisez	A quoi ressemble un bon	En cas d'échec
Administrateurs locaux	Les interfaces GUI, SSH et API acceptent le mot de passe actuel. Les comptes expirés sont poussés vers un changement de mot de passe ou reçoivent HTTP 401.	Confirmez que l'expiration est à 00:00 UTC et que le nouveau mot de passe se trouve en dehors de la fenêtre d'historique.
Administrateurs LDAP	Un administrateur se connecte uniquement lorsque le nom du groupe LDAP correspond exactement au groupe configuré.	Comparez le groupe de répertoires avec le groupe Expressway. N'élargissez pas la correspondance pour forcer une connexion.
Appels SIP ou B2B	Un appel test se connecte dans les deux directions.	Collecter l'historique des appels et un instantané.
Enregistrement H.323 authentifié	Le point d'extrémité s'enregistre avec chaque alias qu'il utilise, y	Ajoutez un mappage d'alias d'informations d'identification pour chaque alias. Les notes de version utilisent `xConfiguration Registration`

Si vous utilisez	A quoi ressemble un bon	En cas d'échec
	compris un ID H.323 et un numéro E.164.	`CredentialAliasMap` avec le type de modèle Exact. La désactivation de `CredentialAliasBinding` sur la sous-zone restaure également l'enregistrement et affaiblit la position de sécurité. Le H.323 lui-même n'est pas supprimé.
MRA ou enregistrement de périphérique	Un terminal connu enregistre et passe un appel. Les SAN de certificat de client UC sont des noms DNS spécifiques, et non des valeurs trop larges ou mal formées.	Comparez les certificats, les identifiants de traversée et le DNS avec la sauvegarde de pré-mise à niveau. Réémettre un certificat dont le SAN est trop large.
Alertes par e-mail	Un message de test quitte le noeud à l'aide de STARTTLS.	Si STARTTLS ne peut pas se terminer, la livraison échoue. Corrigez l'approbation du serveur de messagerie ou TLS. Ne vous attendez pas à une reprise en texte clair.
Licences Smart	L'inscription et l'autorisation correspondent à l'interface utilisateur Web. L'image standard reste dans 2500 sessions de signalisation chiffrées, ou le noeud est Expressway Select.	Vérifiez le transport et le CSSM. La case à cocher CSSM « Autoriser la fonctionnalité contrôlée par l'exportation » ne s'applique pas à Expressway. La révocation du jeton et la suppression de l'instance de produit définissent le noeud sur Désinscrit. Les touches d'option ne constituent pas une solution.
REST ou scripts de configuration	Les noms de compte correspondent aux nouvelles limites de longueur et de caractère. Les écritures de configuration incluent la protection CSRF utilisée par l'interface utilisateur graphique.	Mettez à jour le client par rapport au schéma API d'expédition. Un appel supprimé `/provisioning/optionkey` est censé échouer.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.