

Elenco di controllo per l'aggiornamento di Expressway 15.5.20

Sommario

[Introduzione](#)

[Componenti usati](#)

[Prima dell'aggiornamento](#)

[Come leggere il certificato](#)

[Operazioni da eseguire prima della finestra Manutenzione](#)

[Se l'aggiornamento non riesce](#)

[Aggiornamento interrotto dal controllo preparazione](#)

[Allarme dopo l'accensione di un nodo](#)

[L'amministratore non può accedere](#)

[Errore certificato o identità peer](#)

[Allarme cluster durante o subito dopo l'aggiornamento](#)

[Problemi di accesso dopo l'attivazione del nodo](#)

[Prove da raccogliere nel caso in cui sia necessario un TAC](#)

[Dopo l'aggiornamento](#)

[In ogni nodo](#)

[Solo cluster](#)

[Controlli del servizio in base all'oggetto in uso](#)

Introduzione

Questo documento descrive come preparare Expressway per l'aggiornamento di protezione avanzata X15.5.20. Vengono elencati tutti i prerequisiti e le relative modalità di correzione.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prima dell'aggiornamento



Attenzione: Non avviare l'aggiornamento di un cluster finché ogni peer non supera i controlli di idoneità. Impostare la verifica TLS su Imponi e verificare che il cluster sia integro. Utilizzare un formato di identità peer, non una combinazione di indirizzi IP e

FQDN. Ogni certificato server deve contenere il nome di dominio completo (FQDN) del nodo nella rete SAN o nel CN solo quando la rete SAN è vuota. Se per creare il CSR è stato utilizzato OpenSSL, è possibile che si verifichi una SAN vuota. Se un controllo ha esito negativo, l'aggiornamento viene interrotto senza modificare la configurazione del cluster esistente.

Assegno	Autonomo	Cluster	Se non è vero
Il percorso di aggiornamento corrisponde all' appendice 3	Obbligatorio	Obbligatorio	Prima di X8.11.4, arrestarsi su X8.11.4. Convertire le licenze PAK X12 in licenze Smart prima di X15.x .
Backup corrente e piano di rollback testato	Obbligatorio	Obbligatorio in ogni nodo	Eseguire il backup prima della finestra. Una volta ripristinata in fabbrica, la configurazione viene cancellata.
Integrità del cluster, nessun allarme ingiustificato, replica sincronizzata	Non applicabile	Obbligatorio	Correggere il cluster prima dell'aggiornamento. Un aggiornamento in sequenza utilizza ancora il normale comportamento di split-cluster.
La verifica TLS viene applicata e il cluster è integro	Non applicabile	Obbligatorio prima dell'aggiornamento	Cambiare Permissivo in Imponente, correggere il certificato e confermare la replica. Non visualizzare questo messaggio durante la finestra.
Ogni peer utilizza lo stesso formato di identità e l'elenco dei peer non è vuoto	Passaggi controllo identità peer	Obbligatorio. L'IP e il nome di dominio completo (FQDN) misti sono bloccati prima del riavvio	Standardizzazione su tutti gli FQDN o su tutti gli indirizzi IP, replica della modifica e verifica dello stato di integrità del cluster. Non modificare il formato durante un aggiornamento in sequenza.
Il certificato del server contiene l'FQDN di sistema nella SAN o nel CN solo quando la SAN è vuota	Obbligatorio se l'aggiornamento controlla il certificato	Obbligatorio. L'aggiornamento si interrompe e lascia invariata la configurazione del cluster	Riemettere il certificato. Se esiste una SAN, non affidarsi alla CN. Rifiuta i nomi che contengono un NUL incorporato.
Il certificato è in data, considerato attendibile dai peer, firma RSA 2048+ o P-256+, SHA-2	Consigliato	Obbligatorio	Le firme SHA-1 non sono supportate da X15.2 . Riemettere il certificato. Un certificato autofirmato è accettabile solo quando ogni peer è configurato

Assegno	Autonomo	Cluster	Se non è vero
			esplicitamente per considerarlo attendibile.
TCP 4371 consentito solo da peer noti	Consigliato	Obbligatorio	Limitare il firewall. Questa è una difesa approfondita per ClusterDB; non sostituisce l'upgrade.
Client API di amministrazione esaminati	Obbligatorio se vengono utilizzate le API	Obbligatorio se vengono utilizzate le API	Prevista una convalida più stretta di nome e password, controlli CSRF sulle scritture FormPutXML e nessuna API option-key.
La finestra di manutenzione copre un aggiornamento in sequenza più un possibile breve allarme cluster	Finestra normale	Obbligatorio	La ricrittografia dei cookie può generare un allarme di comunicazione del cluster. Ci si aspetta che sia chiaro da solo.

Come leggere il certificato

Esportare il certificato del server ed esaminarlo.

- FQDN nella SAN. Le [note di rilascio](#) richiedono l'FQDN del sistema in una rete SAN. La CN viene controllata solo quando l'estensione SAN è vuota.
- Nessun fallback CN. Se una SAN è presente e non corrisponde, la [verifica non riesce anche quando la CN è corretta](#). Inserire tutti i nomi DNS o gli indirizzi IP richiesti nel tipo di SAN corretto.
- Caratteri NULL. Un nome di certificato che contiene un NUL incorporato è rifiutato.
- Date. notBefore deve essere nel passato e notAfter nel futuro.
- Chiave. RSA di almeno 2048 bit o una chiave EC su P-256 o superiore.
- Firma. Famiglia SHA-2. Da X15.2, [sha1WithRSAEncryption e ecdsa-with-SHA1](#) non sono supportati.
- Emittente. Se Subject e Issuer coincidono, la firma viene apposta da se stessa. I peer devono già fidarsi.

Operazioni da eseguire prima della finestra Manutenzione

- Prima della finestra, impostare la verifica TLS del cluster su [Imponente](#), riavviare il cluster (partendo dall'editore) e verificare che il cluster sia integro. Modalità di autorizzazione non supportata. È possibile che un valore Permissive legacy rimanga visibile, ma non ignora l'attendibilità del certificato ClusterDB o la convalida dell'identità peer.
- Le identità peer devono essere tutte FQDN o essere tutte indirizzi IP. Non modificare tale

formato durante un aggiornamento in sequenza.

- Per un endpoint H.323 autenticato con più di un alias potrebbe essere necessaria una [definizione alias delle credenziali](#) per ogni alias oppure l'associazione alias delle credenziali potrebbe essere disattivata nella sottozona. La disattivazione dell'associazione indebolisce la postura di sicurezza.
- La scadenza della password dell'amministratore locale rimane disattivata quando PasswordExpiryDays è pari a 0. Quando è attivata, la scadenza viene calcolata alle 00:00 UTC, non alla mezzanotte locale.
- [Il valore predefinito della profondità della cronologia delle password è 12](#). L'intervallo di addestramento è compreso tra 3 e 24. Le password di amministratore vuote vengono rifiutate e le password utilizzate di recente possono essere rifiutate.
- [Il mapping amministratore-ruolo LDAP](#) richiede una corrispondenza esatta del nome del gruppo. Un nome di gruppo che contiene solo il nome configurato non concede più il ruolo.
- Una nuova installazione, una nuova reimpostazione di fabbrica o una distribuzione automatica non può riutilizzare una [password di root predefinita di fabbrica](#). L'aggiornamento non cancella la password amministratore corrente.
- Un amministratore di sola lettura non può più modificare l'attendibilità del provider di identità SAML.
- I messaggi di posta elettronica che non possono completare STARTTLS non vengono inviati in chiaro.
- [Smart Licensing](#) è l'unica modalità di gestione delle licenze. Le chiavi di opzione PAK sono state rimosse in X14.2. L'immagine Expressway standard consente [2500 sessioni di segnalazione crittografate](#); Expressway Select è l'immagine senza cappuccio.

Se l'aggiornamento non riesce

Lasciare il cluster inalterato. Un controllo di conformità non riuscito non modifica la configurazione cluster esistente. Non eseguire la reimpostazione di fabbrica di un nodo per superare l'errore.

Aggiornamento interrotto dal controllo preparazione

Il programma di installazione si arresta prima del riavvio quando il certificato, la verifica TLS o i requisiti di identità peer non riescono. I nodi autonomi superano il controllo di identità peer.

Allarme dopo l'accensione di un nodo

Una frammentazione della ricrittografia del database cluster può generare un allarme di errore di comunicazione del cluster. Dagli tempo di finire. Escalate se rimane attivo.

L'amministratore non può accedere

Trattare questo problema separatamente da un errore di installazione. Le password scadute, riutilizzate o utilizzate per il primo accesso bloccano la sessione. Non significa che l'immagine sia fallita.

Errore certificato o identità peer

1. Scaricare uno snapshot di sistema completo dal nodo arrestato. Aprire install-error nella directory tmp della copia istantanea.
2. Se il messaggio riguarda l'identità dei peer, verificare la presenza di una combinazione di indirizzi IP e FQDN o di un elenco di peer vuoto. Fare in modo che ogni peer utilizzi un unico formato, attendere la replica, verificare che il cluster sia integro e riprovare. Non modificare il formato di identità durante un aggiornamento in sequenza.
3. Se il messaggio riguarda il certificato, confrontarlo con la regola della nota sulla versione: l'FQDN del sistema deve essere nella SAN o nel CN solo quando la SAN è vuota. Non è consentito eseguire il fallback alla rete SAN attuale.
4. Rimettere il certificato con ogni nome DNS o indirizzo IP richiesto nel tipo di SAN corretto. Rifiutare un nome che contiene un NUL incorporato.
5. Confermare che il nuovo certificato sia in data, attendibile, RSA 2048+ o P-256+ e firmato con SHA-2. Non allegare la chiave privata alla richiesta.
6. Impostare la verifica TLS su Imponente, verificare che il cluster sia integro e ripetere l'aggiornamento sul nodo interrotto.
7. Continuare l'aggiornamento in sequenza solo dopo che il nodo è integro. Non aggiornare i nodi rimanenti mentre un nodo è interrotto in questo controllo.

Allarme cluster durante o subito dopo l'aggiornamento

1. Verificare che l'aggiornamento sia stato completato e che il nodo si trovi in X15.5.20.
2. Cercare nel registro eventi i messaggi developer.upgrade relativi alla ricrittografia dei campi di ClusterDB, quindi "Salvataggio dei dati migrati nel CDB".
3. Aspettate che l'allarme scompaia. Il materiale di formazione afferma che viene cancellato al termine della ricrittografia.
4. In caso affermativo, raccogliere lo stato del cluster, gli allarmi e un'istantanea da ogni peer. Non copiare i cookie del cluster o il materiale della chiave nelle note della richiesta.
5. Confermare che i protocolli TCP 4371 e 4372 siano aperti solo tra peer e che il protocollo TLS reciproco abbia esito positivo. Un firewall che consente l'uso di 4371 da qualsiasi luogo non è la soluzione.

Problemi di accesso dopo l'attivazione del nodo

- L'interfaccia utente Web reindirizza a una modifica della password. È necessario immettere la password corrente e la nuova password deve essere diversa. Questo è previsto al primo accesso alla GUI dopo un'installazione o un reset di fabbrica e quando una password locale è scaduta.
- SSH: tastiera interattiva/PAM non riuscita e non apre mai una shell. È necessario modificare una password locale scaduta. La sessione precedente non è concessa.
- REST restituisce 401. Previsto per un amministratore locale scaduto. Il registro eventi può visualizzare la mancata corrispondenza delle password o l'errore taa-chkpasswd per l'area di autenticazione API. Modificare la password, quindi riprovare.
- Nuova password rifiutata. Si trova nella cronologia (ultimo 12 per impostazione predefinita) oppure non è riuscita a rispettare le regole di complessità correnti.

- L'amministratore LDAP ha perso il ruolo previsto. Confrontare il gruppo configurato con il nome esatto del gruppo restituito da LDAP. Una corrispondenza parziale o di sottostringa non concede più il ruolo. Un amministratore di sola lettura non può modificare l'attendibilità del provider di identità SAML.
- Nessuna password di root predefinita in una nuova installazione o in una reimpostazione di fabbrica. Non cercare o distribuire credenziali predefinite. L'aggiornamento non cancella la password corrente dell'amministratore.



Attenzione: Il ripristino in fabbrica non è il passaggio di aggiornamento-ripristino. Elimina l'identità e i cookie del cluster. Una reimpostazione avviata dal sistema dopo il declustering o un database cluster incoerente mantiene l'indirizzo IP e le password di amministrazione e radice, cancella altre configurazioni e registri e restituisce il nodo al relativo certificato temporaneo. Utilizzarlo solo quando richiesto dalle note sulla versione e solo dopo l'esistenza di un backup.

Prove da raccogliere nel caso in cui sia necessario un TAC

1. Versione del software e ruolo di ogni nodo, oltre al nodo arrestato.
2. Snapshot completo del sistema dal nodo non riuscito, incluso tmp/install-error.
3. Testo certificato server (openssl x509 -text -noout). Nessuna chiave privata.
4. Stato del cluster, allarmi e se TlsVerify del cluster xConfiguration mostra Permissive o Enforce.
5. Righe del registro eventi per l'aggiornamento e, se pertinente, errori di autenticazione sshd o httpd. Redigere password e cookie.
6. Utilizzo di amministratori locali, LDAP o SAML, di Smart Licensing e di qualsiasi automazione API.

Dopo l'aggiornamento

In ogni nodo

1. Versione: la build X15.5.20 prevista.
2. Il nodo è raggiungibile con il relativo indirizzo di gestione e viene caricata l'interfaccia utente Web.
3. Non viene lasciato alcun avviso di nuovo hardware, disco o applicazione. (Dopo la ricrittografia viene cancellato un allarme di comunicazione del cluster.)
4. Dopo la stabilità del cluster viene eseguito un nuovo backup.

Solo cluster

1. Ogni peer è attivo, nel cluster e la replica è integra.
2. I peer comunicano con Mutual TLS su TCP 4371 e 4372. (Una connessione senza un certificato client valido deve avere esito negativo).

3. TlsVerify del cluster applicato.

Autorizzazione non supportata. Un valore di tipo Permissive legacy potrebbe essere ancora visibile, ma non ignora la convalida. Impostare Enforcement e verificare che il cluster rimanga integro.

4. Il firewall consente ancora il protocollo TCP 4371 solo dagli indirizzi peer.

5. Nessun cookie del cluster o segreto di diagnostica viene visualizzato nei log o nelle note dello snapshot caricate.

Controlli del servizio in base all'oggetto in uso

Se si utilizza	Aspetto positivo	In caso di esito negativo
Amministratori locali	La GUI, SSH e l'API accettano la password corrente. Gli account scaduti vengono sottoposti a PUSH per la modifica della password o ricevono HTTP 401.	Confermare che la scadenza è alle 00:00 UTC e che la nuova password si trova all'esterno della finestra della cronologia.
Amministratori LDAP	Un amministratore accede solo quando il nome del gruppo LDAP corrisponde esattamente al gruppo configurato.	Confrontare il gruppo di directory con il gruppo Expressway. Non ampliare la corrispondenza per forzare un accesso.
Chiamate SIP o B2B	Una chiamata di prova si connette in entrambe le direzioni.	Raccogliere la cronologia delle chiamate e uno snapshot.
Registrazione H.323 autenticata	L'endpoint viene registrato con tutti gli alias utilizzati, inclusi un ID H.323 e un numero E.164.	Aggiungere una definizione alias credenziali per ogni alias. Le note sulla versione utilizzano xConfiguration Registration CredentialAliasMap con il tipo di modello Exact. La disattivazione di CredentialAliasBinding nella sottozona consente inoltre di ripristinare la registrazione e di indebolire la postura di sicurezza. H.323 non viene rimosso.
Registrazione MRA o dispositivo	Un endpoint noto registra ed effettua una chiamata. Le SAN con certificati client UC sono nomi DNS o indirizzi IP specifici, non valori troppo ampi o non corretti.	Confrontare i certificati, le credenziali trasversali e il DNS con il backup precedente all'aggiornamento. Rimettere un certificato con SAN troppo ampia.
Avvisi e-mail	Un messaggio di prova lascia il nodo utilizzando STARTTLS.	Se STARTTLS non può essere completato, il recapito non verrà chiuso. Correggere l'attendibilità del server di posta o TLS. Non è previsto il fallback del testo non crittografato.

Se si utilizza	Aspetto positivo	In caso di esito negativo
Licenze Smart	La registrazione e l'autorizzazione corrispondono all'interfaccia Web. L'immagine standard rimane all'interno di 2500 sessioni di segnalazione crittografate , oppure il nodo è Expressway Select.	Controllare trasporto e CSSM. La casella di controllo "Consenti funzionalità di controllo dell'esportazione" di CSM non è applicabile a Expressway. La revoca del token e l'eliminazione dell'istanza del prodotto impostano il nodo su Non registrato. Le chiavi di opzione non rappresentano una soluzione.
REST o script di configurazione	I nomi di account corrispondono ai nuovi limiti di lunghezza e di carattere. Le scritture della configurazione includono la protezione CSRF utilizzata dalla GUI.	Aggiornare il client in base allo schema API di spedizione. Una chiamata a <code>/provisioning/optionkey</code> rimossa non riuscirà.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).