

Lista de comprobación de actualización para Expressway 15.5.20

Contenido

[Introducción](#)

[Componentes Utilizados](#)

[Antes de actualizar](#)

[Cómo leer el certificado](#)

[Qué hacer antes de la ventana de mantenimiento](#)

[Si falla la actualización](#)

[La comprobación de preparación detuvo la actualización](#)

[Alarma cuando aparece un nodo](#)

[El administrador no puede iniciar sesión](#)

[Error de certificado o de identidad del mismo nivel](#)

[Alarma de clúster durante o justo después de la actualización](#)

[Problemas de inicio de sesión después de que el nodo esté activo](#)

[Evidencia a recolectar en caso de que el caso TAC sea necesario](#)

[Después de la actualización](#)

[En cada nodo](#)

[Sólo clúster](#)

[Comprobaciones de servicio, según el uso del](#)

Introducción

Este documento describe cómo preparar Expressway para la actualización de protección de seguridad X15.5.20. En ella se enumeran todos los requisitos previos y cómo corregirlos.

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antes de actualizar



Precaución: No inicie una actualización de clúster hasta que cada par pase las comprobaciones de disponibilidad. Establezca la verificación de TLS en Aplicar y confirme que el clúster está correcto. Utilice un formato de identidad de peer, no una mezcla de

direcciones IP y FQDN. Cada certificado de servidor debe contener el FQDN de ese nodo en la SAN o en la CN sólo cuando la SAN está vacía. Una SAN vacía puede ocurrir si se utilizó OpenSSL para crear el CSR. Si se produce un error en una comprobación, la actualización se detiene sin cambiar la configuración del clúster existente.

Cheque	Independiente	Clúster	Si no es verdad
La ruta de actualización coincide con el apéndice 3	Necesario	Necesario	Antes de X8.11.4, deténgase primero en X8.11.4. Convierta las licencias PAK X12 en licencias inteligentes antes de X15.x .
Copia de seguridad actual y un plan de reversión probado	Necesario	Obligatorio en todos los nodos	Tome la copia de seguridad antes de la ventana. Un restablecimiento de fábrica posterior borra la configuración.
Clúster en buen estado, sin alarmas sin explicación, replicación sincronizada	No aplicable	Necesario	Corrija el clúster antes de actualizar. Una actualización sucesiva todavía utiliza el comportamiento normal de split-cluster.
La verificación de TLS es obligatoria y el clúster funciona correctamente	No aplicable	Necesario antes de la actualización	Cambie Permissive a Enforcement, corrija el certificado y confirme la replicación. No lo descubra durante la ventana.
Todos los pares utilizan el mismo formato de identidad y la lista de pares no está vacía	Comprobación de identidad del par superada	Necesario. La IP y el FQDN combinados se bloquean antes del reinicio	Estandarice todos los FQDN o todas las direcciones IP, deje que el cambio se replique y confirme que el clúster está correcto. No cambie el formato durante una actualización sucesiva.
El certificado de servidor contiene el FQDN del sistema en la SAN o en la CN sólo cuando la SAN está vacía	Requerido si la actualización comprueba el certificado	Necesario. La actualización se detiene y no modifica la configuración del clúster	Vuelva a emitir el certificado. Si existe una SAN, no confíe en la CN. Rechazar nombres que contengan un valor NUL incrustado.
El certificado está actualizado, es de confianza para los pares, RSA 2048+ o P-256+, firma SHA-2	Recomendado	Necesario	Las firmas SHA-1 ya no son compatibles con X15.2 . Vuelva a emitir el certificado. Un certificado autofirmado sólo es aceptable cuando cada par está configurado explícitamente para confiar en él.

Cheque	Independiente	Clúster	Si no es verdad
TCP 4371 permitido sólo desde pares conocidos	Recomendado	Necesario	Restrinja el firewall. Esto es defensa en profundidad para ClusterDB; no es un sustituto de la actualización.
Cientes API de administración revisados	Requerido si se utilizan API	Requerido si se utilizan API	Se espera una validación de nombre y contraseña más estricta, comprobaciones CSRF en escrituras FormPutXML y ninguna API de clave de opción.
La ventana de mantenimiento cubre una actualización sucesiva más una posible alarma de clúster corta	ventana Normal	Necesario	El recifrado de cookies puede provocar una alarma de comunicación de clúster. Se espera que se despeje por sí solo.

Cómo leer el certificado

Exporte el certificado del servidor e invítelo.

- FQDN en la SAN. Las [notas de la versión](#) requieren el FQDN del sistema en una SAN. La CN se comprueba sólo cuando la extensión SAN está vacía.
- Sin repliegue CN. Si hay una SAN presente y no coincide, la [verificación falla incluso cuando el CN es correcto](#). Introduzca todos los nombres DNS o direcciones IP necesarios en el tipo de SAN correcto.
- Caracteres NUL. Se rechaza un nombre de certificado que contiene un NUL incrustado.
- Fechas. `notBefore` debe estar en el pasado y `notAfter` en el futuro.
- Clave. RSA tiene al menos 2048 bits, o una clave EC en P-256 o superior.
- Firma. Familia SHA-2. Desde X15.2, no se soportan [sha1WithRSAEncryption](#) y [ecdsa-with-SHA1](#).
- Emisor. Si Asunto y Emisor son iguales, se firmarán a sí mismos. Los pares ya deben confiar en él.

Qué hacer antes de la ventana de mantenimiento

- Antes de la ventana, establezca la verificación de TLS del clúster en [Forzando](#), reinicie el clúster (empezando primero por el editor) y confirme que el clúster está correcto. No se admite el modo permisivo. Un valor permisivo heredado podría permanecer visible, pero no omite la confianza de certificados de ClusterDB o la validación de identidad del mismo nivel.
- Todas las identidades de peer deben ser FQDN o todas deben ser direcciones IP. No cambie ese formato mientras haya una actualización sucesiva en curso.
- Un extremo H.323 autenticado con más de un alias podría necesitar un [mapa de alias de credenciales](#) para cada alias, o un enlace de alias de credenciales desactivado en la subzona. Desactivar la vinculación debilita la condición en materia de seguridad.

- El vencimiento de la contraseña de administrador local permanece desactivado cuando PasswordExpiryDays es 0. Cuando está habilitado, el vencimiento se calcula a las 00:00 UTC, no a medianoche local.
- [El valor predeterminado de la profundidad del historial de contraseñas es 12](#). El intervalo de formación es de 3 a 24. Se rechazan las contraseñas de administrador vacías y se puede rechazar una contraseña utilizada recientemente.
- [La asignación de roles de administrador LDAP](#) requiere una coincidencia exacta de nombre de grupo. Un nombre de grupo que sólo contiene el nombre configurado ya no concede el rol.
- Una instalación nueva, un restablecimiento de fábrica o una implementación desatendida no pueden reutilizar una [contraseña raíz predeterminada de fábrica](#). Una actualización no borra la contraseña de administrador actual.
- Un administrador de solo lectura ya no puede cambiar la confianza de IdP de SAML.
- El correo electrónico que no puede completar STARTTLS no se envía en el campo clear.
- [Smart Licensing](#) es el único modo de licencia. Las claves de opción PAK se eliminaron en X14.2. La imagen estándar de Expressway permite [2500 sesiones de señalización cifradas](#); Expressway Select es la imagen sin cierre.

Si falla la actualización

Deje el clúster tal cual. Una comprobación de preparación con error no cambia la configuración de clúster existente. No restablezca los valores de fábrica de un nodo para superar el error.

La comprobación de preparación detuvo la actualización

El instalador se detiene antes del reinicio cuando falla el certificado, la verificación de TLS o el requisito de identidad de peer. Los nodos independientes pasan la comprobación de identidad del mismo nivel.

Alarma cuando aparece un nodo

Una ráfaga de recifrado de la base de datos del clúster puede generar una alarma de falla de comunicación del clúster. Dale tiempo para terminar. Escalar si se mantiene activa.

El administrador no puede iniciar sesión

Trate esto por separado de un fallo de instalación. Las contraseñas caducadas, reutilizadas o de primer inicio de sesión bloquean la sesión. No significan que la imagen haya fallado.

Error de certificado o de identidad del mismo nivel

1. Descargue una instantánea completa del sistema desde el nodo que se detuvo. Abra install-error en el directorio tmp de esa instantánea.
2. Si el mensaje es acerca de la identidad de peer, verifique si hay una mezcla de direcciones

IP y FQDN, o una lista de peer vacía. Haga que cada par utilice un formato, espere a la replicación, confirme que el clúster está correcto y vuelva a intentarlo. No cambie el formato de identidad en medio de una actualización sucesiva.

3. Si el mensaje es sobre el certificado, compárelo con la regla de la nota de la versión: el FQDN del sistema debe estar en la SAN o en la CN sólo cuando la SAN está vacía. No se permite que una SAN actual vuelva a ser CN.
4. Vuelva a emitir el certificado con cada nombre DNS o dirección IP necesarios en el tipo de SAN correcto. Rechazar un nombre que contiene un valor NUL incrustado.
5. Confirme que el nuevo certificado está en la fecha, es de confianza, RSA 2048+ o P-256+, y está firmado con SHA-2. No adjunte la clave privada al caso.
6. Establezca la verificación TLS en Forzoso, confirme que el clúster está correcto y vuelva a intentar la actualización en el nodo que se detuvo.
7. Continúe con la actualización sucesiva sólo después de que el nodo esté en buen estado. No actualice los nodos restantes mientras haya un nodo detenido en esta comprobación.

Alarma de clúster durante o justo después de la actualización

1. Confirme que la actualización haya finalizado y que el nodo esté en X15.5.20.
2. Busque en el registro de eventos los mensajes developer.upgrade acerca de cómo volver a cifrar los campos ClusterDB y, a continuación, "Guardar datos migrados en CDB".
3. Espere a que se active la alarma. El material de formación indica que se borra cuando finaliza el recifrado.
4. Si permanece, recopile el estado del clúster, las alarmas y una instantánea de cada par. No copie cookies de clúster ni material clave en las notas del caso.
5. Confirme que TCP 4371 y 4372 estén abiertos solamente entre los pares y que TLS mutuo sea exitoso. Un firewall que permita 4371 desde cualquier lugar no es la solución.

Problemas de inicio de sesión después de que el nodo esté activo

- La interfaz de usuario web redirige a un cambio de contraseña. Se debe introducir la contraseña actual y la nueva contraseña debe ser diferente. Esto se espera en el primer inicio de sesión de la GUI después de una instalación o restablecimiento de fábrica, y cuando una contraseña local ha caducado.
- SSH indica que el teclado interactivo/PAM ha fallado y nunca abre un shell. Se debe cambiar una contraseña local caducada. No se concede la sesión anterior.
- REST devuelve 401. Se espera que un administrador local caducado. El registro de eventos puede mostrar Password Mismatch o taa-chkpasswd failure para el rango de la API. Cambie la contraseña y vuelva a intentarlo.
- Nueva contraseña rechazada. Se encuentra en el historial (el último valor predeterminado es 12) o no ha cumplido las reglas de complejidad actuales.
- El administrador de LDAP perdió el rol esperado. Compare el grupo configurado con el nombre de grupo exacto devuelto por LDAP. Una coincidencia parcial o de subcadena ya no concede el rol. Un administrador de solo lectura no puede editar la confianza de IdP de SAML.
- No hay ninguna contraseña raíz predeterminada de fábrica en una instalación nueva o en un restablecimiento de fábrica. No buscar ni distribuir una credencial predeterminada. Una

actualización no borra la contraseña de administrador actual.



Precaución: El restablecimiento de fábrica no es el paso de actualización-recuperación. Elimina la identidad del clúster y las cookies del clúster. Un restablecimiento desencadenado por el sistema después de la desagrupación en clúster o una base de datos de clúster incoherente mantiene la dirección IP y las contraseñas de administrador y raíz, borra otras configuraciones y registros y devuelve el nodo a su certificado temporal. Utilícelo sólo cuando las notas de la versión lo soliciten y sólo después de que exista una copia de seguridad.

Evidencia a recolectar en caso de que el caso TAC sea necesario

1. Versión de software y función de cada nodo, además de qué nodo se detuvo.
2. Instantánea completa del sistema desde el nodo con error, incluido tmp/install-error.
3. Texto de certificado de servidor (openssl x509 -text -noout). No hay clave privada.
4. Estado del clúster, alarmas y si xConfiguration Cluster TlsVerify muestra Permissive o Enforce.
5. Líneas de registro de eventos para la actualización y, si procede, fallos de autenticación sshd o httpd. Rechazar contraseñas y cookies.
6. Si utiliza administradores locales, LDAP o SAML, licencias inteligentes y cualquier automatización de API.

Después de la actualización

En cada nodo

1. La versión es la compilación X15.5.20 prevista.
2. Se puede acceder al nodo en su dirección de administración y se carga la interfaz de usuario web.
3. No se genera ninguna alarma de hardware, disco o aplicación nueva. (Una alarma de comunicación de clúster se borra después del nuevo cifrado.)
4. Se realiza una copia de seguridad nueva después de que el clúster esté estable.

Sólo clúster

1. Todos los pares están activos, en el clúster, y la replicación es saludable.
2. Los pares se comunican con TLS mutuo en TCP 4371 y 4372. (Una conexión sin un certificado de cliente válido debe fallar.)
3. El clúster TlsVerify es obligatorio.

No se admite el permiso. Un valor permisivo heredado podría seguir siendo visible, pero no omite la validación. Establezca Forzando y confirme que el clúster se mantiene en buen estado.

4. El firewall todavía permite TCP 4371 solo desde las direcciones pares.

5. No aparece ninguna cookie de cluster o secreto de diagnóstico en los logs o las notas de instantánea que carga.

Comprobaciones de servicio, según el uso del

Si utiliza	Qué buena pinta tiene	Si falla
Administradores locales	GUI, SSH y API aceptan la contraseña actual. Las cuentas que han vencido se envían a un HTTP 401 para cambiar o recibir una contraseña.	Confirme que el vencimiento es a las 00:00 UTC y que la nueva contraseña está fuera de la ventana del historial.
Administradores LDAP	Un administrador inicia sesión solamente cuando el nombre del grupo LDAP coincide exactamente con el grupo configurado.	Compare el grupo de directorios con el grupo de Expressway. No amplíe la coincidencia para forzar un inicio de sesión.
Llamadas SIP o B2B	Una llamada de prueba se conecta en ambas direcciones.	Recopilar el historial de llamadas y una instantánea.
Registro H.323 autenticado	El terminal se registra con cada alias que utiliza, incluidos un ID H.323 y un número E.164.	Agregue un mapa de alias de credenciales para cada alias. Las notas de la versión utilizan <code>xConfiguration Registration CredentialAliasMap</code> con el tipo de patrón Exact. Al desactivar <code>CredentialAliasBinding</code> en la subzona también se restaura el registro y se debilita la condición de seguridad. H.323 no se elimina.
MRA o registro de dispositivo	Un terminal conocido registra y realiza una llamada. Las SAN de certificados de cliente de UC son nombres DNS o direcciones IP específicos, no valores demasiado amplios o mal formados.	Compare certificados, credenciales transversales y DNS con la copia de seguridad previa a la actualización. Vuelva a emitir un certificado cuya SAN sea demasiado amplia.
Alertas de correo electrónico	Un mensaje de prueba sale del nodo mediante STARTTLS.	Si STARTTLS no se puede completar, la entrega no se cerrará. Corrija la confianza del servidor de correo o TLS. No se espera una reserva de texto sin formato.
Licencias inteligentes	El registro y la autorización coinciden con la interfaz de usuario web. La imagen estándar permanece dentro de 2500 sesiones de señalización cifradas , o el nodo es Expressway Select.	Verifique el transporte y el CSSM. La casilla de verificación CSSM "permitir funcionalidad controlada por exportación" no se aplica a Expressway. Si se revoca el token y se elimina la instancia del producto, el nodo se establece en Anulado del registro. Las teclas de opción no son una solución alternativa.

Si utiliza	Qué buena pinta tiene	Si falla
Scripts de configuración o REST	Los nombres de cuenta coinciden con los nuevos límites de longitud y caracteres. Las escrituras de configuración incluyen la protección CSRF que utiliza la GUI.	Actualice el cliente con el esquema de la API de envío. Se espera que falle una llamada eliminada de /provisioning/optionkey.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).