

Lista de verificação de atualização para Expressway 15.5.20

Contents

[Introdução](#)

[Componentes Utilizados](#)

[Antes da atualização](#)

[Como ler o certificado](#)

[O que fazer antes da Janela de Manutenção](#)

[Se a atualização falhar](#)

[A verificação de preparação interrompeu a atualização](#)

[Alarme após a ativação de um nó](#)

[O administrador não pode entrar](#)

[Falha de certificado ou identidade de mesmo nível](#)

[Alarme de cluster durante ou logo após a atualização](#)

[Problemas de entrada depois que o nó está ativo](#)

[Elementos de prova a recolher em caso de necessidade de TAC](#)

[Após a atualização](#)

[Em cada nó](#)

[Somente cluster](#)

[Verificações de serviço, pelo que o está em uso](#)

Introdução

Este documento descreve como preparar o Expressway para a atualização de proteção de segurança X15.5.20. Ela lista cada pré-requisito e mostra como corrigi-lo.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes da atualização



Caution: Não inicie uma atualização de cluster até que cada peer passe nas verificações de preparação. Defina a verificação TLS como Impondo e confirme se o cluster está íntegro. Use um formato de identidade de peer, não uma combinação de endereços IP e

FQDNs. Cada certificado de servidor deve conter o FQDN do nó na SAN ou no CN somente quando a SAN estiver vazia. Uma SAN vazia poderá ocorrer se o OpenSSL tiver sido usado para criar o CSR. Se uma verificação falhar, a atualização será interrompida sem alterar a configuração do cluster existente.

Verificar	Autônomo	Cluster	Se não for verdade
O caminho de atualização corresponde ao Apêndice 3	Necessário	Necessário	Antes de X8.11.4, pare em X8.11.4 primeiro. Converta o licenciamento PAK X12 para o Smart Licensing antes de X15.x .
Backup atual e um plano de reversão testado	Necessário	Necessário em cada nó	Pegue o backup antes da janela. Uma redefinição de fábrica posterior limpa a configuração.
Cluster íntegro, sem alarmes inexplicáveis, replicação em sincronia	Não aplicável	Necessário	Corrija o cluster antes da atualização. Uma atualização contínua ainda usa o comportamento normal de divisão de cluster.
A verificação TLS está sendo aplicada e o cluster está íntegro	Não aplicável	Necessário antes da atualização	Alterar Permissivo para Imposição, corrigir o certificado e confirmar a replicação. Não o descubra durante a janela.
Cada peer usa o mesmo formato de identidade e a lista de peer não está vazia	A verificação de identidade de mesmo nível é aprovada	Necessário. IP e FQDN mistos são bloqueados antes da reinicialização	Padronize todos os FQDNs ou todos os endereços IP, deixe a alteração ser replicada e confirme se o cluster está íntegro. Não altere o formato durante uma atualização sem interrupção.
O certificado do servidor contém o FQDN do sistema na SAN ou no CN somente quando a SAN está vazia	Necessário se a atualização verificar o certificado	Necessário. A atualização pára e deixa a configuração do cluster inalterada	Emita novamente o certificado. Se houver uma SAN, não dependa da CN. Rejeitar nomes que contenham um NUL incorporado.
Certificado em data, confiável por pares, RSA 2048+ ou P-256+, assinatura SHA-2	Recomendado	Necessário	Já não há suporte para assinaturas SHA-1 de X15.2 . Emita novamente o certificado. Um certificado autoassinado é aceitável somente quando cada par está explicitamente configurado para confiar nele.
TCP 4371 permitido somente de pares	Recomendado	Necessário	Restringir o firewall. Isso é defesa aprofundada para

Verificar	Autônomo	Cluster	Se não for verdade
conhecidos			ClusterDB; não é um substituto para a atualização.
Clientes API de administração revisados	Necessário se as APIs forem usadas	Necessário se as APIs forem usadas	Esperam validação de nome e senha mais rigorosa, verificações de CSRF em gravações de FormPutXML e nenhuma API de chave de opção.
A janela de manutenção cobre uma atualização contínua mais um possível alarme de cluster curto	Janela normal	Necessário	A recriptografia de cookies pode acionar um alarme de comunicação de cluster. Espere-se que ele se limpe sozinho.

Como ler o certificado

Exporte e inspecione o certificado do servidor.

- FQDN na SAN. As [notas de versão](#) exigem o FQDN do sistema em uma SAN. O CN é verificado somente quando a extensão SAN está vazia.
- Sem fallback de CN. Se uma SAN estiver presente e não corresponder, a [verificação falhará mesmo quando o CN estiver correto](#). Coloque cada nome DNS ou endereço IP necessário no tipo de SAN correto.
- caracteres NUL. Um nome de certificado que contém um NUL inserido é rejeitado.
- Datas. `notBefore` deve estar no passado e `notAfter` deve estar no futuro.
- Chave. RSA com pelo menos 2048 bits ou uma chave EC em P-256 ou mais forte.
- Assinatura. Família SHA-2. De X15.2, [sha1WithRSAEncryption](#) e [ecdsa-with-SHA1](#) não são suportados.
- Emissor. Se Assunto e Emissor forem iguais, ele será autoassinado. Os pares já devem confiar nele.

O que fazer antes da Janela de Manutenção

- Antes da janela, defina a verificação TLS de cluster como [Enforcement](#), reinicie o cluster (começando do editor primeiro) e confirme se o cluster está íntegro. Não há suporte para o modo de permissão. Um valor Permissivo herdado pode permanecer visível, mas não ignora a confiança de certificado ClusterDB ou a validação de identidade de mesmo nível.
- Todas as identidades de mesmo nível devem ser FQDNs ou ser endereços IP. Não altere esse formato enquanto uma atualização contínua estiver em andamento.
- Um ponto de extremidade H.323 autenticado com mais de um alias pode precisar de um [mapa de alias de credencial](#) para cada alias ou a associação de alias de credencial desativada na subzona. Desativar a ligação enfraquece a postura de segurança.

- A expiração da senha do administrador local permanece desativada quando PasswordExpiryDays é 0. Quando ativada, a expiração é calculada às 00:00 UTC, não à meia-noite local.
- [A profundidade do histórico de senhas é padronizada como 12](#). O intervalo de treinamento é de 3 a 24. Senhas de administrador vazias são rejeitadas e uma senha usada recentemente pode ser rejeitada.
- [O mapeamento de função de administrador LDAP](#) requer uma correspondência exata de nome de grupo. Um nome de grupo que contém apenas o nome configurado não concede mais a função.
- Uma nova instalação, redefinição de fábrica ou implantação autônoma não pode reutilizar uma [senha raiz padrão de fábrica](#). Uma atualização não apaga a senha atual do administrador.
- Um administrador somente leitura não pode mais alterar a confiança do IdP SAML.
- Um e-mail que não pode concluir STARTTLS não é enviado em branco.
- [O Smart Licensing](#) é o único modo de licenciamento. As chaves de opção PAK foram removidas no X14.2. A imagem padrão do Expressway permite [2.500 sessões de sinalização criptografadas](#); Expressway Select é a imagem sem limites.

Se a atualização falhar

Deixe o cluster como está. Uma verificação de preparação com falha não altera a configuração de cluster existente. Não redefina de fábrica um nó para passar pela falha.

A verificação de preparação interrompeu a atualização

O instalador pára antes da reinicialização quando o certificado, a verificação TLS ou o requisito de identidade de mesmo nível falha. Os nós autônomos passam na verificação de identidade de mesmo nível.

Alarme após a ativação de um nó

Uma rajada de recryptografia de banco de dados de cluster pode acionar um alarme de falha de comunicação de cluster. Dê tempo para terminar. Escale se ele continuar ativo.

O administrador não pode entrar

Trate isso separadamente de uma falha de instalação. As senhas expiradas, reutilizadas ou do primeiro login bloqueiam a sessão. Elas não significam que a imagem falhou.

Falha de certificado ou identidade de mesmo nível

1. Baixe um instantâneo de sistema completo do nó que parou. Abra install-error no diretório tmp desse snapshot.
2. Se a mensagem for sobre identidade de peer, verifique se há uma combinação de

endereços IP e FQDNs ou uma lista de peer vazia. Faça com que cada peer use um formato, aguarde a replicação, confirme se o cluster está íntegro e tente novamente. Não altere o formato da identidade no meio de uma atualização contínua.

3. Se a mensagem for sobre o certificado, compare-a com a regra da nota de versão: o FQDN do sistema deve estar na SAN ou na CN somente quando a SAN estiver vazia. Não é permitido que uma SAN atual recue para o CN.
4. Emita novamente o certificado com cada nome DNS ou endereço IP necessário no tipo de SAN correto. Rejeita um nome que contenha um NUL inserido.
5. Confirme se o novo certificado está em data, confiável, RSA 2048+ ou P-256+ e assinado com SHA-2. Não anexe a chave privada ao caso.
6. Defina a verificação TLS como Impondo, confirme se o cluster está íntegro e repita a atualização no nó que parou.
7. Continue a atualização de rolagem somente depois que o nó estiver íntegro. Não atualize os nós restantes enquanto um nó estiver parado nesta verificação.

Alarme de cluster durante ou logo após a atualização

1. Confirme se o próprio upgrade foi concluído e se o nó está em X15.5.20.
2. Procure no log de eventos as mensagens developer.upgrade sobre a nova criptografia dos campos ClusterDB e, em seguida, "Saving migrated data to CDB" (Salvando dados migrados para CDB).
3. Aguarde até que o alarme seja cancelado. O material de treinamento diz que ele limpa quando a re-criptografia termina.
4. Se ele permanecer, colete o status do cluster, os alarmes e um snapshot de cada peer. Não copie cookies de cluster ou material chave nas notas do caso.
5. Confirme se o TCP 4371 e o 4372 estão abertos apenas entre os correspondentes e se o TLS mútuo é bem-sucedido. Um firewall que permite o 4371 de qualquer lugar não é a solução.

Problemas de entrada depois que o nó está ativo

- A interface do usuário da Web é redirecionada para uma alteração de senha. A senha atual deve ser inserida e a nova senha deve ser diferente. Isso é esperado no primeiro login da GUI após uma instalação ou redefinição de fábrica e quando uma senha local expira.
- O SSH diz que o teclado interativo / o PAM falhou e nunca abre um shell. Uma senha local expirada precisa ser alterada. A sessão antiga não foi concedida.
- REST retorna 401. Esperado para um administrador local expirado. O log de eventos pode mostrar Incompatibilidade de Senha OU falha de taa-chkpasswd para o território da API. Altere a senha e tente novamente.
- Nova senha rejeitada. Ele está no histórico (o padrão são os últimos 12) ou falhou nas regras de complexidade atuais.
- O administrador LDAP perdeu a função esperada. Compare o grupo configurado com o nome exato do grupo retornado pelo LDAP. Uma correspondência parcial ou de substring não concede mais a função. Um administrador somente leitura não pode editar a confiança do IdP SAML.
- Não há senha raiz padrão de fábrica em uma nova instalação ou redefinição de fábrica. Não

pesquisar ou distribuir uma credencial padrão. Uma atualização não limpa a senha atual do administrador.



Caution: A redefinição de fábrica não é a etapa de atualização-recuperação. Exclui a identidade do cluster e os cookies do cluster. Uma redefinição acionada pelo sistema após a remoção de cluster ou um banco de dados de cluster inconsistente mantém o endereço IP e as senhas de administrador e raiz, limpa outras configurações e logs e retorna o nó ao seu certificado temporário. Use-o somente quando as notas de versão chamarem e somente após um backup existir.

Elementos de prova a recolher em caso de necessidade de TAC

1. Versão do software e função de cada nó, mais qual nó parou.
2. Instantâneo completo do sistema do nó com falha, incluindo tmp/install-error.
3. Texto do certificado do servidor (openssl x509 -text -noout). Nenhuma chave privada.
4. Status do cluster, alarmes e se TlsVerify de cluster do xConfiguration mostra Permissive ou Enforce.
5. Linhas do log de eventos para a atualização e, se relevante, falhas de autenticação de sshd ou httpd. Redija senhas e cookies.
6. Seja usando administradores locais, LDAP ou SAML, Smart Licensing e qualquer automação de API.

Após a atualização

Em cada nó

1. A versão é a versão pretendida do X15.5.20.
2. O nó está acessível em seu endereço de gerenciamento e a interface do usuário da Web é carregada.
3. Nenhum alarme novo de hardware, disco ou aplicativo é deixado ativado. (Um alarme de comunicação de cluster é cancelado após a recriptografia.)
4. Um novo backup é feito depois que o cluster fica estável.

Somente cluster

1. Cada peer está ativo, no cluster, e a replicação está íntegra.
2. Os pares se comunicam com TLS mútuo no TCP 4371 e 4372. (Uma conexão sem um certificado de cliente válido deve falhar.)
3. O TlsVerify de Cluster está Impondo.

Não há suporte para permissão. Um valor Permissivo herdado ainda pode estar visível, mas não ignora a validação. Defina Como impor e confirme se o cluster permanece íntegro.

4. O firewall ainda permite o TCP 4371 somente a partir de endereços de mesmo nível.

5. Nenhum cookie de cluster ou segredo de diagnóstico é exibido nos logs ou nas observações de snapshot que você faz upload.

Verificações de serviço, pelo que o está em uso

Se estiver usando	O que parece bom	Se falhar
Administradores locais	GUI, SSH e API aceitam a senha atual. As contas expiradas são enviadas para uma alteração de senha ou recebem HTTP 401.	Confirme se a expiração ocorre às 00:00 UTC e se a nova senha está fora da janela de histórico.
Administradores LDAP	Um administrador se conecta somente quando o nome do grupo LDAP corresponde exatamente ao grupo configurado.	Compare o grupo de diretórios com o grupo Expressway. Não amplie a correspondência para forçar um login.
Chamadas SIP ou B2B	Uma chamada de teste se conecta em ambas as direções.	Colete o histórico de chamadas e um instantâneo.
Registro H.323 autenticado	O ponto final registra com todos os alias que usa, incluindo um ID H.323 e um número E.164.	Adicione um mapa de alias de credencial para cada alias. As notas de versão usam xConfiguration Registration CredentialAliasMap com o tipo de padrão Exact. Desativar CredentialAliasBinding na subzona também restaura o registro e enfraquece a postura de segurança. O próprio H.323 não é removido.
MRA ou registro de dispositivo	Um endpoint conhecido se registra e faz uma chamada. As SANs de certificado de cliente UC são nomes DNS ou endereços IP específicos, não valores muito amplos ou malformados.	Comparar certificados, credenciais transversais e DNS com o backup de pré-atualização. Emita novamente um certificado cuja SAN seja muito ampla.
Alertas por e-mail	Uma mensagem de teste sai do nó usando STARTTLS.	Se STARTTLS não puder ser concluído, a entrega falhará ao fechar. Corrija a confiança do servidor de email ou TLS. Não espere fallback de texto claro.
Smart Licensing	O registro e a autorização correspondem à interface do usuário da Web. A imagem padrão permanece em 2500 sessões de sinalização criptografadas ou o nó é Expressway Select.	Verifique o transporte e o CSSM. A caixa de seleção "permitir funcionalidade de exportação controlada" do CSSM não se aplica ao Expressway. Revogar o token e excluir a instância do produto define o nó como Com registro cancelado. As teclas de opção não são uma solução.

Se estiver usando	O que parece bom	Se falhar
Scripts REST ou de configuração	Os nomes de conta correspondem aos novos limites de comprimento e caracteres. As gravações de configuração incluem a proteção CSRF que a GUI usa.	Atualizar o cliente com base no esquema da API de remessa. Espera-se que uma chamada removida <code>/provisioning/optionkey</code> falhe.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.