Expressway 15.5.20及更高版本的升级核对表

目录

简介

使用的组件

升级前

- 如何读取证书
- 在维护时段之前要执行的操作

如果升级失败

- 就绪性检查已停止升级
- 节点启动后发出警报
- 管理员无法登录
- 证书或对等身份失败
- 在升级期间或升级后立即发出集群警报
- 节点启动后的登录问题
- 需要TAC案例时应收集的证据

升级后

- 在每个节点上
- 仅集群
- 服务检查，按正在使用的内容

简介

本文档介绍如何准备Expressway以升级到X15.5.20或X15.5.21。本文档列出了每个前提条件以及如何更正它。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。



注意：X15.5.21可供下载。它包含2026年10月PHP漏洞的修补程序，也称为PHP2shell(CVE-2026-109618和CVE-2026-109619,Cisco bug ID CSCwx37062。X15.5.20是安全加固版本，不包含此PHP修补程序。使用本文档中的就绪性检查以升级到X15.5.20或X15.5.21。这两个版本的检查相同。从Cisco.com下载X15.5.21。Expressway系列或Expressway Select用于未封顶的映像，然后是Expressway核心和边缘，版本X15.5.21。安全建议仍可以列出15.5.21以待确定。该图像已发布在上面的软件下载页面上。

升级前

⚠ 警告：在每个对等体通过就绪检查之前，请勿启动集群升级。将TLS验证设置为Enforcing，并确认集群运行正常。使用一个对等身份格式，而不是IP地址和FQDN的组合。每个服务器证书必须在SAN中或仅当SAN为空时在CN中包含该节点的FQDN。如果使用OpenSSL创建CSR，则可能会出现空的SAN。如果检查失败，升级将停止，而不会更改现有集群配置。

检查	独立	集群	如果这不是真的
升级路径匹配附录3	必需	必需	在X8.11.4之前，首先在X8.11.4处停止。将X12 PAK许可转换为X15.x之前的智能许可。
当前备份和经过测试的回滚计划	必需	在每个节点上必需	在窗口之前进行备份。以后出厂重置将清除配置。
集群正常，无未解释的警报，同步复制	不适用	必需	在升级之前修复集群。滚动升级仍使用正常的拆分群集行为。
TLS验证正在实施，并且集群运行正常	不适用	升级前必需	将Permissive更改为Enforcing，修复证书并确认复制。请勿在窗口期间发现此问题。
每个对等体使用相同的身份格式，并且对等体列表不为空	对等身份检查通过	必填。在重新启动之前阻止混合IP和FQDN	对所有FQDN进行标准化，复制更改并确认集群运行正常。请参阅更改集群以使用FQDN。在滚动升级过程中请勿更改格式。
服务器证书在SAN中或CN中仅当SAN为空时才包含系统FQDN	如果升级检查证书，则为必需	必填。升级停止，集群配置保持不变	重新颁发证书。如果SAN存在，则不依赖CN。拒绝包含嵌入式NUL的名称。
证书已过期，受对等体、RSA 2048+或P-256+、SHA-2签名信任	推荐	必需	X15.2已不支持SHA-1签名。重新颁发证书。只有当每个对等体都明确配置为信任自签名证书时，该证书才可被接受。
仅允许来自已知对等体的TCP 4371	推荐	必需	限制防火墙。这是ClusterDB的深度防御；它不能代替升级。
已审核管理API客户端	如果使用API，则为必需	如果使用API，则为必需	需要更严格的名称和密码验证、对FormPutXML写入进行CSRF检查，且无选项密钥API。
维护窗口涵盖滚动升级和可能的短集群警报	普通窗口	必需	Cookie重新加密可能会引发集群通信警报。预计它将自行清除。

如何读取证书

导出服务器证书并对其进行检查。

- SAN中的FQDN。版本说明要求在SAN中使用系统FQDN。仅当SAN扩展为空时才检查CN。

- 无CN回退。如果SAN存在且不匹配，即使CN正确，验证也会失败。将每个所需的DNS名称放在正确的SAN类型中。
- NUL字符。包含嵌入式NUL的证书名称被拒绝。
- 日期。`notBefore`必须位于过去，`notAfter`必须位于未来。
- 密钥.RSA至少2048位，或P-256或更强的EC密钥。
- 签名。SHA-2家族。从X15.2中，`sha1WithRSAEncryption`和`ecdsa-with-SHA1`不受支持。
- 颁发者。如果主题和颁发者相同，则它是自签名的。对等体必须已信任它。

在维护时段之前要执行的操作

- 在窗口出现之前，将集群TLS验证设置为Enforcing，重新启动集群（首先从发布服务器启动）并确认集群运行正常。不支持许可模式。传统Permissive值可以保持可见，但它不会绕过ClusterDB证书信任或对等体身份验证。
- 对等体标识必须全部为FQDN。在滚动升级过程中，请勿更改该格式。
- 具有多个别名的已验证H.323终端可能需要每个别名的凭据别名映射，或者在子区域上关闭凭据别名绑定。关闭绑定会削弱安全状态。
- 当`PasswordExpiryDays`为0时，本地管理员密码到期保持关闭。启用后，到期时间在00:00 UTC计算，而不是本地午夜。
- 密码历史记录深度默认为12。培训范围为3至24。会拒绝空管理员密码，而且可以拒绝最近使用的密码。
- LDAP管理员角色映射需要精确的组名匹配。仅包含已配置名称的组名称不再授予该角色。
- 新的安装、出厂重置或无人值守部署无法重用出厂默认根密码。升级不会清除当前的管理员密码。
- 只读管理员无法再更改SAML IdP信任。
- 无法完成STARTTLS的电子邮件不会以明文形式发送。
- 智能许可是唯一许可模式。X14.2删除了PAK选项密钥。标准Expressway映像允许2500个加密信令会话;Expressway选择是未封顶的映像。

如果升级失败

保留集群原样。失败的就绪性检查不会更改现有群集配置。请勿通过出厂重置节点来克服故障。

就绪性检查已停止升级

当证书、TLS验证或对等身份要求失败时，安装程序在重新启动之前停止。独立节点通过对等身份检查。

节点启动后发出警报

群集数据库重新加密的突发，可能会引发群集通信故障警报。给它一点时间完成。保持正常运行状态则进行升级。

管理员无法登录

请将此问题与安装故障分开处理。过期、重用或首次登录密码会阻止会话。它们并不意味着映像失败。

证书或对等身份失败

1. 从停止的节点下载完整的系统快照。在该快照的tmp目录中打开installmage.log。
2. 如果消息是关于对等体身份，请检查IP地址和FQDN的组合或空对等体列表。使每个对等体都使用一种格式，等待复制，确认集群运行正常，然后重试。请勿在滚动升级过程中更改身份格式。
3. 如果消息与证书有关，请将其与版本说明规则进行比较：系统FQDN必须位于SAN中，或仅在SAN为空时才位于CN中。当前SAN不允许回退到CN。
4. 以正确的SAN类型重新颁发包含每个所需DNS名称的证书。拒绝包含嵌入式NUL的名称。
5. 确认新证书已过期、受信任、RSA 2048+或P-256+并使用SHA-2签名。不要将私钥附加到案例。
6. 将TLS验证设置为“实施”，确认集群运行正常，然后在停止的节点上重试升级。
7. 只有在节点运行状况正常之后才继续滚动升级。当一个节点在此检查中暂停时，请勿升级剩余节点。

在升级期间或升级后立即发出集群警报

1. 确认升级本身已完成，并且节点位于目标版本X15.5.20或X15.5.21上。
2. 在事件日志中查找有关重新加密ClusterDB字段的developer.upgrade消息，然后查找“Saving migrated data to CDB”。
3. 等待警报清除。培训材料说重新加密完成后，该功能会清除。
4. 如果保留该属性，请从每个对等体收集集群状态、警报和快照。请勿将群集cookie或关键材料复制到案例说明中。

节点启动后的登录问题

- Web UI重定向到密码更改。必须输入当前密码，新密码必须不同。在安装或出厂重置后第一次GUI登录时，以及本地密码到期时，将会出现这种情况。
- SSH显示键盘交互/PAM失败，并且从未打开外壳。必须更改过期的本地密码。未授予旧会话。
- REST返回401。对于已过期的本地管理员，此值应为预期值。事件日志可以显示API领域的`密码不匹配`或`taa-chkpasswd`失败。请更改密码，然后重试。
- 新密码被拒绝。它位于历史记录中（默认为最后12个），或者它未通过当前的复杂性规则。
- LDAP管理员丢失了预期角色。将已配置的组与LDAP返回的确切组名称进行比较。部分或子字符串匹配不再授予该角色。只读管理员无法编辑SAML IdP信任。
- 新安装或出厂重置时没有出厂默认根密码。请勿搜索或分发默认凭据。升级不会清除当前的管理员密码。

⚠ 警告：出厂重置不是升级 — 恢复步骤。删除群集标识和群集cookie。取消集群后系统触发

的重置或不一致的集群数据库会保留IP地址以及管理员和根密码，清除其他配置和日志，并将节点返回到其临时证书。仅当发行说明需要它时才使用它，并且仅在存在备份之后才使用。

需要TAC案例时应收集的证据

1. 每个节点的软件版本和角色，以及哪个节点已停止。
2. 故障节点的完整系统快照，包括tmp/installimage.log。
3. 服务器证书文本(openssl x509 -text -noout)。 没有私钥。
4. 集群状态、警报以及xConfiguration集群TlsVerify显示许可还是实施。
5. 升级以及sshd或httpd身份验证失败的相关事件日志行。密写密码和cookie。
6. 无论是使用本地、LDAP还是SAML管理员、智能许可和任何API自动化。

升级后

在每个节点上

1. 版本是预期内部版本。当升级针对2026年10月的PHP漏洞时，请使用X15.5.21。X15.5.20不包括此修复。
2. 节点在其管理地址和Web UI加载上可访问。
3. 未引发任何新的硬件、磁盘或应用警报。（重新加密后，集群通信警报会清除。）
4. 在群集稳定后执行新的备份。

仅集群

1. 集群中的每个对等体都处于运行状态，并且复制正常。
2. 对等体在TCP 4371和4372上使用双向TLS进行通信。（没有有效客户端证书的连接必须失败。）
3. 集群TlsVerify正在实施。

不支持允许。旧版允许值仍然可见，但它不会绕过验证。设置Enforcing并确认集群保持正常。

4.防火墙仍然仅允许来自对等体地址的TCP 4371。

5.日志或上传的快照注释中不会显示群集cookie或诊断密钥。

服务检查，按正在使用的内容

如果使用	什么好看的	如果失败
本地管理员	GUI、SSH和API接受当前密码。过期的帐户会被推送到密码更改或接收HTTP 401。	确认到期时间是00:00 UTC，并且新密码不在历史记录窗口内。
LDAP管理员	管理员仅在LDAP组名称与配置的组完全匹配时登录。	将目录组与Expressway组进行比较。不要扩大匹配项以强制登录。
SIP或B2B呼叫	测试呼叫双向连接。	收集呼叫历史记录和快照。

如果使用	什么好看的	如果失败
已验证的H.323注册	终端注册其使用的每个别名，包括H.323 ID和E.164号码。	为每个别名添加凭证别名映射。发行说明将xConfiguration Registration CredentialAliasMap与模式类型Exact配合使用。在子区域上关闭CredentialAliasBinding也会恢复注册，从而削弱安全状态。不会删除H.323本身。
MRA或设备注册	已知终端注册并发出呼叫。UC客户端证书SAN是特定的DNS名称，不是过于宽泛或格式不正确的值。	将证书、遍历凭证和DNS与升级前备份进行比较。重新颁发SAN过宽的证书。
电子邮件警报	测试消息使用STARTTLS离开节点。	如果STARTTLS无法完成，则无法关闭传送。修复邮件服务器信任或TLS。不要期望明文回退。
智能许可	注册和授权与Web UI匹配。标准映像保持在2500个加密的信令会话内，或者节点是Expressway Select。	检查传输和CSSM。CSSM“允许导出控制功能”复选框不适用于Expressway。撤销令牌并删除产品实例会将节点设置为Deregistered。选项键不是解决方法。
REST或配置脚本	帐户名称匹配新的长度和字符限制。配置写入包括GUI使用的CSRF保护。	根据发货API方案更新客户端。已删除/调配/选项密钥调用预期失败。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。