

Expressway 15.5.20升級清單

目錄

[簡介](#)

[採用元件](#)

[升級前](#)

[如何讀取憑證](#)

[在維護時段之前要執行的操作](#)

[如果升級失敗](#)

[就緒性檢查已停止升級](#)

[節點啟動後發出警報](#)

[管理員無法登入](#)

[證書或對等身份失敗](#)

[升級期間或升級後不久發生的群集警報](#)

[節點啟動後的登入問題](#)

[在需要TAC案例的情況下收集的證據](#)

[升級後](#)

[在每個節點上](#)

[僅集群](#)

[服務檢查，按正在使用什麼](#)

簡介

本文檔介紹如何為X15.5.20安全加固升級準備Expressway。列出了每個先決條件以及如何對其進行更正。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

升級前



注意：在每個對等體通過就緒檢查之前，不要啟動群集升級。將TLS驗證設定為「強制實施」並確認群集運行正常。使用一個對等身份格式，而不是IP地址和FQDN的組合。每個伺服器證書必須在SAN中或僅當SAN為空時在CN中包含該節點的FQDN。如果使用OpenSSL來建立CSR，可能會發生空的SAN。如果檢查失敗，升級將停止，而不會更改現有群集配置。

支票	獨立	叢集	如果這不是真的
升級路徑與 附錄3	必需	必需	在X8.11.4之前，首先在X8.11.4停止。將X12 PAK許可轉換為 X15.x之前的智慧許可 。
當前備份和經測試的回滾計畫	必需	每個節點上均需要	在視窗之前進行備份。稍後的出廠重置將清除配置。
群集正常，沒有無法解釋的警報，同步複製	不適用	必需	升級前先修復群集。滾動升級仍使用正常的拆分群集行為。
正在實施TLS驗證 ，並且群集運行正常	不適用	升級前必需	將Permissive更改為Enforcing、修復證書並確認複製。在視窗期間不要發現此問題。
每個對等體使用相同的身份格式，並且對等體清單不為空	對等身份檢查通過	必填。IP和FQDN混合在重新啟動前被阻止	對所有FQDN或所有IP地址進行標準化，讓更改進行複製，並確認群集運行正常。在滾動升級過程中請勿更改格式。
伺服器證書在SAN中或僅當SAN為空時在CN中包含系統FQDN	如果升級檢查證書，則為必需	必填。升級停止，並且保持群集配置不變	重新核發憑證。如果SAN存在，則不依賴CN。拒絕包含嵌入式NUL的名稱。
證書已過期，受對等體、RSA 2048+或P-256+、SHA-2簽名信任	建議	必需	X15.2已不支援SHA-1簽名 。請重新頒發證書。自簽名證書只有在每個對等體都明確配置為信任它時才可接受。
TCP 4371只允許來自已知對等體	建議	必需	限制防火牆。這是ClusterDB的深度防禦；它不能代替升級。
已稽核管理API客戶端	使用API時必需	使用API時必需	需要更嚴格的名稱和密碼驗證、對FormPutXML寫入進行CSRF檢查，並且沒有選項金鑰API。
維護視窗包含滾動升級和可能的短群集警報	正常視窗	必需	Cookie重新加密可能會引發集群通訊警報。預計它將自行清算。

如何讀取憑證

匯出伺服器證書並對其進行檢查。

- SAN中的FQDN。[發行說明](#)要求在SAN中使用系統FQDN。僅當SAN擴展為空時才檢查CN。
- 無CN後援。如果SAN存在且不匹配，則即使[CN正確也驗證失敗](#)。將每個所需的DNS名稱或IP地址放在正確的SAN型別中。
- NUL字元。包含嵌入式NUL的證書名稱被拒絕。
- 日期。notBefore必須位於過去，而非After必須位於未來。
- 主要RSA至少為2048位，或P-256或更強的EC金鑰。
- 簽名。SHA-2家族。在X15.2中，[不支援sha1WithRSAEncryption](#)和[ecdsa-with-SHA1](#)。
- 發行商。如果Subject和Issuer相同，則它是自簽名的。對等體必須已信任它。

在維護時段之前要執行的操作

- 在視窗出現之前，將群集TLS驗證設定為[Enforcing](#)，重新啟動群集（首先從發佈伺服器啟動）並確認群集運行正常。不支援許可模式。舊版Permissive值可以保持可見，但它不會繞過ClusterDB證書信任或對等體身份驗證。
- 對等體標識必須全部為FQDN或全部為IP地址。進行滾動升級時，請勿更改該格式。
- 具有多個別名的經過身份驗證的H.323端點可能需要每個別名的[憑據別名對映](#)，或者子區域上關閉了憑據別名繫結。關閉繫結會削弱安全狀態。
- PasswordExpiryDays為0時，本地管理員密碼到期將關閉。啟用後，到期時間在00:00 UTC計算，而不是本地午夜。
- [密碼歷史記錄深度](#)默認為12。培訓範圍為3到24。系統會拒絕空管理員密碼，最近使用的密碼可能會被拒絕。
- [LDAP管理員角色](#)映射需要精確的組名匹配。僅包含已配置名稱的組名稱不再授予該角色。
- 新的安裝、出廠重置或無人值守部署無法重複使用[出廠預設根密碼](#)。升級不會消除當前的管理員密碼。
- 只讀管理員無法再更改SAML IdP信任。
- 無法完成STARTTLS的電子郵件不會以明文形式傳送。
- [智慧許可](#)是唯一許可模式。X14.2刪除了PAK選項金鑰。標準Expressway映像允許2500個加[密信令會話](#);Expressway Select是未封頂的影像。

如果升級失敗

保留群集不變。失敗的就緒性檢查不會更改現有的群集配置。請勿通過出廠重置節點來克服故障。

就緒性檢查已停止升級

當證書、TLS驗證或對等身份要求失敗時，安裝程式會在重新啟動之前停止。獨立節點通過對等身份檢查。

節點啟動後發出警報

集群資料庫重加密的突發，可能會引發集群通訊故障警報。讓它有時間完成。保持活動狀態時升級。

管理員無法登入

將此問題與安裝故障分開處理。過期、重用或首次登入密碼會阻止會話。它們並不意味著影像失敗。

證書或對等身份失敗

1. 從停止的節點下載完整的系統快照。在該快照的tmp目錄中開啟install-error。
2. 如果消息是關於對等體身份，請檢查IP地址和FQDN的組合或空對等體清單。使每個對等體都使用一種格式，等待複製，確認群集運行正常，然後重試。請勿在滾動升級過程中更改身份格式。
3. 如果訊息是關於憑證的，請將其與版本說明規則進行比較：系統FQDN必須位於SAN中，或僅

在SAN為空時才位於CN中。不允許現有SAN回退到CN。

4. 使用正確的SAN型別中每個必需的DNS名稱或IP地址重新頒發證書。拒絕包含嵌入式NUL的名稱。
5. 確認新證書已過期、受信任、RSA 2048+或P-256+並使用SHA-2簽名。不要將私鑰附加到案例。
6. 將TLS驗證設定為「實施」，確認集群運行正常，然後在已停止的節點上重試升級。
7. 只有在節點正常運行後才能繼續滾動升級。當一個節點在此檢查中暫停時，請勿升級剩餘節點。

升級期間或升級後不久發生的群集警報

1. 確認升級本身已完成，且節點位於X15.5.20上。
2. 在事件日誌中查詢有關重新加密ClusterDB欄位以及「將遷移的資料儲存到CDB」的developer.upgrade消息。
3. 等待警報清除。培訓資料說重新加密完成後，它會清除。
4. 如果保留該屬性，請從每個對等點收集群集狀態、警報和快照。請勿將群集cookie或關鍵材料複製到案例備註中。
5. 確認TCP 4371和4372僅在對等體之間開啟，並且雙方TLS成功。允許從任何地方訪問4371的防火牆不是解決辦法。

節點啟動後的登入問題

- Web UI重定向到密碼更改。必須輸入當前密碼，並且新密碼必須不同。在安裝或出廠重置後第一次GUI登入時，以及本地密碼到期時，將會出現這種情況。
- SSH表示keyboard-interactive / PAM失敗，並且從不開啟外殼。必須更改過期的本地密碼。未授予舊會話。
- REST返回401。對於已過期的本地管理員，此值應為。事件日誌可以顯示API領域的Password Mismatch或taa-chkpasswd失敗。請更改密碼，然後重試。
- 新密碼被拒絕。它位於歷史記錄中（預設值為last 12），或者未通過當前的複雜性規則。
- LDAP管理員失去了預期的角色。將已配置的組與LDAP返回的正確組名進行比較。部分或子字串匹配不再授予該角色。只讀管理員無法編輯SAML IdP信任。
- 新安裝或出廠重置時沒有出廠預設根密碼。不要搜尋或分發預設憑據。升級不會清除當前的管理員密碼。



注意：出廠重置不是升級恢復步驟。刪除群集標識和群集cookie。解除群集後系統觸發的重置或不一致的群集資料庫會保留IP地址以及管理員和根密碼，清除其他配置和日誌，並將節點返回到其臨時證書。僅當發行說明呼叫它時才使用它，並且僅在存在備份之後才使用。

在需要TAC案例的情況下收集的證據

1. 每個節點的軟體版本和角色，以及哪個節點已停止。
2. 故障節點的完整系統快照，包括tmp/install-error。
3. 伺服器證書文本(openssl x509 -text -noout)。無私鑰。
4. 群集狀態、警報以及xConfiguration群集TlsVerify顯示允許還是強制執行。

- 5. 升級的事件日誌行，以及sshd或httpd身份驗證失敗（如果相關）。密寫密碼和cookie。
- 6. 無論使用本地、LDAP還是SAML管理員，還是使用智慧許可和任何API自動化。

升級後

在每個節點上

- 1. 版本是預期的X15.5.20內部版本。
- 2. 節點在其管理地址和Web UI載入上可訪問。
- 3. 未引發新的硬體、磁碟或應用程式警報。(重新加密後，群集通訊警報會清除。)
- 4. 在群集穩定後執行新的備份。

僅集群

- 1. 群集中的每個對等體都處於開啟狀態，複製工作正常。
- 2. 對等體在TCP 4371和4372上使用雙方TLS進行通訊。（沒有有效客戶端證書的連線必須失敗。）
- 3. 集群TlsVerify正在實施。

不支援允許。舊版Permissive值仍然可見，但它不會繞過驗證。設定Enforcing並確認群集保持正常。

- 4.防火牆仍僅允許來自對等體地址的TCP 4371。
- 5.日誌或上載的快照註釋中不會顯示群集cookie或診斷金鑰。

服務檢查，按正在使用什麼

如果使用	什麼好看的	如果失敗
本地管理員	GUI、SSH和API接受當前密碼。過期的帳戶會被推入密碼更改或接收HTTP 401。	確認到期時間為00:00 UTC，並且新密碼不在歷史記錄視窗內。
LDAP管理員	管理員僅在LDAP組名稱與配置的組完全匹配時才登入。	將目錄組與Expressway組進行比較。不要擴大匹配範圍以強制登入。
SIP或B2B呼叫	測試呼叫在兩個方向上連線。	收集呼叫歷史記錄和快照。
已驗證H.323註冊	終端使用它使用的每個別名進行註冊，包括H.323 ID和E.164編號。	為每個別名新增憑據別名對映。 發行說明將 xConfiguration Registration CredentialAliasMap與模式型別Exact一起使用。在子區域上關閉 CredentialAliasBinding也會恢復註冊，從而削弱安全狀態。H.323本身並未移除。
MRA或裝置註冊	已知終端註冊並發出呼叫。UC客戶端證書SAN是特定的DNS名稱或IP地址，不是過於寬泛或格式不正確的值。	將證書、遍歷憑證和DNS與升級前備份進行比較。重新頒發SAN過寬的證書。
電子郵件	測試消息使用STARTTLS離開	如果STARTTLS無法完成，則傳遞無法關閉。修復郵件伺

如果使用	什麼好看的	如果失敗
警報	節點。	伺服器信任或TLS。不要期望明文回退。
智慧型授權	註冊和授權與Web UI匹配。 標準映像保留在2500個加密的信令會話內，或者節點為Expressway Select。	檢查傳輸和CSSM。CSSM「允許匯出控制功能」覈取方塊不適用於Expressway。撤消令牌並刪除產品例項會將節點設定為「已取消註冊」。選項鍵不是解決方法。
REST或配置指令碼	帳戶名與新的長度和字元限制匹配。配置寫入包括GUI使用的CSRF保護。	根據發貨API架構更新客戶端。已刪除/調配/選項金鑰呼叫預期失敗。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。