瞭解ISE證書複製警報並對其進行故障排除

目錄

簡介

本文檔介紹複製警報及其在思科身份服務引擎®(ISE)中的故障排除。

必要條件

需求

思科建議您瞭解思科身份服務引擎®(ISE)。

採用元件

本檔案中的資訊是根據這些硬體和軟體版本。

- Cisco Identity Services Engine®(ISE)3.4及更高版本。

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。

複製警報

思科ISE中的複製警報提供了整個部署中複製框架的運行狀況和同步狀態的可視性。這些警報有助於確定可能影響資料一致性、節點通訊或複製流程的情況，使管理員能夠檢測問題並在它們影響系統操作之前解決問題。瞭解複製警報的用途和重要性對於維護正常的ISE部署並確保配置和運算元據在所有節點間保持同步至關重要。

ISE證書複製警報

證書複製失敗

當Cisco ISE無法將證書相關資料從主管理節點(PAN)複製到部署中的一個或多個節點時，會生成Certificate Replication Failed警報。每當在主PAN上匯入、生成、續訂或修改證書時，ISE會自動複製證書及其相關配置，以維護所有節點的一致性。此警報表示複製過程不成功，導致受影響節點上的證書配置不一致。

警報原因

當Cisco ISE無法在一個或多個節點上成功傳輸、驗證或安裝與證書相關的資料時，可能會發生Certificate Replication Failed警報。常見原因包括

- 網路通訊問題：封包遺失、高網路延遲、防火牆限制封鎖復寫流量、ISE節點之間的路由問題或MTU不相符造成封包分段或捨棄可能會中斷憑證復寫。
- 復制服務問題：如果RabbitMQ、JGroups或其他內部復制服務不可用、重新啟動或無法正常工作，則證書複製可能失敗。
- 證書驗證失敗：如果證書鏈不完整、CA或中間證書丟失、證書過期或損壞，或者其中包含不受支援的金鑰用法或無效格式，則複製可能會失敗。
- 節點通訊問題：如果目標節點處於離線狀態，則無法完成證書複製，或者重新啟動、取消註冊、斷開與部署的連線，或者無法進行複製。
- 磁碟空間不足：目標節點沒有足夠的可用磁碟空間來匯入和安裝複製的證書。
- 內部資料庫問題：如果ISE配置資料庫無法儲存或更新證書後設資料，複製可能會失敗。

警報的影響

此警報的影響取決於複製的證書型別和依賴此型別的服務。失敗的證書複製可能導致ISE節點之間的證書配置不一致、HTTPS證書不匹配、EAP身份驗證失敗、pxGrid信任建立問題、SCEP註冊或證書調配失敗、受信任證書儲存中的不一致以及外部整合的TLS驗證失敗。

證書複製暫時失敗

當Cisco ISE暫時無法將證書相關資料從主管理節點(PAN)複製到部署中的一個或多個節點時，會生成「證書複製暫時失敗」警報。與「證書複製失敗」警報不同，此警報表示複製失敗被認為是暫時的，思科ISE會在解決底層條件時自動重試複製操作。

警報原因

警報通常由於臨時阻止證書複製的瞬態情況而生成。常見原因包括：

- 臨時網路通訊問題：短暫的網路中斷、資料包丟失、高延遲、防火牆延遲或ISE節點之間的臨時路由問題。
- 復制服務初始化或重新啟動：RabbitMQ、JGroups或其他內部復制服務正在重新啟動或暫時不可用。
- 臨時節點不可用：目標節點正在啟動、重新啟動應用程式服務、重新加入部署或暫時無法訪問。
- 臨時系統資源限制：高CPU利用率、記憶體壓力或磁碟I/O爭用會暫時延遲複製處理。
- 併發管理操作：正在進行另一個證書匯入、備份、還原、修補程式安裝或部署同步時，證書複製可能會延遲。
- 臨時資料庫或複製隊列延遲：內部資料庫操作或複製隊列暫時忙於處理其他同步請求。

警報的影響

在大多數情況下，此警報對操作的影響最小，因為思科ISE會自動重試複製操作。但是，在複製成功完成之前，節點之間可能存在臨時不一致，包括：

- 新匯入或更新證書的延遲傳播
- 部署中的臨時證書配置不匹配
- 受影響節點上基於證書的服務的延遲可用性
- HTTPS、EAP、pxGrid或SCEP服務中的臨時延遲（如果它們依賴於複製的證書）

如果警報持續或重複發生，則會導致「證書複製失敗」警報。

排除ISE證書複製警報故障

這些是排除或驗證ISE中的證書複製警報時要驗證的常見因素。

1.驗證節點的部署狀態

為使證書複製成功，輔助節點必須處於Connected狀態（在思科ISE部署中）。導航到Administration > System > Deployment，然後驗證受影響節點的狀態。將滑鼠懸停在節點狀態旁邊的資訊(i)圖示上，以檢視同步詳細資訊和任何待處理的複製消息。

為每個節點顯示的同步狀態表示其當前複製和連線狀態：

- 綠色 — 節點與部署同步，並且複製正常運行。
- 黃色 — 節點不同步、節點註冊失敗或群集連線已丟失。此狀態表示在過去五分鐘內，群集無法訪問該節點。
- 紅色 — 無法到達節點，因此無法通過網路連線檢查（例如ICMP ping或HTTPS）與節點聯絡。

如果節點顯示Yellow或Red狀態，則表明存在影響該節點的複製或連線問題。此外，還要驗證節點資訊中顯示的複製消息數量。掛起的消息計數必須為5,000或更少。包含5,000多條待處理消息的隊列表示複製隊列已累積，這可能會延遲或阻止複製成功。

2.驗證部署中的隊列鏈路警報

思科ISE中的成功複製取決於RabbitMQ消息服務和JGroups群集通信框架的可用性和通訊。如果任一元件遇到通訊問題，思科ISE會生成隊列連結錯誤，這可能會中斷部署節點之間的複製。

要驗證警報狀態，請導航到操作>控制面板>警報，並檢查受影響節點上的隊列連結錯誤。

如果存在隊列連結錯誤，請續訂思科ISE 根CA證書，因為與證書相關的通訊故障通常會導致隊列連結錯誤。解決證書問題後，通常無需額外干預即可自動恢復複製。

附註：有關隊列連結錯誤的詳細資訊，請參閱ISE隊列連結錯誤文檔。

3.檢驗網路延遲和連通性

思科ISE複製依賴於部署節點之間的穩定網路連線。高網路延遲或間歇性連線會延遲複製，並可能導致同步失敗，尤其是在地理上分散的部署中。

使用ping之類的連線測試檢驗受影響節點之間的網路延遲。為了進行可靠的複製，節點之間的往返

延遲必須保持在大約300毫秒內。延遲持續超過此閾值可能會對複製效能和同步產生負面影響。另外，請確認不存在影響部署節點之間通訊的間歇性網路中斷、資料包丟失或防火牆限制。

4.確認受影響的節點上尚未存在證書

如果輔助節點上已存在要複製的證書，則證書複製可能會失敗。

導航到Administration > System > Certificates，選擇受影響的節點，然後驗證是否已安裝證書。如果存在證書，請檢查其屬性，確保它與正在複製的證書相匹配，並確定是否存在任何重複或衝突的證書。

5.驗證系統資源利用率

高系統資源利用率可能會影響思科ISE效能並延遲複製任務。過多的CPU、記憶體或磁碟使用率會阻止複製進程成功完成。

驗證受影響的節點是否有足夠的可用系統資源，以及資源利用率是否保持在建議的運行限制內。如果資源利用率始終很高，請分配更多資源或減少節點上的工作負載，以恢復正常的複製效能。

附註：請參閱效能和可擴充性指南，瞭解推薦的思科ISE部署的硬體大小和資源分配指南。

6.驗證部署和網路中的埠可用性

思科ISE複製要求特定的TCP埠在部署中的所有節點之間保持開放，以確保不間斷通訊和成功複製。如果任何這些埠被防火牆、訪問控制策略或網路裝置阻止，則可能會發生複製失敗或同步問題。

驗證所有Cisco ISE節點之間的這些TCP埠是否開啟且可訪問：

- TCP 443 - HTTPS通訊
- TCP 8443 -管理通訊
- TCP 12001 - JGroups群集通訊和複製
- TCP 6379 -內部報文傳送服務
- TCP 8671 - Cisco ISE消息傳送(RabbitMQ)

登入到Cisco ISE CLI並運行show ports命令以驗證節點中允許的埠。

確認在思科ISE節點上啟用所需的埠，並確保允許這些埠通過網路路徑。驗證沒有中間防火牆、安全裝置或網路策略阻止部署節點之間這些埠上的通訊。

複製警報的日誌收集

這些是在debug模式下設定的常見元件，用於隔離和排除思科ISE中的複製警報。

- 複製部署（replication.log和ise-psc.log）
- Replication-JGroup（replication.log和ise-psc.log）
- 複製跟蹤器(tracking.log)
- hibernate(hibernate.log)
- JMS(replication.log)

參考

- 思科身份服務引擎管理員指南3.5版
- 在ISE上排除故障並啟用調試
- 收集身份服務引擎上的支援捆綁包

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）。