瞭解ISE節點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。

ISE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節點複製警報

複製失敗

當部署中的輔助節點無法使用由部署中的主管理節點複製的消息時，將生成「複製失敗」警報。此警報表示複製過程失敗，受影響的節點不再具有最新的配置或運算元據。

與特定於證書的複製警報不同，此警報表示常規複製框架中的故障，並且可能會影響整個部署中的多個配置對象和服務。

警報原因

當Cisco ISE無法成功傳輸或應用複製的資料時，可能會出現Replication Failed警報。常見原因包括：

- 網路通訊問題：資料包丟失、高網路延遲、防火牆限制、路由問題或MTU不匹配會中斷ISE節點之間的通訊。
- 復制服務問題：RabbitMQ、JGroups或其他內部復制服務不可用、正在重新啟動或運行不正常。
- 節點通訊問題：目標節點處於離線狀態、正在重新啟動、已取消註冊、已斷開與部署的連線，或者無法訪問。
- 資料庫同步問題：由於資料庫錯誤或同步失敗，目標節點無法提交複製的資料。

- 系統資源限制：CPU利用率高、記憶體壓力大、磁碟空間不足或磁碟I/O過大會延遲複製處理。
- DNS或主機名解析問題：正向或反向DNS解析不正確導致節點之間無法成功通訊。
- 版本或部署不一致：如果節點未在受支援的軟體版本上運行，或者在升級或節點註冊後部署處於不一致狀態，則複製將失敗。
- 管理員證書到期:ISE節點的管理員證書已過期/已損壞/無效，因為節點之間的通訊處於危險狀態，導致複製失敗。
- 隊列連結錯誤：部署或受影響的節點顯示隊列連結錯誤，其中ISE消息證書/ISE根CA鏈在埠8671上損壞或無效。
- Stunnel服務已禁用/離線：Stunnel服務在分散式部署的所有節點中運行。禁用/未運行Stunnel服務的狀態會導致複製失敗警報。
- 複製埠被阻止：必須在部署中的節點與網路之間開啟埠12001、8671、443、8443和6379，以實現部署中的無縫複製過程。

警報的影響

影響取決於複製的資料型別。複製失敗可能導致整個ISE節點配置不一致、管理更改的延遲傳播、過時的策略、缺少網路裝置或身份資訊、證書同步失敗以及端點資料不一致。如果複製在較長的一段時間內仍不成功，則整個部署中的管理操作和策略一致性可能會受到影響。

複製已停止

當主管理節點無法將資訊複製到部署的輔助節點時，會生成「已停止複製」警報。此警報表示複製過程失敗，受影響的節點不再具有最新的配置或運算元據。

警報原因

當主管理節點無法成功傳輸複製的資料時，可能會出現「複製已停止」警報。常見原因包括：

- 網路通訊問題：資料包丟失、高網路延遲、防火牆限制、路由問題或MTU不匹配會中斷ISE節點之間的通訊。
- 復制服務問題：RabbitMQ、JGroups或其他內部復制服務不可用，正在重新啟動或在主管理節點中無法正常工作。
- 系統資源限制：CPU使用率高、記憶體壓力大、磁碟空間不足，或主管理節點中延遲複製處理的磁碟I/O過大。

- DNS或主機名解析問題：正向或反向DNS解析不正確導致節點之間無法成功通訊。
- 版本或部署不一致：如果節點未在受支援的軟體版本上運行，或者在升級或節點註冊後部署處於不一致狀態，則複製將失敗。
- 管理員證書到期:ISE節點的管理員證書已過期/已損壞/無效，因為節點之間的通訊處於危險狀態，導致複製失敗。
- 隊列連結錯誤：部署或受影響的節點顯示隊列連結錯誤，其中ISE消息證書/ISE根CA鏈在埠8671上損壞或無效。
- Stunnel服務已禁用/離線：Stunnel服務在分散式部署的所有節點中運行。禁用/未運行Stunnel服務的狀態會導致複製失敗警報。
- 複製埠被阻止：必須在部署中的節點與網路之間開啟埠12001、8671、443、8443和6379，以實現部署中的無縫複製過程。

警報的影響

當複製停止時，部署中的節點不再從主管理節點接收配置更新。這會導致策略不一致、網路裝置定義過時、端點資訊丟失、證書同步延遲以及整個部署中的配置不匹配。如果複製在較長的一段時間內保持停止狀態，則在主PAN上進行的管理更改在同步恢復之前無法在受影響的節點上生效。

對複製失敗和複製停止警報進行故障排除

慢速複製警報

每當在主PAN上進行配置更改時，Cisco ISE將更改放入複製隊列中，並將其同步到輔助節點。在正常情況下，複製在短時間內完成。但是，如果複製隊列開始建立或目標節點處理複製請求的時間比預期長，思科ISE會生成慢速複製警報。

思科ISE將這些警報分為三個嚴重級別：

- 慢速複製資訊
- 複製速度慢警告
- 慢速複製錯誤

警報原因

「慢速複製」警報通常由於延遲複製處理的臨時情況而生成。常見原因包括：

- 臨時系統資源利用率：短時間的高的CPU利用率、記憶體使用率或增加的磁碟I/O可能會延遲複製處理。
- 網路延遲：網路延遲的短暫增加或ISE節點之間的微小資料包丟失可能會減緩資料傳輸速度。
- 大型配置更改：批次終端匯入、策略更新、證書匯入或其他大型管理更改會增加要複製的資料量。
- 後台系統操作：備份、恢復、清除、修補程式安裝或升級活動會暫時增加系統負載。
- 複製隊列積壓工作：在短時間內執行多次配置更改可能會暫時增加複製隊列。
- 臨時服務延遲：RabbitMQ、JGroups或資料庫服務在繼續正常運行的同時會遇到短暫的處理延遲。

慢速複製警報 — 資訊

當掛起的消息計數超過10000或複製消息所用時間超過一小時時，將檢測到慢速或停滯的複製。

驗證：驗證掛起的同步消息計數。導航到Administration > System > Deployment，選擇受影響的節點，然後按一下Information(i)圖示以檢視掛起的複製消息數。

慢速複製警報 — 警告

當掛起的郵件計數大於20000或複製郵件所花費的時間超過三小時時，將檢測到慢速或停滯的複製。

驗證：驗證掛起的同步消息計數。導航到Administration > System > Deployment，選擇受影響的節點，然後按一下Information(i)圖示以檢視掛起的複製消息數。

慢速複製警報 — 錯誤

當掛起的郵件計數大於40000或複製郵件所花費的時間超過五小時時，將檢測到慢速或停滯的複製。

驗證：驗證掛起的同步消息計數。導航到Administration > System > Deployment，選擇受影響的節點，然後按一下Information(i)圖示以檢視掛起的複製消息數。

節點複製警報故障排除

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.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。

5.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。

6.驗證DNS解析

思科ISE複製依賴於部署中的所有節點之間的成功通訊。為使節點間通訊正常工作，必須能夠到達節點，而且必須配置轉發和反向DNS解析並正常工作。DNS解析問題可能會阻止節點通訊，從而導

致複製失敗。

要驗證ISE節點中的DNS解析，請登入思科ISE CLI並使用nslookup 命令驗證部署中每個節點的正向和反向DNS解析。

舉例來說：

- 轉發DNS查詢：nslookup www.example.com命令必須返回對應思科ISE節點的IP地址。
- 反向DNS查詢： nslookup 10.x.x.1 命令必須返回對應思科ISE節點的完全限定域名(FQDN)。

7.管理員和ISE消息證書驗證

思科ISE使用Admin證書和ISE消息證書建立複製所需的安全節點間通訊。如果任一證書無效、expired、corrupted或untrusted，部署節點之間的複製可能會失敗。

要驗證證書狀態，請導航到Administration > System > Certificates，選擇受影響的節點，然後檢視Admin和ISE消息傳送證書。驗證證書是否有效、未過期、受信任並處於正常狀態。

如果Admin certificate或ISE Messaging certificate無效、已損壞或已過期，請替換或更新證書。一旦解決了證書問題，在節點之間重新建立安全通訊後，複製將恢復。

附註：有關證書續訂的詳細資訊，請參閱ISE隊列連結錯誤和在ISE中安裝證書。

8.驗證ISE Stunnel服務的狀態

思科ISE中的Stunnel服務是一種內部服務，為ISE元件和外部服務之間的通訊提供安全SSL/TLS隧道。ISE使用Stunnel作為包裝，將SSL/TLS加密新增到通過普通TCP通訊的服務上，而不是在每個應用中獨立實施TLS加密。這提高了安全性，同時簡化了安全通訊的實施。

在Cisco ISE部署的所有節點上，Stunnel服務必須處於Running狀態，才能使複製正常工作。服務依賴於有效的ISE管理員和ISE消息證書以在複製過程中在節點之間建立安全TLS通訊。使用命令show tech-support可從Cisco ISE CLI驗證服務狀態 |包括特技頻道

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）。