瞭解ISE複製並對其進行故障排除

目錄

簡介

本文檔介紹思科身份服務引擎®(ISE)中的複製及其故障排除。

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 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。

思科ISE中的複製

ISE中的複製是在部署中的多個節點之間同步配置和運算元據以保持一致的過程。

主管理節點負責將部署中所做的更改複製到部署中的所有其他（輔助）節點。

思科ISE使用JGroups（一個可靠的組通訊框架）作為其複製架構的一部分。JGroups使ISE部署中的節點能夠相互通訊並交換複製資料。它提供了消息傳遞框架，可幫助在節點之間傳遞配置和資料庫更新，同時保持跨部署的同步。

- JGroups是Cisco ISE用於複製的通訊框架；它不儲存複製的資料本身。
- 並非思科ISE中的所有資料都通過JGroups複製。根據傳輸的資料型別，不同的服務使用不同的通訊機制。
- 如果複製暫時中斷，則一些Cisco ISE服務可以使用本地可用資料繼續運行，直到恢復同步。

資料傳輸方法示例

資料	通訊方法
配置和複製消息	JGroups
支援捆綁包集合	HTTPS API（TCP埠443）
調試配置	HTTPS API（TCP埠443）
即時日誌和報告	RabbitMQ或UDP，取決於部署配置

思科ISE複製的關鍵必備條件和驗證檢查

- DNS解析：對於參與部署的所有思科ISE節點，必須成功解析正向和反向DNS查詢。節點通訊和複製操作需要正確的DNS解析。
- NTP同步：所有思科ISE節點必須同步到可靠的NTP源，以在部署中保持一致的系統時間。時間同步對於複製和證書驗證至關重要。
- 證書：每個思科ISE節點上安裝的管理員證書必須有效且受信任。複製過程依賴管理員證書在節點之間進行安全通訊。
- 埠要求：網路連線必須允許通過複製和節點間服務所需的埠進行通訊：

服務	協定/埠
HTTPS(SOAP)	TCP/443
資料同步和複製(JGroups)	TCP/12001
管理訪問	TCP/8443
ISE訊息服務(SSL)	TCP/8671
Profiler端點所有權同步	TCP/6379

- 網路連通性：思科ISE節點之間的網路連線必須穩定，延遲不得超過300毫秒。驗證節點之間的延遲和丟包有助於確保可靠的複製。
- 隊列連結狀態：思科ISE消息傳送證書用於通過TCP埠8671保護節點間通訊。無效或損壞的消息傳遞證書可能會導致隊列連結錯誤和複製失敗。在這種情況下，必須根據情況重新生成ISE根CA證書或ISE消息傳遞證書。
- ISE Stunnel服務：思科ISE Stunnel服務在分散式部署中運行，並促進節點之間的安全通訊。該服務必須在所有適用節點上運行才能支援複製。可使用以下命令從Cisco ISE CLI驗證服務狀態：
  show tech-support |包括特技頻道
- ISE補丁和版本：主管理節點和加入節點（獨立節點）必須具有相同的版本和補丁級別進行節點註冊和同步，才能無縫工作。

思科ISE中的複製階段

思科ISE中的複製包括三個不同的階段，這些階段相互合作，在部署中的所有節點間建立和維護同步。每個階段都有其特定的用途，從加入節點開始，然後是初始資料庫同步，最後是持續交換增量更新以保持所有節點同步。

- 節點註冊
- 完全同步
- 增量同步

瞭解思科ISE中的節點註冊

節點註冊是思科ISE節點加入現有部署並與主要管理節點(PAN)建立通訊的流程。

在節點註冊期間：

步驟 1:加入節點（獨立節點）發起與主管理節點的通訊。

步驟 2:使用思科ISE管理員證書執行相互證書驗證。

步驟 3:DNS解析、NTP同步、網路可達性和所需的埠可達性均作為通訊過程的一部分進行驗證。

步驟 4:主管理節點驗證獨立節點/加入節點運行相容的思科ISE版本和補丁級別。

步驟 5:交換部署資訊、節點角色和信任關係。

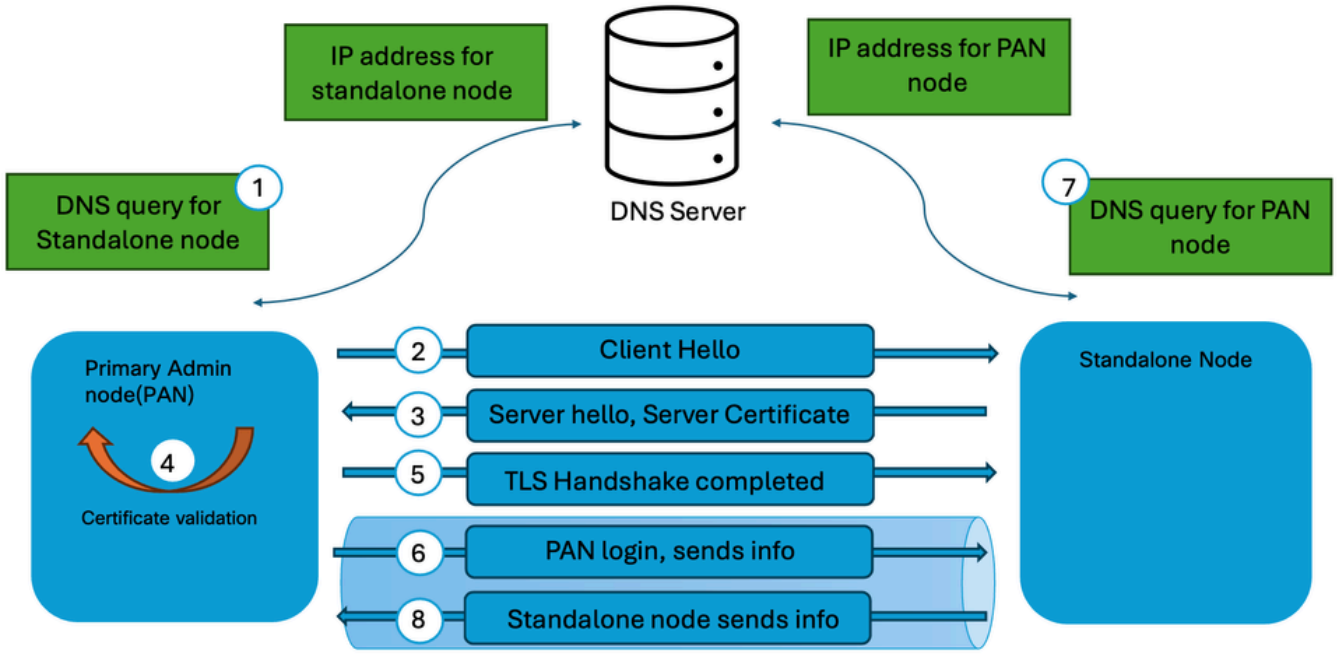
步驟 6:資料庫復制服務已初始化並準備好進行同步。

成功完成節點註冊後，該節點將成為部署的受信任成員，並允許開始複製過程。

主要特徵

- 將新節點新增到部署時發生。
- 建立信任和通訊管道。
- 不會立即傳輸完整的配置資料庫。
- 充當後續同步操作的先決條件。

有關節點註冊過程的詳細說明，請參閱瞭解思科ISE中的節點註冊流程。



節點註冊流程

附註：要新增到部署的節點必須是獨立節點。此外，主要管理節點(PAN)必須在部署中啟用主要管理角色，以允許在Cisco ISE中註冊節點。

瞭解思科ISE中的完全同步

完全同步是一個完整的資料庫複製過程，在此過程中，整個配置資料庫從主PAN傳輸到另一個節點。完全同步不會只傳輸已修改的記錄。相反，將在接收節點上重建整個配置資料集。

在下列情況下可能會發生完全同步：

- 節點註冊後的初始同步。
- 從複製失敗中恢復。
- 資料庫嚴重不一致。
- 將節點重新加入部署。
- 通過Cisco TAC故障排除過程啟動手動同步。
- 內部複製機制確定增量同步無法再恢複資料庫一致性。

在完全同步期間：

步驟 1:主管理節點準備一個完整的資料庫快照。

步驟 2:配置資料打包在.dmp檔案中並傳輸到接收節點。

步驟 3:接收節點上的現有複製資料將被驗證和更新。

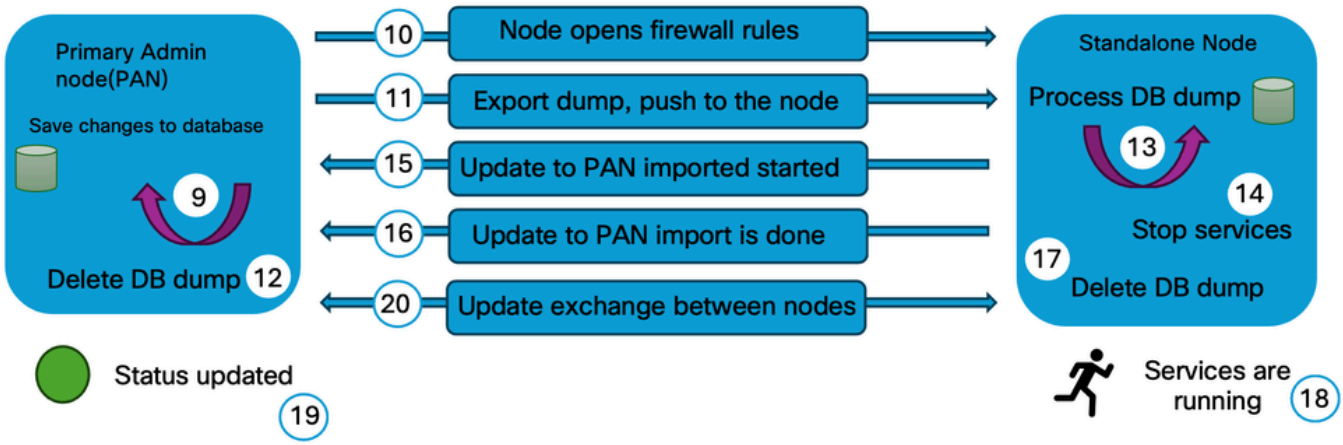
步驟 4:重建整個配置資料庫以匹配主管理節點。

步驟 5:複製狀態在完成時進行驗證。

因為完全同步涉及的資料比增量同步要多得多，所以需要額外的處理時間和網路資源。

完全同步的特徵

- 傳輸完整的配置資料庫。
- 消耗更多頻寬和系統資源。
- 比增量同步要長。
- 在檢測到差異時恢複資料庫一致性。
- 通常比增量同步發生頻率低。



完全同步進程

瞭解思科ISE中的增量同步

增量同步是思科ISE在節點成功加入部署後用於分發配置更改的持續複製機制。當管理員在PAN上進行配置更改時，思科ISE不會傳輸整個資料庫。相反，只有修改後的記錄會複製到訂閱伺服器節點。

通過增量同步複製更改的示例包括：

- 策略修改
- 網路裝置新增或更新
- 終端組更改
- 授權配置檔案更新
- 與證書相關的配置更改
- 身份源配置更新

增量同步過程持續運行，旨在維護所有節點的一致性，同時最大限度地降低頻寬利用率和複製開銷。

增量同步的優點

- 減少複製流量。
- 最大程度地縮短同步時間。
- 允許快速傳播配置更改。
- 在整個部署中保持接近即時的一致性。

複製工作流

步驟 1:配置更改發生在主管理節點上。

步驟 2:更改將寫入主管理節點資料庫。

步驟 3:復制服務標識已修改的記錄。

步驟 4:主管理節點將新事件/更改寫入事務表中。

步驟 5:獨立於PAN的執行緒將資訊/更改發佈到部署中的輔助節點。

步驟 6:部署中的輔助節點從主管理節點接收更改。

步驟 7:部署中的輔助節點應用從主管理節點接收的更改。

步驟 8:複製狀態在成功完成時更新。

在正常操作條件下，思科ISE中的大多數複製活動通過增量同步進行。

附註：如果輔助節點標識缺少的複製消息，它將向主管理節點(PAN)發起請求，以檢索缺少的消息並保持同步

複製順序概述和同步狀態

思科ISE部署中的整體複製工作流程可以總結如下：

1.節點註冊：建立信任並將節點新增到部署中。

2.初始完全同步：將完整的配置資料庫傳輸到新註冊的節點。

3.增量同步：在正常操作中持續傳播配置更改。

4.完全同步（如果需要）：如果檢測到複製問題或資料庫不匹配，則重建資料庫一致性。

此階段化方法使Cisco ISE能夠跨所有節點維護一致的配置資料庫，同時最佳化網路利用率和複製效能。

同步狀態

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（過去五分鐘群集無法訪問該節點）。
- 紅色 — 該節點在物理上無法訪問，無法通過網路連線檢查（例如ICMP ping和HTTPS）與其聯絡。

附註：如果複製沒有正確執行，您可以通過登入到主管理節點來使用主管理節點執行到輔助節點的手動同步，導航到Administration > System > Deployment >選擇節點，然後按一下Sync up。

終端複製

終端複製是ISE通過此過程在所有策略服務節點(PSN)和主管理節點(PAN)之間同步終端資料庫資訊，以在整個部署中維護一致的終端身份檢視。

- 思科ISE維護一個集中終端資料庫，儲存有關連線到網路的裝置的資訊。此資訊包括靜態配置的端點和通過身份驗證、分析、狀態評估或與外部身份源整合動態獲取的端點。
- 當建立或修改終端資訊時，思科ISE將更改複製到部署中的其他節點。此同步使每個策略服務節點都能夠使用相同的端點資訊評估身份驗證和授權請求，而不管哪個PSN處理該請求。
- 端點複製由Cisco ISE自動處理，並構成整體資料庫複製機制的一部分。在正常操作過程中，管理員不需要手動啟動端點同步。

終端複製的工作原理

- 終端更新：終端通過身份驗證、分析、狀態或手動配置建立或更新。
- 更改檢測：思科ISE檢測終端更改並為復製做好準備。
- 複製：使用ISE複製框架將更新的終端資訊複製到部署中的其他節點。
- 資料庫同步：輔助節點使用複製的資訊更新其本地終端資料庫。
- 一致的策略實施：同步完成後，所有策略服務節點將使用相同的端點資訊來進行身份驗證和授權決策。

從Cisco ISE版本3.3中，動態發現的終端不會自動複製到所有節點。可從「端點複製」視窗中啟用或禁用此功能。導覽至Administration > System > Settings > Endpoint Replication，根據需要啟用或禁用。

附註：必須將終端複製與會話複製區分開來。端點複製同步永久端點資料庫記錄（如MAC地址、端點組和分析資訊），而會話複製同步運行時會話資訊以支援策略實施和操作連續性。這些機制獨立運行，在Cisco ISE架構內提供不同的功能。

常見節點複製問題

案例 1:由於DNS解析失敗，節點註冊失敗

節點註冊失敗，錯誤原因為「主機名無法解析。請檢查您的DNS配置」。

驗證步驟

- 確保在主管理節點和獨立節點中配置了有效的DNS伺服器。使用命令show running-config驗證DNS伺服器配置 | include name-server
- 使用用於轉發DNS查詢的節點的命令nslookup　FQDN和用於反向DNS查詢的節點的nslookup ip地址，驗證主管理節點和獨立節點中的正向和反向DNS解析。
- 使用命令ping　DNS伺服器IP（從ISE節點的CLI中），從主管理節點和獨立節點驗證DNS伺服器的可訪問性。

案例 2:由於管理員證書過期，節點註冊失敗

節點註冊失敗，錯誤原因為「載入證書時出錯。此時無法到達節點。請稍後再試」。

驗證步驟

- 驗證主管理節點和獨立節點的管理員證書，以確保有效性和證書狀態。導航到Administration > System > Certificates，選擇節點，然後驗證管理員證書的有效性和狀態。
- 如果Admin證書已過期，請替換或更新證書，並確保分配了Admin用法。

案例 3:由於版本不匹配，節點註冊失敗

節點註冊失敗，錯誤原因為「版本/修補程式詳細資訊不匹配」。

驗證步驟

- 使用命令show version驗證軟體版本以及主管理節點和獨立節點的補丁程式，以確保版本詳細資訊匹配。

調試日誌的元件

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中的複製故障。

- 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)
- ca-service(caservice.log)
- admin-ca(ise-psc.log)

參考

- 在ISE上排除故障並啟用調試
- ISE — 隊列連結錯誤
- 思科身份服務引擎管理員指南3.4版
- 思科身份服務引擎管理員指南3.5版

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）。