Firepower使用者身份：從使用者代理遷移到身份服務引擎

簡介

在未來版本中，Firepower使用者代理不再可用。它被身份服務引擎(ISE)或身份服務引擎 — 被動ID聯結器(ISE-PIC)取代。 如果您當前使用使用者代理並考慮遷移到ISE，本文檔提供遷移注意事項和策略。

使用者身份概述

目前有兩種方法可從現有身份基礎設施中提取使用者身份資訊：使用者代理和ISE整合。

使用者代理

使用者代理是在Windows平台上安裝的應用程式。它依賴Windows Management Instrumentation(WMI)協定來訪問使用者登入事件（事件型別4624），然後將資料儲存到本地資料庫。使用者代理檢索登入事件的方法有兩種：在使用者登入時即時更新（僅限Windows Server 2008和2012），或輪詢每個可配置間隔的資料。同樣，使用者代理會將從Active Directory(AD)接收的資料即時傳送到Firepower管理中心(FMC)，並定期將批次登入資料傳送到FMC。

使用者代理可檢測的登入型別包括直接或通過遠端案頭登入到主機；檔案共用登入；電腦帳戶登入。使用者代理不支援其他型別的登入，如Citrix、網路登入和Kerberos登入。

使用者代理具有可選功能，可檢測對映使用者是否已註銷。如果啟用了註銷檢查，它將定期檢查「explorer.exe」進程是否在每個對映端點上運行。如果在72小時之後無法檢測到進程正在運行，則將刪除此使用者的對映。

身分識別服務引擎

身份服務引擎(ISE)是管理使用者網路登入會話的強大AAA伺服器。由於ISE直接與網路裝置（如交換機和無線控制器）通訊，因此可以訪問有關使用者活動的最新資料，使其成為比使用者代理更好的身份源。當使用者登入到終端時，通常會自動連線到網路，如果網路啟用了dot1x身份驗證，ISE會為此使用者建立身份驗證會話並保持其活動狀態，直到使用者從網路中註銷。如果ISE與FMC整合，則會將使用者 — IP對映（以及ISE收集的其他資料）資料轉發到FMC。

ISE可以通過pxGrid與FMC整合。pxGrid是一種用於在ISE伺服器之間和其他產品之間集中分發會話資訊的協定。在此整合中，ISE充當pxGrid控制器，FMC向控制器訂閱接收會話資料（FMC不會向ISE發佈任何資料，除非在稍後將討論的補救期間），並將資料傳遞到感測器以實現使用者感知。

身份服務引擎被動身份聯結器(ISE-PIC)本質上是一個具有受限許可證的ISE例項。ISE-PIC不執行任何身份驗證，而是充當網路中各種身份源的中央中心，收集身份資料並將其提供給使用者。ISE-PIC類似於使用者代理，因為它還使用WMI從AD收集登入事件，但具有更強大的功能，稱為被動身份。它還通過pxGrid與FMC整合。

遷移注意事項

許可要求

FMC不需要額外的許可證。如果身份服務引擎尚未在基礎設施中部署，則需要許可證。有關詳細資訊，請參閱思科ISE許可模式文檔。ISE被動ID聯結器是完整ISE部署中已存在的功能集，因此如果存在現有ISE部署，則無需其他許可證。有關ISE-PIC的新部署或單獨部署，請參閱Cisco ISE-PIC許可文檔以瞭解詳細資訊。

SSL證書

雖然使用者代理不要求與FMC和Active Directory進行通訊的公開金鑰基礎設施(PKI)，但ISE或ISE-PIC整合要求僅出於身份驗證目的在ISE和FMC之間共用SSL證書。該整合支援證書頒發機構簽名的證書和自簽名的證書，前提是在證書中同時新增「伺服器身份驗證」和「客戶端身份驗證」EKU（擴展金鑰用法）。

身份源覆蓋

使用者代理僅涵蓋Windows案頭上的Windows登入事件，並檢測基於輪詢的註銷。ISE-PIC涵蓋Windows案頭登入以及其他身份源，例如AD代理、Kerberos SPAN、系統日誌解析器和終端服務代理(TSA)。 完整ISE具有所有ISE-PIC的覆蓋範圍以及來自非Windows工作站和流動裝置等功能的網路身份驗證。

	使用者代理	ISE-PIC	ISE
Active Directory案頭登入	是	是	是
網路登入	否	否	是
終端探測	是	是	是
InfoBlox/IPAM	否	是	是
LDAP	否	是	是
安全Web網關	否	是	是
REST API源	否	是	是
系統日誌分析器	否	是	是
網路Span	否	是	是

使用者代理壽命終止

支援使用者代理的Firepower的最後版本是6.6，它提供了在升級到更高版本之前必須禁用使用者代理的警告。如果需要升級到高於6.6的版本，必須在升級之前完成從使用者代理到ISE或ISE-PIC的遷移。有關詳細資訊，請參閱使用者代理配置指南。

相容性

請檢視Firepower產品相容性指南，以確保整合中涉及的軟體版本相容。請注意，對於未來的Firepower版本，對較新ISE版本的支援可能需要特定修補程式級別。

遷移策略

從使用者代理遷移到ISE或ISE-PIC需要仔細的規劃、執行和測試，以確保平穩過渡FMC的使用者身份源並避免對使用者流量產生任何影響。本節提供了此練習的最佳實踐和建議。

準備遷移

後續步驟可在從使用者代理切換到ISE整合之前完成。

步驟1.配置ISE或ISE-PIC以啟用PassiveID，並與Active Directory建立WMI連線。請參閱ISE-PIC管理指南。

步驟2.準備FMC的身份證書。它可以是由FMC簽發的自簽名證書，也可以是在FMC上產生的由私人或公共證書頒發機構(CA)簽名的證書簽名請求(CSR)。 必須在ISE上安裝自簽名證書或CA的根證書。有關詳細資訊，請參閱ISE和FMC整合指南。

步驟3.在FMC上安裝簽署ISE的pxGrid證書的CA根證書（如果自簽，則安裝pxGrid證書）。有關詳細資訊，請參閱ISE和FMC整合指南。

轉換過程

如果不禁用FMC上的使用者代理配置，則無法配置FMC-ISE整合，因為這兩種配置是互斥的。這可能會在變更期間影響使用者。建議在維護時段期間執行這些步驟。

步驟1.啟用並驗證FMC-ISE整合。有關詳細資訊，請參閱ISE和FMC整合指南。

步驟2.確保在FMC上導航到**Analysis > User > User Activities**頁向FMC報告使用者活動。

步驟3.檢查以下對象上的受管裝置上可用的使用者IP對映和使用者組對映：
Analysis > Connections > Events > Table View of Connection Events。

步驟4.修改訪問控制策略，將操作臨時更改為**Monitor**，使其更改為根據使用者名稱或使用者組條件阻止流量的任何規則。對於允許基於發起程式使用者或組的流量的規則，請建立允許流量而不使用使用者條件的重複規則，然後禁用原始規則。此步驟的目的是確保關鍵業務流量在維護時段後的測試階段不會受到影響。

步驟5.在維護時段過後，在正常的工作時間內，觀察FMC上的連線事件以監控使用者IP對映。請注意，連線事件僅在存在需要使用者資料的已啟用規則時顯示使用者資訊。因此，在上一步中建議監視操作的原因。

步驟6.一旦達到所需狀態，只需恢復對訪問控制策略所做的更改，並將策略部署推送到受管裝置。

其他資訊

- 影片教程：使用者代理過渡到ISE-PIC
- 思科ISE 2.4管理指南：授權
- 身份服務引擎被動身份聯結器(ISE-PIC)安裝和管理員指南2.2版
- 使用者代理配置指南
- 思科Firepower相容性指南
- 配置ISE 2.4和FMC 6.2.3 pxGrid整合