User-ID 最佳做法

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

November 16, 2020

Table of Contents

User-ID 最佳做法

開始使用 User-ID 最佳做法

User-ID™ 利用大範圍存放庫（例如目錄伺服器、無線 LAN 控制器、VPN、NAC、Proxy 等）中的使用者內容，可讓您：

- 識別使用者，並根據信任層級和行為來將最低權限主體套用至使用者，不論：
  - 使用者位置（例如辦公室或住家）
  - 他們正在使用的裝置（例如 iOS、Android 行動裝置、macOS、Windows、Linux 桌上型電腦、膝上型電腦、Citrix、Microsoft VDI 或終端機伺服器）
  - 使用者正在存取的應用程式
- 保護公司認證不將它用於第三方網站，以及防止重複使用遭竊的認證，方法是針對任何應用程式在網路層啟用多因素驗證 (MFA)，而不對應用程式進行任何變更。

不論使用者身在何處一律都能在網路上找到他們的能力，可以更恰當地查看使用者活動、啟用基於使用者和群組的安全性政策，以及協助您取得更具洞察力的分析（記錄、報告和鑑識）。使用下列最佳做法指導方針，以了解如何在網路中規劃、部署和維護 User-ID。

User-ID 支援數個功能；本指南涵蓋下列功能：

- GlobalProtect
- Syslog 監控
- 重新分配
- 群組對應
- 動態使用者群組

本指南中尚未涵蓋的其他功能包含：

- Panorama 受管理 Prisma 存取
- 認證網路釣魚防禦
- IP 位址至使用者名稱對應，從：
  - 網路存取控制 (NAC) 裝置
  - 驗證入口網站
  - Active Directory

GlobalProtect 的 User-ID 最佳做法

Palo Alto Networks 建議 GlobalProtect 作為 User-ID 的最佳做法解決方案。它提供遠端使用者的連線功能，以及使用內部閘道來收集內部網路上使用者的對應。因為 GlobalProtect 需要使用者只要網路連線、裝置狀態或使用者驗證狀態變更就利用其認證進行驗證，所以確保基於使用者的政策強制執行的精確使用者對應。

規劃 GlobalProtect 部署的 User-ID 最佳做法

- 遵循 GlobalProtect 快速設定指南，以判斷如何最佳部署 GlobalProtect。針對 User-ID，使用一直開啟 VPN 設定和混合的內部與外部閘道設定。
- 在所有您想要識別使用者的端點上，安裝 GlobalProtect 應用程式。
- 判定您用於 GlobalProtect 驗證之使用者名稱的目錄屬性（例如 UserPrincipalName、sAMAccountName 或 common-name）。指定這些屬性作為群組對應設定檔中的主要或替代使用者名稱。
- 如果您使用用戶端憑證驗證，則憑證「主旨名稱」欄位必須識別使用者名稱。User-ID 不支援電腦憑證。
- 如果您只有一個內部閘道，但有其他防火牆需要了解該閘道的對應，則請規劃如何部署重新散佈，以將對應傳送至其他防火牆。
- 判定您是否接收到來自多個來源的對應。如果是這樣，則請使用網頁介面或 CLI 來評估來源，判定提供可能比 GlobalProtect 較不精確或及時之對應的來源是否可以覆寫收集自 GlobalProtect 的 IP 位址至使用者名稱對應。

使用 User-ID 最佳做法部署 GlobalProtect

- 部署 GlobalProtect 入口網站和閘道。同時部署內部和外部閘道來持續識別使用者，而不論身在何處。
- 使用預登入（一直開啟）或使用者登入（一直開啟）連線方法，以在同時使用內部和外部閘道時存取網路。
- 如果您使用憑證進行驗證，則請使用簡易憑證註冊通訊協定 (SCEP) 部署驗證的使用者特定用戶端憑證。
- 如果您使用內部閘道，則請使用內部主機偵測，讓 GlobalProtect 應用程式知道何時將使用者傳送至內部閘道。
- 只在來源區域中啟用使用者識別。例如，如果您使用 GlobalProtect 外部閘道，則請在與通道介面相關聯的區域中啟用 User-ID（**Network**（網路）> **Zones**（區域）> *tunnel-zone*）。
- 如果您接收到來自多個來源的使用者對應，則請在 User-ID 代理程式上排除外部 GlobalProtect 閘道的 GlobalProtect 子網路，這樣提供可能比 GlobalProtect 較不精確或及時之對應的來源不會覆寫 GlobalProtect 所提供的使用者對應。
- 設定重新散佈，以共用 GlobalProtect 閘道所收集與其他防火牆的對應。
- 指定可讓使用者向 GlobalProtect 驗證為群組對應設定檔中主要使用者名稱或替代使用者名稱屬性的所有使用者名稱格式。如果使用者未在 GlobalProtect 驗證期間提供網域名稱，則請啟用 **Allow matching usernames without domains**（允許不需網域進行使用者名稱匹配）（**Device**（裝置）> **User Identification**（使用者識別）> **User Mapping**（使用者對應）> **Palo Alto Networks User-ID Agent Setup**（**Palo Alto Networks User-ID** 代理程式設定））。
- 建立安全性政策規則，並測試它們是否符合預期的使用者流量流程。

使用 User-ID 的 GlobalProtect 後部署最佳做法

- 維護和更新端點上的 GlobalProtect 應用程式。如果您要更新多個端點，則請在網頁伺服器代管應用程式更新，以減少使用者連線並下載應用程式或使用軟體散佈工具將更新推送至受管理主機時的防火牆負載。
- 在 GlobalProtect 應用程式上，確認使用者可以成功地連線至外部閘道。
- 確認防火牆從 GlobalProtect 接收到 IP 位址至使用者名稱對應。

- 在網頁介面上，選取 **Monitor**（監控） > **User-ID**，然後確認 **User**（使用者）欄中顯示的使用者名稱。
- 使用 CLI 命令確認防火牆正確地接收到對應。

Syslog 監控的 User-ID 最佳做法

Palo Alto Networks 防火牆可以剖析 Syslog 訊息以取得 IP 位址至使用者名稱對應。您可以使用來自現有網路服務和裝置的驗證事件，例如第三方 VPN 解決方案、網路存取控制 (NAC) 解決方案，或使用 Syslog 訊息的安全性資訊和事件管理 (SIEM) 系統。若要保持最新的使用者對應，您還可以設定防火牆來剖析登出事件的 Syslog 訊息，以自動刪除過期對應。

規劃 Syslog 監控部署的 User-ID 最佳做法

- 檢閱 Syslog 寄件者用來判斷所使用語法的格式、是否包含網域名稱，以及它們是否符合準則。
- 判定您是否想要監控登入事件、登出事件或兩者。如果您想要監控登出事件，則請確認 Syslog 寄件者在訊息中包含 IP 位址和使用者名稱。
- 根據 Syslog 訊息，判斷您是否需要使用 regex 或欄位識別碼。如果 Syslog 訊息一致且可預測，則請使用欄位識別碼。如果訊息更為複雜且更無法預測，則請使用 regex。
- 規劃在防火牆上使用 PAN-OS 整合式 User-ID 代理程式部署 Syslog 監控，而不是使用 Windows User-ID 代理程式。

使用 User-ID 最佳做法部署 Syslog 監控

- 如果 Syslog 寄件者使用不同的格式，則請設定每種格式的 Syslog 剖析設定檔。
- 如果您想要監控登入和登出事件，則請設定每種事件類型的 Syslog 剖析設定檔。
- 如果 Syslog 訊息未包含網域名稱，而且使用者名稱在所有網域中都是唯一的，則請啟用 **Allow matching usernames without domains**（允許不需網域進行使用者名稱匹配）。
- 在 PAN-OS 整合式 User-ID 代理程式上，因為已加密流量，所以請一律使用 SSL 來接聽 Syslog 訊息。因為 UDP 以純文字傳送流量，所以如果您必須使用 UDP，則請確定 Syslog 寄件者和用戶端都位在專用的安全網路上，以防止不受信任的主機將 UDP 流量傳送至防火牆。
- 確認您想要監控的所有 Syslog 寄件者都包含為 [Server Monitoring（伺服器監控）] 清單中的項目，因為防火牆忽略來自不在此清單中的寄件者的任何 Syslog 訊息。
- 依最可能相符項的順序，來排序 [Filter（篩選）] 清單中的項目。例如，如果您認為 80% 的 Syslog 訊息將符合 filter1，而 20% 將符合 filter2，則請確定 filter1 在清單中會在 filter2 的前面。

使用 User-ID 的 Syslog 監控後部署最佳做法

- 驗證 Syslog 訊息符合 Syslog 剖析設定檔，以及防火牆從 Syslog 訊息接收到 IP 位址至使用者名稱對應。
- 使用 `show user server-monitor statistics` CLI 命令，驗證防火牆接收到來自 Syslog 寄件者的訊息，並正確地對應使用者。

重新散佈的 User-ID 最佳做法

在大型網路中，您可以設定防火牆透過重新散佈來收集其他防火牆上已存在的對應資訊，以流暢執行資源使用，而不需要設定所有防火牆直接查詢對應資訊來源。

規劃重新散佈部署的 User-ID 最佳做法

- 規劃重新分配架構。需考慮的一些因素包括：
  - 哪些防火牆將對所有資料類型強制執行政策（例如 IP 位址至使用者名稱對應或裝置隔離資訊），以及哪些防火牆應該接收資料子集？
  - 哪些 IP 範圍需要 IP 位址至使用者名稱對應？
  - 如果您的內部閘道提供使用者對應，則哪些其他裝置需要該資料？它們將具有何種功能和角色？
  - 如何最小化彙總所有資料所需的躍點數？IP 位址至使用者名稱對應的最大允許躍點數為十，而使用者名稱至標籤對應和 IP 位址至標籤對應的最大允許躍點數為一。
  - 您如何將查詢使用者對應資訊來源的防火牆數目減到最少？查詢防火牆數目越少，防火牆和來源上的處理負載越少。
- 決定重新散佈中樞的最佳選項：
  - 專用 VM-Series 防火牆最適合大規模 User-ID 部署。如果您只重新散佈使用者對應，則 VM-50 就已足夠。如果您規劃一併重新散佈 IP 位址至標籤對應，則建議使用 VM-300 或更高的系列。
  - Panorama 最適合小到中型環境，以及您未使用 Syslog 或伺服器監控來收集使用者對應時。
- 根據網路需求，判定您想要使用的拓撲類型：
  - 單一地區的中樞和支點
  - 多個地區的中樞和支點
  - 階層式

使用 User-ID 最佳做法部署重新散佈

- 設定您想要重新散佈的資訊來源：
  - User-ID IP 位址至使用者名稱對應（包含 Windows User-ID 代理程式）
  - 動態位址群組的 IP 位址至標籤對應
  - 動態使用者群組的使用者名稱至標籤對應
  - 基於 HIP 的政策強制執行的資料
  - 裝置隔離資訊
- 設定您想要一或多個代理程式在資料重新散佈中包含的網路，以及您想要從重新散佈 IP 位址至標籤對應或 IP 位址至使用者名稱對應中排除的網路。
- 使用包含/排除網路清單可定義重新散佈代理程式在重新散佈對應時包含或排除的子網路。
- 設定透過重新散佈接收到特定資料類型的網路或資源。
- 啟用使用重新散佈自訂憑證進行驗證，以使用自訂憑證進行重新散佈代理程式與用戶端之間的相互驗證。
- 使用 VM 系列防火牆或 Panorama 來重新散佈資料。因為 Panorama 可以是代理程式或用戶端，所以請使用 **Panorama** > **Data Redistribution**（資料重新散佈）以在 Panorama 上設定資料重新散佈。
- 如果強制執行政策的防火牆因為也是 GlobalProtect 閘道和資料中心而需要遠端和本機使用者的對應，則請啟用雙向重新散佈。
- 為了確保最佳復原，您只應該在地區內啟用雙向重新散佈，而不是在地區之間。

使用 User-ID 的重新散佈後部署最佳做法

- 遵循設定資料重新散佈中的最後兩個步驟，驗證代理程式將資料正確地重新散佈至用戶端。

群組對應的 User-ID 最佳做法

根據使用者群組成員資格（而不是個別使用者）來定義原則規則，將可簡化管理作業，因為您無須在每次有群組成員身份發生變更時更新規則。建議使用下列最佳做法來設定 Lightweight Directory Access Protocol（輕量型目錄存取協定 - LDAP）部署的群組對應。

下列各節描述用於部署內部部署目錄服務之群組對應的最佳做法。

規劃群組對應部署的 User-ID 最佳做法

- 識別目錄服務（例如 Active Directory 或基於 LDAP 的服務，例如 OpenLDAP），以及識別目錄伺服器的拓撲。需考慮的一些問題包括：
  - 有多少目錄伺服器、資料中心和網域控制器？
  - 群組資訊的主要來源為何？
  - 網域控制器與目錄伺服器的相對位置為何？
  - 目錄伺服器和網域控制器是否位在不同的地區？
  - 哪些是本機資源，哪些是已地區設定資源？
- 針對群組對應的主要來源是 Active Directory 伺服器的部署：
  - 如果您只有一個網域，則您只需要一個帶有 LDAP 伺服器設定檔的群組對應組態，即可以最佳連線能力將防火牆連接到網域控制器。最多將四個網域控制站新增至 LDAP 伺服器設定檔，以用作備援。
  - 如果具有萬用群組，請您建立一個 LDAP 伺服器設定檔以連線到用於 SSL 的 3268 或 3269 連接埠上的通用類別目錄伺服器的根網域，然後使用 LDAPS 建立另一個 LDAP 伺服器設定檔以在連接埠 636 連線至根網域控制器。如果您未使用 TLS，則請使用連接埠 389。這有助於確保使用者和群組資訊可用於所有網域和子網域。
  - 如果您沒有萬用群組，而且有多個網域或多個樹系，則必須建立具有 LDAP 伺服器設定檔的群組對應設定，以將防火牆連線至每個網域/樹系中的網域伺服器。採取步驟以確保使用者名稱在分開的樹系中為唯一。
  - 使用群組對應之前，為基於使用者的安全性政策規則設定主要使用者名稱，因為此屬性會在政策設定、日誌和報告中識別使用者。
- 若要建立 LDAP Directory 中還沒有的自訂群組，請使用使用者屬性來建立自訂群組。
- 如果您建立使用同一基本識別名稱 (DN) 或 LDAP 伺服器的多個群組對應設定，則請確定群組對應設定未包含重疊群組。例如，一個群組對應設定的包含清單不能包含也在不同群組對應設定中的群組。
- 確定每個網域內所有使用者和群組的使用者名稱和群組屬性都是唯一的。
- 只擷取您將在基於群組的安全性政策和設定中使用的群組，方法是使用群組包含清單或套用自訂搜尋篩選器。
- 評估目錄中群組的變更頻率，以判定群組對應設定檔的最佳 **Update Interval**（更新間隔）值。例如，如果您的群組頻繁地變更，則請設定較小的值，但是，如果它們通常是靜態，則請輸入較大的值。
- 判定您想要在日誌、報告和政策設定中代表使用者的使用者名稱屬性。如果您的 User-ID 來源以不同的格式傳送使用者名稱，則請將這些使用者名稱指定為替代屬性。

確定每位使用者的主要使用者名稱、替代使用者名稱和電子郵件屬性都是唯一的。

使用 User-ID 最佳做法部署群組對應

- 如果您只要使用目錄中的自訂群組，則請將未使用的群組新增至包含清單，以防止 User-ID 擷取目錄中的所有群組。

- 使用 **Group Include List**（群組包含清單），將政策規則限定於特定群組。或者，輸入 **Search Filter**（搜尋篩選器）（LDAP 查詢）和 **Object Class**（物件類別）（群組定義），以篩選防火牆為群組對應所追蹤的群組。如果您在 LDAP Directory 中還沒有群組，則可以使用使用者屬性，以在防火牆上建立自訂群組。確定用來形成自訂群組的屬性是目錄上的索引屬性。
- 指定可識別報告和日誌中使用者的主要使用者名稱。

使用 User-ID 的群組對應後部署最佳做法

- 若要確認 LDAP 伺服器的連線功能，請使用 `show user group-mapping state all` CLI 命令。
- 若要檢視群組成員資格，請執行 `show user group name <group name>` 命令。
- 先確認使用者存在於群組中，再於安全性政策中使用該群組。若要驗證您目前可在政策規則中使用的群組，請使用 `show user group` CLI 命令。
- 如果您變更群組對應，則請手動重新整理快取。若要手動重新整理快取，請執行 `debug user-id refresh group-mapping all` 命令。

動態使用者群組的 User-ID 最佳做法

動態使用者群組可讓您回應使用者行為、業務需求或潛在威脅變更，而不需要手動變更政策或是建立和更新群組。動態使用者群組可協助您建立所提供的安全性政策：

- 使用者的時間繫結資源存取權
- 自動修復異常使用者行為和惡意活動，同時保持使用者洞察性

在您使用標籤來定義群組準則並提交變更之後，會根據使用者標籤來自動更新動態使用者群組的成員資格。

規劃動態使用者群組部署的 User-ID 最佳做法

- ❑ 根據業務需求或使用者行為變更這類因素，識別您想要防火牆如何控制使用者存取權：
  - ❑ 您是否想要透過安全性政策來允許或限制存取權？
  - ❑ 您是否想要針對使用者要求 MFA？
  - ❑ 您是否想要解密使用者流量以更深入查看使用者活動？
- ❑ 判定使用者在特定動態使用者群組中的成員資格持續時間。
  - ❑ 防火牆是否應該根據時間（例如，承包商存取臨時資源所需的時數）自動從群組中移除使用者？
  - ❑ 防火牆是否應該需要特定事件才能產生或取消使用者與群組的關聯（例如，惡意活動）？
- ❑ 評估由防火牆產生而且可以識別使用者行為或業務需求變更的事件。您可以透過 API、自動標籤或手動使用網頁介面來指派標籤。
  - ❑ 根據您的使用案例，判定您將用來將使用者群組在一起的標籤，以及您將如何產生標籤。
  - ❑ 例如，根據安全性裝置和應用程式洞察來評估根據高風險、中風險和低風險這類行為的使用者風險層級，並根據這些事件自動將標籤指派給使用者。
- ❑ 識別標籤的使用者資訊來源：
  - ❑ 防火牆日誌
    - 對於驗證、資料、威脅、流量、通道檢查、URL 和 WildFire 日誌，建立日誌轉送設定檔，然後使用內建動作。
    - 對於 User-ID，HIP 匹配，GlobalProtect 和IP-Tag 標籤日誌，請設定日誌設定。
  - ❑ Cortex XSOAR
  - ❑ 安全性資訊和事件管理系統 (SIEMS)，例如 Splunk
  - ❑ 自訂 API 指令碼
- ❑ 合併多個來源的標籤，以定義動態使用者群組的準則。例如，建議您只有在接收到來自多個根據信任層級而已危害使用者認證之安全性應用程式的警示時，才拒絕使用者存取權，而不只是單一應用程式。

使用 User-ID 最佳做法部署動態使用者群組

- ❑ 如果您有大量使用者想要新增至動態使用者群組，或者想要根據來自其他安全性應用程式的事件來新增使用者，請使用 API 來新增使用者，而不是網頁介面。
- ❑ 使用 API，或手動定義 **Timeout**（逾時），以代表何時從此群組中移除使用者（例如合約到期時）。
- ❑ 建立安全性政策規則，而這些規則使用動態使用者群組作為來源使用者來控制使用者存取權、啟用 MFA，或解密作為動態使用者群組成員之使用者的流量。
- ❑ 設定來源來提供使用者標籤的資訊：
  - ❑ 如果您使用防火牆日誌，則請設定自動標籤來標籤使用者。
  - ❑ 如果您使用 Splunk，則可以使用 Splunk 的 Palo Alto Networks 應用程式將標籤指派給使用者。
  - ❑ 在 Cortex XSOAR 或其他 Security Orchestration, Automation, and Response (SOAR) 平台中使用劇本，以根據特定事件將標籤套用至使用者。
  - ❑ 如果您使用自訂指令碼，則請使用 API 修改指令碼來填入標籤。

- 使用防火牆的網頁介面，手動將使用者新增至群組。

使用 User-ID 的動態使用者群組後部署最佳做法

- 檢閱群組成員資格，確定只有您想要包含的使用者才是群組成員。如果群組包含不屬於群組的使用者（例如，「contractor-access」群組中的永久員工），則請**Unregister Users**（取消註冊使用者）以移除其使用者名稱至標籤對應，並將它們從群組中 **Delete**（刪除）。
- 檢閱 User-ID 日誌，確認防火牆已正確產生使用者的標籤。
- 使用 CLI 命令，進一步了解動態使用者群組（例如，查看哪些使用者與群組相關聯）。
- 使用流量和威脅日誌上的動態使用者群組欄，確定防火牆符合預期安全性政策群組。
- 將使用者標籤重新散佈至其他防火牆，確保所有防火牆都持續套用安全性政策。請記住，您可以只為一個躍點重新散佈使用者標籤。