

# UNIX特權存取套件

簡化UNIX安全性與管理並符合法規遵循要求

## 效益

- 簡化跨越不同環境的身分識別與存取管理
- 將UNIX身分識別管理統合到 Active Directory之內
- 強制實現最小權限存取
- 彈性的UNIX授權能力
- 從一個單一控制台執行全面的管控
- 讓整個UNIX環境輕鬆符合資料法規與稽核需求
- 跨越UNIX/Linux伺服器的集中化政策管理

## 系統需求

完整系統需求資訊請參觀  
[oneidentity.com/privileged-access-suite-for-unix](https://oneidentity.com/privileged-access-suite-for-unix)

UNIX 系統 ( 包括 Linux 和 Mac OS ) 本質上在安全性和管理方面面臨著不同的挑戰，這是因為基於本地的 UNIX 系統並沒有相互連結，因此每一台伺服器或作業系統執行個體 (instance) 都需要各自的認證與授權源，包括透過 root 帳號執行的 superuser authorization。

若欠缺有效管理跨越 UNIX 和 non-UNIX 系統身分識別，以及控制和稽核 root 帳號使用情況的方法，組織將因此呈現不連貫、沒效率且高度不一致的管理狀態，其可能會帶來潛在的災難性安全風險。

Privileged Access Suite for UNIX 是 One Identity 產品的一部分，它解決了 UNIX-based 系統的這些固有安全與管理問題，同時協助企業輕易滿足資料法規要求。它統合身分識別，分配個人歸責，以及提供集中化的 UNIX 使用者和管理者存取報告。

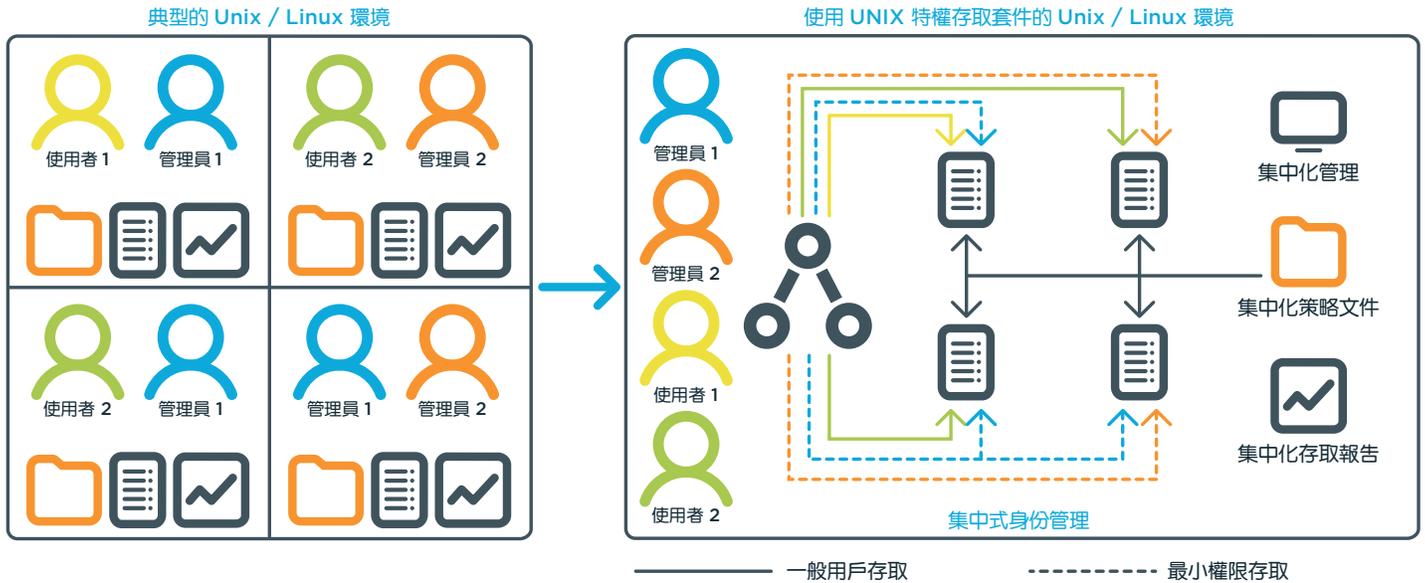


Figure 1 –Privileged Access Suite for UNIX 統一和整合身分，同時提供根據單一策略文件的個人權限歸責和最小權限存取，以及跨整個 UNIX / Linux 環境的集中報告。

Privileged Access Suite for UNIX 是一套完整的 UNIX 安全方案，在一個統合的控制台結合了 Microsoft Active Directory bridge 和 root 授權方案，為企業提供集中化能見度並簡化整個 UNIX 環境的身分識別與存取權限管理。

### Active Directory 橋接方案

Privileged Access Suite for UNIX 利用 Active Directory 橋接方案將 Active Directory (AD) 的統合認證與授權延伸至 UNIX、Linux 和 Mac OS 系統。Authentication Services 是 One Identity 的 AD 橋接方案，捨棄本地 UNIX 的獨立認證與授權要求，以支援源自 Windows 系統 AD 的單一身分識別、單一帳號、單點管理。透過一個管理良善的單一帳號，UNIX 系統在功能上成為 AD 內的「完整公民」，可改善身分識別生命週期管理效率，並藉由 AD 的認證功能讓 UNIX 可以利用安全的 Kerberos 認證以強化安全性。

### Root 授權

Privileged Access Suite for UNIX 提供二種不同的 UNIX root 帳號授權方式。它讓你可以配合需求而選擇強化或取代 sudo。如果你選擇以 Privilege Manager for Sudo 來強化 sudo，你將可以保有熟知的每一項功能，同時享有諸多強化能力，包括一個中央政策伺服器、集中化管理、有關存取權與活動的集中化報告、以及對透過 sudo 執行的活動進行鍵盤側錄等。

如果選擇以 Privilege Manager for UNIX 取代 sudo，你仍可以根據集中化存取權政策報告來執行 UNIX root 授權，但是擁有較細緻分級的權限，並且從使用者登入的那一刻開始就可以側錄所有鍵盤活動，而不是只有側錄那些前置 "su" 的指令。此外，這個選項能夠藉由限制 shell 和遠端主機指令執行進一步強化安全性，同時強化二進碼以避免迴避偵測而提高存取權限。

### 功能

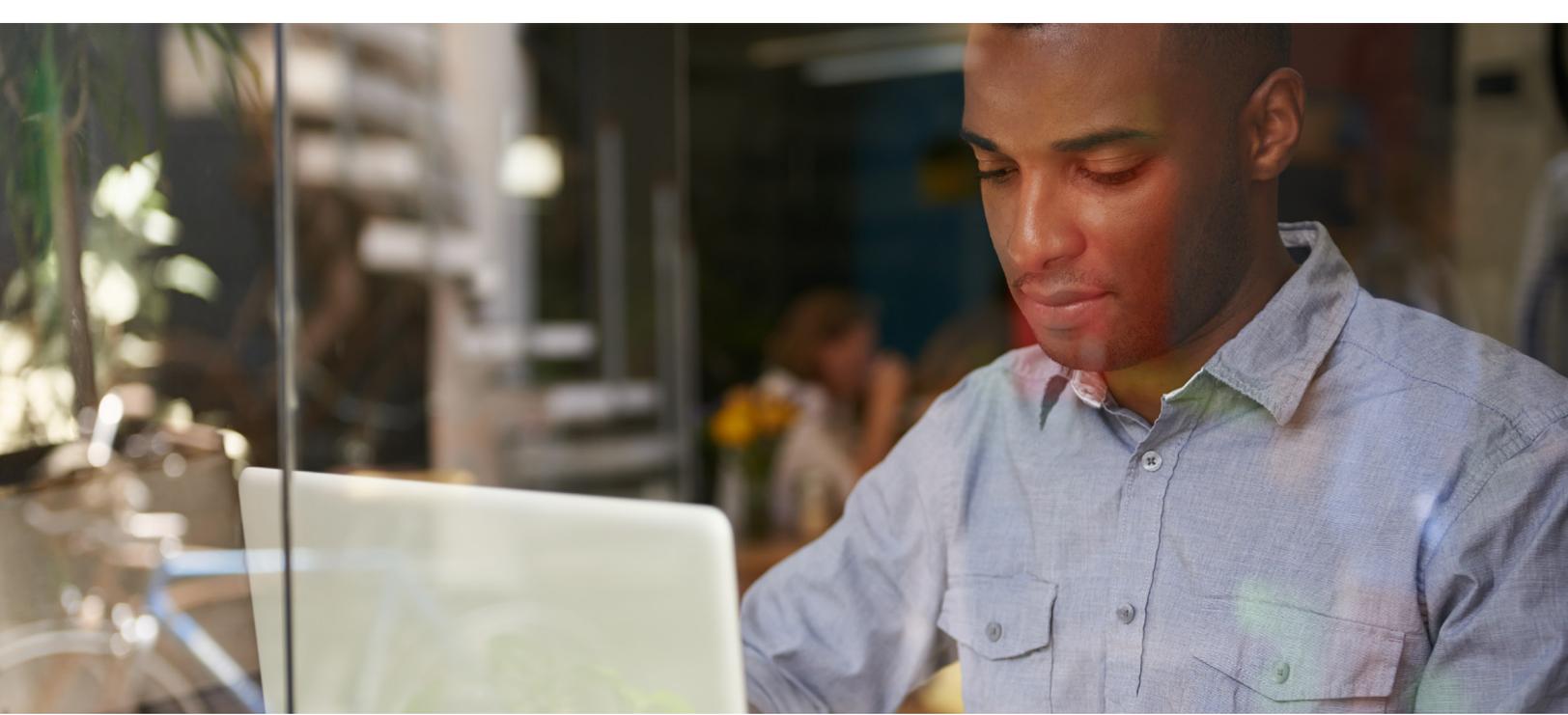
**統合身分識別** – 統合 UNIX 帳號以簡化身分識別管理，透過 Active Directory 和一個單一 AD identity 建立集中的 role-based 存取管理。

**最小權限存取** – 僅授予管理者工作執行所需的足夠權限，避免過多存取權限而產生風險。每一位管理者只被授予工作所需的權限。

**集中化管理** – 涵蓋整個 UNIX 環境的存取政策集中化組態與執行。

**Sudo 報告** – 輕鬆報告 sudo 存取權，解決企業在 sudo 支援上的最大難題之一。終端使用者的作業方式不會有任何改變，意即不需要新的訓練，只是簡化存取報告以配合稽核與法規遵循要求。

**全方位能見度** – 以一個單一控制台提供有關 UNIX/Linux 活動的整合、完整控制與能見度。輕易掌握何人建立一個存取政策、其內容為何、以及何時生效等。



此外，Privileged Access Suite for UNIX 是唯一提供個人 sudo 存取權集中化報告的方案，同時也是綁定使用者 AD 帳戶資料的企業授權方案。

**信任而驗證** – 為符合法規遵循與安全需求的活動和權利提供個人權限歸責和能見度。稽核能力包括政策報告、權限報告與歷史、變更追蹤與回溯、以及鍵盤側錄。

**單一登入** – 使你能夠在整個 UNIX、Linux 和 Mac OS 環境，以及基於關鍵標準的應用程式（如 SAP、Siebel 等）上實現「真正的」單一登入。

#### 詳細資訊

關於 Privileged Access Suite for UNIX 詳細資訊請參觀 [oneidentity.com/privileged-access-suite-for-unix](http://oneidentity.com/privileged-access-suite-for-unix)

#### 關於 One Identity

One Identity 身分識別與存取管理 (IAM) 系列方案提供符合真實世界需求的 IAM 技術，包括以商務為中心、模組化與整合、以及未來成長彈性，協助建立最佳的身分識別管理、存取管理與特權管理。

詳細資訊請參觀：[OneIdentity.com](http://OneIdentity.com)