DATASHEET

One Identity Safeguard Authentication Services

次世代 Active Directory 橋接技術

優點

- 藉由讓 UNIX、Linux 和 Mac OS X 系統做為 “full citizens” 加入 Active Directory 來消除複雜性
- 整合啟用 AD 的系統和 AD Bridge 的管理
- 提供嚴格的身分認證作為 AD Bridge 解決方案的一部分
- 提供集中式身分認證和單一登入 (SSO)
- 促使所有系統和使用者遷移到單一的以 Active Directory 為基礎的架構上
- 簡化安全性和合規性的執行程序

簡介

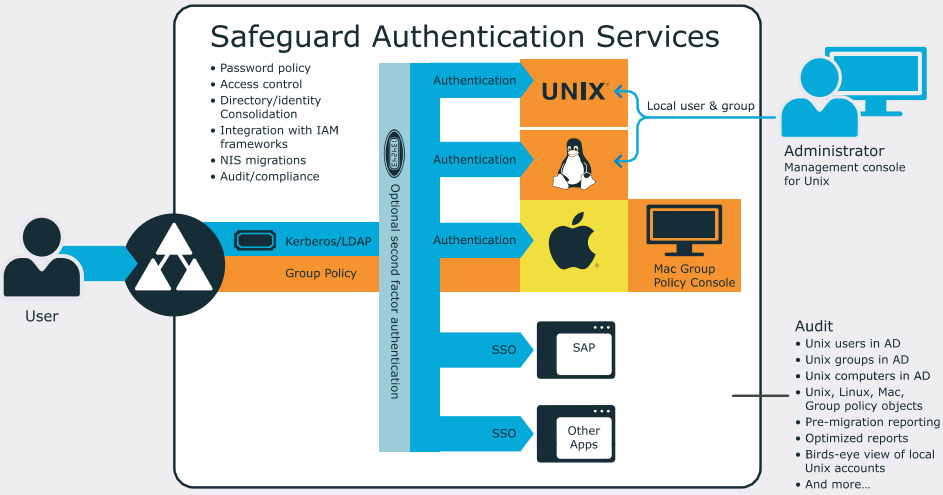
One Identity Safeguard Authentication Services 利用組織既有的 Active Directory (AD) 基礎架構，為 UNIX、Linux 和 Mac OS X 系統提供企業範圍內的存取、認證及授權。Safeguard Authentication Services 的專利技術可讓非 Windows 資源成為 AD 受信任領域的一部分，並將 AD 的安全性、合規性和認證功能延伸到 UNIX、Linux 和 Mac OS X 上。

擁有近 1,500 個客戶和超過 500 萬個已部署授權的 Safeguard Authentication Services，毫無疑問的是 Active Directory Bridge 市場的領導者。Safeguard Authentication Services 提供的功能性、靈活性和整合範圍，可以滿足最複雜和要求最嚴格的異構全球組織的需求。

管理 AD Bridge 的工具

Safeguard Authentication Services 具有強大且靈活的 UNIX 工具程式，以及靈活的部署選項。它包含一系列用於建立和管理 AD Bridge 的強大工具：

- 產品配置和授權
- 可幫助初始設定和整合 AD 系統的指南手冊
- 廣泛的遷移和部署選項
- 提供遷移前評估和事前準備的 NIS 遷移工具



Safeguard Authentication Services 在本地端的 Unix 和 Linux 系統上實施 Kerberos、LDAP 及單一登入，其實施方式與在 Windows 中的方式相同。

> **“整體而言，安裝 One Identity 軟體產品可以有效的減少停機時間，且每年幫銀行節省了大約 100 天的人力工作日。”**
>
> Alexander Nesterenko, IT 支援部門副主管

- 群組原則及本地 UNIX 使用者和群組管理工具
- 簡單且合規的稽核和報表
- 針對非 Windows 系統嚴格的身分認證

嚴格的身分認證

Safeguard Authentication Services 的授權包括強大的 AD-based、一次性密碼 (OTP)，以及所有支援的 UNIX、Linux 和 Mac OS X 平台的嚴格的身分驗證。 此外，Safeguard Authentication Services 將以 Windows 為基礎的智能卡延伸到 UNIX 和 Linux 以及支援第三方 OTP 解決方案上。

稽核、告警和變更追蹤

Safeguard Authentication Services 可收集稽核員所要求的重要資料。Safeguard Authentication Services 讓您能進行稽核、告警，以及提供被 Active Directory 所管理的、以 UNIX 為中心的管理資訊的詳細變動歷史紀錄。

合規性

Safeguard Authentication Services 採用和 AD 相同的行業標準，為多重身分儲存和身分認證，以及不合規的目錄 (如：NIS) 提供合規替代方案。Safeguard Authentication Services 還可以快速輕鬆地收集稽核人員所需的關鍵資訊，並為非 Windows 系統無縫促成嚴格的身分認證。

遷移

理想情況下，大多數異構組織都希望將其所有系統整合到一個安全且強大的目錄中。藉由簡化將 UNIX、Linux 和 Mac OS X 系統和使用者整合到 AD 網域的過程，Safeguard Authentication Services 可以幫助您快速實現此目標。Safeguard Authentication Services 也有助於從多個身分認證機制、身分和目錄的情況中，快速且準確地遷移到單一 AD-based 的基礎架構。功能包括：

- 使用者對映模式為完全遷移提供了一個更好的替代方案。它允許按照自己的節奏進行遷移，同時快速解決最緊迫的合規性要求。使用者對映模式使組織能夠在不影響 Active Directory 架構的情況下立即實現合規性。
- UNIX Personality Management 使用以預設 AD 模式為基礎所定義的標準模式屬性，建立備用的 UNIX “personalities” 為不同系統在 AD 中定義設定檔。
- Ownership Alignment 工具簡化了在遷移結束時解決使用者 ID 衝突的最後一個耗時的步驟。
- Safeguard Authentication Services 提供一系列的靈活工具來調整衝突檔案的所有權。讓您在主要遷移到 AD 之前、期間或之後能快速重新調整使用者命名空間的衝突。
- 完整的 RFC 2307 NIS Map Support 為使用者將其 NIS 基礎架構遷移到 Active Directory 的 RFC 2307 NIS 映射提供全面支援，使他們能夠完全淘汰現有的 NIS 基礎架構。RFC 2307 支援先進的 NIS 映射匯入精靈、Windows 的 NIS 映射編輯器，以及 Safeguard Authentication Services NIS proxy 中的完整 RFC 2307 支援。
- UNIX 帳號匯入精靈可將使用者和群組從 NIS、本地檔案或遠端 shell 等來源匯入 personalities。UNIX 帳號匯入精靈也可讓您從彈出視窗中選擇複雜的匹配標準 (用於連接到主要帳號)，大大簡化了將使用者遷移到 AD 的繁瑣工作。

企業的群組原則

Safeguard Authentication Services 提供了一個容易實施、無限擴充、本機整合擴展到 UNIX、Linux 和 Mac OS 系統的 Windows Rights Management Service Group Policy。透過此框架，您可以利用產品內建既有的群組原則進行擴充，或在簡單的 ADM 模板方法的基礎上開發自有的，或者擴充更強大的客戶端功能。Safeguard Authentication Services 包含通用腳本、檔案複製和自定義，以及強大的預包裝群組原則和靈活的政策管理。此外，Safeguard Authentication Services 利用現有的 Windows 安全性原則，使 AD 對 UNIX、Linux 和 Mac OS X 存取控制具有完全權威性。Safeguard Authentication Service 對於 Mac OS X 系統也擁有一個強大的群組原則介面。此介面提供對整個 Mac 策略和優先權的控制，也包括透過偏好清單整合第三方應用程式的支援。Safeguard Authentication Services 還可以對群組原則物件的異動進行稽核和追蹤。

適用於 UNIX、Linux 和 Mac OS X 的 Active Directory

Safeguard Authentication Services 將既有的 AD 基礎架構無縫延伸到企業的其他部分。Safeguard Authentication Services 本機整合了 UNIX、Linux 和 Mac OS X 系統，允許它們能夠在 AD 中做為 "full citizens" 行動，並從 AD 的安全性和合規性優勢中獲得好處。主要功能包括：

- 將 AD 密碼策略延伸到 UNIX、Linux 和 Mac OS X
- 支援最複雜的 AD 環境，包括多重網域、跨樹系信任和巢狀群組
- 為 UNIX、Linux 和 Mac OS X 使用 AD AES 128 加強性加密 (128 位密鑰) 以提高安全性
- 將 UNIX 系統與 AD 時間同步
- 支援 RFC 2307 架構定義
- 支援自定義架構配置以及沒有擴充的 pre-R2 架構的實施選項

集中身分認證和單一登入

Safeguard Authentication Services 在本地端的 Unix 和 Linux 系統上實施 Kerberos 和 LDAP，其方式與在 Windows 中的實施方式相同。 此外，它還提供了單一登入 SAP，這是一個強大的應用程式介面 (API)，允許您將單一登入功能添加到內部開發的應用程式中，以及為許多普及的應用程式 (如：DB2、PuTTY、Samba 和 Apache) 建立單一登入的指南手冊。

集中存取控制

Safeguard Authentication Services 使您能夠使用多個選項配置存取規則：

- 本地、以檔案為基礎的存取清單來決定使用者可以在 UNIX 和 Linux 機器上存取哪些內容 (降低至個人服務的級別)，並進一步透過群組策略集中管理這些存取清單
- UNIX Personality Management 藉由為一組特定的電腦主機定義使用者命名空間來幫助控制存取
- Windows 安全性原則和使用者工作站功能可以為 AD 中的 UNIX 電腦物件提供精細的、per-user 的存取控制

簡化身分管理

Safeguard Authentication Services 使您能夠透過現有的 AD 投資去簡化身分管理。使用 Safeguard Authentication Services，可以將來自其他供應商的以 AD 為基礎的身分管理解決方案 (包括用於配置、密碼管理、嚴格的身分認證、特權帳號管理以及審核和報表的解決方案等)，自然地延伸到非 Windows 系統。Safeguard Authentication Services 可以和既有的 IAM 框架搭配使用，以減少需要自定義整合和單獨管理連接器的系統數量。支援廣泛跨平台的 Safeguard Authentication Services 為 Solaris、IBM AIX、HP-UX、SUSE、RedHat、Fedora、VMware 等普及化的 UNIX、Linux 和 Mac OS X 平台提供集中式身分認證支援。更多完整的支援平台清單請參考

oneidentity.com/Safeguard-Authentication-Services

關於 One Identity

One Identity by Quest 幫助組織在內部部署、雲端或複合式環境中實施以身分識別為中心的安全性策略。憑藉其獨一無二、廣泛的身分和存取管理產品組合，包括帳號管理、身分治理與管理、特權存取管理，組織可充分發揮自身潛能，並以身分識別做為計畫核心，啟用對所有使用者類型、系統及資料的適當存取權，藉此達成安全性目標。更多詳細資訊請至 OneIdentity.com

Datasheet_2020_SG-AuthServices_RS_60344