semperis

ACTIVE DIRECTORY 樹系修復

Active Directory 的網路優先災害修復。

Active Directory 修復的需求已變更。當勒索軟體或抹除式攻擊破壞網域控制站時，傳統的修復流程可能會耗個數天甚至數週。Semperis 精心設計了一套完全自動化的樹系修復流程——避免人為錯誤、將停機時間從幾天至幾週降至幾分鐘，並消除惡意程式碼再次感染的風險。

網路優先的災害修復

即使網域控制站被感染或抹除也能復原 AD

隨處修復

將 AD 還原至備用硬體 （虛擬或實體）

無害還原

從系統層備份消除惡意程式碼，避免再次感染

進階自動化

將整個修復流程自動化，並減少停機時間

處理無法想像的狀況

AD 停機：員工無所事事、作業停滯不前、客戶陷入困境。威脅是真實的：

- 勒索軟體或抹除式攻擊破壞您的網域控制站（DC）
- 駭客獲得存取權限，而損壞程度未知
- 惡意系統管理員掌控了目錄服務
- 架構擴展、樹系層級升級，或其他不可逆的變更導致目錄無法操作

無論是什麼原因，您都需要立即(在相同或不同的伺服器上)還原AD。且不能有任何殘留的惡意程式碼或不良行為者，造成對您的網路嚴重破壞。

修復 受攻擊後的企業營運（不要只是重啟）

在網路攻擊之後，企業經常爭先恐後地恢復營運。但假如缺乏一套完整、經過全面測試的 Active Directory 修復流程，系統將容易再次受到相同類型的攻擊，讓組織率先陷入停頓。Semperis 的 ADFR 確保完整、快速、無惡意程式碼的 AD 修復。

semperis

將整個 Active Directory 樹系的修復時間縮短 90%

在過去的美好日子裡，Active Directory 中斷僅限於自然災害或操作錯誤時發生。考慮到與自然災害相比，網路攻擊造成更大破壞，襲擊也更頻繁，現在是思考「網路優先」的時候了。您的災害復原教戰手冊能否處理這個現實問題？Semperis 做到了。
利用 Semperis 的專利技術，即使是最災難性的 AD 災害，您也能迅速且自信地修復。

圖 1.0——ADFR 修復選項

Semperis 的優勢

必須從頭開始修復 AD 的想法已失去理論基礎。現在它絕對是事件應變規劃的一個關鍵部分。樹系修復並非輕鬆的任務，而且 Semperis 的 AD 專家已正面迎接挑戰。為此，Semperis 的 ADFR 提供獨有的功能。

全球 500 強零售商

「Semperis 正是我期盼在 AD 復原工具中所提供的。多年來，我對樹系修復有許多疑慮，而 Semperis 公司解決了所有這些問題。」

——InfoSec 身分識別和目錄負責人

semperis

隨處修復

將 AD 還原至任何虛擬或實體硬體——無論內部部署或雲端中。

無害還原

為防止再次引入 Rootkit 和其他惡意程式碼，ADFR 從乾淨的 Windows 作業系統開始，並僅還原作為 DC、DNS 伺服器等伺服器角色所需的內容。

進階自動化

將整個修復流程自動化，包括還原 DC、重建通用類別目錄、清理中繼資料和 DNS 命名空間、重組站台拓撲的結構、重新升級 DC 等。

零維護

消除開發和維護指令碼或手動更新設定資訊的需求——以及當這些事情未完成時所發生的復原失敗。

備份完整性

檢查每個備份組，確認其包含成功修復樹系所需的所有資料，以及該資料已成功寫入一個或多個位置。還會通知您備份工作中的任何缺口。

不共享的結構

獨立於 AD 執行——不依賴 Windows 驗證、DNS 或其他 AD 服務——因此即使 AD 完全停機，您也可以立即修復。

輕量的 AD 備份

僅備份 AD 元件。這導致備份規模較小，意味著要擷取、處理和傳輸的資料更少——並且在還原期間執行這些作業的時間更少。

簡單的 DR 測試

在隔離的實驗室中使用可用的伺服器，編製生產 AD 樹系的精確複本，便可輕鬆地測試修復程序，並記錄結果，以遵守內部和外部法規。

多樹系支援

使用單一管理伺服器和入口網站管理多個 AD 樹系的備份和復原，簡化設置和持續管理。

POWERSHELL 支援

包含自動化 Semperis ADFR 管理的 PowerShell 指令，更方便管理備份群組、備份規則、代理程式，以及發佈點。

實驗室設置

Semperis AD 樹系修復`還可以輕鬆地在實驗室中產生 production DC 的副本，大大減少維護開發 / 測試、預備、訓練和支援環境的時間。

分散式備份故障移轉

利用發佈點伺服器，在網域控制站附近儲存備份，減少網路流量及備份和修復時間。

安全的備份加密

為備份組中每個 DC 產生一個獨特的一次性加密金鑰——防止攻擊者使用單一金鑰解密所有備份。更顯示哪些備份規則已啟用加密。

SAML 驗證

支援使用 SAML 的單一登入（SSO），將使用者登入頻率降至最低——使用者可使用他們選取的 IdP 認證登入系統管理入口網站。

進階搜尋

利用進階搜尋功能簡化作業記錄檔記錄擷取，有助您按屬性進行篩選，例如特定日期範圍的元件等。

Active Directory 是網路攻擊的主要目標。利用 Semperis，確保您可迅速且熟練地復原。

立即與我們連絡以獲得免費試用。

semperis

全球 500 強零售商

一切都以 ID 和密碼開始。您需要率先修復的，是進行其他任何類型修復的認證。

——沃爾瑪公司前資訊安全長（CISO）克里·基爾克（Kerry Kilker）

航空公司

「Semperis 平台幫助以色列航空公司達到一個我們確信能夠克服任何 Active Directory 中斷的境界。」

——以色列航空公司基礎建設副處長

Semperis
IT 防衛協調流程

5 ★★★★★

資料來源：Gartner Peer Insights 平台

info@semperis.com
www.semperis.com

Semperis 公司總部
221 River Street 9th Floor Hoboken, NJ 07030

+1-703-918-4884

semperis

對於負責保護混合式和多雲端環境的安全性團隊，Semperis 在網路殺傷鏈的每個步驟中確保關鍵企業目錄服務的完整性和可用性，並將復原時間縮短 90%。Semperis 的專利技術專為確保混合式 Active Directory 環境的安全而組建，保護超過 4,000 萬個識別身分免於網路攻擊、資料外洩和操作錯誤。世界一流的組織都信賴 Semperis 可發現目錄漏洞、攔截進行中的網路攻擊，並從勒索軟體和其他資料完整性緊急情況中迅速復原。Semperis 總部位於紐澤西州，營運遍佈國際，其研發團隊分佈在舊金山和特拉維夫之間。

Semperis 主辦備受讚譽的混合式身分識別保護會議。本公司已獲得業界最高榮譽；最近被《SC 雜誌》 2020 年信任獎評為最佳業務連續性 / 災害復原解決方案。Semperis 已獲 Microsoft 官方認證及高德納公司（Gartner）認可。

Microsoft Partner
Enterprise Cloud Alliance

企業雲端聯盟
Microsoft 加速器校友
Microsoft 共同銷售