特殊權限使用者癱瘓 ACTIVE DIRECTORY 的三種方法

以及將風險降至最低或大幅提升復原能力的八種方法

Quest

引言

警世故事

UBS Paine Webber IT 管理員 Roger Duronio 不滿他的獎金，於是寫了 50 行程式碼，透過用來將合法檔案放入公司電腦的標準 Unix 系統管理工具，放入公司網路的上千部電腦。

接著便辭職。

但他的邏輯炸彈沒跟著他走。程式碼盡責倒數了幾週，讓 Duronio 有時間花 2 萬美元賣空 UBS/PW 股票。然後一天早上這顆炸彈就爆炸了。裝載據說爲「rm -rf /」，表示刪除「所有東西」。

那只有一片混亂能形容。UBS/PW 不得不以紙筆進行交易。他們光是諮詢費就給了 IBM 300 萬美元，使用備份來復原系統。總金額更是令人不敢想像。

關於本文件

這只是 心懷怨懟 或粗心的特殊權限使用者如何 能造成大災難的其中一個例子。

事實上，這在 Windows 環境中非常輕易就能 辦到， 因爲每件事都仰賴 Active Directory (AD)。即便伺服器和應用程式都沒問題，但只要 Active Directory 故障，整個網路都會故障。

有多簡單呢？ 本電子書只介紹衆多方法中的三種方法，說明特殊權限使用者 (或者該說具有偷來特殊權限憑證的攻擊者) 如何能癱瘓 AD，進一步癱瘓網路其他部分。

接著會探討八種重要的最佳作法，有助於減少這類風險，並提升最糟情況下的復原能力。

特殊權限使用者癱瘓 AD 的三種方法

方法 1：拒絕登入權限

使用者可透過五種方法登入 Windows：本機、從網路、以批次工作、以服務方式，以及透過遠端桌面服務。每種登入方法都有一對登入權限，一個用以允許登入，另一個則是拒絕登入。

以正確方式指派五種拒絕登入權限，特殊權限使用者便能停止系統運作：

- 使用者無法登入自己的工作站。
- 系統管理員無法使用網域控制站，或甚至是使用主控台本機鍵盤和畫面。
- 服務帳戶無法登入。
- 應用程式無法啓動。

這造成進退兩難的狀況：因無法使用網域帳戶登入，就無法遠端修復問題。因此您必須實際存取您的 DC，才能重新開啓 DSRM，並透過 DSRM 進行復原作業。

以正確方式指派拒絕登入權限，特殊權限使用者便能停止系統運作：

方法 2：癱瘓 DNS

Active Directory 使用 DNS 當成找到網域控制站 (DC) 的機制。每個 Windows Server 2003 或更新版本的 Active Directory 網域都有 DNS 網域名稱，而每部執行 Windows Server 2003 或更新版本的電腦也都有 DNS 名稱。

要癱瘓您的 Active Directory，特殊權限使用者要做的，就是刪除一個 DC 的所有 DNS 項目。這些變更很快就會透過快取的 DNS，複寫到其他所有 DC 。接著 DNS 快取就會逾時，所有人就會突然找不到任何東西。更明確地說，工作站就無法透過 DNS 找到網域控制站。工作站會求助 NetBIOS 名稱解決方案，但可能沒用。

如果 DNS 故障，一切都會故障。

Quest

方法 3：入侵作業系統漏洞

某天，使用 Windows Server 2008 的組織發現所有 DC 不斷重新開機。最後發現是特殊權限使用者進入子網路，不小心將 IPv6 設定改爲無效的 IP 位址。知識一致性檢查程式 (KCC) 複寫設定程序遇到無效設定時就會當機。這導致 DC 重新開機，但之後無效設定複寫到整個環境的其他 DC，導致所有 DC 開始不斷重新開機。

未知或未修補的漏洞可能會癱瘓您的 AD。

Microsoft 已修復這個問題，所以如果您仍使用 Windows 2008 或 2008 R2，務必安裝最新修補程式。但這不保證 沒有其他漏洞可能遭特殊權限使用者故意入侵或不小心犯錯，而導致同樣慘重的後果。

不只有心懷怨懟的內部人員

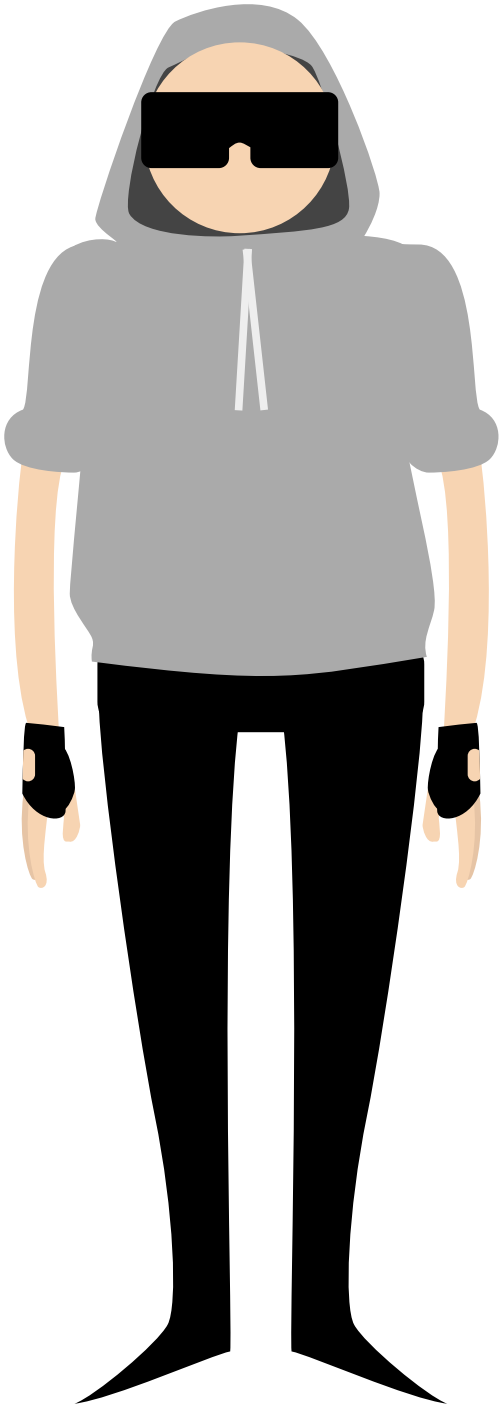
太多組織企圖宣稱他們沒有任何心懷不滿或惡意的特殊權限使用者會構成內部威脅，而不去想這些情況的風險。即便您可以保證真的沒有 (無論現在和未來)，您仍有風險，有兩個原因： 第一，即便最厲害的系統管理員也可能犯錯，如同剛剛談到的無效 IPv6 設定。第二，下列多種惡意威脅攻擊者發動的網路攻擊，可能會讓特殊權限憑證遭竊或不當使用：

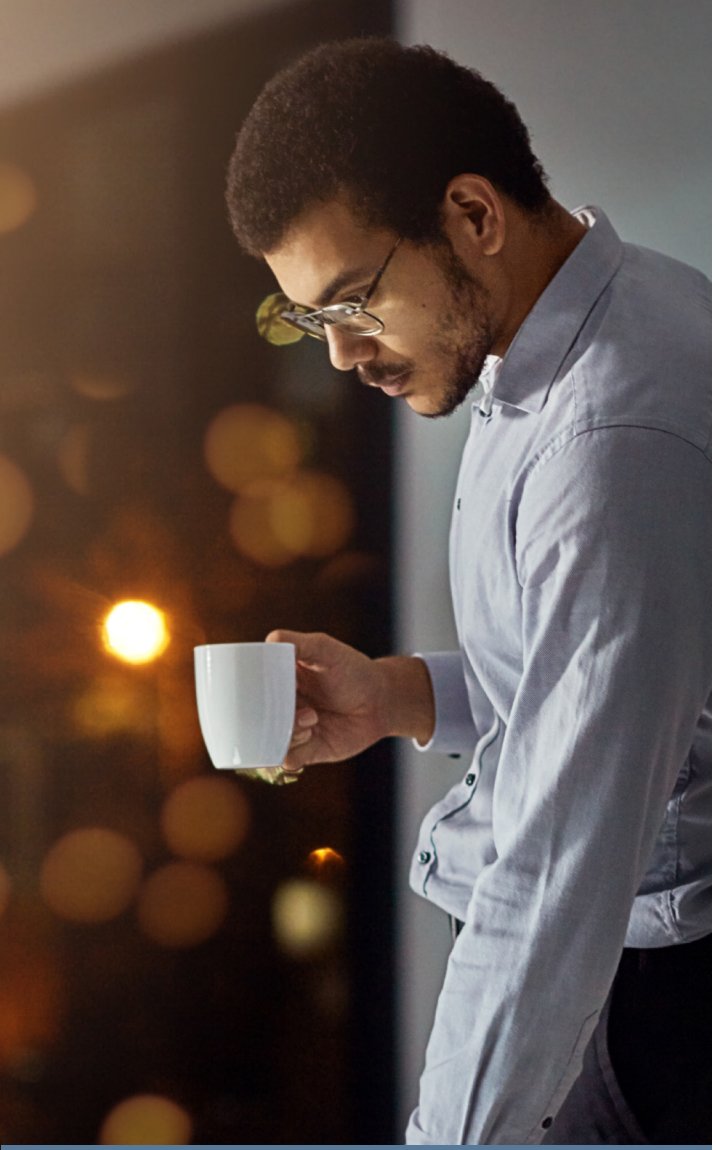
- 激進駭客
- 敵對國家指使的集團
- 競爭對手
- 受冤枉的人
- 虛無主義者

公司擔心由於使用者粗心、過失或憑證遭駭而導致資料外洩 (51%)，與擔心惡意內部人員造成資料外洩 (47%) 的程度差不多。

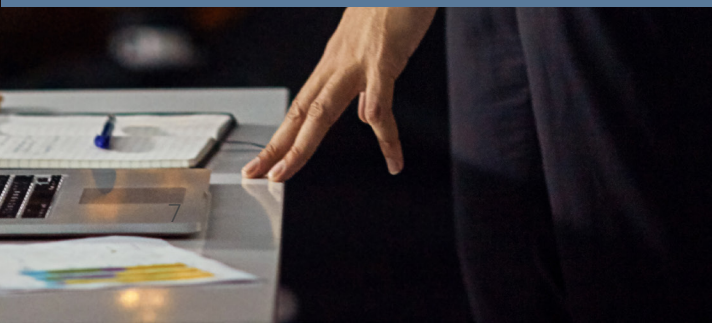
資料來源：*《2018 年內部威脅報告》(2018 Insider Threat Report)*，***Cybersecurity Insiders***

請注意，不是 所有 攻擊者都想要花時間和精力竊取您的資料， 有些只是想癱瘓您的服務並摧毀您的企業，這相對簡單得多。





嚴格控管特殊權限群組的成員非常重要。



八種 AD 安全性最佳作法

很明顯，特殊權限帳戶就是眞實存在的嚴重風險， 但您當然不能就這樣刪除這些帳戶，他們對維持系統運作非常重要。還好，您可以採取下列經證實有效的措施，降低特殊權限帳戶遭蓄意或非蓄意不當使用，並確保 這些 預防措施 要是 無效，能盡快復原。下列是可實作的八種重要最佳作法。

1. 限制特殊權限存取權限。

嚴格控管特殊權限群組的成員非常重要，其中包含下列群組：

- Domain Admins (網域系統管理員)
- Enterprise Admins (企業系統管理員)
- Schema Admins (架構管理員)
- Administrators (系統管理員)
- DHCP Administrators (DHCP 系統管理員)
- Group Policy Creator Owners (群組原則 Creator Owner)
- Domain Controllers (網域控制站)
- Network Configuration Operators (網路設定操作員)
- Server Operators (伺服器操作員)
- Backup Operators (備份操作員)

此外，請嚴密控管會影響網域控制站的群組原則物件 (GPO) 以及所有安裝於 DC 的軟體。例如，若安裝代理程式，可使用代理程式的用戶就可能是非常有用的網域系統管理員。

控管特殊權限存取權限最好的方式，就是使用完整特殊權限帳戶管理 (PAM) 和特殊權限工作階段管理 (PSM) 解決方案，再針對會影響整個網域的存取權限等級，搭配人工審核與即時監控。由於沒有人每天都得接觸網域控制站，因此所有活動都由兩人進行就非常實際：一位進行所有活動作業，另一位則負責監督。即便是遠端監控或由同事監控，都能減弱單獨犯案者能對您企業造成損害的能力。此外，改善責任歸屬及有兩雙眼睛盯著，可降低犯下代價高昂錯誤的風險。

Quest

2. 透過 RED FOREST 保護特殊權限帳戶。

要強化生產樹系至足以保護具有最高特殊權限的系統管理員帳戶，同時不影響網域運作，非常困難。因此，Microsoft 現在提供方法將這類帳戶存放在專屬系統管理樹系，正式名稱爲「強化安全管理環境服務」(Enhanced Security Admin Environment，ESAE)，俗稱爲「Red Forest」，「red」是得名於憑證的重要程度。

Red Forest 模型的重要特色是系統管理帳戶會分爲三個安全等級：

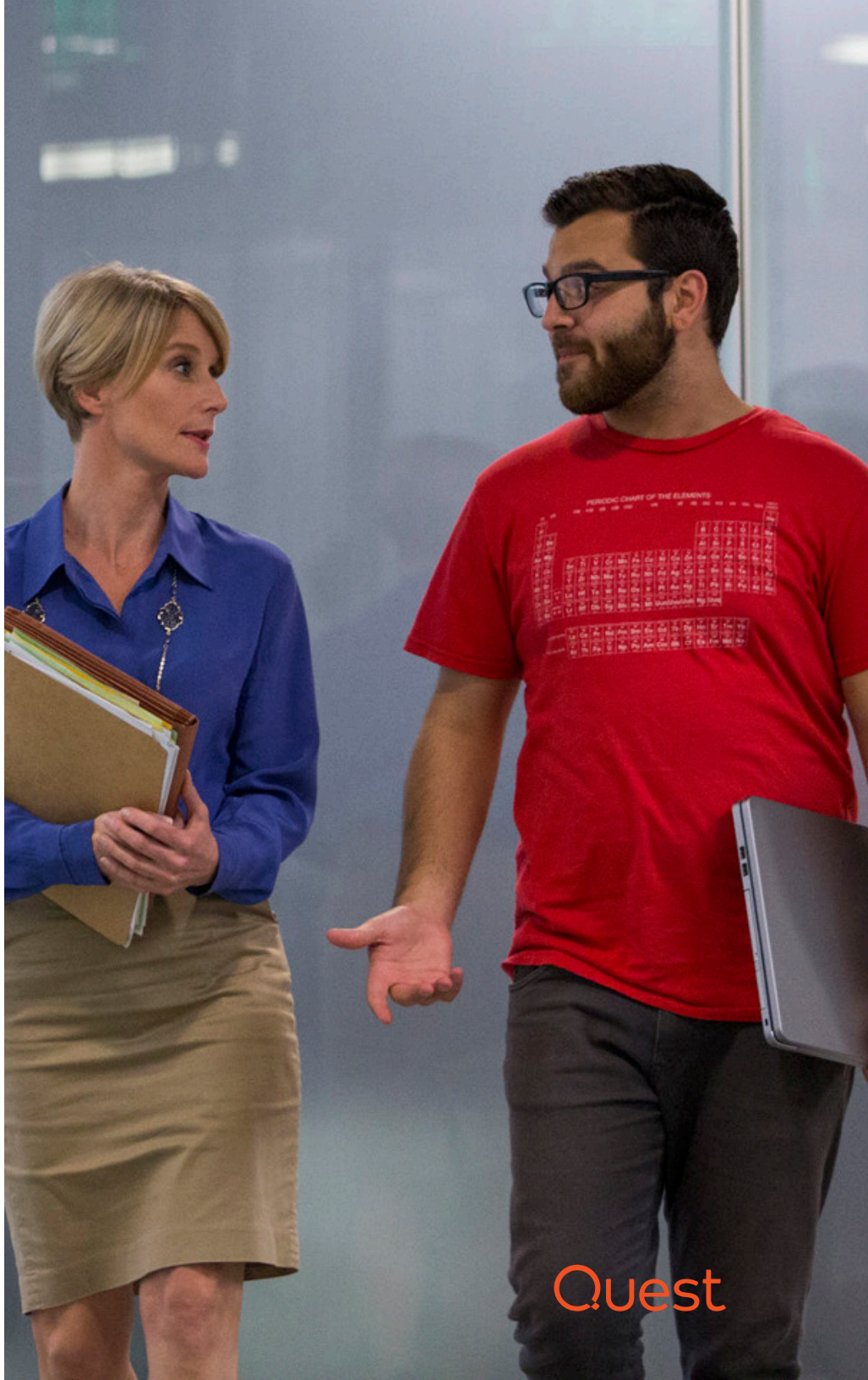
- **層級 0 —** 樹系等級系統管理員授權 (企業系統管理員)
- **層級 1 —** 伺服器、應用程式和雲端系統管理員授權
- **層級 2 —** 工作站和裝置系統管理控制權

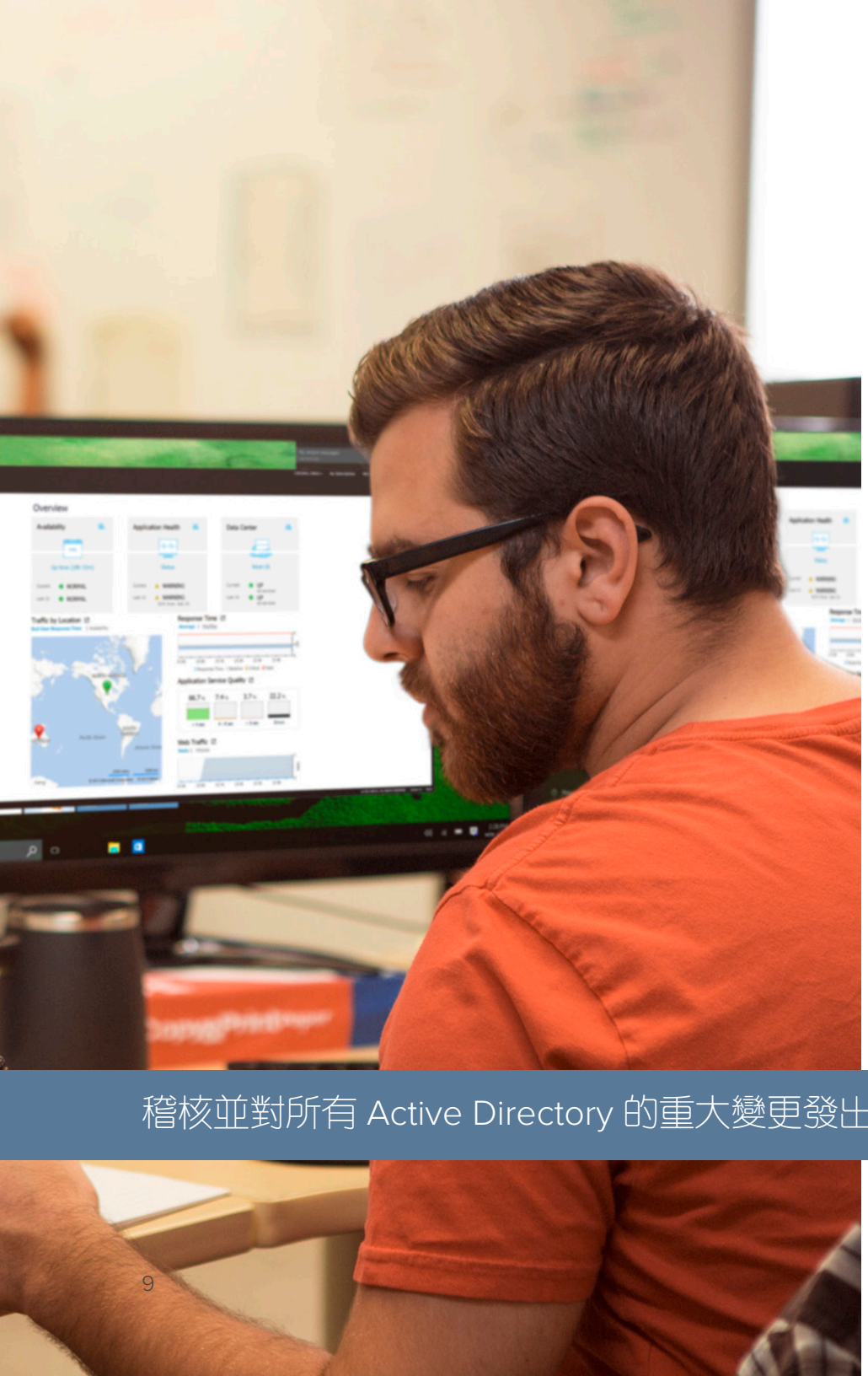
將所有層級 0 的帳戶放至個別樹系，可更輕鬆就近看照，並輕鬆套用其他安全性規定，例如要求帳戶從經強化的工作站或透過雙重驗證登入。

當然，部署系統管理樹系絕非小事一件。如需詳細資訊，請觀看錄製的網路廣播，安全專家 Randy Franklin Smith 會說明可能遭遇這個重大問題的原因，以及 Red Forest 模型的限制。

3. 先測試變更再投入生產。

若要降低失誤癱瘓 AD 的機率，請建立測試實驗室，查看升級或其他變更造成的影響，再投入生產環境使用。測試實驗室與生產環境越相似越好。





稽核並對所有 Active Directory 的重大變更發出警告。

4. 稽核。

全面稽核之所以重要有幾個原因。這有助於確保責任歸屬，可恫嚇內部人員的惡意行動，並讓 非惡意的 特殊權限使用者更加小心，降低錯誤發生數量和嚴重性。也可讓您快速判斷錯誤並採取修正行爲，同時知道如何不讓相同問題再次發生。

確保稽核記錄包含原生事件、應用程式系統安全性記錄、目錄服務記錄和其他重要資料，以及您可快速查看、搜尋和分析這些資料。同時確保 AD 故障時，仍可存取稽核系統。

5. 監控並對重大變更發出警告。

確保能立即得知重要物件有變更，例如會影響網域控制站的特殊權限群組或 GPO。由於這類變更不常見，因此您不會收到過多警告。合法變更警告是用於確認監控系統可運作， 而未經授權變更的警告，則讓您可快速應變，或許可及時阻止嚴重後果發生。

6. 記錄 AD 架構。

花點時間記錄 AD 架構。時時更新記錄，並儲存至離線位置 (如 Dropbox)，讓您在 AD 故障時也能存取。記錄務必包含下列資訊：

- 樹系
- 網域
- 信任
- DNS
- 這些物件間的子網路和複寫連結
- 每個網域控制站，包含其 IP 位址、實體位置、控制哪些網域、彈性單一主機操作，以及是否爲通用類別目錄

Quest

7. 備份 ACTIVE DIRECTORY。

使用企業備份解決方案備份 Active Directory。不要只用資源回收桶來復原。

請記住，資源回收桶只是方便而已。這個方法有多種嚴重限制，我們會在《Windows Server 2016 與 Azure AD 資源回收桶，以及 Quest 復原解決方案》(The Windows Server 2016 and Azure AD Recycle Bins, and Quest Recovery Solutions) 白皮書中加以探討。還記得我們先前提過，有人能刪除所有 DNS 記錄來癱瘓 AD 嗎？ 惡意使用者可能不會刪除 DNS 記錄，而是以無效 IP 位址取代設定。這樣一來，資源回收桶就無法幫您復原這些屬性。

8. 測試備份。

除非經認證可用，否則應該將備份視爲有所缺陷，這一點非常重要。請實際掛載備份並讀取其中物件，以確認備份可用。此外，請定期在測試環境重建 Active Directory 樹系，確保能快速從重大問題中復原。

使用企業備份解決方案備份 Active Directory，並測試備份是否可用。

結論

電話響起，一切都停止運作時，您還不知道發生什麼事或問題有多嚴重。可能 是 心懷不滿的內部人員剛採取行動破壞、 遭惡意軟體武器攻擊， 或者因無心錯誤導致 AD 癱瘓。

依照本文所列的最佳作法實作可降低這類令人不悅的情況發生機率，但仍沒有辦法完全消除風險。因此，您也須採取措施讓 Active Directory 能快速復原，這包含維持清楚而完整的稽核記錄，以及確認備份可用。

您大概聽過要在週末重建 AD 的可怕故事。復原 AD 不如復原刪除的檔案簡單。此外，也不易測試或模擬，部分是因爲正確的 AD 復原程序是依據個別災難情況而定。

但有合適的解決方案在手，按一下就能重建整個 Active Directory 樹系。若要深入瞭解，請參閱我們的《可怕的一天：Active Directory 災難與預防解決方案》(That Dreaded Day: Active Directory Disasters & Solutions for Preventing Them) 白皮書。

有合適的解決方案在手，按一下就能重建整個 Active Directory 樹系。

Quest

關於 QUEST

Quest 的宗旨是以簡單的解決方案解決複雜的問題。爲了達成此理念，我們堅持提供優異的產品和服務，並秉持簡單經營業務的整體目標。我們期望能爲您帶來兼顧效率與效益的技術，讓您和貴公司可以減少管理 IT 工作的時間，進而投入更多時間發展業務創新。

如果您對使用這份資料有任何疑問，請連絡：

Quest Software Inc.
收件者：LEGAL Dept
請參閱我們的網站 (www.quest.com)，以取得各地區及各國的辦公室資訊。

Ebook-3WaysToHoseYourAD-US-GM-zh_TW-WL-32410