TECH BRIEF

Active Directory 網域服務管理的 12 個基本任務

使用正確的工具和管理流程有助於減少管理開銷並能強化目錄服務的運作

摘要

Active Directory 網域服務 (AD DS) 已經是企業 IT 的核心基礎架構。管理 AD DS 包含了 12 個主要的任務，這些任務涉及了廣泛的企業 IT 業務需求，也因此能夠有效率的管理 Active Directory 對 IT 部門來說已經是一個重要的課題。管理 Active Directory 並不需要全部由 Active Directory 管理員執行。事實上，管理員可以並且應該將某幾項管理任務委託給其他管理人員或 Help Desk 人員，甚至用戶如行政助理、秘書等。委託管理是一種減少管理員在管理 Active Directory 時所需的工作量的方式，它只能解決 12 個任務中的一個或兩個任務，例如使用者和群組管理以及 PC 的管理。而另外十個工作量繁重的任務 - 安全、網路設備管理、組織及部門管理、Group Policy 管理等等 - 會佔用過多的時間。你可以依靠微軟內建的管理工具來減少一些這樣的工作量，但是這些內建的工具足夠了嗎？也許現在是透過自動化與 IT 內部安全緊密結合來降低 AD DS 管理負擔的時候了。首先要解決這個問題，必須先確定 Active Directory 的十二項基本管理工作是什麼，然後了解如何建置適當的管理工具來減少管理 AD DS 的工作負載。

威雲科技 WeiCloudTech

ONE IDENTITY™

Active Directory 網域服務是保護和管理 Windows 網路的重要手段。

Active Directory 網域服務管理

任何系統管理員都會同意 Active Directory 域服務（AD DS）爲管理網路提供全面的服務。事實上，AD DS 管理的範圍超出了大多數的簡單輕量級目錄存取協議（LDAP）服務。LDAP 服務旨在提供一組經常使用階層式結構的有條理記錄。例如，組織、部門或人員的資訊。

Active Directory 網域服務是一種目錄服務，提供了一個保護和管理 Windows 網路的方法。它還支援與其他基於 Windows 服務的連接和整合的功能。因爲，AD DS 是爲了在統計和管理分佈於網路結構中用戶，PC 和伺服器的主目錄。

然而，AD DS 是一個目錄式的資料庫 - 一個樹狀結構的資料庫（見圖 1）。因此，目錄資料庫包含各種不同資料的組成格式 (schema) - 結構。這些格式用於每個 AD DS 的建置，並且可爲任何支援 AD DS 的應用程式添加新的資料格式（如 Microsoft Exchange，Microsoft SharePoint 等）進而整合到網路架構中。

AD DS 實例被定義爲 Active Directory 森林。森林是 AD DS 資料庫結構中最大的單個分區。參與森林的每個對象都將共享一組給定的屬性和對象類型。森林可以組成一個群組以共享某些資訊。Windows Server 2003 引入了森林信任的概念，它允許森林與他人共享其 Active Directory 資料庫的部分，反之亦然。這個概念在 Windows Server 2008 中更加強化。

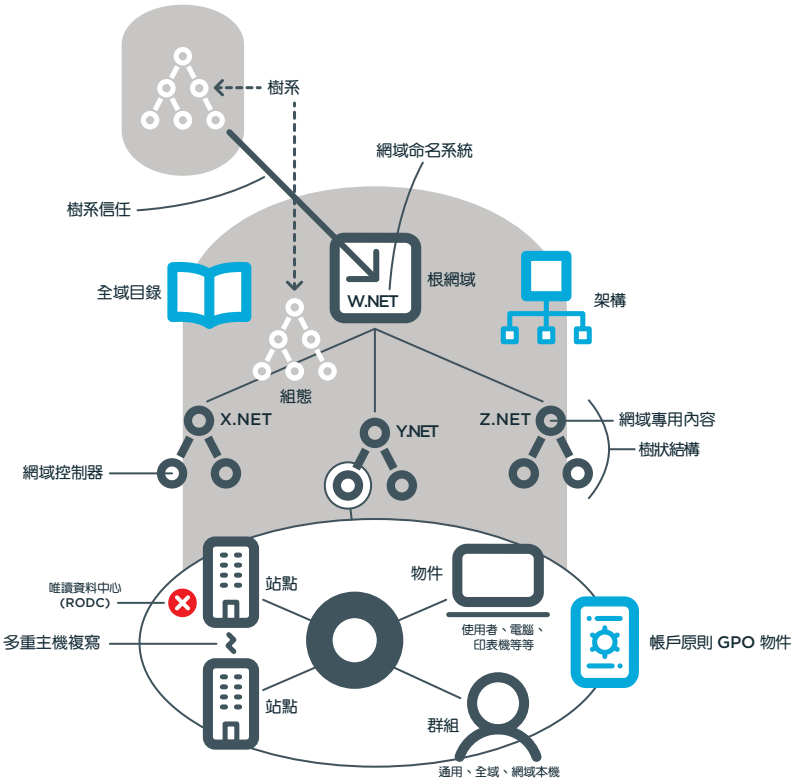

圖 1：Active Directory 網域服務資料庫結構

預設情況下，AD DS 資料庫包含 200 多個對象類型和超過 1,000 個屬性。擴展 AD DS 資料庫時，可以添加更多的對象類型或屬性。例如，當 Microsoft Exchange 安裝在 AD DS 環境中時，Microsoft Exchange 實際上將森林中的對象類型和屬性數量加倍。

像任何資料庫一樣，AD DS 對其所包含的對象進行分類，但與關連式資料庫不同，AD DS 資料庫結構是樹狀分層的，基於域名命名系統（DNS）的結構上。在一個森林裡，根節點 - 類似於 DNS 結構中的主節點是根網域。每個 AD DS 森林必須包含至少一個網域。網域作爲森林內的所有子結點對象的容器。網域可以重新組合成樹。樹與樹之間透過其 DNS 名稱彼此隔離。

每個森林將至少包括一個樹和一個網域。網域是森林中的安全策略和管理邊界。包含了用戶，PC，伺服器，網域控制器（DC），印表機，檔案共享，應用程式等對象。如果您在林中有多個網域，它將通過網域雙向信任機制自動連接到所有其他網域。

網域被定義爲一個安全邊界，因爲它包含了管理網域內所有對象的適用規則。這些規則可以是安全原則或群組原則（GPO）的形式。安全原則是適用於全網域的規則，但也可以針對不同的對象去套用規則，例如密碼策略，可以針對網域內不同的群組或組織去應用。群組原則（GPO）傾向於適用在更分散的適用法則而且必須應用在特定的容器對象。雖然網域和網域之間可以是分散不相同的安全邊界，但森林將保持在 AD DS 結構中的最終安全邊界。安全邊界也可以稱爲管理邊界，因爲適用於其對象的策略不跨越該安全邊界。

網域的組成可以透過群組式的對像類型（例如組織單位（OU）或群組（Group））來進一步分類。組織單位提供分組（部門、位置等）的機制來對分組對象進行管理或委派。群組主要用於應用程式的授權權限或電子郵件群組分發列表。

森林，樹，網域，組織單位，群組，使用者和 PC 都是儲存在 AD DS 資料庫中的對象。因此，它們可以在全域或本地透過網域控制器（DC）進行管理。

Active Directory 和關連式資料庫的一個主要區別是，除了是樹狀結構之外，它還是可以分佈在不同的伺服器中。資訊可以保留在每個網域控制器中 — 唯讀式的網域控制器（RODC）除外 — 當任一 DC 進行異動，更改過的資訊將會複製到其他的 DC。

如您所見，AD DS的環境是相當的複雜，對管理上所造成的負擔也是不言可喻。

此外，AD DS 有兩個明確的管理工作：

- 服務管理 - 確保 AD DS 功能運行正常
- 資料管理 - 提供依靠 AD DS，如用戶，應用程式，服務等等，正常運行所所需要的資料。

AD DS 管理員通常對 AD DS 的運作服務進行管理。而資料的管理通常會被委託給組織的其他成員，例如個人用戶，管理員，以及在向應用程式提供資訊的情況下的應用程式開發人員和管理員。

12 種 AD DS 管理工作的分類

當您了解 AD DS 資料庫內容和運作的複雜性時，可以看到有幾種不同的操作類型需要確保 AD DS 環境運行有效和可靠。事實上，Active Directory 網域服務管理涵蓋 12 個主要的活動。這些活動所覆蓋的範圍將在表 1 中進行說明，其中也描述了哪些任務著重於資料或內容管理，哪些任務主要集中在服務管理上，還有哪些可以委派管理，哪些管理需要更高層級的權限。

根據您的網域大小，表 1 中的每個活動可能僅僅是由一個全職角色的管理員來進行。在跨組織和地理位置的環境下，將這些工作分類並進行委派將有助於降低過於集中的工作量以及管理技能的分享。但是，目前微軟提供的工具對於今天企業所需的這種分佈式管理來說並不是很好。委派授權，稽核記錄，報表和管理面的控管都是一個有效率的 IT 運作所必須的，主要由企業的管理階層所規定的稽核機制驅動。所有 12 個主要的 AD DS 管理工作必須可稽核，可報告，可控和可管理。

12 個任務的管理

管理這些任務需要大量的工作。這也就是爲什麼要盡可能地讓某些任務自動化地執行非常重要的原因。Windows PowerShell 是一個很好的工具，Active Directory 管理控制台（ADAC）也是如此，但這一切都取決於您的網路組織方式以及需要管理的用戶或計算機數量。小型網路可以由一個人管理。中型網絡開始需要多個人，也需要授權及委派。大型網路或全球網路需要更強化任務和責任的劃分，最大限度的授權和完全自動化。

沒錯，您可以使用內建的管理工具和 Windows Server 本身的自動化功能來執行大部分任務，但您也必須花費時間來成爲 PowerShell 專家，並充分了解 AD DS 環境的複雜性。

第三方管理工具的使用

雖然微軟在 Windows Server 2008 中導入了新的工具，將 AD DS 管理工作集中在一起，但仍然存在很多問題。爲了使 AD DS 管理更容易，是第三方產品（如 Active Roles）的目標。

在尋求第三方工具時，您的目標應該是減少管理上的開銷，並確保一個完整的 AD DS 管理機制。

表 1：AD DS 管理的 12 項任務

任務	描述	服務	資料
1. 使用者和群組的管理	這包含了使用者的密碼重置，建立新使用者，刪除使用者或終止使用者，群組建立，群組成員管理等等。 • 密碼重置的工作應該委派給 Help Desk 成員。 • 使用者帳戶的異動以及服務帳戶（Service Account）管理應由管理員負責。 • 全網域類型的群組成員管理應由用戶代表管理。		✓
2. 設備管理	所有在 Windows 網路環境中的計算機必須具有計算機帳戶。這是它們可以與 AD DS 進行互動以及 AD DS 與它們進行互動。 • 應授權給技術人員		✓
3. 網路服務管理	這包括網路共享的發佈，印表機，分散式文件系統（DFS 共享，應用程式目錄分區，Exchange 電子郵件等）。 • 應依據不同的服務授權給相對應的技術人員。	✓	✓
4. 群組原則（GPO）管理	群組原則（GPO）替 Windows Server 強化了大部分的管理模式 • 應委派給合適的技術人員。	✓	
5. DNS 管理	DNS 與目錄服務密切相關，目錄服務的操作需要依賴正常運行的動態 DNS 基礎架構。 • 由於目錄整合了 DNS，目錄 DNS 的管理應由網域管理員負責。	✓	
6. Active Directory 網路拓撲與複製管理	複製是目錄服務操作的核心。它涵蓋了子網域，站台，站台連接器（site links），網站連結橋接器（site link bridges）和橋頭伺服器（bridgehead servers）的配置。這個操作必須依賴知識一致性檢查器（Knowledge Consistency Checker） - 根據您提供的規則和準則自動生成複製拓撲的服務 - 來控制複製。 • 這是網域管理員的責任。	✓	
7. Active Directory 配置管理	配置管理涉及了森林，網域和組織單位（OU）的設計和部署。它還涉及靈活的單主機操作（Flexible Single Master Operations）角色，通用類別目錄伺服器和網域控制站（DCs）放置，包括唯讀網域控制站（RODC）。與配置管理相關的一個額外活動是時間同步。AD DS 依賴於 PDC 模擬器角色來同步網路中的時間。 • 這些任務是森林和網域管理員的責任。	✓	

表 1：AD DS 管理的 12 項工作（續）

任務	描述	服務	資料
8. Active Directory schema 管理	AD DS 是一個分散式的資料庫。因此，它包括資料庫結構（Schema）。結構一但被用來建立對象後，就不能任意修改或刪除，但它們可以被禁用，重新命名和提供其他結構使用。 • 這是森林管理員的責任。	✓	
9. 資訊管理	這是指對目錄建立、異動、刪除資訊的管理，包含了用戶、共享檔案夾、計算機的擁有者、群組的成員、印表機、計算機的位置資訊等。Active Directory 結構（Schema）管理控制台可在全局目錄（Global Category）中添加或刪除內容，並確定對像是否應進行索引。您也可以分配 NTDS 配額以確保沒有人能夠添加或讀取目錄中所允許的更多資訊。 • 盡可能將大量的資訊管理任務委託給組織內適當的人員。		✓
10. 安全管理	安全管理涵蓋了從設置網域帳戶和詳細的密碼策略，分配用戶權限，管理信任以及存取控制列表（Access Control List）和存取控制入口（Access Control Entry）等各方面的管理。 • 安全管理是屬於網域管理員的責任或您也可以委派給指定的人員管理。	✓	
11. 資料庫管理	資料庫管理涉及 Ntds.dit 維護以及 AD DS 對象和 GPO 的保護。包括管理 LostandFound 和 LostandFoundConfig 容器，它們的目的是在收集目錄中無家可歸的對象。還包括壓縮每個 DC 上的目錄資料庫。雖然 AD DS 經常自動壓縮自己的資料庫，但手動壓縮它是個好習慣。這還包括從 AD DS 垃圾桶中回復的對象。 • 這是網域管理員的責任。	✓	
12. AD 報告	透過目錄生成的報告，您可以了解其結構，包含內容以及運行方式。AD DS 預設下並沒有集中式的報告工具，但您可以在目錄的多個層級中導出數據。您還可以使用群組策略（Group Policy）管理控制台生成 GPO 報告。 • 這是網域管理員和 GPO 管理者的責任。	✓	✓

這就是爲什麼您需要一個完善的工具，先解決 12 個任務類別中的每一個，接下來爲委派提供支援以及完整的系統自動化。依照這個需求，這個工具應該提供以下大部分功能：

1. 能夠自動化的建立用戶和群組，減少群組和用戶管理的負擔。
2. 計算機帳號自動配置。
3. 確保網路服務和其他的任務的管理授權，可以完全信任的委派給合適的人員。
4. 整合群組策略以減少 GPO 管理負擔。
5. 整合 DNS 管理，簡化階層資料庫結構管理。
6. 使用拓墣和複製管理工具，以確保目錄始終在最佳狀態下工作。
7. 當您的組織產生異動，配置管理能幫您根據需要搬移或異動森林（Forest）。
8. 控管資料庫格式的修改，以確保 AD DS 資料庫的穩定性。
9. 自動化使用者的自助服務以支援目錄內的資訊管理。
10. 完整的目錄安全管理，讓防火牆圍繞目錄以確保目錄不受侵擾。
11. 資料庫管理能力，確保 NTDS，DIT 資料庫能夠以最佳狀態運行。
12. 全面的線上和離線的目錄操作報告，以確保讓您能即時了解目錄的結構和運作。

這 12 個功能集中在 AD DS 的 12 個基本任務上，但是還應該有其他功能，如：

- 將管理工具與 Windows 整合。
- PowerShell 可以自動生成新腳本。
- 變動控制，確保具有權限異動的人員在對主要服務修改時，提供簽字，並保證能對所有的更動進行追蹤。

讓自動化和管理工作的整合能夠持續擴展來簡化目錄的管理。最後，您將會看到使用單一的管理工具來大大簡化大型目錄結構的管理，並提供一致且簡單的方法來管理這樣一個複雜的環境。

總結

管理大型目錄結構可能是一個很吃重的工作，特別是如果您沒有合適的工具來正確的進行委派，管理和審核操作。即使如此，當您嘗試使用 Microsoft 所提供的各種內件工具來執行工作時，您最終必須成爲至少十二個不同任務類別的專家，並且最終可能無法符合其他要求的風險，例如：稽核，報告 並管理外部或分散的資源。

現今的需求都需用更少的資源做更多的事情，但大多數的管理者並沒有多餘的空閒時間來面對，最好的方式就是能夠透過單一的工具使用單一的介面來處理所有目錄的任務。這就是 Active Roles 這樣的工具可以大大簡化 AD DS 的管理任務，同時保持目錄完整安全。更好的是，Active Roles 可以幫助您自動執行最常規的任務，以保持目錄服務持續運轉。您是否採取積極措施來減少工作量？ 下載免費試用版，了解更多資訊在 **oneidentity.com/products/active-roles/**。

關於作者

原文是由 Resolutions Enterprises Ltd 的 Nelson Ruest 和 Danielle Ruest 所撰寫。Rutests 是專注於 IT 基礎設施設計和優化的技術引領者。原始內容已由 One Identity 團隊更新 - 主編 Todd Peterson。

更多詳細資訊

關於 One Identity

One Identity 系列的身份和存取管理 (IAM) 解決方案可爲現實世界提供 IAM，包括以業務爲中心、模組化與整合式以及能滿足未來需求的身份管理、存取管理和權限管理解決方案。

如果您對使用這份資料有任何疑問，請連絡：

One Identity LLC
收件人：法律部門
4 Polaris Way
Aliso Viejo, CA 92656

請參閱我們的網站 (**www.oneidentity.com**)，
以取得各地區及各國的辦公室資訊。