Directory and Resource Administrator

管理員指南

2018 年 **7** 月

法律聲明

Micro Focus 及其關係企業和授權者 (“Micro Focus”) 之產品與服務的保固，僅載於該項產品與服務隨附的明確保固聲明中。本文中任何內容不得解釋為構成其他保固。對於本文中之技術或編輯錯誤或疏漏，Micro Focus 不負任何責任。本文資訊如有更動，恕不另行通知。

關於本指南

本*管理員指南*提供關於 Directory and Resource Administrator 產品的概念資訊。本書籍定義詞彙和各種相關概念。它也提供許多組態和作業任務的逐步指引。

適用對象

本書提供的資訊適合負責瞭解管理概念和實作安全的分散式管理模型的人員。

其他文件

本指南為 Directory and Resource Administrator 文件集的一部分。如需支援此版本的出版物完整清單，請造訪 文件網站 (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)。

聯絡銷售支援

若有關於產品、價格及功能等方面的問題，請聯絡當地合作夥伴。如果您無法聯絡合作夥伴，請聯絡我們的銷售支援團隊。

全球：	www.netiq.com/about_netiq/officelocations.asp
美國和加拿大：	1-888-323-6768
電子郵件：	info@netiq.com
網站：	www.netiq.com

聯絡技術支援

若有關於特定產品的問題，請聯絡我們的技術支援團隊。

全球：	www.netiq.com/support/contactinfo.asp
北美與南美：	1-713-418-5555
歐洲、中東和非洲：	+353 (0) 91-782 677
電子郵件：	support@netiq.com
網站：	www.netiq.com/support

聯絡文件支援

我們的目標是提供符合您需求的文件。若您有任何改善文件的建議，請按一下HTML版文件任一頁面底部的**對本主題發表備註**。您也可以將電子郵件寄至Documentation-Feedback@netiq.com。我們重視您的意見並期待您提出建議。

聯絡線上使用者社群

NetIQ線上社群NetIQ Communities是一個協同網路，將您與同行和NetIQ專家聯繫起來。透過提供更多即時的資訊、有用資源的實用連結以及諮詢NetIQ專家的管道，NetIQ Communities協助確保您精通必要知識，以充分發揮您所仰賴之 IT 投資的全部潛力。如需詳細資訊，請造訪 http://community.netiq.com。

1 入門

在安裝和配置 Directory and Resource Administrator™ (DRA) 的所有元件之前，您應該了解 DRA 對企業的基本租用戶有何用處，以及 DRA 元件在產品架構中的角色。

1.1 何謂 Directory and Resource Administrator

Directory and Resource Administrator 為 Microsoft Active Directory (AD) 提供安全有效率的特權身分管理。DRA 執行「最少權限」的精細委託，讓管理員和使用者只獲得完成其特定職責所需的許可。DRA 也強制遵守規則，提供詳細的活動稽核與報告，以及利用 IT 程序自動化來簡化完成重複的工作。這些功能中的每一項都能保護客戶的 AD 和 Exchange 環境，以避免權限擴張、發生錯誤、惡意活動和違反法規的情況，同時向使用者、業務經理和服務台人員授予自助能力，以降低管理員的負擔。

DRA也延伸了MicrosoftExchange的強大功能，以實現與Exchange物件的無接縫管理。DRA可透過單一、相同的使用者介面來提供規則式管理，可管理整個 Microsoft Exchange 環境的信箱、公用資料夾和配送清單。

DRA 提供您需要的解決方案，讓您控制和管理 Active Directory、Microsoft Windows、Microsoft Exchange 和 Microsoft Office 365 環境。

- **支援 Active Directory、Office 365、Exchange 和商務用 Skype：** 可讓管理員管理 Active Directory、內部部署 Exchange Server、內部部署商務用 Skype、Exchange Online 和商務用 Skype Online。
- **精細的使用者和管理權限存取控制：** 專利的 ActiveView 技術可以僅指派完成特定職責所需的權限，以避免權限擴張。
- **可自定的 Web 主控台：** 直覺方式可讓非技術性人員透過受限制 (和指定的) 能力與存取，輕鬆安全地執行管理任務。
- **深度活動稽核與報告：** 對於使用產品所執行的所有活動，提供了一個綜合性的稽核記錄。安全地儲存長期資料，並向稽核員(例如，PCIDSS、FISMA、HIPAA和NERCCIP)展示已備妥AD存取的控管程序。
- **IT 程序自動化：** 將各種任務的工作流程自動化，例如佈建和取消佈建、使用者和信箱動作、規則強制執行，以及受管制的自助任務；提高業務效率並減少手動和重複的管理工作。
- **作業完整性：** 為管理員提供精細存取控制，並管理對系統和資源的存取，以防止惡意或不正確的變更，而影響系統和服務的效能。
- **程序強制執行：** 維護重要變更管理程序的完整性，協助您改善生產力、減少錯誤、節省時間和提高管理效率。
- **與 Change Guardian 整合：** 在 DRA 和工作流程自動化之外對 Active Directory 中產生的事件加強稽核。

1.2 了解 Directory and Administrator 元件

您會一直用來管理特權存取的 DRA 元件包括主要和次要伺服器、管理員主控台、報告元件，以及用於工作流程處理自動化的 Aegis 工作流程引擎。

下表指出各種 DRA 使用者所使用的一般使用者介面和管理伺服器：

DRA 使用者類型	使用者介面	管理伺服器
DRA 管理員 (維護產品組態的人員)	委託和組態主控台	主要伺服器
	DRA 報告 Center 設定 (NRC) CLI *(選擇性)* DRA ADSI 提供者 *(選擇性)*	次要伺服器
服務台臨時管理員	帳戶和資源管理主控台	次要伺服器
服務台臨時管理員	Web 主控台	任何已安裝 DRA REST 的 DRA 伺服器

1.2.1 DRA 管理伺服器

DRA 管理伺服器儲存組態資料 (環境、委託存取和規則)、執行操作人員和自動化任務，以及稽核全系統活動。除了可支援數個主控台和應用程式介面 (Application Programming Interfaces, API) 層級用戶端外，基於備援和地理隔離的需要，伺服器主要是透過多主機組 (Multi-Master Set, MMS) 擴充模型來提供高可用性。在此模型中，每一個DRA環境都需要一部主要DRA管理伺服器，以同步化許多其他的次要 DRA 管理伺服器。

強烈建議不要將管理伺服器安裝在 Active Directory 網域控制器上。對於 DRA 管理的每一個網域，請確保管理伺服器所在的同一個網站中至少有一部網域控制器。依預設，管理伺服器會存取最近的網域控制器，以處理所有讀取和寫入作業；在執行特定網站的任務時，例如密碼重設，您可以指定網站專用的網域控制器來處理作業。最佳實務是以次要管理伺服器來專門執行報告、批次處理和自動化工作負載。

1.2.2 委託和組態主控台

「委託和組態主控台」是可安裝的使用者介面，可讓系統管理員存取 DRA 組態和管理功能。

- **委託管理：** 可讓您以精細方式指定，並將受管理的資源和任務的存取權指派給助理管理員。
- **規則和自動化管理：** 可讓您定義和強制執行規則，以確保遵守環境的標準和慣例。
- **組態管理：** 可讓您更新 DRA 系統設定和選項、新增自定，以及設定受管理的服務 (Active Directory、Exchange、Office 365 等)。

1.2.3 帳戶和資源管理主控台

「帳戶和資源管理主控台」是可安裝的使用者介面，可讓助理管理員檢視和管理所連接之網域和服務的委託物件。

1.2.4 Web 主控台

「Web主控台」是Web型使用者介面，可讓助理管理員快速輕鬆地存取，以檢視和管理所連接之網域和服務的委託物件。管理員可以自定外觀及使用「Web 主控台」來納入自定的企業品牌和自定的物件內容。

DRA 管理員也可以建立和修改自動化工作流程表單，而於觸發時執行例行的自動化任務。

「整合的變更歷程」是Web主控台的另一項功能，可以與「變更歷程」伺服器整合，以便於DRA之外稽核對 AD 物件所做的變更。變更歷程報告選項包括：

- 變更套用至...
- 變更者...
- 信箱建立者...
- 使用者、群組和聯絡人電子郵件地址的建立者...
- 使用者、群組和聯絡人電子郵件地址的刪除者...
- 虛擬屬性建立者...
- 物件移動者...

1.2.5 報告元件

DRA 報告提供內建、可自訂的 DRA 管理樣板，以及 DRA 管理的網域和系統的詳細資料：

- AD 物件的資源報告
- AD 物件資料報告
- AD 摘要報告
- DRA 組態報告
- Exchange 組態報告
- Office 365 Exchange Online 報告
- 詳細活動趨勢報告 (按照月份、網域和尖峰)
- 彙總的 DRA 活動報告

DRA 報告可以透過 SQL Server Reporting Services 來排程和發佈，方便分發給利益相關者。

1.2.6 工作流程引擎

DRA與Aegis工作流程引擎整合，透過Web主控台將工作流程任務自動化，助理管理員可以在主控台設定工作流程伺服器，並執行自訂的自動化工作流程表單，然後檢視這些工作流程的狀態。如需關於工作流程引擎的詳細資訊，請參閱 DRA 文件網站 (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)。

1.2.7 產品架構


內部部署網路
DRA 伺服器
Web 伺服器(IIS)
報告
工作流程引擎
主要站台
主要站台
郵件伺服器
公用資料夾
Active Directory
受控網域
受信任的網域
受控服務
商務用 Skype
受控資源
電腦
印表機
DRA 管理伺服器
主要/次要 (高可用性)
托管網站
報告
工作流程引擎
DRA 用戶端
Web 主控台
委託和組態主控台
帳戶管理主控台
PowerShell 指令行
REST 用戶端
低速連結
遠端站台
遠端環境
Active Directory
交換
受控服務
受控資源
遠端 DRA 環境
DRA 次要管理伺服器
DRA 用戶端
Azure
Office 365
Exchange Online
Skype Online
授權

2 產品安裝與升級

本章描述 Directory and Resource Administrator 所需的建議硬體、軟體和帳戶需求。然後以核對清單逐步引導您安裝每一個元件。

2.1 規劃部署

當您規劃 Directory and Resource Administrator 部署時，請利用本節來評估軟硬體環境的相容性，並了解您需要為部署所設定的連接埠和通訊協定。

2.1.1 經過測試的資源建議

本節提供基本資源建議的規模大小資訊。根據可用的硬體、特定的環境、所處理的具體資料類型及其他因素，您的結果可能有所不同。可能另有更大型、更強大的硬體組態可以處理更多的負載。如有疑問，請洽詢 NetIQ 諮詢服務。

在大約有一百萬個 Active Directory 物件的環境中執行：

元件	CPU	記憶體	儲存
DRA 管理伺服器	4 CPU (x64)/核心 2.0 GHz	16 GB	100 GB
DRA Web 主控台	2 CPU (x64)/核心 2.0 GHz	8 GB	100 GB
DRA 報告	4 CPU (x64)/核心 2.0 GHz	16 GB	100 GB
DRA 工作流程伺服器	4 CPU (x64)/核心 2.0 GHz	16 GB	100 GB

2.1.2 虛擬環境資源佈建

DRA 會保持大型記憶體區段長時間運作。佈建資源給虛擬環境時，請採用下列建議：

- 將儲存體配置為「完整佈建」
- 將記憶體保留設為「保留所有訪客記憶體(全部鎖定)」
- 確定分頁檔足夠因應虛擬層可能的氣泡式記憶體重新配置

2.1.3 必要的連接埠和通訊協定

本節提供 DRA 通訊所需的連接埠和通訊協定。

- 可設定的連接埠以一個星號 * 表示
- 需要證書的連接埠以兩個星號 ** 表示

DRA 管理伺服器

通訊協定和連接埠	方向	目的地	用法
TCP 135	雙向	DRA 管理伺服器	端點對映程式、DRA通訊的基本需求；讓管理伺服器在 MMS 中找到彼此
TCP 445	雙向	DRA 管理伺服器	委託模型複製；MMS 同步期間的檔案複製 (SMB)
動態TCP連接埠範圍*	雙向	Microsoft Active Directory 網域控制器	依預設，DRA會從TCP連接埠範圍1024至65535內動態指定連接埠。不過，您可以使用元件服務來設定此範圍。如需詳細資訊，請參閱使用分散式 COM 搭配防火牆 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 50000 *	雙向	DRA 管理伺服器	屬性複製和DRA伺服器ADAM通訊。(LDAP)
TCP 50001 *	雙向	DRA 管理伺服器	SSL 屬性複製 (ADAM)
TCP/UDP 389	向外	Microsoft Active Directory 網域控制器	Active Directory 物件管理 (LDAP)
	向外	Microsoft Exchange Server	信箱管理 (LDAP)
TCP/UDP 53	向外	Microsoft Active Directory 網域控制器	名稱解析
TCP/UDP 88	向外	Microsoft Active Directory 網域控制器	允許從 DRA 伺服器向網域控制器驗證 (Kerberos)
TCP 80	向外	Microsoft Exchange Server	內部部署 Exchange 伺服器 2010 至 2013 所需的 (HTTP)
	向外	Microsoft Office 365	遠端 PowerShell 存取 (HTTP)
TCP 443	向外	Microsoft Office 365、Change Guardian	圖形 API 存取和 Change Guardian 整合 (HTTPS)
TCP443、5986、5985	向外	Microsoft PowerShell	原生 PowerShell Cmdlet (HTTPS) 和 PowerShell 遠端
TCP 8092 * **	向外	工作流程伺服器	工作流程狀態和觸發 (HTTPS)
TCP 50101 *	向內	DRA 用戶端	在變更歷程報告上按右鍵移至 UI 稽核報告。可在安裝期間設定。
TCP 8989	Localhost	記錄歸檔服務	記錄歸檔通訊 (不必透過防火牆開啟)
TCP 50102	雙向	DRA 核心服務	記錄歸檔服務
TCP 50103	Localhost	DRA 快取服務	DRA 伺服器上的快取服務通訊 (不需要透過防火牆開啟)
TCP 1433	向外	Microsoft SQL Server	報告資料收集
UDP 1434	向外	Microsoft SQL Server	SQL Server 瀏覽器服務使用此連接埠來識別具名例項的連接埠。

通訊協定和連接埠	方向	目的地	用法
TCP 8443	雙向	Change Guardian 伺服器	整合的變更歷程

DRA REST 伺服器

通訊協定和連接埠	方向	目的地	用法
TCP 8755 * **	向內	IIS 伺服器、DRA PowerShell Cmdlet	執行 DRA REST 為基礎的工作流程活動 (ActivityBroker)
TCP 11192 * **	向外	DRA 主機服務	適用於DRAREST服務和DRA管理服務之間的通訊
TCP 135	向外	Microsoft Active Directory 網域控制器	使用服務連接點 (SCP) 來自動探索
TCP 443	向外	Microsoft AD 網域控制器	使用服務連接點 (SCP) 的自動探索

Web 主控台 (IIS)

通訊協定和連接埠	方向	目的地	用法
TCP 8755 * **	向外	DRA REST 服務	適用於DRAWeb主控台、DRAPowerShell和DRA 主機服務之間的通訊
TCP 443	向內	用戶端瀏覽器	開啟 DRA 網站
TCP 443 **	向外	Advanced Authentication 伺服器	Advanced Authentication

DRA 委託和管理主控台

通訊協定和連接埠	方向	目的地	用法
TCP 135	向外	Microsoft Active Directory 網域控制器	使用 SCP 來自動探索
動態 TCP 連接埠範圍 *	向外	DRA 管理伺服器	DRA配接器工作流程活動。依預設，DCOM會從 TCP 連接埠範圍 1024 至 65535 內動態指定連接埠。不過，您可以使用元件服務來設定此範圍。如需詳細資訊，請參閱使用分散式 COM 搭配防火牆 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 50102	向外	DRA 核心服務	產生變更歷程報告

工作流程伺服器

通訊協定和連接埠	方向	目的地	用法
TCP 8755	向外	DRA 管理伺服器	執行 DRA REST 為基礎的工作流程活動 (ActivityBroker)
動態 TCP 連接埠範圍 *	向外	DRA 管理伺服器	DRA配接器工作流程活動。依預設，DCOM會從 TCP 連接埠範圍 1024 至 65535 內動態指定連接埠。不過，您可以使用元件服務來設定此範圍。如需詳細資訊，請參閱使用分散式 COM 搭配防火牆 (http://go.microsoft.com/fwlink/?LinkID=46088) (DCOM)
TCP 1433	向外	Microsoft SQL Server	工作流程資料儲存
TCP 8091	向內	Operations 主控台和組態主控台	工作流程 BSL API (TCP)
TCP 8092 **	向內	DRA 管理伺服器	工作流程 BSL API (HTTP)和 (HTTPS)
TCP 2219	Localhost	命名空間提供者	由命名空間提供者用來執行配接器
TCP 9900	Localhost	Correlation Engine	由 Correlation Engine 用來與工作流程引擎和命名空間提供者通訊
TCP 10117	Localhost	資源管理命名空間提供者	由資源管理命名空間提供者使用

2.1.4 支援的平台

如需所支援軟體平台的最新資訊，請參閱 NetIQ 網站上的 Directory and Resource Administrator 頁面： https://www.netiq.com/support

受管理系統	先決條件
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3 (公用資料夾除外) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online

受管理系統	先決條件
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ 適用於 Windows PowerShell 的 Windows Azure Active Directory 模組 https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ 商務用 Skype Online、Windows PowerShell 模組 https://www.microsoft.com/en-us/download/details.aspx?id=39366
商務用 Skype	◆ Microsoft 商務用 Skype 2015
變更歷程	◆ Change Guardian 5.0、5.1
網頁瀏覽器	◆ Microsoft Internet Explorer 11、Edge ◆ Google Chrome ◆ Mozilla Firefox
自動化工作流程	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2

2.1.5 DRA 管理伺服器需求

對於軟體和帳戶，DRA 具有下列伺服器要求：

軟體要求

元件	先決條件
安裝目標	**NetIQ 管理伺服器作業系統：**
作業系統	◆ Microsoft Windows Server 2012、2012 R2、2016 ◆ Microsoft Windows 2008 R2 僅支援升級。 **附註：** 伺服器也必須是受支援的 Microsoft Windows Server 原生網域的成員。 **Windows DRA 介面：** ◆ Microsoft Windows Server 2012、2012 R2、2016 ◆ Microsoft Windows 8.1 (x86 & x64)、10 (x86 & x64)
安裝程式	◆ Microsoft .Net Framework 4.5.2 和更新版本

元件	先決條件

管理伺服器	**Directory and Resource Administrator：**
	◆ Microsoft .Net Framework 4.5.2 和更新版本
	◆ 以下之一：
	  ◆ Microsoft Visual C++ 2015 (Update 3) 可轉散發套件 (x64 和 x86)
	  ◆ Microsoft Visual C++ 2017 (Update 3) 可轉散發套件 (x64 和 x86)
	◆ Microsoft Message Queuing
	◆ Microsoft Active Directory 輕量型目錄服務角色
	◆ 已啟動的遠端登錄服務
	Microsoft Office 365/Exchange Online 管理：
	◆ 適用於 Windows PowerShell 的 Windows Azure Active Directory 模組
	◆ 適用於 IT 專業人員的 Microsoft Online Services 登入小幫手
	◆ 商務用 Skype Online、Windows PowerShell 模組
	如需詳細資訊，請參閱支援的平台。

舊版 Web 元件	**Web 伺服器：** ◆ Microsoft Internet Information Services (IIS) 版本 8.0、8.5、10 **Microsoft IIS 元件：** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Microsoft IIS 安全性角色服務 **Windows DRA 介面：** ◆ Microsoft .NET Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) 可轉散發套件 (x86)

帳戶需求

帳戶	描述	許可權
AD LDS 群組	必須將DRA服務帳戶新增至此群組才能存取 AD LDS	◆ 網域本機安全性群組

帳戶	描述	許可權
DRA 服務帳戶	執行 NetIQ 管理服務所需的許可權	◆ 「Distributed COM Users」許可權 ◆ AD LDS 管理員群組的成員 ◆ 帳戶操作員群組 ◆ 記錄歸檔群組 (OnePointOp ConfgAdms & OnePointOp) **附註：** 如需設定最低權限網域存取帳戶的相關資訊，請參閱：最低權限 DRA 存取帳戶。
DRA 管理員	佈建給內建DRA管理員角色的使用者帳戶或群組	◆ 網域本機安全性群組或網域使用者帳戶 ◆ 管理的網域或受信任的網域的成員 ◆ 如果您從受信任的網域指定帳戶，請確定管理伺服器電腦可以驗證此帳戶。
DRA Assistant Admin 帳戶	透過 DRA 來委託權限的帳戶	◆ 將所有 DRA Assistant Admin 帳戶新增至「Distributed COM Users」群組，讓他們可以從遠端用戶端連接至 DRA 伺服器。 **附註：** 在安裝期間可設定 DRA 來替您管理這方面。

最低權限 DRA 存取帳戶

以下是指定的帳戶所需的許可和權限，以及您需要執行的組態指令。

網域存取帳戶： 將下列 Active Directory 許可指定給網域存取帳戶：

- 「完整」控制內建網域物件
- 「完整」控制電腦物件
- 「完整」控制聯絡人物件
- 「完整」控制容器物件
- 「完整」控制動態通訊群組
- 「完整」控制群組物件
- 「完整」控制 Inetorgperson 物件
- 「完整」控制 MsExchSystemObjectContainer 物件
- 「完整」控制組織單位物件
- 「完整」控制印表機物件
- 「完整」控制公用資料夾
- 「完整」控制使用者物件

將下列具有「此物件和所有子物件」範圍的權限指定給網域存取帳戶：

- 允許建立電腦物件

- 允許建立聯絡人物件
- 允許建立容器
- 允許建立群組物件
- 允許建立 MsExchDynamicDistiributionList
- 允許建立組織單位物件
- 允許建立公用資料夾
- 允許建立服務連接點
- 允許建立使用者物件
- 允許刪除電腦物件
- 允許刪除聯絡人物件
- 允許刪除容器
- 允許刪除群組物件
- 允許刪除 InetOrgPerson 物件
- 允許刪除 MsExchDynamicDistiributionList
- 允許刪除組織單位物件
- 允許刪除公用資料夾
- 允許刪除服務連接點
- 允許刪除使用者物件

Office 365 租用戶存取帳戶： 將下列 Active Directory 許可指定給 Office 365 租用戶存取帳戶：

- Office 365 中的使用者管理管理員
- Exchange Online 中的收件者管理

Exchange 存取帳戶： 將**組織管理**角色指定給 Exchange 存取帳戶來管理 Exchange 2010。

Skype 存取帳戶： 確保此帳戶為可使用 Skype 的使用者，且至少為下列其中一個角色的成員：

- CSAdministrator 角色
- CSUserAdministrator 與 CSArchiving 角色

公用資料夾存取帳戶： 將下列 Active Directory 許可指定給公用資料夾存取帳戶：

- 公用資料夾管理
- 已啟用郵件功能的公用資料夾

DRA 安裝之後：

- 從 DRA 安裝資料夾執行下列指令，將許可委託給「刪除的物件容器」(注意：必須由網域管理員執行此指令)：

  DraDelObjsUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*Account Name*>

- 從 DRA 安裝資料夾執行下列指令，將許可委託給「NetIQReceyleBin OU」(注意：只有在新增要由 DRA 管理的各個網域之後才能這麼做)：

  DraRecycleBinUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*AccountName*>

- 在 DRA 將管理資源 (例如印表機、服務、事件記錄、裝置等) 的每一部電腦上，將最低權限覆寫帳戶新增至「本機系統管理員」群組。
- 將佈建主目錄的共享資料夾或 DFS 資料夾上的「完整許可」，授予最低權限覆寫帳戶。
- 將最低權限覆寫帳戶新增至「組織管理」角色來管理 Exchange 物件。

2.1.6 DRA Web 主控台和延伸功能需求

Web 主控台和 REST 延伸功能的需求包括：

軟體要求

元件	先決條件
安裝目標	**作業系統：** ◆ Microsoft Windows Server 2016、Microsoft Windows 10 (含 Microsoft IIS 10) ◆ Microsoft Windows Server 2012、2012 R2 (含 Microsoft IIS 8.0、8.5)
DRA 主機服務	◆ Microsoft .NET Framework 4.5.2 ◆ DRA 管理伺服器
DRA REST 端點和服務	◆ Microsoft .NET Framework 4.5.2
PowerShell 延伸功能	◆ Microsoft .NET Framework 4.5.2 ◆ PowerShell 4.0

元件	先決條件
DRA Web 主控台	**Web 伺服器:** ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft Internet Information Services WCF (啟用) **Microsoft IIS 元件：** ◆ 網路伺服器 ◆ 通用 HTTP 功能 ◆ 靜態內容 ◆ 預設文件 ◆ 目錄瀏覽器 ◆ HTTP 錯誤 ◆ 應用程式開發 ◆ ASP ◆ 狀態及診斷 ◆ HTTP 記錄 ◆ 申請監視器 ◆ 安全性 ◆ 基本驗證 ◆ 效能 ◆ 靜態內容壓縮 ◆ Web 伺服器管理工具

2.1.7 報告需求

DRA 報告的需求包括：

軟體要求

元件	先決條件
安裝目標	**作業系統：** ◆ Microsoft Windows Server 2012、2012 R2、2016

元件	先決條件
NetIQ Reporting Center (3.2 版)	**資料庫：** ◆ Microsoft SQL Server 2012、2014、2016 ◆ Microsoft SQL Server Reporting Services **Web 伺服器:** ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft IIS 元件： ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** 連接至 DRA Reporting 的每一部 DRA Administration 伺服器，另外還需要 .NET Framework 3.5。 **附註：** 在 SQL Server 電腦上安裝 NetIQ Reporting Center (NRC) 時，.NET Framework 3.5 在安裝 NRC 之前，可能需要手動安裝。
DRA 報告	**資料庫：** ◆ Microsoft SQL Server Integration Services ◆ Microsofte SQL Server Agent

2.1.8 授權需求

授權決定您可使用的產品和功能。DRA 需要有隨著管理伺服器一起安裝的授權金鑰。

安裝管理伺服器之後，您可以使用「狀態檢查公用程式」來安裝試用授權金鑰 (TrialLicense.lic)，這可讓您管理無限制數量的使用者帳戶和信箱 30 天。

如需授權定義和限制的其他資訊，請參閱產品最終使用者授權合約 (EULA)。

2.2 產品安裝

本章引導您安裝 Directory and Resource Administrator。如需規劃安裝或升級的相關資訊，請參閱規劃部署。

2.2.1 安裝 DRA 管理伺服器

您可以將 DRA 管理伺服器安裝為環境中的主要或次要節點。主要和次要管理伺服器的需求相同，不過，每個 DRA 部署都必須包含一部主要管理伺服器。

互動式安裝核對清單

步驟	詳細資料
登入目標伺服器	登入目標 Microsoft Windows 伺服器，以使用具有本機管理權限的帳戶來安裝。
複製和執行 NetIQ 管理員安裝套件	執行 DRA 安裝套件 (NetIQAdminInstallationKit.msi)，將 DRA 安裝媒體解壓縮至本機檔案系統。 **附註：** 必要的話，安裝套件會在目標伺服器上安裝 .NET Framework。
執行 DRA 安裝	啟動 DRA 安裝。 **附註：** 若要稍後安裝，請導覽至安裝媒體的解壓縮位置，然後執行 Setup.exe。
選取 NetIQ 管理伺服器元件和安裝目標	選擇要安裝的元件，並接受預設安裝位置 C:\Program Files (x86)\NetIQ\DRA，或指定其他安裝位置。元件選項： **NetIQ 管理伺服器** ◆ 記錄歸檔資源套件 ◆ NetIQ DRA SDK **舊版 Web 元件** **使用者介面** ◆ 帳戶和資源管理 ◆ DRA ADSI 提供者 ◆ 指令行介面 ◆ 委託和組態
驗證必要條件	**Prerequisites** (必要條件) 對話方塊會根據選擇要安裝的元件來顯示必要軟體清單。安裝程式會引導您安裝任何遺漏的必要條件，以確保成功完成安裝。
接受 EULA 授權合約	接受最終使用者授權合約的條款。
選取伺服器操作模式	選取 **Primary** (主要) 安裝多主機組的一部 DRA 管理伺服器 (部署中只會有一部主要伺服器)，或選取 **Secondary**，(次要) 將新的 DRA 管理伺服器加入現有的多主機組。 如需多主機組的詳細資訊，請參閱 設定多主機組。
指定安裝帳戶和身分證明	◆ DRA 服務帳戶 ◆ AD LDS 群組 ◆ DRA 管理員 詳細相關資訊請參閱：DRA 管理伺服器需求。
設定 DCOM 許可	可讓 DRA 設定「分散式 COM」存取給已驗證的使用者。
設定連接埠	如需預設連接埠的相關資訊，請參閱必要的連接埠和通訊協定。
指定儲存位置	指定本端檔案位置供 DRA 儲存稽核和快取資料。
驗證安裝組態	在按一下**安裝**來繼續安裝之前，您可以先在安裝摘要頁面驗證組態。
安裝之後驗證	安裝完成之後，「健康情況檢查程式」會執行來驗證安裝並更新產品授權。

2.2.2 安裝 DRA 用戶端

您可以在安裝目標執行 DRAInstaller.msi 搭配對應的 .mst 套件，以安裝特定的 DRA 主控台和指令行用戶端：

NetIQDRAUserConsole.mst	安裝帳戶和資源管理主控台
NetIQDRACLI.mst	安裝指令行介面
NetIQDRAADSI.mst	安裝 DRA ADSI 提供者
NetIQDRAClients.mst	安裝所有 DRA 使用者介面

若要將特定的 DRA 用戶端部署到企業內的多部電腦，請設定群組規則物件來安裝特定的 .MST 套件。

1. 啟動「Active Directory 使用者和電腦」並建立群組規則物件。
2. 將 DRAInstaller.msi 套件新增至這個群組規則物件。
3. 確保此群組規則物件具有下列其中一個內容：
   - 群組中的每一個使用者帳戶具有適當電腦的「進階使用者」許可。
   - 啟用「永遠以高權限來安裝」規則設定。
4. 將使用者介面 .mst 檔案 (例如 NetIQDRAUserConsole.mst) 新增至這個群組規則物件。
5. 分發群組規則。

附註： 如需群組規則的相關資訊，請參閱 Microsoft Windows 說明。若要在整個企業內輕鬆安全地測試和部署群組規則，請使用 *Group Policy Administrator*。

2.2.3 安裝 DRA REST 延伸功能

DRA REST 延伸功能套件有四種功能：

- **NetIQ DRA 主機服務：** 與 DRA 管理服務通訊所用的閘道。此服務必須在已安裝 DRA 管理服務的電腦上執行。
- **DRA REST 服務和端點：** 提供RESTful介面，讓DRAWeb主控台和非DRA用戶端要求DRA操作。此服務必須在已安裝 DRA 主控台或 DRA 管理服務的電腦上執行。
- **PowerShell 延伸功能：** 提供 PowerShell 模組，讓非 DRA 用戶端使用 PowerShell Cmdlet 來要求 DRA 操作。
- **DRA Web 主控台：** 主要由助理管理員使用的 Web 用戶端介面，但也包含自定選項。

步驟	詳細資料
登入目標伺服器	登入目標 Microsoft Windows 伺服器，以使用具有本機管理權限的帳戶來安裝。
安裝 SSL 證書	如果尚未於 Windows 伺服器上安裝 SSL 證書，您必須先安裝 SSL 證書，才能執行安裝。
複製和執行 NetIQ 管理員安裝套件	將 DRA 安裝套件 NetIQAdminINstallationKit.msi 複製到目標伺服器，然後按兩下檔案或從指令行呼叫來執行套件。安裝套件會將 DRA 安裝媒體解壓縮至本端檔案系統上的可自訂位置。

步驟	詳細資料
執行DRAREST延伸功能安裝程式	DRA安裝套件完成解壓縮安裝媒體之後會提示您開始安裝DRA。導覽至安裝媒體的解壓縮位置，在 DRARESTExtensionsInstaller.exe 檔案上按右鍵，並選取 **Run as administrator** (以系統管理員身分執行)。
接受 EULA 授權合約	接受最終使用者授權合約的條款。
選取元件和 指定安裝的目標位置	從安裝 **Select Components** (選取元件) 對話方塊，安裝所有選項：DRA 主機服務、DRA REST 端點和服務、PowerShell 延伸功能和 DRA Web 主控台。 接受預設安裝位置 C:\Program Files (x86)\NetIQ\DRA Extensions，或指定其他安裝位置。
驗證必要條件	**Prerequisites** (必要條件) 對話方塊會根據選擇要安裝的元件來顯示必要軟體清單。安裝程式會引導您安裝任何遺漏的必要條件，以確保成功完成安裝。
指定服務帳戶作為執行身分	依預設會顯示DRA伺服器的現有服務帳戶。指定服務帳戶密碼。如需為DRA管理伺服器設定服務帳戶的相關資訊，請參閱 DRA 管理伺服器需求。
指定 REST 服務 SSL 證書	選取要用於 REST 服務的 SSL 證書，並指定 REST 和主機服務連接埠。
指定 Web 主控台 SSL 證書	指定要用於 HTTPS 繫結的 SSL 證書。
驗證安裝組態	在按一下 **Install** (安裝) 來繼續安裝之前，您可以先在安裝摘要頁面驗證組態。

2.2.4 安裝工作流程伺服器

如需安裝工作流程伺服器的相關資訊，請參閱《自動化工作流程管理員指南》。

2.2.5 安裝 DRA 報告

您需要從 NetIQ DRA 安裝套件中安裝兩個執行檔，才能使用 DRA 報告：NRCSetup.exe 和 DRAReportingSetup.exe。

步驟	詳細資料
登入目標伺服器	登入目標 Microsoft Windows 伺服器，以使用具有本機管理權限的帳戶來安裝。確保此帳戶在 SQL Server 上具有本機和網域管理權限，以及「系統管理員」權限。
複製和執行 NetIQ 管理員安裝套件	將 DRA 安裝套件 NetIQAdminINstallationKit.msi 複製到目標伺服器，然後按兩下檔案或從指令行呼叫來執行套件。安裝套件會將 DRA 安裝媒體解壓縮至本端檔案系統上的可自訂位置。此外，必要的話，安裝套件會在目標伺服器上安裝 .NET Framework，以滿足 DRA 產品安裝程式的必要條件。
執行 NetIQ Reporting Center (NRC) 安裝	當 DRA 安裝套件完成解壓縮安裝媒體之後，請導覽至安裝媒體的解壓縮位置，並執行 NRCSetup.exe。
選取 NetIQ Reporting Center 元件	從安裝 **Select Components** (選取元件) 對話方塊，使用預設“NetIQ Reporting Center” 元件來安裝四個 NRC 元件。
指定安裝的目標位置	接受預設安裝位置 C:\Program Files (x86)\NetIQ\Reporting Center，或指定其他安裝位置。

步驟	詳細資料
驗證和安裝必要條件	**Prerequisites** (必要條件) 對話方塊會根據選擇要安裝的元件來顯示必要軟體清單。安裝程式會引導您安裝任何遺漏的必要條件，以確保成功完成安裝。 **重要：** 安裝 NRC 之前，必須在報告伺服器上手動安裝 .NET Framework 3.5。
接受 EULA 授權合約	接受最終使用者授權合約的條款。
安裝組態資料庫	在 **Configuration Database Installation - SQL Server Logon** (組態資料庫安裝 - SQL Server 登入) 對話方塊中使用預設值，或提供 SQL 驗證來完成 NRC 安裝。如果您使用 Default (預設) 例項進行 SQL Server 安裝，則 Instance (例項) 欄位應該保持空白。
執行 DRA 報告安裝	導覽至安裝媒體的解壓縮位置，然後執行 DRAReportingSetup.exe 來安裝 DRA 報告整合的管理元件。
接受 EULA 授權合約	接受最終使用者授權合約的條款以完成執行安裝。

2.3 產品升級

本章提供程序來協助您按部就班升級或移轉分散式環境。

本章假設您的環境包含多部管理伺服器，其中有部分伺服器位於遠端網站。此組態稱為「多主機組」(MMS)。MMS由一部主要管理伺服器及一或多部相關聯的次要管理伺服器所組成。如需 MMS如何運作的詳細資訊，請參閱設定多主機組。

2.3.1 規劃 DRA 升級

執行 NetIQAdminInstallationKit.msi 來解壓縮 DRA 安裝媒體，並安裝和執行「健康情況檢查公用程式」。

開始升級程序之前，務必先規劃 DRA 部署。規劃部署時，請考量下列準則：

- 將升級推送至生產環境之前，先在實驗室環境中測試升級程序。測試可讓您發現並解決任何非預期的問題，而不影響日常管理任務。
- 檢閱必要的連接埠和通訊協定。
- 判斷有多少個AA依賴每一個MMS。如果大多數AA依賴特定的伺服器或伺服器組，請先在離峰期間升級這些伺服器。
- 判斷哪些 AA 需要「委託和組態」主控台。您可以透過下列其中一種方式取得此資訊：
  - 檢閱哪些 AA 與內建 AA 群組相關聯。
  - 檢閱哪些 AA 與內建 ActiveView 相關聯。
  - 使用「Directory and Resource Administrator 報告」來產生安全性模型報告，例如「ActiveView 助理管理員詳細資料」和「助理管理員群組」報告。

將您的使用者介面升級計劃告知這些 AA。

- 判斷哪些 AA 需要連接至主要管理伺服器。一旦您升級主要管理伺服器，這些 AA 就必須升級其用戶端電腦。

  將您升級管理伺服器和使用者介面的計劃告知這些 AA。

- 開始升級程序之前，決定您是否需要執行任何委託、組態或規則變更。視環境而定，此決策可能依每個網站而不同。
- 協調升級用戶端電腦和管理伺服器，以確保停機時間縮到最短。請注意，DRA 不支援在相同的管理伺服器或用戶端電腦上同時執行先前的 DRA 版本與目前的 DRA 版本。

2.3.2 升級前任務

在開始升級安裝之前，請遵循下列預先升級步驟，以準備將每個伺服器進行升級。

步驟	詳細資料
備份 AD LDS 例項	開啟「健康情況檢查公用程式」，並執行 **AD LDS 例項備份**檢查，以建立您目前 AD LDS 例項的備份。
建立部署計劃	建立部署計劃來升級管理伺服器和使用者介面 (AA 用戶端電腦)。如需詳細資訊，請參閱規劃 DRA 升級。
使用次要伺服器來專門執行先前的 DRA 版本	*選用：*升級網站時，使用次要管理伺服器來專門執行先前的 DRA 版本。
對此 MMS 進行必要變更	對此MMS的委託、組態或規則設定，進行任何必要變更。使用主要管理伺服器來修改這些設定。
同步化 MMS	同步化伺服器集，讓每一部管理伺服器包含最新組態和安全性設定。
製作主要伺服器登錄的備份	從主要管理伺服器製作登錄的備份。先前登錄設定的備份可讓您輕鬆復原先前的組態和安全性設定

附註： 如果您需要還原 AD LDS 例項，請進行下列工作：

1. 在「電腦管理」>「服務」中，停止 AD LDS 例項。這會有不同的標題：NetIQDRASecureStoragexxxxx。
2. 將 **current** adamnts.dit 檔案取代為 **backup** adamnts.dit 檔案，如下所示：
   - 目前檔案位置：%ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/
   - 備份檔案位置：%ProgramData%/NetIQ/ADLDS/
3. 重新啟動 AD LDS 例項。

使用本機管理伺服器來專門執行先前的 DRA 版本

在升級期間，使用一或多部次要管理伺服器於網站本端專門執行先前的 DRA 版本，有助於將停機時間縮到最短，也避免浪費成本連接至遠端網站。此為選用步驟，可讓 AA 在整個升級過程中使用先前的 DRA 版本，直到部署完成。

如果您有下列一或多個升級需求，請考慮採用此選項：

- 您要求最短停機時間，或完全沒有停機時間。

- 您必須支援大量 AA，但無法立即升級所有用戶端電腦。
- 升級主要管理伺服器之後，您想要繼續支援存取先前的 DRA 版本。
- 環境中有一個 MMS 橫跨多個站點。

您可以安裝新的次要管理伺服器或指定現有的次要伺服器，用於執行先前的 DRA 版本。如果想要升級此伺服器，此伺服器必須是最後升級的伺服器。否則，請於成功完成升級時，從這部伺服器完全解除安裝 DRA。

設定新的次要伺服器

在本端網站安裝新的次要管理伺服器，有助於避免浪費成本來連接至遠端網站，並確保AA可以繼續不間斷地使用先前的 DRA 版本。如果環境中有一個 MMS 橫跨多個網站，請考慮採用此選項。例如，若 MMS 由倫敦網站的主要管理伺服器和東京網站的次要管理伺服器組成，請考慮在倫敦網站安裝一部次要伺服器，再新增至對應的MMS。此額外的伺服器可讓來自倫敦網站的AA使用先前的DRA版本，直到升級完成。

使用現有的次要伺服器

您可以將現有的次要管理伺服器當作專用伺服器來執行先前的 DRA 版本。如果不打算升級某個網站的次要管理伺服器，請考慮採用此選項。如果現有的次要伺服器不能作為專用，請考慮安裝新的管理伺服器作為此用途。使用一或多部次要伺服器來專門執行先前的DRA版本，可讓AA繼續不間斷地使用先前的 DRA 版本，直到升級完成。在使用集中式管理模型的較大型環境中，最適合採用此選項。

同步化前一個 DRA 版本伺服器集

在製作前一個 DRA 版本登錄的備份或開始升級程序之前，務必同步化伺服器集，讓每一部管理伺服器包含最新組態和安全性設定。

附註： 對此MMS的委託、組態或規則設定，務必進行所有必要變更。使用主要管理伺服器來修改這些設定。一旦升級主要管理伺服器，就無法將委託、組態或規則設定同步化到任何執行舊版 DRA 的管理伺服器。

同步化現有的伺服器集：

1. 以「內建管理員」身分登入主要管理伺服器。
2. 啟動 MMC 介面。
3. 在左窗格中，展開 **Configuration Management** (組態管理)。
4. 按一下 **Administration servers** (管理伺服器)。
5. 在右窗格中，為此伺服器集選取適當的主要管理伺服器。
6. 按一下**Properties** (內容)。
7. 在 Synchronization schedule (同步化排程) 索引標籤上，按一下 **Refresh Now** (立即重新整理)。
8. 驗證已成功完成同步化，且所有次要管理伺服器都可使用。

備份管理伺服器登錄

備份管理伺服器登錄可確保您能夠回復到先前的組態。例如，若您必須完全解除安裝目前的 DRA 版本，並使用前一個 DRA 版本，則先前登錄設定的備份可讓您輕鬆復原先前的組態和安全性設定。

不過，請小心編輯登錄。如果登錄有錯誤，管理伺服器可能無法正常運作。如果升級期間發生錯誤，您可以使用登錄設定的備份來還原登錄。如需詳細資訊，請參閱*登錄編輯程式說明*。

重要： 還原登錄時，DRA 伺服器版本、Windows OS 名稱和管理的網域組態必須完全相同。

重要： 升級之前，請將裝載DRA的機器製作Windows OS的備份，或建立機器的虛擬機器快照影像。

備份管理伺服器登錄：

1. 執行 regedit.exe。
2. 在 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\MissionCriticalSoftware\OnePoint 節點上按右鍵，選取 **Export** (匯出)。
3. 指定用來儲存登錄機碼的檔案名稱和位置，然後按一下 **Save** (儲存)。

2.3.3 升級 DRA 管理伺服器

下列核對清單引導您完成整個升級程序。使用此程序來升級環境中的每一個伺服器集。使用「健康情況檢查公用程式」來建立目前 AD LDS 例項的備份 (如果還未這樣做)。

您可以將此升級程序延伸為多個階段，一次只升級一個MMS。此升級程序也可讓您在相同的MMS中，暫時包含執行先前DRA版本的次要伺服器，以及執行目前DRA版本的次要伺服器。在執行先前DRA版本的管理伺服器與執行目前DRA版本的伺服器之間，DRA支援同步化。不過，請注意DRA不支援在相同的管理伺服器或用戶端電腦上執行先前的 DRA 版本與目前的 DRA 版本。

在DRA 9.2或更新版本中，Workflow Automation伺服器組態會儲存在AD LDS而非登錄。從DRA 9.1或更舊版本升級至 DRA 9.2 或更新版本時，登錄組態會自動移至 AD LDS，並複製到所有次要伺服器。

警告： 在升級該 MMS 的主要管理伺服器之前，請勿升級次要管理伺服器。

步驟	詳細資料
執行健康情況檢查公用程式	安裝獨立 DRA 健康情況檢查公用程式，並使用服務帳戶來執行。修復任何問題。
執行測試升級	在實驗室環境中執行測試升級，以發現潛在的問題，將生產停機時間縮到最短。
決定升級順序	決定伺服器集的升級順序。
準備升級每一個 MMS	準備升級每一個 MMS。如需詳細資訊，請參閱升級前任務。
升級主要伺服器	升級適當 MMS 中的主要管理伺服器。
安裝新的次要伺服器	*(選用)* 若要將遠端網站的停機時間縮到最短，請安裝執行最新版 DRA 的本機次要管理伺服器。
部署使用者介面	部署使用者介面給助理管理員。
升級次要伺服器	升級 MMS 中的次要管理伺服器。
升級 DRA 報告	升級 DRA 報告。
升級 REST 延伸功能	執行 DRA REST 延伸功能安裝程式。
執行健康情況檢查公用程式	執行隨著升級一起安裝的「健康情況檢查公用程式」。修復任何問題。

升級主要管理伺服器

成功準備MMS之後，請升級主要管理伺服器。在完成升級主要管理伺服器之前，請勿升級AA用戶端電腦上的使用者介面。如需詳細資訊，請參閱部署 DRA 使用者介面。

附註： 如需更詳細的升級考量和指示，請參閱 *Directory and Resource Administrator 版本資訊*。

升級之前，請在您打算啟動此程序時通知 AA。如果您使用次要管理伺服器來專門執行先前的 DRA 版本，則也要識別此伺服器，讓 AA 在升級期間能夠繼續使用前一個 DRA 版本。

附註： 一旦升級主要管理伺服器，就無法從這部伺服器將委託、組態或規則設定，同步化到執行前一個 DRA 版本的次要管理伺服器。

安裝目前 DRA 版本的本機次要管理伺服器

在本端網站安裝新的次要管理伺服器來執行目前的 DRA 版本，有助於避免浪費成本來連接至遠端網站，同時縮短整體停機時間，以加速部署使用者介面。此為選用步驟，可讓AA在整個升級過程中使用目前的 DRA 版本和先前的 DRA 版本，直到部署完成。

如果您有下列一或多個升級需求，請考慮採用此選項：

- 您要求最短停機時間，或完全沒有停機時間。
- 您必須支援大量 AA，但無法立即升級所有用戶端電腦。
- 升級主要管理伺服器之後，您想要繼續支援存取先前的 DRA 版本。
- 環境中有一個 MMS 橫跨多個站點。

例如，若MMS由倫敦站點的主要管理伺服器和東京站點的次要管理伺服器組成，請考慮在東京站點安裝一部次要伺服器，再新增至對應的 MMS。此額外的伺服器更能平衡東京網站的日常管理負載，可讓來自任一網站的AA使用先前的DRA版本和目前的DRA版本，直到升級完成。此外，AA不會經歷停機時間，因為您可以立即部署目前的 DRA 使用者介面。如需升級使用者介面的相關資訊，請參閱部署 DRA 使用者介面。

部署 DRA 使用者介面

通常，在升級主要管理伺服器和一部次要管理伺服器之後，您應該部署目前的 DRA 使用者介面。不過，對於必須使用主要管理伺服器的 AA，務必先安裝「委託和組態」主控台來升級其用戶端電腦。如需詳細資訊，請參閱規劃 DRA 升級。

如果您時常透過 CLI 或 ADSI 提供者來執行批次處理，或經常產生報告，請考慮在專用的次要管理伺服器上安裝這些使用者介面，以適當維持整個 MMS 的負載平衡。

您可以讓AA安裝DRA使用者介面，或透過群組規則來部署這些介面。您還可以輕鬆快速地將Web主控台部署給多個 AA。

附註： 您無法在相同的DRA伺服器並存執行多個版本的DRA元件。如果您打算逐漸升級AA用戶端電腦，請考慮安裝 Web 主控台，以確保可立即存取執行目前 DRA 版本的管理伺服器。

升級次要管理伺服器

升級次要管理伺服器時，視管理需求而定，您可以視需要升級每一部伺服器。另外也要考慮您打算如何升級和部署 DRA 使用者介面。如需詳細資訊，請參閱部署 DRA 使用者介面。

例如，一般升級途徑可能包含下列步驟：

1. 升級一部次要管理伺服器。
2. 指示使用此伺服器的 AA 安裝適當的使用者介面，例如「帳戶和資源管理」主控台。
3. 重複上述步驟 1 和 2，直到完成升級 MMS。

升級之前，請在您打算啟動此程序時通知 AA。如果您使用次要管理伺服器來專門執行先前的 DRA 版本，則也要識別此伺服器，讓AA在升級期間能夠繼續使用前一個DRA版本。當您完成此MMS的升級程序，且所有 AA 用戶端電腦都執行已升級的使用者介面時，請將剩餘的任何舊版 DRA 伺服器離線。

2.3.4 升級 DRA REST 延伸功能

若要將 Web 主控台和 REST 延伸功能升級至 Directory and Resource Administator 9.2，您必須使用 DRA 9.0.1 或更新版本。關於需求資訊，請參閱 DRA Web 主控台和延伸功能需求。

升級 DRA Web 主控台和延伸功能：

1. 安裝 DRA 安裝套件之後，導覽至安裝媒體的解壓縮位置，在 DRARESTExtensionsInstaller.exe 檔案上按右鍵，並選取 **Run as administrator** (以系統管理員身分執行)。
2. 遵循安裝精靈的指示進行，直到安裝完成，然後按一下 **Finish** (完成)。

如需安裝精靈各步驟的詳細資訊，請參閱新安裝的步驟：安裝 DRA REST 延伸功能。

升級未封裝內容

升級至更新版本的DRA時，您需要保留您對Web伺服器上的Web主控台所做的一切自訂。為了輕鬆完成此工作，DRA提供內建於DRAREST延伸功能安裝程式的「自訂升級」公用程式。當您在Web伺服器上執行 DRARESTExtensionsInstaller.exe 來升級 REST 延伸功能時，此公用程式會自動執行。您也可以在安裝之外，從 DRA 安裝目錄手動重新執行此公用程式。

「自訂升級」公用程式的部分程序是在升級開始之前製作自訂的備份。在升級過程中，此公用程式會對因為升級而發生的所有變更建立記錄檔案，而且對於無法自動更新的任何自訂項目，也會加入警告。

在最佳實務上，建議您在升級之後檢閱記錄。必要的話，您可以從備份資料夾中複製升級前的自訂來復原。當「自訂升級」公用程式開啟時，您可以定義升級自訂的資料夾路徑，或使用預設路徑 (自動填入)。

以下提供升級自訂和自訂備份的預設路徑：

- 預設值 CustomFolderPath：C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom
- 預設備份資料夾：$CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup

2.3.5 升級報告

升級 DRA 報告之前，請確定環境符合 NRC 3.2 的最低需求。如需安裝需求和升級考量的相關資訊，請參閱《*NetIQ Reporting Center 報告指南*》。

步驟	詳細資料
停用 DRA 報告支援	若要確保升級過程中不執行報告收集器，請在「委託和組態」主控台的 Reporting Service Configuration (報告服務組態) 視窗中，停用 DRA 報告支援。
使用適當的身分證明登入 SQL 例項伺服器	使用系統管理員帳戶，登入您已經為報告資料庫安裝 SQL 例項的 Microsoft Windows 伺服器。確保此帳戶在 SQL Server 上具有本機管理權限及「系統管理員」權限。
執行 DRA 報告安裝程式	從安裝套件執行 DRAReportingSetup.exe，並遵循安裝精靈的指示進行。
執行 NRC 安裝程式	*條件式：*如果 NRC Web 服務安裝在不同電腦上，請登入已安裝此 Web 服務的電腦，然後執行 NRCSetup.exe 來升級 NRC Web 服務。 **附註：** 如果組態資料庫安裝在不同的伺服器，則必須先升級
在用戶端電腦上執行 NRC 安裝程式	在所有 NRC 用戶端電腦上執行 NRCSetup.exe。
啟用 DRA 報告支援	在主要管理伺服器上，在「委託和組態主控台」啟用報告。

如果環境使用SSRS整合，則您需要重新部署報告。如需關於重新部署報告的詳細資訊，請參閱文件網站上的《*報告中心指南*》。

3 元件和程序組態

本章節提供第一次設定 DRA 的相關資訊，包括伺服器和伺服器自定、主控台和主控台自定、Office 365、公用資料夾管理及連接至伺服器。

3.1 啟始組態

如果您是第一次安裝 Directory and Resource Administrator，本節描述必要的組態步驟。

3.1.1 組態核對清單

使用下列核對清單來引導您設定首次使用 DRA。

步驟	詳細資料
安裝 DRA 授權	使用「健康情況檢查公用程式」來套用 DRA 授權。如需 DRA 授權的相關資訊，請參閱授權需求。
設定 DRA 伺服器和功能	設定 MMS、複製例外狀況、檔案複寫、事件戳記、快取、ADLDS、動態群組、資源回收筒、報告、整合的變更歷程以及工作流程伺服器。
設定委託和組態用戶端	設定在存取項目的方式，以及將如何在「組態和委託用戶端」中顯示項目。
設定 Web 用戶端	設定自動登出、證書、伺服器連線以及驗證元件

3.1.2 安裝或升級授權

DRA 需要授權金鑰檔案。此檔案包含授權資訊，且安裝在管理伺服器上。安裝管理伺服器之後，使用「健康情況檢查公用程式」來安裝 NetIQ 公司提供給您的試用授權金鑰檔案 (TrialLicense.lic)。

若要升級現有或試用授權，請開啟「委託和組態」主控台，然後導覽至**組態管理**> **更新授權**。升級授權時，請在每一部管理伺服器上升級授權檔案。

您可以透過「委託和組態」主控台或「帳戶和資源管理」主控台來檢視產品授權。若要檢視您的產品授權，請導覽至**檔案**功能表 > **DRA 內容** > **授權**。

3.1.3 設定 DRA 伺服器和功能

使用 DRA 來管理 Active Directory 任務的最低存取權限時有許多需要設定的元件和程序。包括一般和用戶端元件組態。本節提供需要針對 DRA 設定之一般元件和程序的資訊。

設定多主機組

MMS環境會使用多部管理伺服器來管理相同的網域和成員伺服器組。MMS由一部主要管理伺服器及多部次要管理伺服器所組成。

管理伺服器的預設模式是「主要」。當您將次要伺服器新增至MMS環境時，請謹記次要管理伺服器只能屬於一個伺服器組。

若要確保組合中每部伺服器管理相同的資料，請定期同步化次要伺服器與主要管理伺服器。若要減少維護，請對網域樹系中的所有管理伺服器使用相同的服務帳戶。

重要：

- 安裝次要伺服器時,請選取安裝程式中的 **次要管理伺服器**。
- 新的次要伺服器的DRA版本必須與主要DRA伺服器相同，才能在次要伺服器中使用所有主要伺服器提供的功能。

新增次要管理伺服器

您可以將次要管理伺服器新增至「委託和組態」用戶端中現有的 MMS。您必須擁有適當的權限，才能新增次要伺服器。例如，包含在內建的「設定伺服器和網域」角色中的權限。

附註： 為了成功新增次要伺服器，您必須先在管理伺服器電腦上安裝 Directory and Resource Administrator 產品。如需詳細資訊，請參閱 安裝 DRA 管理伺服器。

若要新增次要管理伺服器，請以滑鼠右鍵按一下「組態管理」節點上的 **Administration Servers (管理伺服器)**，然後選取 **Add Secondary Server (新增次要伺服器)**。

升級次要管理伺服器

您可以將次要管理伺服器升級為主要管理伺服器。當您將次要管理伺服器升級為主要管理伺服器時，現有的主要管理伺服器會變成伺服器組中的次要管理伺服器。您必須擁有適當的權限，才能升級次要管理伺服器，例如，包含在內建的「設定伺服器和網域」角色中的權限。在升級次要管理伺服器之前請同步化 MMS，以便讓它具有最新的組態。

如需同步化 MMS 的詳細資訊，請參閱 排程同步。

附註： 新升級的主要伺服器只能連接至在升級程序期間可用的次要伺服器。如果次要伺服器在升級程序期間變成無法使用，請聯絡技術支援。

若要升級次要管理伺服器：

1. 導覽至**Configuration Management (組態管理)** > **Administration Servers (管理伺服器)** 節點。
2. 在右窗格中，選取您想要升級的次要管理伺服器。
3. 在「任務」功能表上，按一下 **Advanced (進階)** > **Promote Server (升級伺服器)**。

重要： 當次要伺服器的服務帳戶與主要伺服器不同，或是次要伺服器安裝在與主要伺服器不同的網域上 (受信任網域/非受信任網域)，而且您升級次要伺服器時，請確定您在升級次要伺服器之前委託下列角色：**稽核所有物件**、**設定伺服器和網域**以及**產生 UI 報告**。然後驗證 MMS 同步化已成功。

降級主要管理伺服器

您可以將主要管理伺服器降級為次要管理伺服器。您必須擁有適當的權限，才能降級主要管理伺服器，例如，包含內建的「設定伺服器和網域」角色中的權限。

若要降級主要管理伺服器：

1. 導覽至 **Configuration Management (組態管理)** > **Administration Servers (管理伺服器)** 節點。
2. 在右窗格中，選取您想要降級的主要管理伺服器。
3. 在「任務」功能表上，按一下 **Advanced (進階)** > **Demote Server (降級伺服器)**。
4. 指定您想要指定為新主要管理伺服器的電腦，然後按一下**確定**。

排程同步

同步會確定MMS中的所有管理伺服器都使用相同的組態資料。雖然您可以隨時手動同步化伺服器，但是預設排程設為每 4 小時同步化 MMS。您可以修改此排程以符合您的企業需求。

您必須擁有適當的權限，才能修改同步排程或是手動同步化MMS伺服器，例如，包含在內建的「設定伺服器和網域」角色中的權限。

若要存取同步排程或者要手動同步化，請導覽至 **Configuration Management (組態管理)** > **Administration Servers (管理伺服器)**，然後使用 **Tasks (任務)** 功能表或以滑鼠右鍵按一下所選伺服器上的選項。同步排程位於所選伺服器的「內容」中。

瞭解同步選項

同步 MMS 伺服器基本上有四個不同的選項：

- 選取主要伺服器並且同步化所有次要伺服器「Synchronize All Servers」(同步化所有伺服器)
- 選取次要伺服器並且僅同步化該伺服器
- 針對主要和次要伺服器獨立設定同步排程
- 針對所有伺服器設定同步排程。當您在主要伺服器同步排程中選取下列設定時，系統會啟用此選項：

  Configure secondary Administration servers when refreshing the primary Administration server (當重新整理主要管理伺服器時設定次要管理伺服器)

  附註： 如果您取消勾選此選項，組態檔案會複製到主要排程上的次要伺服器，但是屆時不會由次要伺服器載入，而是根據在次要伺服器上設定的排程來載入。如果伺服器是在不同的時區，這個選項相當實用。例如，即使時間會因為時區而不同，您可以將所有伺服器設定為在午夜時重新整理其組態。

管理 Clone Exceptions (複製例外狀況)

複製例外狀況可讓您定義使用者、群組、聯絡人及電腦的內容，在複製其中一個物件時不會複製該項目。

如果擁有適當權限，您便可以管理複製例外狀況。「管理複製例外狀況」角色會授與檢視、建立及刪除複製例外狀況的能力。

若要檢視或刪除現有複製例外狀況，或者要建立新的複製例外狀況，請導覽至 **Configuration Management (組態管理)** > **Clone Exceptions (複製例外狀況)** > **Tasks (任務)** 或以滑鼠右鍵按一下功能表。

File Replication (檔案複寫)

當您建立自定工具時，可能需要先安裝 DRA 用戶端電腦上的自定工具所使用的支援檔案，自定工具才能夠執行。您可以使用 DRA 檔案複寫功能快速輕易地將自定工具支援檔案從主要管理伺服器複寫至MMS中的次要管理伺服器，以及複寫至DRA用戶端電腦。檔案複寫也可以用來將觸發程序檔從主要伺服器複寫至次要伺服器。

您可以一併使用自定工具和檔案複寫來確保DRA用戶端電腦可以存取自定工具檔案。DRA會將自定工具檔案複寫至次要管理伺服器，以確保連接至次要管理伺服器的DRA用戶端電腦可以存取自定工具。

DRA會在MMS同步程序期間，將主要管理伺服器上的自定工具檔案複寫至次要管理伺服器。當DRA用戶端電腦連接至管理伺服器時，DRA 會將自定工具檔案下載到 DRA 用戶端電腦。

附註： DRA 會將自定工具檔案下載到 DRA 用戶端電腦上的下列位置：

{DRAInstallDir}\{MMS ID}\Download

MMSID 是多主機組的識別碼，DRA 會從該位置下載自定工具檔案。

上傳自定工具檔案以進行複寫

當您將檔案上傳至主要管理伺服器時，您會在MMS組合中的主要管理伺服器與所有次要管理伺服器之間指定想要上傳及複寫的檔案。DRA 可讓您上傳文件庫檔案、程序檔檔案及可執行檔檔案。

「複寫檔案」角色可讓您從主要管理伺服器將檔案複寫至MMS中的所有次要管理伺服器以及DRA用戶端電腦。「複寫檔案」角色包含下列權限：

- **從伺服器刪除檔案：** 這個權限可讓DRA刪除不再存在於主要管理伺服器、次要管理伺服器及DRA用戶端電腦上的檔案。
- **設定檔案資訊：** 這個權限可讓 DRA 更新在次要管理伺服器上之檔案的檔案資訊。
- **將檔案上傳至伺服器：** 這個權限可讓 DRA 從 DRA 用戶端電腦將檔案上傳至主要管理伺服器。

附註： 使用「委託和組態」主控台中的「檔案複寫」使用者介面時，您一次只能上傳一個檔案進行複寫。

若要將自定工具檔案上傳至主要管理伺服器：

1. 導覽至 **Configuration Management (組態管理)** > **File Replication (檔案複寫)**。
2. 在「任務」功能表上，按一下**上傳檔案**。
3. 若要搜尋及選取您想要上傳的檔案，請按一下**瀏覽**。
4. *如果您想要將選取的檔案下載至所有 DRA 用戶端電腦*，請選取**Download to all client computers (下載至所有用戶端電腦)** 核取方塊。
5. *如果您想要註冊 COM 文件庫*，請選取 **Register COM library (註冊 COM 文件庫)** 核取方塊。
6. 按一下**「確定」**。

附註：

- DRA 會將需要複寫至其它次要管理伺服器的程序檔檔案或支援檔案，上傳至主要管理伺服器的 *{DRAInstallDir}*\FileTransfer\Replicate 資料夾。
  {DRAInstallDir}\FileTransfer\Replicate 資料夾也稱為 *{DRA_Replicated_Files_Path}*。

- DRA 會將需要複寫的程序檔檔案或支援檔案，上傳至 DRA 用戶端電腦中主要管理伺服器的 *{DRAInstallDir}*\FileTransfer\Download 資料夾。
- 上傳至主要管理伺服器的自定工具檔案會在下一個編程同步化時或者透過手動同步，分散到次要管理伺服器。

在管理伺服器之間複寫多個檔案

如果您有多個檔案想要在MMS中的主要管理伺服器與次要管理伺服器之間上傳及複寫，您可以藉由將檔案複製到主要管理伺服器複寫目錄 (位置如下)，手動上傳這些檔案以進行複寫：

{DRAInstallDir}\FileTransfer\Replicate

複寫目錄是在安裝 DRA 時建立的。

管理伺服器會自動識別複寫目錄中的檔案，並且在下一個編程同步化期間於管理伺服器之間複寫檔案。同步之後，DRA 會在「委託和組態」主控台的「檔案複寫」視窗中顯示已上傳的檔案。

附註： 如果您想要複寫的檔案包含必須註冊的COM文件庫，您就無法手動將檔案複製到管理伺服器複寫目錄。您必須使用「委託和組態」主控台來上傳每個檔案並且註冊 COM 文件庫。

將多個檔案複寫至 DRA 用戶端電腦

如果您有多個檔案想要在主要管理伺服器與 DRA 用戶端電腦之間複寫，您可以將檔案複製到主要管理伺服器上的用戶端複寫目錄，位置如下：

{DRAInstallDir}\FileTransfer\Download

用戶端複寫目錄是在安裝 DRA 時建立的。

管理伺服器會自動識別下載資料夾中的檔案，並且在下一個編程同步化期間將檔案複寫至次要管理伺服器。同步之後，DRA 會在「委託和組態」主控台的「檔案複寫」視窗中顯示已上傳的檔案。DRA 會在 DRA 用戶端電腦於複寫之後第一次連接至管理伺服器時，將複寫的檔案下載至 DRA 用戶端電腦。

附註： 如果您想要複寫的檔案包含必須註冊的COM文件庫，您就無法將檔案複製到管理伺服器下載目錄。您必須使用「委託和組態」主控台來上傳每個檔案並且註冊 COM 文件庫。

Event Stamping (事件戳記)

當啟用AD Domain Services稽核時，如果已設定DRA服務帳戶或網域存取帳戶其中之一，則DRA事件會記錄為已由上述其中一個帳戶產生。「事件戳記」會進一步採用這個功能，產生額外的ADDS事件，該事件會識別執行操作的助理管理員。

針對要產生的事件，您必須設定AD DS稽核並且在DRA管理伺服器上啟用「事件戳記」。啟用「事件戳記」後，您將能檢視助理管理員在「變更監控事件」報告中所做的變更。

- 若要設定 AD DS 稽核，請參閱 AD DS 稽核 (https://technet.microsoft.com/en-us/library/cc731607(v=ws.10).aspx)
- 若要設定「變更監控」整合，請參閱設定整合的變更歷程伺服器。
- 若要啟用「事件戳記」，請以DRA管理員身分開啟「委託和組態」主控台，然後執行下列動作：
  1. 導覽至 **Configuration Management (組態管理)** > **Update Administration Server Options (更新管理伺服器選項)** > **Event Stamping (事件戳記)**。

2. 選取物件類型，然後按一下更新。
3. 選取要用於該物件類型之「事件戳記」的屬性。

   DRA 目前針對使用者、群組、聯絡人、電腦及組織單位支援「事件戳記」。

   DRA 也需要屬性存在於您每個管理的網域的 AD 綱要中。如果您在設定「事件戳記」之後新增受管理的網域，您應該要知道這個情形。如果您新增的管理的網域其中未包含選取的屬性，來自該網域的操作不會以「事件戳記」資料進行稽核。

   DRA 將會修改這些屬性，因此您應該選取 DRA 或您的環境中任何其它應用程式未使用的屬性。

如需關於「事件戳記」的詳細資訊，請參閱事件戳記的運作方式。

針對群組啟用多管理員

當您啟用多管理員管理群組的支援時，系統會使用兩個預設屬性其中之一來儲存群組的管理員。當執行MicrosoftExchange時的屬性是msExchCoManagedByLink屬性。未執行MicrosoftExchange時的預設屬性是 nonSecurityMember 屬性。後者選項可以修改。但是，如果您需要變更此設定，我們建議您聯絡技術支援以決定適當的屬性。

若要針對群組啟用多管理員支援：

1 在左側窗格中，按一下 **Configuration Management (組態管理)**。

2 在右窗格的「通用任務」下方，按一下 **Update Administration Server Options (更新管理伺服器選項)**。

3 在「啟用群組多管理員支援」索引標籤上，選取 **Enable support for group's multiple managers (啟用群組的多管理員支援)** 核取方塊。

加密的通訊

此功能可讓您啟用或停用在「委託和組態」與ARM用戶端及管理伺服器之間使用加密的通訊。根據預設，DRA會加密帳戶密碼。此功能不會加密Web用戶端或PowerShell通訊，這些項目由伺服器證書個別處理。

使用加密的通訊會影響效能。加密的通訊預設為停用。如果您啟用此選項，使用者介面與管理伺服器之間通訊期間的資料會加密。DRA 會針對遠端程序呼叫 (RPC) 使用 Microsoft 標準加密。

若要啟用加密的通訊，請導覽至**(Configuration Management)組態管理**>**Update Administration Server Options (更新管理伺服器選項)** > **General (一般)** 索引標籤，然後選取 **Encrypted Communications (加密的通訊)** 核取方塊。

附註： 若要加密管理伺服器與使用者介面之間的所有通訊，您必須擁有適當的能力，例如內建「設定伺服器和網域」角色中所包含的權限。

Defining Virtual Attributes (定義虛擬屬性)

使用虛擬屬性，您可以建立新的內容並且讓這些內容與使用者、群組、動態通訊群組、聯絡人、電腦及 OU 產生關聯。虛擬屬性可讓您建立新的內容，而不需要您延伸 Active Directory 綱要。

使用虛擬屬性，您可以將新內容新增至 Active Directory 中的物件。您只能建立、啟用、停用、關聯及取消關聯主要管理伺服器上的虛擬屬性。DRA會儲存您在ADLDS中建立的虛擬屬性。DRA會在MMS同步程序期間，將主要管理伺服器上的虛擬屬性複寫至次要管理伺服器。

如果擁有適當權限，您便可以管理虛擬屬性。「管理虛擬屬性」角色會授與建立、啟用、關聯、取消關聯、停用及檢視虛擬屬性的權限。

建立虛擬屬性

您需要*建立虛擬屬性*權限才能建立虛擬屬性，需要*檢視虛擬屬性*權限才能檢視虛擬屬性。

若要建立虛擬屬性，請導覽至 **Configuration Management (組態管理)** > **Virtual Attributes (虛擬屬性)** > **Managed Attributes (受管理的屬性)** 節點，然後按一下「任務」功能表上的 **New Virtual Attribute (新增虛擬屬性)**。

讓虛擬屬性與物件產生關聯

您只能讓已啟用的虛擬屬性與 Active Directory 物件產生關聯。一旦讓虛擬屬性與物件產生關聯，虛擬屬性就可以作為物件內容的一部分。

若要透過 DRA 使用者介面公開虛擬屬性，您需要建立自定內容頁。

若要讓虛擬屬性與物件產生關聯，請導覽至 **Configuration Management (組態管理)** > **Virtual Attributes (虛擬屬性)** > **Managed Attributes (受管理的屬性)** 節點，以滑鼠右鍵按一下您想要使用的虛擬屬性，然後選取 **Associate (關聯)** > (物件類型)。

附註：

- 您只能讓虛擬屬性與使用者、群組、動態通訊群組、電腦、聯絡人及 OU 產生關聯。
- 當您讓虛擬屬性與物件產生關聯時，DRA 會自動建立兩個預設自定權限。助理管理員需要這些自定權限才能管理虛擬屬性。

取消關聯虛擬屬性

您可以從 Active Directory 物件取消虛擬屬性的關聯。您建立的任何新物件在物件內容中都不會顯示取消關聯的虛擬屬性。

若要從 Active Directory 物件取消虛擬屬性的關聯，請導覽至 **Configuration Management (組態管理)** > **Virtual Attributes(虛擬屬性)** > **Managed Classes (受管理的類別)** > (物件類型) 節點。以滑鼠右鍵按一下虛擬屬性，然後選取 **Disassociate (取消關聯)**。

停用虛擬屬性

如果虛擬屬性未與 Active Directory 物件產生關聯，您可以停用虛擬屬性。當您停用虛擬屬性時，管理員無法檢視或讓虛擬屬性與物件產生關聯。

若要停用虛擬屬性，請導覽至 **Configuration Management (組態管理)** > **Managed Attributes (受管理的屬性)**。在清單窗格中以滑鼠右鍵按一下想要的屬性，然後選取 **Disable (停用)**。

設定快取

管理伺服器會建立及維護**帳戶快取**，其中包含 Active Directory 的管理的網域部分。DRA 會在管理使用者帳戶、群組、聯絡人及電腦帳戶時，使用帳戶快取來改善效能。

您必須擁有適當的權限，才能排程快取重新整理時間或檢視快取狀態，例如，包含在內建的「設定伺服器和網域」角色中的權限。

附註： 若要在包含受管理子樹狀結構的網域中執行遞增的帳戶快取，請確保服務帳戶具有「刪除的物件」容器的讀取權限，以及子樹狀結構網域中所有物件的讀取權限。您可以使用「刪除的物件公用程式」來驗證及委託適當的權限。

完整重新整理與遞增的重新整理

遞增的帳戶快取重新整理只會更新自從上次重新整理之後變更的資料。遞增的重新整理提供簡化的方式，與您持續變化的 Active Directory 保持同步。使用遞增的重新整理以快速地更新帳戶快取，而且對企業產生最小的影響。

重要： Microsoft 伺服器將同時連線至 WinRM/WinRS 工作階段的使用者數量限制為五位，並將每位使用者的 Shell 數量限制為五個，以確保 DRA 次要伺服器的相同使用者帳戶受到五個 Shell 的限制。

遞增的重新整理會更新下列資料：

- 新的和複製的物件
- 刪除的和移動的物件
- 群組成員
- 已修改物件的所有已快取物件內容

完整帳戶快取重新整理會針對指定的網域重建 DRA 的帳戶快取。

附註： 當完整帳戶快取重新整理執行時，DRA 使用者無法使用網域。

執行完整帳戶快取重新整理

您必須擁有適當的權限，才能重新整理帳戶快取，例如，包含在內建的「設定伺服器和網域」角色中的權限。

若要執行立即完整帳戶快取重新整理：

1. 導覽至 **Configuration Management (組態管理)** > **Managed Domains (受管理的網域)**。
2. 以滑鼠右鍵按一下想要的網域，然後選取內容。
3. 按一下 **Full refresh (完整重新整理)** 索引標籤中的 **Refresh Now (立即重新整理)**。

預設排程時間

您應該重新整理帳戶快取的頻率，取決於您的企業變更的頻率。使用遞增的重新整理以經常更新帳戶快取，確保 DRA 具有最新的 Active Directory 相關資訊。

根據預設，管理伺服器會在以下時間執行遞增的帳戶快取重新整理：

領域類型	預設排程重新整理時間
受管理的網域	每 5 分鐘
信任的網域	每小時

您無法排程 FACR，但是，DRA 會在以下情況時執行自動 FACR：

- 在您第一次設定受管理的網域之後。

- 在您將 DRA 從舊版升級到完整版本之後。
- 在您安裝 DRA 服務包之後。

執行完整帳戶快取重新整理需要數分鐘的時間。

考量事項

您必須定期重新整理帳戶快取，以確保 DRA 具有最新的資訊。在執行或排程帳戶快取重新整理之前，請檢閱下列考量事項：

- 若要執行遞增的帳戶快取重新整理，管理伺服器服務帳戶或存取帳戶必須有存取受管理或受信任網域之 Active Directory 中已刪除物件的權限。
- 當 DRA 執行帳戶快取重新整理時，管理伺服器不會包含來自受信任網域的網域本機安全性群組。因為快取不包含這些群組，所以 DRA 不允許您從受信任網域將網域本機安全性群組，新增至受管理成員伺服器上的本機群組。
- 如果您從帳戶快取重新整理略過受信任網域，管理伺服器也會從網域組態重新整理略過該網域。
- 如果您在帳戶快取重新整理中包含先前略過的受信任網域，則會針對管理的網域執行完整帳戶快取重新整理。這樣可確保管理的網域之管理伺服器上的帳戶快取，會正確反映您受管理或受信任網域中的群組成員資格資料。
- 如果您將遞增的帳戶快取重新整理間隔設為永不，管理伺服器只會執行完整帳戶快取重新整理。完整帳戶快取重新整理需要一些時間，在這段時間內您無法管理此網域中的物件。
- DRA 無法自動判斷變更是何時透過其它工具 (例如 Microsoft Directory Services) 執行的。在 DRA 外部執行的操作會影響快取資訊的正確性。例如，如果您使用其它工具將信箱新增至使用者帳戶，在您更新帳戶快取之前，無法使用 Exchange 來管理此信箱。
- 執行完整帳戶快取重新整理會刪除快取中維護的上次登入統計資料。然後管理伺服器會從所有網域控制器收集上次登入資訊。

啟用 Active Directory 印表機收集

AD 印表機收集預設為停用。若要啟用，請導覽至**組態管理**>**更新管理伺服器選項**>**一般**索引標籤，然後選取「收集印表機」核取方塊。

AD LDS

您可以對特定網域設定ADLDS清理重新整理以在排程時間執行。預設設定是「永不」重新整理。您也可以檢視清理狀態以及檢視與 AD LDS (ADAM) 組態相關的特定資訊。

若要設定排程或檢視ADLDS清理的狀態，以滑鼠右鍵按一下**AccountandResourceManagement(帳戶和資源管理)** > **All My Managed Objects (我的所有受管理物件)** 節點中想要的網域，然後分別選取 **Properties (內容)**> **Adlds Cleanup Refresh Schedule (Adlds 清理重新整理排程)** 或 **Adlds Cleanup status (Adlds 清理狀態)**。

若要檢視AD LDS (ADAM)組態資訊，請導覽至**Configuration Management (組態管理)** > **Update Server Options (更新伺服器選項)** > **ADAM Configuration (ADAM 組態)**。

動態群組

動態群組是一個其成員資格變更，根據您在群組內容中設定之已定義準則組的群組。在「網域內容」中，您可以設定特定網域的動態群組重新整理在排程時間執行。預設設定是「永不」重新整理。您也可以檢視重新整理狀態。

若要設定排程或檢視動態群組重新整理的狀態，以滑鼠右鍵按一下**AccountandResourceManagement (帳戶和資源管理)** > **All My Managed Objects (我的所有受管理物件)** 節點中想要的網域，然後分別選取 **Properties (內容)** > **Dynamic group refresh (動態群組重新整理)** 或 **Dynamic group status (動態群組狀態)**。

如需關於動態群組的詳細資訊，請參閱DRA 動態群組。

設定資源回收筒

您可以針對每個 Microsoft Windows 網域或每個網域內的物件啟用或停用資源回收筒，以及設定您想要在何時及如何進行資源回收筒清理。

如需關於使用資源回收筒的詳細資訊，請參閱資源回收筒。

啟用資源回收筒

您可以針對特定MicrosoftWindows網域和這些網域內的物件啟用資源回收筒。根據預設，DRA會針對它管理的每個網域及網域的所有物件啟用資源回收筒。您必須是DRA管理員或DRA組態管理員群組的成員，才能啟用資源回收筒。

如果您的環境包含下列組態，請使用資源回收筒公用程式以啟用此功能：

- DRA 管理此網域的子樹狀結構。
- 管理伺服器服務或存取帳戶沒有建立資源回收筒容器、將帳戶移至此容器，以及修改此容器中帳戶的權限。

您也可以使用資源回收筒公用程式，來驗證管理伺服器服務或存取帳戶在資源回收筒容器上的權限。

若要啟用資源回收筒，以滑鼠右鍵按一下**資源回收筒**節點中想要的網域，然後選取**啟用資源回收筒**。

停用資源回收筒

您可以針對特定 Microsoft Windows 網域和這些網域內的物件停用資源回收筒。如果已停用的資源回收筒包含帳戶，您就無法檢視、永久刪除或還原這些帳戶。

您必須是 DRA 管理員或 DRA 組態管理員 AA 群組的成員，才能停用資源回收筒。

若要停用資源回收筒，以滑鼠右鍵按一下**資源回收筒**節點中想要的網域，然後選取**停用資源回收筒**。

設定資源回收筒物件和清理

資源回收筒清理的預設設定為每天。您可以將此組態變更為每 x 天清理網域資源回收筒。在排程清理期間，資源回收筒會刪除比您針對每個物件類型所設定天數更舊的物件。每個類型的預設設定是刪除 1 天以前的物件。您可以藉由停用、重新啟用及設定要針對每個物件類型刪除的物件留存期，自定資源回收筒清理的行為。

若要設定資源回收筒清理，請選取「委託和組態」主控台中想要的網域，然後移至**任務**>**內容**>**資源回收筒**索引標籤。

Reporting Configuration (報告組態)

下列章節提供 DRA 管理報告和您可以啟用之報告收集器的概念資訊。若要存取您可以在其中設定收集器的精靈，請導覽至 **Configuration Management (組態管理)** > **Update Reporting Service Configuration (更新報告服務組態)**。

設定 Active Directory Collector

Active Directory Collector 會從 Active Directory 收集 DRA 中每個受管理使用者、群組、聯絡人、電腦、OU及動態通訊群組的指定屬性組。這些屬性是儲存在報告資料庫中，用來在報告主控台中產生報告。

您可以設定 Active Directory Collector 以指定要收集哪些屬性以及在報告資料庫中儲存哪些屬性。您也可以設定收集器在哪個 DRA 管理伺服器上執行。

設定 DRA Collector

DRA Collector 會收集您的 DRA 組態的相關資訊，並且將該資訊儲存在報告資料庫中，該資訊是用來在報告主控台中產生報告。

若要啟用 DRA Collector，您必須指定收集器在哪個 DRA 管理伺服器上執行。最佳實務是您排程 DRA Collector在 Active Directory Collector 成功執行之後執行，以及在伺服器負載最少或一般上班時間以外的期間執行。

設定 Office 365 租用戶收集器

Office 365 租用戶收集器會收集已同步化到 Office 365 之受管理使用者的相關資訊，並且將該資訊儲存到報告資料庫中，該資訊是用來在報告主控台中產生報告。

若要啟用 Office 365 收集器，您必須指定收集器在哪個 DRA 管理伺服器上執行。

附註： Office 365 租用戶只能在其對應的網域 Active Directory Collector 成功執行收集之後，成功執行收集。

設定管理報告收集器

管理報告收集器會收集 DRA 稽核資訊，並且將該資訊儲存在報告資料庫中，該資訊是用來在報告主控台中產生報告。當您啟用收集器時，可以針對在 DRA 報告工具中執行的查詢，設定資料在資料庫中更新的頻率。

此組態需要 DRA 服務帳戶具有報告伺服器上 SQL Server 中的 **sysadmin** 權限。可設定選項定義如下：

- **稽核輸出資料間隔：**這是稽核資料從DRA追蹤記錄(LAS)輸出到SQLServer中「SMCubeDepot」資料庫的時間間隔。
- **管理報告摘要間隔：**這是稽核資料從SMCubeDepot資料庫抽入DRA報告資料庫的時間間隔，稽核資料可以在該報告資料庫中由 DRA 報告工具查詢。

蒐集上次登入統計資料

您可以設定 DRA 從管理的網域中的所有網域控制器收集上次登入統計資料。您必須擁有適當的權限，才能啟用及排程上次登入統計資料蒐集，例如，包含在內建的「設定伺服器和網域」角色中的權限。

根據預設，上次登入統計資料蒐集功能為停用。如果您想要蒐集上次登入統計資料，則必須啟用此功能。一旦您啟用上次登入統計資料蒐集，您便可以檢視特定使用者的上次登入統計資料，或顯示上次登入統計資料蒐集的狀態。

若要蒐集上次登入統計資料：

1. 導覽至 **Configuration Management (組態管理)** > **Managed Domains (受管理的網域)**。
2. 以滑鼠右鍵按一下想要的網域，然後選取**內容**。
3. 按一下**上次登入排程**索引標籤以設定上次登入統計資料收集。

整合的變更歷程

根據預設，整合的變更歷程 (UCH) 功能可讓您針對 DRA 所做的變更產生報告。

委託整合的變更歷程權限

若要管理整合的變更歷程，請將「整合的變更歷程伺服器管理」角色或以下適當的權限指定給助理管理員：

- 刪除整合的變更歷程伺服器組態
- 設定整合的變更歷程組態資訊
- 檢視整合的變更歷程組態資訊

若要委託 UCH 權限：

1. 按一下「委託管理」節點中的**權限**，然後使用搜尋物件功能以尋找並選取您想要的 UCH 物件。
2. 以滑鼠右鍵按一下其中一個選取的 UCH 權限，然後選取**委託角色和權限**。
3. 搜尋您想要委託權限的特定使用者、群組或 AA 群組。
4. 使用**物件選擇器**以尋找及新增您想要的物件，然後按一下**精靈**中的**角色和權限**。
5. 按一下 **ActiveView**，然後使用**物件選擇器**以尋找及新增您想要的物件。
6. 按**下一步**然後按一下**完成**以完成委託程序。

設定整合的變更歷程伺服器

若要設定 UCH 伺服器：

1. 啟動 Web 主控台，並且以 AA 身分證明登入。
2. 移至**管理 > 整合 > 整合的變更歷程**，然後按一下**新增**圖示。
3. 在「整合的變更歷程」組態中指定 UCH 伺服器名稱或 IP 位址、連接埠號碼、伺服器類型及存取帳戶詳細資料。
4. 測試伺服器連接然後按一下**確定**以儲存組態。
5. 視需要新增額外伺服器。

工作流程伺服器

若要在DRA中使用自動化工作流程，您必須在WindowsServer上安裝工作流程引擎，然後透過Web主控台設定「自動化工作流程」伺服器。

若要設定「自動化工作流程」伺服器，請登入 Web 主控台然後導覽至**管理**>**整合**>**自動化工作流程**。

如需安裝工作流程引擎的詳細資訊，請參閱《*自動化工作流程管理員指南*》。

3.1.4 設定委託和組態用戶端

「委託和組態」用戶端提供組態和委託任務的存取權，處理企業從分散式管理到規則強制的管理需求。您可以透過「委託和組態」主控台，設定有效管理企業所需的安全性模型和伺服器組態。

若要設定委託和組態用戶端：

1. 啟動「委託和組態」用戶端，然後導覽至 **Configuration Management (組態管理)** > **Update Administration Server Options (更新管理伺服器選項)**。
2. 按一下**用戶端選項**索引標籤，並且從顯示的組態選項中定義偏好的設定：
   - 允許使用者透過 ActiveView 進行搜尋
   - 從主控台清單隱藏僅來源物件
   - 顯示進階 Active Directory 物件
   - 顯示安全性指令
   - 當搜尋使用者時顯示資源和共享的信箱
   - 將使用者 UPN 字尾預設值設為目前網域
   - 一次可編輯的項目上限 (多重選取)
   - 搜尋設定
   - 回行選項
   - Exchange 信箱儲存限制單位

3.1.5 設定 Web 用戶端

您可以設定 Web 主控台使用智慧卡或多重要素驗證來進行驗證，也可以使用您自己的標誌和應用程式標題來自定品牌。

啟動 Web 主控台

您可以從執行網頁瀏覽器的任何電腦、iOS 裝置或 Android 裝置啟動 Web 主控台。若要啟動主控台，請在您的網頁瀏覽器地址欄位中指定適當的URL。例如，如果您已在HOUserver電腦上安裝Web元件，請在網頁瀏覽器的地址欄位中輸入 https://HOUserver/draclient。

附註： 若要在 Web 主控台中顯示最新的帳戶和 Microsoft Exchange 資訊，請將您的網頁瀏覽器設為在每次造訪時檢查快取頁面的新版本。

自動登出

您可以定義 Web 主控台在非使用狀態之後自動登出的時間增量，或者設為永不自動登出。

若要在 Web 主控台中設定自動登出，請導覽至**管理**>**組態**>**自動登出**。

DRA 伺服器連線

您可以在Web主控台中設定三個選項其中之一，以定義在登入時的DRA伺服器連線選項。一旦設定之後，管理員和助理管理員在登入 Web 主控台時，在**選項**下拉式面板中的連線組態便會相同。

- 一律使用預設 DRA 伺服器位置 (**一律**)
- 永不使用預設 DRA 伺服器位置 (**永不**)
- 僅在選取時使用預設 DRA 伺服器位置 (**僅在選取時**)

登入時每個選項的行為如下所述：

連線組態	登入螢幕 - 選項	連線選項描述
永遠	無	選項組態已停用
從未：	使用自動探查	自動尋找 DRA 伺服器，沒有組態選項可用
	連接至特定 DRA 伺服器	使用者設定伺服器和連接埠
	連接至管理特定網域的伺服器	使用者提供受管理的網域並且選擇連線選項： ◆ 使用自動探查 (在提供的網域中) ◆ 此網域的主要伺服器 ◆ 搜尋 DRA 伺服器 (在提供的網域中)
僅在選取時	使用自動探查	自動尋找 DRA 伺服器，沒有組態選項可用
	連接至預設 DRA 伺服器	已選取預設伺服器，且 DRA 伺服器組態已停用
	連接至特定 DRA 伺服器	使用者設定伺服器和連接埠
	連接至管理特定網域的伺服器	使用者提供受管理的網域並且選擇連線選項： ◆ 使用自動探查 (在提供的網域中) ◆ 此網域的主要伺服器 ◆ 搜尋 DRA 伺服器 (在提供的網域中)

若要在 Web 主控台中設定 DRA 伺服器連線，請導覽至**管理**>**組態**> **DRA 伺服器連接**。

REST 伺服器連線

REST 服務連接的組態包含設定預設伺服器位置和連線逾時 (以秒為單位)。您可以在 Web 主控台中設定三個選項其中之一，以定義在登入時的REST服務連線選項。一旦設定之後，管理員和助理管理員在登入 Web 主控台時，在**選項**下拉式面板中的連線組態便會相同。

- 一律使用預設 REST 服務位置 (**一律**)

- 永不使用預設 REST 服務位置 (永不)
- 僅在選取時使用預設 REST 服務位置 (僅在選取時)

登入時每個選項的行為如下所述：

連線組態	登入螢幕 - 選項	連線選項描述
永遠	無	選項組態已停用
從未：	使用自動探查	自動尋找 REST 伺服器，沒有組態選項可用
	連接至特定 REST 伺服器	使用者設定伺服器和連接埠
	連接至特定網域中的 REST 伺服器	使用者提供受管理的網域並且選擇連線選項： ◆ 使用自動探查 (在提供的網域中) ◆ 搜尋 REST 伺服器 (在提供的網域中)
僅在選取時	使用自動探查	自動尋找 REST 伺服器，沒有組態選項可用
	連接至預設 REST 伺服器	已選取預設 REST 伺服器，且 REST 伺服器組態已停用
	連接至特定 REST 伺服器	使用者設定伺服器和連接埠
	連接至特定網域中的 REST 伺服器	使用者提供受管理的網域並且選擇連線選項： ◆ 使用自動探查 (在提供的網域中) ◆ 搜尋 REST 伺服器 (在提供的網域中)

若要在 Web 主控台中設定 REST 服務連線，請導覽至**管理**>**組態**> **REST 服務連線**。

驗證

本節包含使用 Advanced Authentication 整合來設定智慧卡驗證、Windows 驗證及多重要素驗證的資訊。

智慧卡驗證

若要設定 Web 主控台根據使用者智慧卡的用戶端身分證明來接受使用者，您必須設定 Internet Information Services (IIS) 和 REST 服務組態檔案。

重要： 請確定智慧卡的證書也安裝在 Web 伺服器上的根證書儲存區，因為 IIS 必須要找到符合智慧卡上這些項目的證書。

1. 在 Web 伺服器上安裝驗證元件。
   - **1a** 啟動伺服器管理員。
   - **1b** 按一下 **Web 伺服器 (IIS)**。
   - **1c** 移至「角色服務」區段，然後按一下**新增角色服務**。
   - **1d** 移至「安全性」角色服務節點，然後選取 **Windows 驗證**和**用戶端證書對應驗證**。

2 在 Web 伺服器上啟用驗證。

2a 啟動 **IIS 管理員**。

2b 選取您的 Web 伺服器。

2c 在 IIS 區段下方尋找**驗證**圖示，並且連按兩下。

2d 啟用「Active Directory 用戶端證書驗證」和「Windows 驗證」。

3 設定 DRA 用戶端。

3a 選取您的 DRA 用戶端。

3b 在 IIS 區段下方尋找**驗證**圖示，並且連按兩下。

3c 啟用「Windows 驗證」並且停用「匿名驗證」。

4 在 DRA 用戶端上啟用 SSL 和用戶端證書。

4a 在 IIS 區段下方尋找 **SSL 服務**圖示，並且連按兩下。

4b 選取**需要 SSL**，然後在「用戶端」證書下方選取**需要**。

提示： 如果選項可以使用，請選取**需要 128 位元的 SSL**。

---

5 設定 REST 服務 Web 應用程式。

5a 選取您的 REST 服務 Web 應用程式。

5b 在 IIS 區段下方尋找**驗證**圖示，並且連按兩下。

5c 啟用「Windows 驗證」並且停用「匿名驗證」。

6 在 REST 服務 Web 應用程式上啟用 SSL 和用戶端證書。

6a 在 IIS 區段下方尋找 **SSL 服務**圖示，並且連按兩下。

6b 選取**需要 SSL**，然後在「用戶端」證書下方選取**需要**。

提示： 如果選項可以使用，請選取**需要 128 位元的 SSL**。

---

7 設定 WCF Web 服務檔案。

7a 選取您的 REST 服務 Web 應用程式並且切換至「內容檢視」。

7b 找到 .svc 檔案並且按一下滑鼠右鍵。

7c 選取**切換至功能檢視**。

7d 在 IIS 區段下方尋找**驗證**圖示，並且連按兩下。

7e 啟用「匿名驗證」並且停用其它所有驗證方法。

8 編輯 REST 服務組態檔案。

8a 使用文字編輯器以開啟 C:\inetpub\wwwroot\DRAClient\rest\web.config 檔案。

8b 找到 <authentication mode="None" /> 行並加以刪除。

8c 在 <system.serviceModel> 行下方新增以下幾行：

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy"> <endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding" name="webHttpEndpoint"
contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </services>
```

8d 在 <serviceDebug includeExceptionDetailInFaults="false"/> 行下方新增以下幾行：

```
<serviceAuthorization impersonateCallerForAllOperations="true" /> <serviceCredentials> <clientCertificate>
<authentication mapClientCertificateToWindowsAccount="true" /> </clientCertificate> </serviceCredentials>
```

8e 在 <serviceHostingEnvironment multipleSiteBindingsEnabled="true" /> 行上面新增以下幾行：

```
<bindings> <webHttpBinding> <binding name="webHttpEndpointBinding"> <security mode="Transport"> <transport clientCredentialType="Certificate" /> </security> </binding> </webHttpBinding> </bindings>
```

9 儲存檔案並重新啟動 IIS 伺服器。

Windows 驗證

若要在 Web 主控台上啟用 Windows 驗證，您必須設定 Internet Information Services (IIS) 和 REST 服務組態檔案。

1. 開啟 IIS 管理員。
2. 在「連線」窗格中，找到 REST 服務 Web 應用程式並且選取。
3. 在右窗格中，移至 IIS 區段並且連按兩下**驗證**。
4. 啟用 **Windows 驗證**並且停用其它所有驗證方法。
5. 使用文字編輯器以開啟 C:\inetpub\wwwroot\DRAClient\rest\web.config 檔案，並且找到 <authentication mode="None" /> 行。
6. 將 "None" 變更為 "Windows" 並且儲存檔案。
7. 重新啟動 IIS 伺服器。

具有 Advanced Authentication 的多重要素驗證

Advanced Authentication 架構 (AAF) 是我們的頂級軟體套件，可讓您從簡單的使用者名稱和密碼，提升到更安全的多重要素驗證機密資訊保護方式。

Advanced Authentication 支援下列安全性通訊協定：

- TLS 1.2 (預設設定)、TLS 1.1 和 TLS 1.0
- SSL 3.0

多重要素驗證是電腦存取控制的方法，需要來自不同身分證明類別的多個驗證方法，以便驗證使用者的身分。

有三種類型的驗證類別或要素：

- *知識*。這個類別要求您知道特定的資訊片段，例如密碼或啟用代碼。
- *持有*。這個類別要求您擁有驗證裝置，例如智慧卡或智慧型手機。
- *本文*。這個類別要求您使用身體特徵的部分 (例如您的指紋) 作為驗證方法。

每個驗證要素都包含至少一個驗證方法。驗證方法是特定技術，您可以用來建立使用者的身分，例如使用指紋或要求密碼。

如果驗證程序使用一種以上類型的驗證方法 (例如需要密碼和指紋)，您便可以將其視為增強式驗證。

Advanced Authentication 支援下列驗證方法：

- LDAP 密碼
- 遠端驗證撥號使用者服務 (RADIUS)
- 智慧型手機

提示： 智慧型手機方法需要使用者下載 iOS 或 Android 應用程式。如需詳細資訊，請參閱《*Advanced Authentication - 智慧型手機應用程式使用者指南*》，這可以從 NetIQ 文件網站取得。

使用下列章節中的資訊來設定 Web 主控台使用多重要素驗證。

重要： 雖然下列章節中的某些步驟會在Web主控台中進行，但是大部分多重要素驗證組態程序需要存取 AAF。這些程序假設您已安裝 AAF 並且具有 AA 說明檔案的存取權。

將儲存庫新增至 Advanced Authentication 架構

設定Web主控台的第一步是使用多重要素驗證以將包含由DRA管理之DRA管理員和助理管理員的所有 Active Directory 網域新增至 AAF。這些網域稱為儲存庫，它們包含您想要驗證之使用者和群組的身分屬性。

1. 使用管理員層級使用者名稱和密碼登入 AAF 管理入口網站。
2. 移至左面板然後按一下**儲存庫**。
3. 按一下**新增**。
4. 填入表單。

   提示： **LDAP 類型**是 **AD**。

   提示： 在對應欄位輸入管理員層級使用者名稱和密碼。
5. 按一下**新增伺服器**。
6. 在**位址**欄位中輸入 LDAP 伺服器的 IP 位址。
7. 按一下**儲存**。
8. 針對 DRA 管理的其它所有 AD 儲存庫重複步驟 3 到 7。
9. 針對「儲存庫」頁面上列出的每個儲存庫，按一下**立即同步**以讓它與 AAF 伺服器同步。

建立驗證鏈

驗證鏈包含至少一個驗證方法。鏈中的方法會以它們新增至鏈的順序來叫用。使用者若要獲得驗證，必須通過鏈中的所有方法。例如，您可以建立包含LDAP密碼方法和SMS方法的鏈。當使用者嘗試使用此鏈來驗證，她必須先使用她的LDAP密碼進行驗證，然後包含一次性密碼的簡訊會傳送到她的行動電話。在她輸入密碼之後，鏈中的所有方法將會完成，如此即驗證成功。驗證鏈可以指定給特定使用者或群組。

若要建立驗證鏈：

1. 使用管理員層級使用者名稱和密碼登入 AAF 管理入口網站。
2. 移至左面板然後按一下**鏈**。右面板會顯示目前可用鏈的清單。
3. 按一下**新增**。
4. 填入表單。需要填寫所有欄位。

   重要： 以應該叫用方法的順序來新增方法，也就是說，如果您想要使用者先輸入 LDAP 密碼，則先將 LDAP 密碼新增至鏈。

重要： 確定**如果由端點擁有者使用時套用**切換為「關閉」。

5 將**啟用**切換為「開啟」。

6 在**角色和群組**欄位中輸入受限於驗證要求之角色或群組的名稱。

提示： 如果您想要將鏈套用至所有使用者，則在**角色和群組**欄位中輸入所有使用者，然後從產生的下拉式清單中選取**所有使用者**。

您選取的任何使用者或群組都會新增至**角色和群組**欄位下方。

7 按一下**儲存**。

建立驗證事件

驗證事件是由應用程式觸發，在此案例中是想要驗證使用者的 Web 主控台。必須至少將一個驗證鏈指定至事件，當觸發事件時，與事件相關聯之鏈中的方法才會叫用，以便驗證使用者。

端點是實際裝置，例如電腦或智慧型手機，該裝置會執行觸發驗證事件的軟體。DRA 將在您建立事件之後，向 AAF 註冊端點。

您可以使用「端點」白名單方塊來限制對於特定端點之事件的存取權，或者可以允許所有端點存取事件。

若要建立驗證事件：

1 使用管理員層級使用者名稱和密碼登入 AAF 管理入口網站。

2 移至左面板然後按一下**事件**。右面板會顯示目前可用事件的清單。

3 按一下**新增**。

4 填入表單。需要填寫所有欄位。

重要： 確定**啟用**切換為「開啟」。

5 如果您想要限制特定端點的存取，請移至「端點」白名單區段然後將目標端點從*可用*清單移至*使用*清單。

提示： 如果*使用*清單中沒有任何端點，則事件適用於所有端點。

啟用 Web 主控台

在您設定鏈和事件之後，您能以管理員身分登入 Web 主控台，並啟用 Advanced Authentication。

一旦啟用驗證，就會要求每個使用者先透過 AAF 進行驗證，才能獲得 Web 主控台的存取權。

重要： 在啟用 Web 主控台之前，您必須已在 Web 主控台用來驗證使用者的驗證方法中註冊。請參閱《*Advanced Authentication 架構使用者指南*》以瞭解如何在驗證方法中註冊。

若要啟用 Advanced Authentication，請登入 Web 主控台，然後導覽至「**管理** > **組態** > **Advanced Authentication**」。選取**已啟用**核取方塊，然後根據針對每個欄位提供的指示來設定表單。

提示： 在您儲存組態之後，系統將在 AAF 中建立端點。若要檢視或編輯端點，請以管理員層級使用者名稱和密碼登入 AAF 管理入口網站，然後按一下左窗格中的**端點**。

最終步驟

1. 以管理員層級使用者名稱和密碼登入 AAF 管理入口網站，然後按一下左窗格中的**事件**。
2. 編輯每個 Web 主控台事件：
   - **2a** 開啟事件以進行編輯。
   - **2b** 移至「端點」白名單區段，然後將您在設定 Web 主控台時建立的端點從**可用**清單移至**使用**清單。如此將會確保只有 Web 主控台可以使用這些事件。
3. 按一下**儲存**。

3.2 連接受管理的系統

本節提供連接及設定與網域和 Microsoft Exchange 元件 (包含公用資料夾、Exchange、Office 365 及商務用 Skype Online) 相關之受管理系統的資訊。

3.2.1 管理 Active Directory 網域

您可以在安裝管理伺服器之後，透過「委託和組態」用戶端來新增受管理的網域和電腦。您也可以新增子樹狀結構和受信任的網域，以及為它們設定網域和Exchange存取帳戶。您必須擁有適當的權限，才能新增管理的網域和電腦，例如，包含在內建的「設定伺服器和網域」角色中的權限。

附註： 完成新增管理的網域之後，請確定這些網域的帳戶快取重新整理排程正確。

若要新增管理的網域和電腦：

1. 導覽至**組態管理**>**新增管理的網域**。
2. 指定您想要管理之網域或電腦的名稱，然後按**下一步**。
3. 在「存取帳戶」索引標籤上，指定您想要讓 DRA 用來存取此網域或電腦的帳戶身分證明。根據預設，DRA 會使用管理伺服器服務帳戶。
4. 檢閱摘要，然後按一下**完成**。
5. 若要開始管理此網域或電腦的物件，請重新整理網域組態。

指定網域存取帳戶

針對每個管理的網域或子樹狀結構，您可以指定要使用的帳戶而不是管理伺服器服務帳戶，以存取該網域。這個替代帳戶稱為存取帳戶。您必須擁有適當的權限，才能設定存取帳戶，例如，包含在內建的「設定伺服器和網域」角色中的權限。

若要指定成員伺服器的存取帳戶，您必須擁有管理網域成員所在之網域的權限。您只有在網域成員存在於可以透過管理伺服器存取的管理的網域中時，才能管理網域成員。

若要指定存取帳戶：

1. 導覽至**組態管理**>**受管理的網域**節點。
2. 以滑鼠右鍵按一下您想要對其指定存取帳戶的網域或子樹狀結構，然後按一下**內容**。
3. 在「網域存取帳戶」索引標籤上，按一下**使用下列帳戶來存取此網域**。
4. 指定此帳戶的身分證明並確認，然後按一下**確定**。

如需設定這個最低權限帳戶的詳細資訊，請參閱最低權限 DRA 存取帳戶。

指定 Exchange 存取帳戶

針對DRA中的每個網域，您可以使用DRA網域存取帳戶或個別的Exchange存取帳戶來管理Exchange物件。您必須擁有適當的權限，才能設定 Exchange 存取帳戶，例如，包含在內建的「設定伺服器和網域」角色中的權限。

重要： Microsoft 伺服器將同時連線至 WinRM/WinRS 工作階段的使用者數量限制為五位，並將每位使用者的 Shell 數量限制為五個，以確保 DRA 次要伺服器的相同使用者帳戶受到五個 Shell 的限制。

若要指定 Exchange 存取帳戶：

1. 導覽至**組態管理**>**受管理的網域**節點。
2. 以滑鼠右鍵按一下您想要對其指定存取帳戶的網域或子樹狀結構，然後按一下**內容**。
3. 在「Exchange 存取帳戶」索引標籤上，按一下**使用下列帳戶來存取所有 Exchange 伺服器**。
4. 指定此帳戶的身分證明並確認，然後按一下**確定**。

如需設定這個最低權限帳戶的詳細資訊，請參閱最低權限 DRA 存取帳戶。

新增受管理的子樹狀結構

安裝管理伺服器之後，您可以從特定的 Microsoft Windows 網域新增受管理的和遺漏的子樹狀結構。您必須擁有適當的權限，才能新增受管理的子樹狀結構，例如，包含在內建的「設定伺服器和網域」角色中的權限。

如需受支援 Microsoft Windows 版本的詳細資訊，請參閱DRA 管理伺服器需求。

藉由管理 Windows 網域的子樹狀結構，您可以使用 DRA 來保護較大型公司網域內的部門或事業處。

例如，您可以在SOUTHWEST網域中指定休士頓子樹狀結構，讓DRA安全地管理僅包含在休士頓OU及其子 OU 中的那些物件。這樣的彈性可讓您管理一或多個子樹狀結構，而不需要整個網域的管理權限。

附註：

- 若要確保指定的帳戶具有許可來管理此子樹狀結構和執行遞增的帳戶快取重新整理，請使用「刪除的物件」公用程式來驗證和委託適當的許可。
- 完成新增管理的子樹狀結構之後，請確定相應網域的帳戶快取重新整理排程正確。

若要新增受管理的子樹狀結構：

1. 導覽至**組態管理**>**新增管理網域**。
2. 在「網域或伺服器」索引標籤上，按一下**管理網域**，然後指定您想要管理的子樹狀結構網域。
3. 指定您想要管理的子樹狀結構網域。
4. 選取**管理此網域的子樹狀結構**，然後按**下一步**。
5. 在「子樹狀結構」索引標籤上，按一下**新增**以指定您想要管理的子樹狀結構。您可以指定一個以上的子樹狀結構。
6. 在「存取帳戶」索引標籤上，指定您想要讓DRA用來存取此子樹狀結構腦的帳戶身分證明。根據預設，DRA 會使用管理伺服器服務帳戶。
7. 檢閱摘要，然後按一下**完成**。
8. 若要開始管理此子樹狀結構的物件，請重新整理網域組態。

新增受信任網域

受信任網域會在您的整個環境中的受管理系統上啟用使用者驗證。一旦您新增受信任網域，您便可以指定網域和Exchange存取帳戶、排程快取重新整理，以及在網域的內容中採取其它動作，與受管理的網域相同。

若要新增受信任網域：

1. 在**組態管理**>**受管理的網域**節點中，選取具有相關聯受信任網域的管理的網域。
2. 在「詳細資料」窗格中按一下**受信任網域**。「詳細資料」窗格必須在「檢視」功能表上切換。
3. 以滑鼠右鍵按一下受信任網域，然後選取**內容**。
4. 取消勾選**略過此受信任網域**，然後套用您的變更。

附註： 新增受信任網域會起始完整帳戶快取重新整理，但是您會在按一下**套用**時收到通知，其中含有確認提示。

3.2.2 連接公用資料夾

DRA 可讓您管理 Microsoft Exchange 公用資料夾。您可以使用 DRA，藉由設定公用資料夾樹系網域以及將權限授與助理管理員，來管理公用資料夾的部分內容。

重要： 若要管理公用資料夾管理，您必須先在 DRA 中啟用 Microsoft Exchange 支援，並且擁有適當權限。

- 如需啟用 Microsoft Exchange 的詳細資訊，請參閱啟用 Microsoft Exchange 支援。
- 如需帳戶許可的詳細資訊，請參閱最低權限 DRA 存取帳戶。

若要設定 Exchange 公用資料夾支援：

1. 以滑鼠右鍵按一下「組態和管理」節點中的**受管理公用資料夾樹系**，然後按一下**新增公用資料夾樹系**。
2. 按一下**樹系網域**，指定公用資料夾物件所在的作用中目錄樹系，然後按**下一步**。
3. 在**網域存取**中，指定存取帳戶：
   - **使用目錄和資源管理員服務帳戶：** 如果您想要使用您的 DRA 服務帳戶。
   - **使用下列帳戶來存取此網域：** 如果您想要使用網域存取帳戶。

   重要： 如果您使用次要伺服器，則可以使用**使用主要管理伺服器網域存取帳戶**選項。

   ---
4. 在 **Exchange 存取**中，指定您希望 DRA 用於安全存取 Exchange 伺服器的帳戶：
   - **針對所有 Exchange 伺服器使用網域存取帳戶：** 如果您想要使用網域存取帳戶。
   - **使用下列帳戶來存取所有 Exchange 伺服器：** 如果您想要使用 Exchange 存取帳戶。

   重要： 如果您使用次要伺服器，則可以使用**使用主要管理伺服器 Exchange 存取帳戶**選項。

   ---
5. 在 **Exchange 伺服器**中，選取您希望 DRA 用於管理公用資料夾的 Exchang 伺服器。
6. 在**摘要**中，檢閱帳戶詳細資料和 Exchange 伺服器詳細資料，然後按一下**完成**以完成程序。

   DRA 伺服器會在公用資料夾上執行完整帳戶快取重新整理。新的公用資料夾樹系會在快取重新整理完成之後出現在主控台中，可能需要數分鐘的時間。

附註： 您可以從任務或以滑鼠右鍵按一下功能表，來移除選取的公用資料夾樹系網域。

檢視及修改公用資料夾網域內容

若要檢視或修改公用資料夾網域內容：

1. 在「組態管理」節點中按一下**受管理公用資料夾樹系**，以檢視公用資料夾。
2. 以滑鼠右鍵按一下您想要檢視的公用資料夾帳戶，然後選取**內容**。
3. 在「**公用資料夾樹系**」內容中，您可以執行下列動作：
   - **一般：** 檢視公用資料夾帳戶詳細資料並且更新**Exchange伺服器**欄位，DRA伺服器會使用該伺服器在公用資料夾伺服器上執行 Exchange 活動。
   - **統計資料：** 檢視公用資料夾數目以及已啟用郵件的公用資料夾數目。
   - **遞增的狀態：** 檢視或更新遞增的帳戶快取狀態。
   - **遞增的排程：** 檢視遞增的快取重新整理排程，並重新排程快取重新整理。
   - **完整狀態：** 檢視完整帳戶快取重新整理狀態。
   - **完整重新整理：** 立即執行完整帳戶快取重新整理。

     NetIQ 建議您只有在公用資料夾快取資料已損毀時才執行**完整重新整理**。
   - **網域存取：** 檢視 DRA 服務帳戶詳細資料或覆寫存取帳戶。
   - **Exchange 存取：** 檢視或更新 Exchange 伺服器的安全存取。

委託公用資料夾權限

使用 activeview 以定義權限及管理公用資料夾委託。您可以指定規則以新增受管理物件、選擇網域以及指定權限，然後將那些公用資料夾權限委託給助理管理員。

若要建立 activeview 以及委託公用資料夾權限：

1. 在**委託管理**節點中，按一下 **ActiveView**。
2. 在**建立 ActiveView > 精靈**中按**下一步**，從**新增**下拉式清單中選取必要的規則，然後選擇公用資料夾作為物件類型。例如，若要建立物件比對規則：選取**符合規則的物件**，然後選擇**公用資料夾**作為物件類型。
3. 指定您想要新增至公用資料夾的 activeview 規則，然後按**下一步**。
4. 指定 activeview 的名稱，然後按一下**完成**。
5. 以滑鼠右鍵按一下 **ActiveView** 並移至**委託管理**>**助理管理員**，然後從**精靈**中的**新增**下拉式清單中指定管理員類型。
6. 搜尋您想要委託權限的特定使用者、群組或 AA 群組。
7. 使用**物件選擇器**以尋找及新增您想要的物件，然後按一下**精靈**中的**角色和權限**。
8. 從**新增**下拉式清單選取**角色**，然後搜尋公用資料夾管理角色並新增。
9. 從**新增**下拉式清單選取權限，然後尋找您想要指定給助理管理員 (不屬於公用資料夾管理角色) 的任何額外權限並新增。
10. 按**下一步**然後按一下**完成**以完成委託程序。

在您完成公用資料夾權限的委託之後，獲授權的使用者就可以使用 Web 主控台，在已設定網域的公用資料夾內容中執行建立、讀取、更新及刪除操作。

3.2.3 啟用 Microsoft Exchange 支援

啟用 Microsoft Exchange 支援可讓您利用 Exchange 功能，例如 Microsoft Exchange 規則、整合的信箱，以及已啟用郵件的物件管理。您可以針對下列平台上的每個管理伺服器啟用或停用 Microsoft Exchange 支援：Microsoft Exchange Server 2010 和 Microsoft Exchange Server 2013 及更新版本。

您必須擁有適當的權限，才能啟用 Microsoft Exchange 支援，例如，包含內建的「管理規則和自動化觸發」角色中的權限，且您的授權必須支援 Exchange 產品。如需 Microsoft Exchange 需求的詳細資訊，請參閱支援的平台。

若要啟用 Microsoft Exchange 的支援：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**。
2. 選取**啟用 Exchange 規則**，然後按一下**套用**。

   DRA會驗證在管理伺服器上安裝哪個版本的Exchange管理工具，並且啟用選項，讓您可以選取適當版本的 Exchange 支援。
3. *如果已選取「啟用Exchange 規則」，而讓您可以選取Exchange 支援的選項未啟用*，請按一下**重新整理**讓 DRA 驗證在管理伺服器上安裝哪個版本的 Exchange 管理工具。
4. 若要啟用Exchange管理支援，請選取選項以啟用您想要以此管理伺服器管理之Exchange的版本支援。
5. 按一下**「確定」**。

3.2.4 啟用 Exchange Online 和商務用 Skype Online

您必須擁有適當的權限，才能在 Office 365 中啟用 Exchange Online 信箱和商務用 Skype Online，例如，包含在內建的「管理規則和自動化觸發」角色中的權限。您的授權也必須支援 Microsoft Exchange 產品。

重要： Microsoft 伺服器將同時連線至 WinRM/WinRS 工作階段的使用者數量限制為五位，並將每位使用者的 Shell 數量限制為五個，以確保 DRA 次要伺服器的相同使用者帳戶受到五個 Shell 的限制。

若要啟用 Exchange Online 和商務用 Skype Online 的支援：

1. 如果尚未安裝，請安裝以下指示的 Microsoft 元件：
   - PowerShell 5.0+
   - 適用於 IT 專業人員 RTW 的 Microsoft Online Services 登入小幫手

     https://www.microsoft.com/en-us/download/details.aspx?id=41950
   - 商務用 Skype Online、Windows PowerShell 模組

     https://www.microsoft.com/en-us/download/details.aspx?id=39366
     - 開啟 PowerShell 然後執行 Install-Module MSOnline。

   如需詳細資訊，請參閱 https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell。
2. 開啟「電腦管理」主控台，然後重新啟動 **NetIQ 管理服務**。
3. 在左窗格中，按一下**規則和自動化管理**。
4. 導覽至**規則和自動化管理**>**設定 Office 365 規則**，然後按一下**啟用 Exchange Online 管理支援**。

3.2.5 新增 Office 365 租用戶

若要管理 Exchange Online 和商務用 Skype Online，您必須管理一或多個 Office 365 租用戶。您必須先啟用 Exchange Online 或商務用 Skype Online 的支援，才能管理 Office 365 租用戶。

重要： Microsoft 伺服器將同時連線至 WinRM/WinRS 工作階段的使用者數量限制為五位，並將每位使用者的 Shell 數量限制為五個，以確保 DRA 次要伺服器的相同使用者帳戶受到五個 Shell 的限制。

如需啟用 Exchange Online 或商務用 Skype Online 的詳細資訊，請參閱：

- 啟用 Microsoft Exchange 支援
- 啟用 Exchange Online 和商務用 Skype Online

在您設定 DRA 以管理您的 Exchange Online 租用戶之前，必須在 Office 365 入口網站中建立具有下列許可的帳戶：

DRA 將會使用此帳戶來執行所有 Exchange Online 管理任務。

- Office 365 中的使用者管理管理員
- Exchange Online 中的收件者管理

附註： 此帳戶可以與您的 Active Directory 環境同步，或者裝載於 Microsoft Office 365 雲端中。DRA 不需要此帳戶位於 Active Directory 即可執行管理任務。

如需帳戶許可的詳細資訊，請參閱最低權限 DRA 存取帳戶。

管理 Office 365 租用戶和建立服務主體

一旦您在 DRA 中啟用線上規則，就可以存取在名為 **Office 365 租用戶**之「組態管理」下方的新節點，您可以在其中管理新的 Office 365 租用戶。

若要新增 Office 365 租用戶，請導覽至**組態管理**> **Office 365 租用戶**，然後遵循精靈中的指示，包括新增 Office 365 租用戶存取帳戶及設定重新整理和更新排程。

DRA 需要具有「目錄讀取者」許可的服務主體，才能收集租用戶中物件的相關資料。

若要建立服務主體，您可以將具有 Office 365 中「公司管理員」角色的使用者帳戶身分證明提供給 DRA，DRA 會為您建立服務主體，或者您可以離線建立服務主體。

附註：

- DRA 不會儲存提供來建立服務主體的「公司管理員」身分證明。
- 如果您離線建立服務主體，必須在精靈中提供服務主體識別碼和密碼。

新增 Office 365 租用戶可能需要數分鐘的時間。一旦成功新增租用戶，DRA 就會為租用戶執行完整帳戶快取重新整理 (FACR)。當快取重新整理完成時，您可以開始管理租用戶的 Office 365 授權和信箱。

4 委託模型

DRA 會藉由提供有彈性的控制組以將細微能力授與企業中的特定受管理物件，讓管理員執行「最低權限」許可規劃。透過這些委託，管理員可以確保助理管理員只收到完成它們的特定角色和職責所需的許可。

4.1 瞭解動態委託模型

DRA 可讓您在委託模型內容中管理對於您的企業的管理存取。委託模型可讓您透過會隨著企業變更和發展而調適的動態控制組，為助理管理員設定「最低權限」存取。委託模型提供管理存取控制，更能貼近地表示貴公司的運作方式：

- 使用彈性範圍規則，管理員可以根據業務需求而不是企業結構，將許可的目標設為特定受管理物件。
- 角色型委託會確保授與的許可一致，並且簡化佈建。
- 權限指定可以從單一位置，在網域、雲端租用戶及受管理應用程式之間進行管理。
- 細微能力可讓您量身訂做要授與助理管理員的特定存取。

4.1.1 委託模型控制

管理員會使用下列控制，透過委託模型來佈建存取：

- **委託:** 管理員會藉由指定角色以將存取佈建給使用者和群組，該角色具有 ActiveView (提供範圍) 內容中的指定許可。
- **ActiveView：** ActiveView 代表特定範圍的受管理物件，這些物件是由一或多個規則定義的。ActiveView 中各個規則所定義的受管理物件，會一併結集到整合的範圍。
- **ActiveView 規則：** 規則是由符合受管理物件組的運算式，根據一些條件 (例如物件類型、位置、名稱等) 來定義的。
- **角色：** 角色代表執行特定管理功能所需的特定權限 (許可) 組。DRA 針對通用業務功能提供一些內建角色，您可以定義最適合您組織需求的自定角色。
- **權限：** 權限會定義受管理物件支援之任務的特定許可，例如檢視、修改、建立和刪除等。關於修改受管理物件的許可可以進一步細分為可變更的特定內容。DRA 為支援的受管理物件提供廣泛的內建權限清單，且可以定義自定權限以延伸可透過委託模型佈建哪些項目。

4.1.2 DRA 如何處理要求

當管理伺服器收到動作要求時 (例如變更使用者密碼)，它會使用下列程序：

1. 搜尋 Activeview，它設定為管理操作的目標物件。
2. 驗證指定給要求動作之帳戶的權限。
    a. 評估所有「作用中檢視」指定，其中包含要求操作的助理管理員。

b. 一旦完成該清單，建立所有 ActiveView 的清單，其中同時包含目標物件和助理管理員。

c. 比較能力與要求操作所需的權限。

3. *如果帳戶具有正確的權限*，管理伺服器就會允許執行動作。

   如果帳戶沒有正確的權限，管理伺服器就會傳回錯誤。

4. 更新 Active Directory。

4.1.3 DRA 如何處理委託指定的範例

下列範例說明在 DRA 處理要求時如何評估委託模型所發生的通用案例：

範例 1：變更使用者的密碼

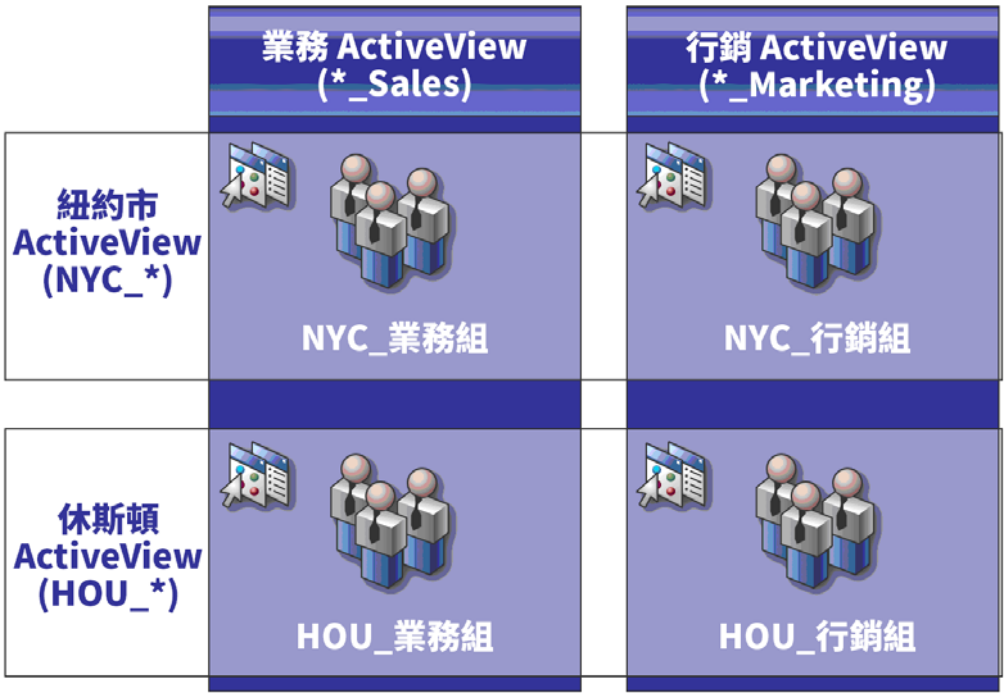
當助理管理員嘗試為 JSmith 使用者帳戶設定新密碼時，管理伺服器會尋找包含 JSmith 的所有 ActiveView。這個搜尋會尋找直接指定 JSmith、透過萬用字元規則，或透過群組成員資格的任何 ActiveView。如果 ActiveView 包含其它 ActiveView，管理伺服器也會搜尋這些額外的 ActiveView。管理伺服器會判斷這些 ActiveView 中的助理管理員是否具有*重設使用者帳戶密碼*權限。如果助理管理員具有*重設使用者帳戶密碼*權限，管理伺服器會重設 JSmith 的密碼。如果沒有此權限，管理伺服器會拒絕要求。

範例 2：重疊 ActiveView

權限會定義助理管理員可以在您管理的網域或子樹狀結構中檢視、修改或建立之物件的內容。一個以上的 ActiveView 可以包含相同物件。此組態稱為**重疊 ActiveView**。

當 ActiveView 重疊時，您可以在相同物件上累積一組不同的權限。例如，如果一個 ActiveView 允許您將使用者帳戶新增至網域，而另一個 ActiveView 允許您從相同網域刪除使用者帳戶，則您可以在該網域中新增或刪除使用者帳戶。如此一來，您對於指定物件所具有的權限就是累計的。

請務必瞭解 ActiveView 可以重疊的方式，以及您可以在這些 ActiveView 中所包含物件上擁有增加的權限。請考量下圖中所示的 ActiveView 組態。



白色索引標籤會依據位置來識別 ActiveView，*紐約市*和*休士頓*。黑色索引標籤會依據其組織功能來識別 ActiveView，*銷售*和*行銷*。儲存格會顯示每個 ActiveView 中所包含的群組。

NYC_Sales 群組和 HOU_Sales 群組都會在銷售 ActiveView 中顯示。如果您具有銷售 ActiveView 中的權限，可以管理NYC_Sales和HOU_Sales群組的任何成員。如果您也有紐約市ActiveView中的權限，這些額外的權限會套用至 NYC_Marketing 群組。如此一來，權限會累積為 ActiveView 重疊。

重疊 ActiveView 可以提供強大且彈性的委託模型。但是，此功能可能也會產生意外的結果。請謹慎規劃您的 ActiveView 以確保每個 AA 都只有您想要讓它對於每個使用者帳戶、群組、OU、聯絡人或資源具備的權限。

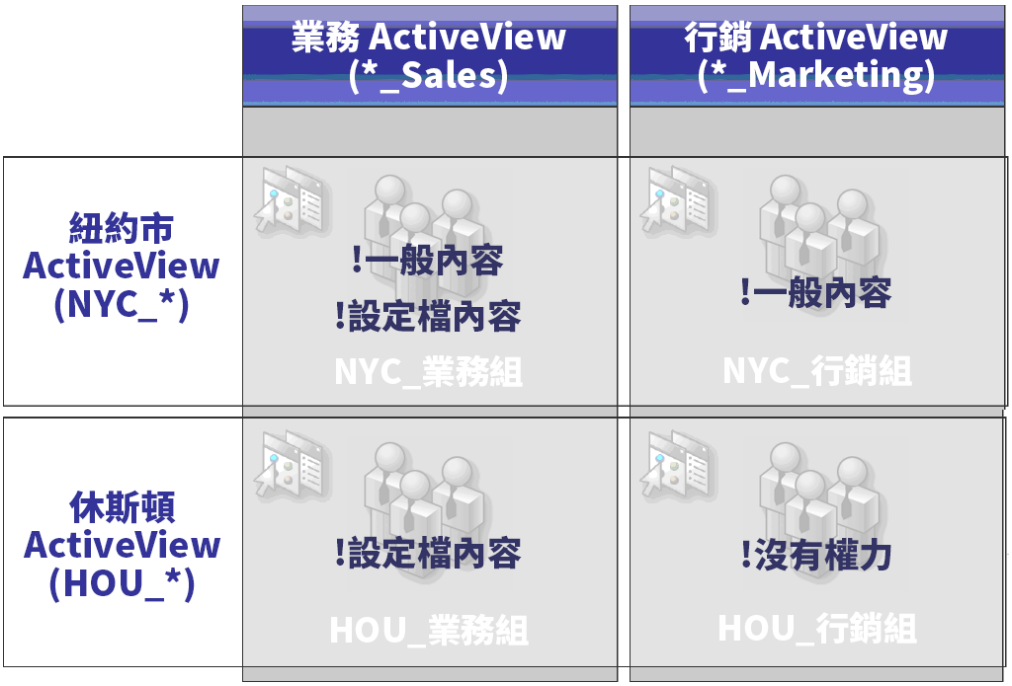
多個 ActiveView 中的群組

在此範例中，NYC_Sales 群組出現在一個以上的 ActiveView。NYC_Sales 群組的成員出現在紐約市 ActiveView 中，因為群組名稱符合 NYC_* ActiveView 規則。群組也會在銷售 ActiveView 中，因為群組名稱符合 *_Sales ActiveView 規則。藉由在多個 ActiveView 中包含相同群組，您可以允許不同的助理管理員分別管理相同物件。

在多個 ActiveView 中使用權限

假設有一位助理管理員 JSmith，它具有紐約市 ActiveView 中的*修改一般使用者內容*權限。此第一個權限允許 JSmith 在使用者內容視窗的「一般」索引標籤上編輯所有內容。JSmith 具有銷售 ActiveView 中的*修改使用者設定檔內容*權限。此第二個權限允許 JSmith 在使用者內容視窗的「設定檔」索引標籤上編輯所有內容。

下圖指出 JSmith 對於每個群組所具有的權限。



JSmith 具有下列權限：

- NYC_* ActiveView 中的一般內容
- *_Sales ActiveView 中的設定檔內容

這些重疊 ActiveView 中的權限委託可讓 JSmith 修改 NYC_Sales 群組的「一般」和「設定檔」內容。因此，JSmith 獲得授與所有 ActiveView 中代表 NYC_Sales 群組的所有權限。

4.2 ActiveView

ActiveView 可讓您執行具有下列功能的委託模型：

- 獨立於您的 Active Directory 結構
- 可讓您指定權限以及定義與現有工作流程相互關聯的規則。
- 提供自動化以協助您進一步整合及自定您的企業
- 動態回應變更

ActiveView 代表一或多個管理的網域內的一組物件。您可以將物件納入一個以上的 ActiveView。您也可以從多個網域或 OU 納入許多物件。

4.2.1 內建 ActiveView

內建 ActiveView 是 DRA 提供的預設 ActiveView。這些 ActiveView 代表所有目前的物件和安全性設定。因此，內建 ActiveView 提供您所有物件和設定的立即存取，以及預設委託模型。您可以使用這些 ActiveView 來管理物件，例如使用者帳戶和資源，或者將預設委託模型套用至您目前的企業組態。

DRA 提供數個內建 ActiveView，可以代表您的委託模型。內建 ActiveView 節點包含下列 ActiveView：

所有物件

包含所有管理的網域中的所有物件。您可以透過此 ActiveView 來管理您企業的任何層面。將此 ActiveView 指定給管理員或需要跨企業稽核能力的 AA。

目前使用者以 Windows 管理員身分管理的物件

包含來自目前管理的網域的物件。您可以透過此 ActiveView 來管理使用者帳戶、群組、聯絡人、OU 及資源。將此 ActiveView 指定給原生管理員，該管理員負責管理的網域中的帳戶和資源物件。

管理伺服器和管理的網域

包含管理伺服器電腦和管理的網域。您可以透過此 ActiveView 來管理您的管理伺服器的每日維護。將此 ActiveView 指定給 AA，其職責包含監視同步狀態或執行快取重新整理。

DRA 規則和自動化觸發

包含所有管理的網域中的所有規則和自動化觸發物件。您可以透過此 ActiveView 來管理規則內容和範圍，以及自動化觸發內容。將此 ActiveView 指定給負責建立及維護貴公司規則的 AA。

DRA 安全性物件

包含所有安全性物件。您可以透過此 ActiveView 來管理 ActiveView、AA 群組及角色。將此 ActiveView 指定給負責建立及維護您的安全性模型的 AA。

所有受管理和受信任網域的 SPA 使用者

包含受管理和受信任網域的所有使用者帳戶。您可以透過此 ActiveView 藉由安全密碼管理員 (SPA) 來管理使用者密碼。

存取內建 ActiveView

存取內建 ActiveView 以稽核預設委託模型或管理您自己的安全性設定。

若要存取內建 ActiveView：

1. 導覽至**委託管理**>**管理 ActiveView**。
2. 確定搜尋欄位是空白的，然後按一下**列出符合我的準則的項目**窗格中的**立即尋找**。
3. 選取適當的 ActiveView。

使用內建 ActiveView

您無法刪除、複製或修改內建 ActiveView。但是，您可以將這些 ActiveView 併入您現有的委託模型，或使用這些 ActiveView 來設計您自己的模型。

您可以下列方式使用內建 ActiveView：

- 將個別內建 ActiveView 指定給適當的 AA 群組。這個關聯可讓 AA 群組成員以適當的權限管理對應的一組物件。
- 請參閱內建 ActiveView 規則和關聯，作為設計及導入您的委託模型的指導方針。

如需設計動態委託模型的詳細資訊，請參閱瞭解動態委託模型。

4.2.2 導入自定 ActiveView

ActiveView 提供一或多個網域或 OU 內特定物件的即時存取。您可以從 ActiveView 新增或移除物件，而不需要變更基礎網域或 OU 結構。

您可以將 ActiveView 視為虛擬網域或 OU，或者是針對關連式資料庫選取陳述或資料庫檢視的結果。ActiveView 可以包含或排除任何物件組、包含其它 ActiveView，以及具有重疊內容。ActiveView 可以包含不同網域、樹狀結構及樹系的物件。您可以設定 ActiveView 以符合任何企業管理需求。

ActiveView 可以包含下列物件類型：

帳戶:

- 使用者
- 群組
- 電腦
- 聯絡人
- 動態通訊群組
- 已發佈印表機
- 已發佈印表機列印工作
- 資源信箱
- 共享信箱
- 公用資料夾

目錄物件：

- 組織單位
- 領域
- 成員伺服器

委託物件：

- ActiveView
- 自助管理
- 直屬下屬
- 受管理群組

資源:

- 連接的使用者
- 裝置
- 事件記錄
- 開啟檔案
- 印表機
- 列印工作
- 服務
- 共享

隨著您的企業變更及成長，ActiveView 會變更以包含或排除新物件。因此，您可以使用 ActiveView 來降低模型的複雜度、提供您需要的安全性，以及給予您比其它企業組織工具還要大的彈性。

ActiveView 規則

ActiveView 可以由包含或排除物件的規則組成，例如使用者帳戶、群組、OU、聯絡人、資源、電腦、資源信箱、共享信箱、動態通訊群組及 ActiveView。這個彈性讓 ActiveView 變得動態。

這些相符項目稱為**萬用字元**。例如，您可以定義規則以包含名稱符合DOM*的所有電腦。這個萬用字元規格將會搜尋名稱開頭為字元字串DOM的任何電腦帳戶。萬用字元比對讓管理變得動態，因為在帳戶符合規則時會自動納入。因此，當您使用萬用字元時，不需要隨著組織變更而重新設定 ActiveView。

其它範例是根據群組成員資格定義 ActiveView。您可以定義規則，包含以字母 NYC 開頭之群組的所有成員。然後，隨著成員新增至任何符合此規則的群組，這些成員會自動納入此 ActiveView。隨著您的企業變更或成長，DRA 會重新套用規則以在適當 ActiveView 中包含或排除新物件。

4.3 角色

本節包含內建至 DRA 之角色的清單及描述、如何使用這些角色，以及建立和管理自定角色的相關資訊。

如需角色的描述及其一般用途，請參閱委託模型控制。

4.3.1 內建角色

內建AA角色提供常用權限組的立即存取。您可以藉由使用這些預設角色以將權限委託給特定使用者帳戶或其它群組，來延伸您目前的安全性組態。

這些角色包含執行通用管理任務所需的權限。例如，DRA 管理角色包含管理物件所需的所有權限。然而，若要使用這些權限，角色必須與使用者帳戶或 AA 群組和受管理 ActiveView 相關聯。

因為內建角色屬於預設委託模型，您可以使用內建角色快速地委託權限和執行安全性。這些內建角色會處理您可以透過 DRA 使用者介面執行的通用任務。下列清單說明每個內建角色並摘要與該角色相關聯的權限。

應用程式伺服器管理

提供設定、檢視及刪除應用程式伺服器組態所需的權限。

稽核所有物件

提供檢視整個企業所有物件、規則及組態之內容所需的所有權限。此角色不允許 AA 修改內容。將此角色指定給負責整個企業稽核動作的 AA。允許 AA 檢視「自定工具」節點以外的所有節點。

稽核限制帳戶和資源內容

提供所有物件內容的權限。

稽核資源

提供檢視受管理資源之內容所需的所有權限。將此角色指定給負責稽核資源物件的 AA。

稽核使用者和群組

提供檢視使用者帳戶和群組內容所需的所有能力，但是不提供修改這些內容的權限。將此角色指定給負責稽核帳戶內容的 AA。

內建規劃程式 - 僅限內部使用

提供排程 DRA 重新整理快取時機的權限。

複製使用者與信箱

提供複製現有使用者帳戶以及帳戶信箱所需的所有權限。將此角色指定給負責管理使用者帳戶的 AA。

附註： 若要允許 AA 在複製任務期間將新使用者帳戶新增至群組，也要指定「管理群組成員資格」角色。

電腦管理

提供修改電腦內容所需的所有權限。此角色可讓 AA 新增、刪除及關閉電腦，以及同步化網域控制器。將此角色指定給負責管理 ActiveView 中電腦的 AA。

設定伺服器和網域

提供修改管理伺服器選項和管理的網域所需的所有權限。同時提供設定及管理 Office 365 租用戶所需的權限。將此角色指定給負責監視及維護管理伺服器的 AA。

聯絡人管理

提供建立新聯絡人、修改聯絡人內容或刪除聯絡人所需的所有權限。將此角色指定給負責管理聯絡人的 AA。

建立及刪除電腦帳戶

提供建立及刪除電腦帳戶所需的所有權限。將此角色指定給負責管理電腦的 AA。

建立及刪除群組

提供建立及刪除群組所需的所有權限。將此角色指定給負責管理群組的 AA。

建立及刪除資源信箱

提供建立及刪除信箱所需的所有權限。將此角色指定給負責管理信箱的 AA。

建立及刪除資源

提供建立及刪除共享和電腦帳戶與清除事件所需的所有權限。將此角色指定給負責管理資源物件和事件記錄的 AA。

建立及刪除使用者帳戶

提供建立及刪除使用者帳戶所需的所有權限。將此角色指定給負責管理使用者帳戶的 AA。

DRA 管理

提供所有權限給AA。此角色會給予使用者在DRA內執行所有管理任務的許可。此角色等同於管理員的許可。與「DRA 管理」角色相關聯的 AA 可以存取所有「目錄和資源管理員」節點。

動態群組管理

提供管理 Active Directory 動態群組所需的所有權限。

執行進階查詢

提供執行已儲存進階查詢所需的所有權限。將此角色指定給負責執行進階查詢的 AA。

群組管理

提供管理群組和群組成員資格，以及檢視對應使用者內容所需的所有權限。將此角色指定給負責管理群組或透過群組管理帳戶和資源物件的 AA。

服務台管理

提供檢視使用者帳戶內容以及變更密碼和密碼相關內容所需的所有權限。此角色也會允許 AA 停用、啟用及解除鎖定使用者帳戶。將此角色指定給負責服務台職責以確保使用者具有其帳戶適當存取的 AA。

信箱管理

提供管理 Microsoft Exchange 信箱內容所需的所有權限。如果您使用 Microsoft Exchange，請將此角色指定給負責管理 Microsoft Exchange 信箱的 AA。

管理 Active Directory Collector、DRA Collector 及 Management Reporting Collector

提供管理 Active Directory Collector、DRA Collector、Office 365 租用戶收集器及 Management Reporting Collector 以進行資料收集所需的所有權限。將此角色指定給負責管理報告組態的 AA。

管理 Active Directory Collector、DRA Collector、Management Reporting Collector 及資料庫組態

提供管理 Active Directory Collector、DRA Collector、Management Reporting Collector 及資料庫組態以進行資料收集所需的所有權限。將此角色指定給負責管理報告和資料庫組態的 AA。

管理進階查詢

提供建立、管理及執行進階查詢所需的所有權限。將此角色指定給負責管理進階查詢的 AA。

管理及執行自定工具

提供建立、管理及執行自定工具所需的所有權限。將此角色指定給負責管理自定工具的 AA。

管理複製例外狀況

提供建立及管理複製例外狀況所需的所有權限。

管理電腦內容

提供管理電腦帳戶所有內容所需的所有權限。將此角色指定給負責管理電腦的 AA。

管理資料庫組態

提供管理資料庫組態以產生各項管理報告所需的所有權限。將此角色指定給負責管理報告資料庫組態的 AA。

管理動態通訊群組

提供管理 Microsoft Exchange 動態通訊群組所需的所有權限。

管理 Exchange 信箱權限

提供管理 Microsoft Exchange 信箱安全性和權限所需的所有權限。如果您使用 Microsoft Exchange，請將此角色指定給負責管理 Microsoft Exchange 信箱許可的 AA。

管理群組電子郵件

提供檢視、啟用或停用群組電子郵件地址所需的所有權限。將此角色指定給負責針對帳戶物件管理群組或電子郵件地址的 AA。

管理群組成員資格安全性

提供指定誰可以透過 Microsoft Outlook 檢視及修改 Microsoft Windows 群組成員資格所需的所有權限

管理群組成員資格

提供從現有群組新增及移除使用者帳戶或群組，以及檢視使用者或電腦帳戶主要群組所需的所有權限。將此角色指定給負責管理群組或使用者帳戶的 AA。

管理群組內容

提供管理群組所有內容所需的所有權限。將此角色指定給負責管理群組的 AA。

管理信箱移動要求

提供管理信箱移動要求所需的所有權限。

管理規則和自動化觸發

提供定義規則和自動化觸發所需的所有權限。將此角色指定給負責維護公司規則和自動化工作流程的 AA。

管理印表機和列印工作

提供管理印表機、列印佇列及列印工作所需的所有權限。若要管理與使用者帳戶相關聯的列印工作，列印工作和使用者帳戶必須包含在相同的 ActiveView 中。將此角色指定給負責維護印表機及管理列印工作的 AA。

管理資源信箱內容

提供管理信箱所有內容所需的所有權限。將此角色指定給負責管理信箱的 AA。

管理受管理使用者的資源

提供管理與特定使用者帳戶相關聯之資源所需的所有權限。AA 和使用者帳戶必須包含在相同的 ActiveView 中。將此角色指定給負責管理資源物件的 AA。

管理安全性模型

提供定義管理規則 (包括 ActiveView、AA 及角色) 所需的所有權限。將此角色指定給負責導入及維護您的安全性模型的 AA。

管理服務

提供管理服務所需的所有權限。將此角色指定給負責管理服務的 AA。

管理共享資料夾

提供管理共享資料夾所需的所有權限。將此角色指定給負責管理共享資料夾的 AA。

管理暫時群組指定

提供建立及管理暫時群組指定所需的所有權限。將此角色指定給負責管理群組的 AA。

管理 UI 報告

針對使用者、群組、聯絡人、電腦、組織單位、能力、角色、ActiveView、容器、已發佈印表機及助理管理員提供產生及輸出「活動詳細資料」報告所需的所有權限。將此角色指定給負責產生報告的 AA。

管理使用者撥號內容

提供修改使用者帳戶撥號內容所需的所有權限。將此角色指定給負責管理使用者帳戶 (具有企業的遠端存取) 的 AA。

管理使用者電子郵件

提供檢視、啟用或停用使用者帳戶電子郵件地址所需的所有權限。將此角色指定給負責針對帳戶物件管理使用者帳戶或電子郵件地址的 AA。

管理使用者密碼和解除鎖定帳戶

提供重設密碼、指定密碼設定以及解除鎖定使用者帳戶所需的所有權限。將此角色指定給負責維護使用者帳戶存取的 AA。

管理使用者內容

提供管理使用者帳戶所有內容 (包括 Microsoft Exchange 信箱內容) 所需的所有權限。將此角色指定給負責管理使用者帳戶的 AA。

管理虛擬屬性

提供建立及管理虛擬屬性所需的所有權限。將此角色指定給負責管理虛擬屬性的 AA。

管理 WTS 環境內容

提供變更使用者帳戶之WTS環境內容所需的所有權限。將此角色指定給負責維護WTS環境或管理使用者帳戶的 AA。

管理 WTS 遠端控制內容

提供變更使用者帳戶之WTS遠端控制內容所需的所有權限。將此角色指定給負責維護WTS存取或管理使用者帳戶的 AA。

管理 WTS 工作階段內容

提供變更使用者帳戶之WTS工作階段內容所需的所有權限。將此角色指定給負責維護WTS工作階段或管理使用者帳戶的 AA。

管理 WTS 終端機內容

提供變更使用者帳戶之WTS終端機內容所需的所有權限。將此角色指定給負責維護WTS終端機內容或管理使用者帳戶的 AA。

OU 管理

提供管理組織單位所需的所有權限。將此角色指定給負責管理 Active Directory 結構的 AA。

公用資料夾管理

提供建立、修改、刪除、啟用或停用郵件以及檢視公用資料夾內容的權限。您可以將此角色指定給負責管理公用資料夾的所有 AA。

重新命名群組及修改描述

提供修改群組名稱和描述所需的所有權限。將此角色指定給負責管理群組的 AA。

重新命名使用者及修改描述

提供修改使用者帳戶名稱和描述所需的所有權限。將此角色指定給負責管理使用者帳戶的 AA。

複寫檔案

提供上傳、刪除及修改檔案資訊所需的所有權限。將此角色指定給負責從主要管理伺服器將檔案複寫到 MMS 和 DRA 用戶端電腦中其它管理伺服器的 AA。

重設本機管理員密碼

提供重設本機管理員帳戶密碼以及檢視電腦管理員名稱的所有權限。將此角色指定給負責管理管理員帳戶的 AA。

重設密碼

提供重設及修改密碼所需的所有權限。將此角色指定給負責密碼管理的 AA。

使用 SPA 重設密碼及解除鎖定帳戶

提供使用安全密碼管理員來重設密碼及解除鎖定使用者帳戶所需的所有權限。

重設整合通訊 PIN 碼內容

提供重設使用者帳戶之整合通訊 PIN 碼內容所需的所有權限。

資源管理

提供修改受管理資源的內容 (包括與任何使用者帳戶相關聯的資源) 所需的所有權限。將此角色指定給負責管理資源物件的 AA。

資源信箱管理

提供管理資源信箱所需的所有權限。

自助管理

提供修改基本內容 (例如您自己的使用者帳戶的電話號碼) 所需的所有權限。將此角色指定給 AA 以允許它們管理它們自己的個人資訊。

共享信箱管理

提供建立、修改、刪除及檢視您的共享信箱內容所需的所有權限。將此角色指定給負責管理共享信箱的 AA。

啟動及停止資源

提供暫停、啟動、繼續或停止服務；啟動或停止裝置或印表機；關閉電腦或同步化您網域控制器所需的所有權限。同時提供暫停、繼續及啟動服務；停止裝置或列印佇列以及關閉電腦所需的所有權限。將此角色指定給負責管理資源物件的 AA。

轉換使用者

提供從範本帳戶中找到的群組新增或移除使用者所需的所有能力，包括在轉換使用者時修改使用者內容的權限。

整合的變更歷程伺服器管理

提供設定、檢視及刪除整合的變更歷程伺服器組態所需的權限。

使用者管理

提供管理使用者帳戶、相關聯 Microsoft Exchange 信箱及群組成員資格所需的所有權限。將此角色指定給負責管理使用者帳戶的 AA。

檢視 Active Directory Collector、DRA Collector、Management Reporting Collector 及資料庫組態資訊

提供檢視 AD 收集器、DRA收集器、Management Reporting Collector 及資料庫組態資訊所需的所有權限。

檢視所有電腦內容

提供檢視電腦帳戶內容所需的所有權限。將此角色指定給負責稽核電腦的 AA。

檢視所有群組內容

提供檢視群組內容所需的所有權限。將此角色指定給負責稽核群組的 AA。

檢視所有資源信箱內容

提供檢視資源信箱內容所需的所有權限。將此角色指定給負責稽核資源信箱的 AA。

檢視所有使用者內容

提供檢視使用者帳戶內容所需的所有權限。將此角色指定給負責稽核使用者帳戶的 AA。

自動化工作流程伺服器管理

提供設定、檢視及刪除自動化工作流程伺服器組態所需的權限。

WTS 管理

提供管理 ActiveView 中使用者帳戶之 Windows Terminal Server (WTS) 內容所需的所有權限。如果您使用 WTS，請將此角色指定給負責維護使用者帳戶之 WTS 內容的 AA。

存取內建角色

存取內建角色以稽核預設委託模型或管理您自己的安全性設定。

若要存取內建角色：

1. 導覽至**委託管理**>**管理角色**。
2. 確定搜尋欄位是空白的，然後按一下**列出符合我的準則的項目**窗格中的**立即尋找**。
3. 選取適當的角色。

使用內建角色

您無法刪除或修改內建角色。但是，您可以將內建角色併入您現有的委託模型，或使用這些角色來設計及執行您自己的模型。

您可以下列方式使用內建角色：

- 讓內建角色與使用者帳戶或 AA 群組產生關聯。此關聯提供使用者或 AA 群組成員對於任務的適當權限。
- 複製內建角色並且使用該複製作為自定角色的基礎。您可以將其它角色或能力新增至這個新角色，以及移除原始包含在內建角色的權限。

如需設計動態委託模型的詳細資訊，請參閱瞭解動態委託模型。

4.3.2 建立自定角色

藉由建立角色，您可以快速且輕易地委託一組權限，代表管理任務或工作流程。您可以從「委託和組態」主控台中的**委託管理**>**角色**節點中，建立及管理角色。在此節點中，您可以執行下列動作：

- 建立新角色
- 複製現有角色
- 修改角色內容
- 刪除角色
- 管理角色指定
  - 委託新指定
  - 移除現有指定
  - 檢視已指定助理管理員的內容
  - 檢視指定的 ActiveView 的內容
- 管理角色和角色中的權限 (角色可以是巢狀的)
- 產生角色變更報告

執行在本節中識別之任何動作的一般工作流程，即選取**角色**節點，然後執行下列其中一項操作：

- 使用**任務**或以滑鼠右鍵按一下功能表，以開啟適用的精靈或對話方塊並遵循必要的動作。
- 在**列出符合我的準則的項目**窗格中尋找角色物件，然後使用**任務**或以滑鼠右鍵按一下功能表，以選取及開啟適用的精靈或對話方塊並遵循必要的動作。

若要執行上述的任何動作，您必須擁有適當的能力，例如「管理安全性模型」角色中所包含的權限。

4.4 權限

能力是「最低權限」管理的初始建置組塊。將能力指定給使用者可協助您執行及維護您的動態安全性模型。您會在「委託和組態」主控台中執行這些程序。

4.4.1 內建權限

在定義角色及進行委託指定，以指定管理物件和執行通用管理任務的職責時，您可以運用超過 390 個內建權限。內建權限無法刪除，但是您可以複製它們以製作自定權限。一些內建權限範例如下：

建立群組及修改所有內容

提供建立群組以及在群組建立期間指定所有內容的權限。

刪除使用者帳戶

如果已啟用資源回收筒，提供將使用者帳戶移除到資源回收筒的權限。如果已停用資源回收筒，提供永久刪除使用者帳戶的權限。

修改所有電腦內容

提供修改電腦帳戶所有內容的權限。

4.4.2 導入自定權限

若要建立自定能力，您要建立新能力或複製現有權限。在委託新能力時，您可以使用現有能力做為範本。權限會定義助理管理員可以在您管理的網域或子樹狀結構中檢視、修改或建立之物件的內容。自定權限可以包含多個內容的存取，例如*檢視所有使用者內容*權限。

附註： 無法複製所有內建權限。

您從「委託和組態」主控台中的**委託管理**>**權限**節點，執行自定權限。在此節點中，您可以執行下列動作：

- 檢視所有權限內容
- 建立新權限
- 複製現有權限
- 修改自定權限
- 產生權限變更報告

若要執行這些動作，您必須擁有適當的能力，例如「管理安全性模型」角色中所包含的權限。

在嘗試建立新權限之前，請考量下列程序。

1. 檢閱 DRA 隨附的權限。
2. 決定您是否需要自定權限。如果適用，您可以複製現有自定權限。
3. 完成適當的精靈驅動程序。例如，完成「新增權限」精靈。
4. 檢視您的新權限。
5. 視需要修改您的新權限。

執行在本節中識別之任何動作的一般工作流程，即選取**權限**節點，然後執行下列其中一項操作：

- 使用「任務」或以滑鼠右鍵按一下功能表，以開啟適用的精靈或對話方塊並遵循必要的動作。
- 在**列出符合我的準則的項目**窗格中尋找權限物件，然後使用**任務**或以滑鼠右鍵按一下功能表，以選取及開啟適用的精靈或對話方塊並遵循必要的動作。

4.4.3 延伸權限

您可以藉由延伸權限，將許可或功能新增至該權限。

例如，若要允許AA建立使用者帳戶，您可以指定*建立使用者及修改所有內容*權限或*建立使用者及修改有限的內容*權限。如果您同時指定*將新使用者新增至群組*權限，AA 可以在使用「建立使用者」精靈時將這個新使用者帳戶新增至群組。在此案例中，*將新使用者新增至群組*權限提供額外的精靈功能。*將新使用者新增至群組*權限是**延伸權限**。

延伸權限無法自行新增許可或功能。若要成功委託任務 (其中包含延伸權限)，您必須隨著想要延伸的權限一併指定延伸權限。

附註：

- 若要成功建立群組並且在 ActiveView 中包含新群組，您必須在指定的 ActiveView 中具有*將新群組新增至 ActiveView* 權限。指定的 ActiveView 也必須包含 OU 或內建容器，在其中包含新群組。
- 若要成功複製群組並且在 ActiveView 中包含新群組，您必須在指定的 ActiveView 中具有*將複製的群組新增至 ActiveView* 權限。指定的 ActiveView 也必須包含來源群組以及 OU 或內建容器，在其中包含新群組。

下表列出一些動作範例，這些動作可以在建立新權限或修改現有權限的內容時進行設定：

委託此任務	指定此權限	以及此延伸權限
複製群組並且將新群組納入指定的 ActiveView	複製群組及修改所有內容	將複製的群組新增至 ActiveView
建立群組並且將新群組納入指定的 ActiveView	建立群組及修改所有內容	將新群組新增至 ActiveView
建立已啟用郵件的聯絡人	建立聯絡人及修改所有內容 建立聯絡人及修改有限的內容	針對新聯絡人啟用電子郵件
建立已啟用郵件的群組	建立群組及修改所有內容	針對新群組啟用電子郵件
建立已啟用郵件的使用者帳戶	建立使用者及修改所有內容 建立使用者及修改有限的內容	針對新使用者啟用電子郵件
建立使用者帳戶並且將新帳戶新增至特定群組	建立使用者及修改所有內容 建立使用者及修改有限的內容	將新使用者新增至群組

4.5 委託指定

您可以從「委託和組態」主控台中的**委託管理**>**助理管理員**節點，管理委託指定。在此節點中，您可以檢視指定給助理管理員的權限和角色，以及管理角色和 ActiveView 的指定。您也可以對「助理管理員」群組執行下列動作：

- 新增群組成員
- 建立群組
- 複製群組
- 刪除群組
- 修改群組內容

若要檢視及管理指定並且對「助理管理員」群組進行變更，您必須擁有適當的權限，例如「管理安全性模型」角色中所包含的權限。

執行在本節中識別之任何動作的一般工作流程，即選取**助理管理員**節點，然後執行下列其中一項操作：

- 使用「任務」或以滑鼠右鍵按一下功能表，以開啟適用的精靈或對話方塊並遵循必要的動作。
- 在**列出符合我的準則的項目**窗格中尋找群組或助理管理員，然後使用**任務**或以滑鼠右鍵按一下功能表，以選取及開啟適用的精靈或對話方塊並遵循必要的動作。

5 規則和程序自動化

本章節提供的資訊可以協助您瞭解規則如何在 DRA 環境中運作，以及這些規則的選項。也會說明如何使用觸發和自動化工作流程，在使用 Active Directory 中的物件時自動化程序。

5.1 瞭解 DRA 規則

DRA 可讓您設定各種規則，這些規則可以協助您保護您的企業並且預防資料損毀。這些原則是在動態安全性模型的內容內運作，確保強制執行的原則可自動與您日新月異的企業保持同步。建立規則 (例如命名慣例、磁碟使用量限制及內容驗證) 可讓您強制規則，協助維護企業資料的完整性。

在 DRA 中，您可以快速地針對這些企業管理區域定義規則：

- Microsoft Exchange
- Office 365
- 主目錄
- 密碼產生

DRA 也提供適用於群組、使用者帳戶及電腦的內建規則。

若要管理或定義規則，您必須擁有適當的權限，例如「DRA 管理員」或「管理規則和自動化觸發」角色中所包含的權限。為了協助您管理您的規則，DRA 提供「規則詳細資料」報告。此報告提供下列資訊：

- 指出規則是否已啟用
- 列出相關聯的操作
- 列出受此規則治理的物件
- 提供規則範圍詳細資料

您可以使用此報告來確保已適當定義您的規則。您也可以使用此報告來比較規則內容、捕捉衝突，以及在您整個企業之間更佳地強制規則。

5.1.1 管理伺服器強制執行規則的方式

您可以讓每個任務或管理操作與一或多個規則產生關聯。當您執行與規則相關聯的操作時，管理伺服器會執行規則並且強制執行指定的規則。如果伺服器偵測到違反規則，則它會傳回錯誤訊息。如果伺服器未偵測到違反規則，則它會完成操作。您可以藉由讓規則與特定 ActiveView 或「助理管理員」群組產生關聯，來限制規則的範圍。

如果操作與一個以上的規則相關聯，管理伺服器會以字母順序強制執行規則。也就是說，規則 A 會在規則 B 前面強制執行，不論指定規則為何。

若要確保您的規則不會彼此衝突，請使用下列指導方針：

- 命名規則，讓它們以適當的順序執行

- 驗證每個規則不會影響由其它規則執行的驗證或動作
- 在您的線上環境導入自定規則之前，進行徹底的測試

管理伺服器會在每次規則執行時，將規則狀態輸入到稽核記錄中。這些記錄項目會記錄傳回碼、相關聯的操作、執行的物件以及自定規則是否成功。

警告： 規則是使用管理服務帳戶來執行的。因為服務帳戶具有管理員許可，所以規則具有所有企業資料的完整存取。因此，與內建「管理規則和自動化觸發」角色相關聯的 AA 可以取得比您預期還要多的權限。

5.1.2 內建規則

內建規則會在您安裝管理伺服器時執行。當您使用這些規則時，您可能會遇到下列字詞：

規則範圍

定義要套用 DRA 原則的物件或內容。例如，某些規則可讓您將規則套用至特定 ActiveView 中的特定 AA。某些規則可讓您從不同的物件類別中選擇，例如使用者帳戶或群組。

全域規則

在管理的網域中指定類別或類型的所有物件上強制執行規則。全域規則不會讓您限制要套用規則的物件範圍。

規則關係

定義規則是共同套用還是自行套用。若要建立規則關係，請定義套用至相同動作之兩個以上的規則，然後選擇規則群組選項的成員。如果操作參數或內容符合任何規則，操作就會成功。

瞭解內建規則

內建規則提供商務規則，以處理常見的安全性和資料完整性問題。這些規則屬於預設安全性模型，可讓您將 DRA 安全性功能整合至您現有的企業組態。

DRA 提供兩種方式來強制執行規則。您可以建立自定規則或是從數個內建規則中選擇。內建規則方便套用規則，不需要開發自定程序檔。如果您需要執行自定規則，可以將現有內建規則調適為符合您的需求。大部分規則可讓您修改錯誤訊息文字、重新命名規則、新增描述及指定如何套用規則。

一些內建規則會在您安裝 DRA 時啟用。依預設會執行下列規則。如果您不想要強制執行這些規則，可以停用或刪除它們。

規則名稱	預設值	描述
$ComputerNameLengthPolicy	64 15 (Windows 2000 以前版本)	限制電腦名稱或 Windows 2000 以前版本電腦名稱中的字元數
$GroupNameLengthPolicy	64 20 (Windows 2000 以前版本)	限制群組名稱或 Windows 2000 以前版本群組名稱中的字元數
$GroupSizePolicy	5000	限制群組中的成員數
$NameUniquenessPolicy	無	確保Windows2000以前版本和CN名稱在所有管理的網域中都是唯一的。
$SpecialGroupsPolicy	無	防止環境中有未檢查的權限擴張。

規則名稱	預設值	描述
$UCPowerConflictPolicy	無	藉由讓「使用者複製」與「使用者建立」能力互斥，來防止權限擴張
$UPNUniquenessPolicy	無	確保UPN名稱在所有管理的網域中是唯一的
$UserNameLengthPolicy	64 20 (舊版登入名稱)	限制使用者登入名稱或舊版登入名稱中的字元數

可用規則

DRA 提供數個規則，您可以針對您的安全性模型加以自定。

附註： 您可以針對DRA使用者介面目前沒有顯示的內容，建立一個需要輸入內容資料的原則。如果原則需要某項資料，但是使用者介面未提供欄位以供輸入值，例如為新使用者帳戶輸入部門資料，則您將無法建立或管理該物件。若要避免這個問題，如果是設定需要輸入內容資料的原則，請僅使用那些可以從使用者介面存取的內容。

建立自定規則

允許您將程序檔或可執行檔連結至 DRA 或 Exchange 操作。自定原則可讓您驗證您選擇的任何操作。

強制執行名稱長度上限

允許您全域地針對使用者帳戶、群組、OU、聯絡人或電腦強制執行名稱長度上限。

規則會檢查名稱容器 (通用名稱或 cn) 以及 Windows 2000 以前版本名稱 (使用者登入名稱)。

強制執行群組成員數上限

允許您全域地針對群組的成員數強制執行限制。

強制執行唯一的 Windows 2000 以前版本帳戶名稱

確認 Windows 2000 以前版本名稱在所有管理的網域之間是唯一的。在 Microsoft Windows 網域中，Windows2000以前版本名稱在網域內必須是唯一的。此全域規則會在所有管理的網域之間強制執行此規則。

強制執行唯一的使用者主體名稱 (UPN)

確認使用者主體名稱(UPN)在所有管理的網域之間是唯一的。在MicrosoftWindows網域中，UPS在網域內必須是唯一的。此規則會在所有管理的網域之間強制執行此規則。因為這是全域規則，所以 DRA 會提供規則名稱、描述及規則關係。

限制對於特殊群組成員的動作

防止您管理管理員群組的成員，除非您是該管理員群組的成員。此全域規則預設為啟用。

當您限制對於管理員群組成員的動作時，「建立規則精靈」不需要額外資訊。您可以指定自定錯誤訊息。因為這是全域規則，所以 DRA 會提供規則名稱、描述及規則關係。

防止 AA 在相同的 AV 中建立及複製使用者

防止可能的權限擴張。當此規則啟用時，您可以建立使用者帳戶或複製使用者帳戶，但是您無法同時具有這兩項權限。此全域規則會確保您無法在相同 ActiveView 中建立及複製使用者帳戶。

此規則不需要額外資訊。

設定命名慣例規則

允許您建立命名慣例，套用至特定 AA、ActiveView 及物件類別，例如使用者帳戶或群組。

您也可以指定此規則監控的確切名稱。

建立規則以驗證特定內容

允許您建立規則以驗證 OU 或帳戶物件的任何內容。您可以指定預設值、內容格式遮罩及有效值和範圍。

使用此規則，藉由在您建立、複製或修改特定物件的內容時驗證特定項目欄位，以強制執行資料完整性。此規則提供相當大的彈性和權限來驗證項目、提供預設項目及限制各種內容欄位的項目選項。藉由使用此規則，您可以在任務完成之前要求製作正確的項目，進而維護管理的網域之間的資料完整性。

例如，假設您有三個部門：製造、銷售和管理。您可以將 DRA 接受的項目限制為只有這三個值。您也可以使用此規則來強制執行適當電話號碼格式、提供有效資料範圍或要求電子郵件地址欄位的項目。若要為電話號碼指定多個格式遮罩，例如 (123)456 7890 以及 456 7890，請將內容格式遮罩定義為 (###)### ####,### ####。

建立規則以強制執行 Office 365 授權

允許您建立規則以根據 Active Directory 群組成員資格來指定 Office 365 授權。當成員從相關 Active Directory 群組中移除時，此規則也會強制執行 Office 365 授權的移除。

如果將未同步至雲端的使用者新增至 Active Directory 群組，使用者會在 Office 365 授權指定給該使用者之前進行同步化。

在建立規則期間，您可以指定數個內容和設定，例如規則名稱和 AA 嘗試的動作違反此規則時所顯示之錯誤訊息的用字。

根據預設，您建立以強制執行 Office 365 授權的規則，在變更是於 DRA 外部進行時不會套用，除非您也在租用戶內容頁面上啟用授權更新排程。

使用內建規則

因為內建規則屬於預設安全性模型，所以您可以使用這些規則來強制執行您目前的安全性模型，或修改它們以更加符合您的需求。您可以變更數個內建規則的名稱、規則設定、範圍、規則關係及錯誤訊息。您可以啟用或停用每個內建規則。

您也可以輕易地建立新規則。

5.1.3 導入自定規則

自定規則可讓您完整利用預設安全性模型的權限和彈性。藉由使用自定規則，您可以整合 DRA 與現有企業元件，同時確保強制執行您的專屬規則。您可以使用自定規則功能來延伸您的企業規則。

您可以藉由讓可執行檔或程序檔關聯至管理操作，來建立及強制執行自定規則。例如，與 UserCreate 操作相關聯的規則程序檔會檢查您的人力資源資料庫，以查看指定的員工是否存在。如果員工存在於人力資源資料庫中而沒有現有帳戶，則程序檔會從資料庫擷取員工 ID、名字和姓氏。操作順利完成並且以正確的資訊填入使用者帳戶內容視窗。但是，如果員工已經有帳戶，則操作會失敗。

程序檔給予您相當大的彈性和權限。若要建立您自己的規則程序檔，可以使用 Directory and Resource Administrator ADSI Provider (ADSI 提供者)、軟體開發套件 (SDK) 及 PowerShell Cmdlet。如需建立您自己的規則程序檔的詳細資訊，請參閱 DRA 文件網站上的「參考」區段。

5.1.4 限制原生內建安全性群組

為了提供更安全的環境，DRA可讓您限制給予Microsoft Windows內建安全性群組的權限。修改群組成員資格、內建安全性群組內容或群組成員內容的能力，可能會產生重要的安全性影響。例如，如果您可以變更「伺服器操作人員」群組中使用者的密碼，則您可以該使用者的身分登入並且行使委託給此內建安全性群組的權限。

DRA會藉由提供規則，檢查您對於原生內建安全性群組及其成員所具備的能力，來防止此安全性問題。此驗證會確保您要求的動作不會擴張這些權限。在您啟用此規則之後，身為內建安全性群組 (例如「伺服器操作人員」群組) 成員的 AA 只能管理相同群組的其它成員。

您可以限制的原生內建安全性群組

您可以使用 DRA 規則，限制下列 Microsoft Windows 內建安全性群組的權限：

- 帳戶操作人員
- 管理員
- 備份操作人員
- Cert Publishers (憑證發行者)
- DNS 管理員
- 網域管理員
- 企業管理員
- 群組規則建立者擁有者
- 列印操作人員
- Schema Admins (架構管理員)

附註： DRA會根據內建安全性群組的內部識別碼進行參考。因此，即使這些群組重新命名，DRA也支援這些群組。此功能會確保 DRA 支援在不同國家、具有不同名稱的內建安全性群組。例如，DRA 會參考具有相同內部識別碼的「管理員」群組和 *Administratoren* 群組。

限制對於原生內建安全性群組的動作

DRA 會使用規則來限制原生內建安全性群組及其成員可以行使的權限。此規則稱為 $SpecialGroupsPolicy，會限制原生內建安全性群組的成員對於其它成員或其它原生內建安全性群組可以執行的動作。DRA 依預設會啟用此規則。如果您不想要限制對於原生內建安全性群組及其成員的動作，則可以停用此規則。

當此規則啟用時，DRA 會使用下列驗證測試來判斷是否允許對原生內建安全性群組或其成員執行某個動作：

- 如果您是 Microsoft Windows 管理員，則可以對您具有適當權限的原生內建安全性群組及其成員執行動作。
- 如果您是內建安全性群組的成員，只要您具有適當權限，就可以對相同內建安全性群組及其成員執行動作。
- 如果您不是內建安全性群組的成員，您無法修改內建安全性群組或其成員。

例如，如果您是「伺服器操作人員」和「帳戶操作人員」群組的成員且具有適當權限，您可以對「伺服器操作人員」群組的成員、「帳戶操作人員」群組的成員或這兩個群組的成員執行動作。但是，如果某個使用者帳戶同時是 Print Operators (列印操作員) 群組和 Account Operators (帳戶操作員) 群組的成員，您就無法對其執行動作。

DRA 會限制您對原生內建安全性群組執行下列動作：

- 複製群組
- 建立群組
- 刪除群組
- 新增成員至群組
- 從群組移除成員
- 將群組移至 OU
- 修改群組的內容
- 複製信箱
- 移除信箱
- 複製使用者帳戶
- 建立使用者帳戶
- 刪除使用者帳戶
- 將使用者帳戶移至 OU
- 修改使用者帳戶內容

DRA 也會限制動作以確保您無法透過物件獲得其權限。例如，當您將使用者帳戶新增至群組時，DRA 會檢查以確保您不會因為這個使用者帳戶是該群組的成員而另外獲得其權限。這個驗證有助於防止能力擴張。

5.1.5 管理政策

您可以透過「規則和自動化管理」節點來存取 Microsoft Exchange 和主目錄規則，以及內建和自定規則。使用下列通用任務來改善您的企業的安全性和資料完整性。

設定 Exchange 規則

讓您定義 Microsoft Exchange 組態、信箱規則、自動化命名及 proxy 產生規則。這些規則可以定義當 AA 建立、修改或刪除使用者帳戶時，如何管理信箱。

設定 Office 365 規則

讓您強制執行無效字元和字元長度規則，以防止目錄同步失敗。

Office 365 規則可讓您指定當您建立或刪除使用者帳戶時，Exchange Online 如何管理 Office 365 信箱。

設定主目錄規則

讓您在 AA 建立、重新命名或刪除使用者帳戶時，自動建立、重新命名或刪除主目錄和主目錄共享。主目錄規則也可讓您啟用或停用 Microsoft Windows 伺服器以及非 Windows 伺服器上主目錄的磁碟配額支援。

設定密碼產生規則

讓您定義由 DRA 產生之密碼的需求。

Microsoft Exchange 規則

Exchange 提供數個規則，協助您更有效率地管理 Microsoft Exchange 物件。Microsoft Exchange 規則可讓您自動化信箱管理、強制執行別名和信箱儲存區的命名慣例，以及自動產生電子郵件地址。

這些規則可協助您簡化工作流程及維護資料完整性。例如，您可以指定當您建立、修改或刪除使用者帳戶時，Exchange 如何管理信箱。若要定義及管理 Microsoft Exchange 規則，您必須擁有適當的能力，例如內建「管理規則和自動化觸發」角色中所包含的能力。

指定預設電子郵件地址規則

若要指定預設電子郵件地址規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的能力，且您的授權必須支援 Exchange 產品。

若要指定預設電子郵件地址規則：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**>**Proxy 產生**。
2. 指定 Microsoft Exchange 伺服器的網域。
   - **2a** 按一下**瀏覽**。
   - **2b** 視需要指定額外搜尋準則，然後按一下**立即尋找**。
   - **2c** 選取要設定的網域，然後按一下**確定**。
3. 指定所選取網域的 Proxy 產生規則。
   - **3a** 按一下**新增**。
   - **3b** 選取 Proxy 類型。例如，按一下**網際網路位址**。
   - **3c** 接受預設值或輸入新的 Proxy 產生規則，然後按一下**確定**。

     如需 Proxy 產生規則之支援替代字串的詳細資訊，請參閱委託及設定用戶端規則
4. 按一下**自定屬性**以編輯自定信箱內容的自定名稱。
   - **4a** 選取屬性然後按一下**編輯**按鈕。
   - **4b** 在「屬性內容」視窗中，在**自定名稱**欄位中輸入屬性名稱，然後按一下**確定**。
5. 按一下**「確定」**。

附註： DRA 規則管理員應該具有*管理自定工具*權限，以修改 Microsoft Exchange 規則中的自定屬性。

信箱規則

信箱規則可讓您指定當 AA 建立、複製、修改或刪除使用者帳戶時，Exchange 如何管理信箱。信箱規則會根據 AA 管理相關聯使用者帳戶的方式，自動管理 Microsoft Exchange 信箱。

附註： 在 Microsoft Windows 網域中啟用**不允許助理管理員建立沒有信箱的使用者帳戶**選項時，請確保 AA 具有複製或建立使用者帳戶的能力。啟用此選項需要 AA 建立具有信箱的 Windows 使用者帳戶。

若要指定 Microsoft Exchange 信箱規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限，且您的授權必須支援 Exchange 產品。

若要指定 Exchange 信箱規則：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**>**信箱規則**。
2. 選取您想要 Exchange 在建立或修改使用者帳戶時強制執行的信箱規則。
3. 按一下**「確定」**。

Office 365 規則

若要指定 Office 365 信箱規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。您的授權也必須支援 Microsoft Exchange 產品。

若要使用與 Office 365 同步的內容來限制無效字元和字元長度，請按一下 **Office 365 規則**，然後選取核取方塊：**針對無效字元和字元長度強制執行線上信箱規則**。

允許 DRA 管理您的 Office 365 授權 (選擇性)

如果您想要允許 DRA 管理您的 Office 365 授權，您必須執行下列動作：

- 建立授權強制規則。
- 啟用租用戶內容頁面上的**授權更新排程**。

建立規則以強制執行 Office 365 授權

若要建立規則以強制執行 Office 365 授權，請按一下「委託和組態」主控台中的**規則和自動化管理**節點，然後選取**新增規則 > 建立新規則以強制執行 Office 365 授權**。

當規則強制執行且使用者新增至 Active Directory 時，DRA 會使用群組成員資格自動將 Office 365 授權指定給使用者。

Office 365 授權更新排程

您建立以強制執行 Office 365 授權的規則，在變更是於 DRA 外部進行時不會套用，除非您也在租用戶內容頁面上啟用**授權更新排程**。授權更新工作會確保指定給使用者的 Office 365 授權與您的 Office 365 授權規則相符。

授權更新工作和 Office 365 授權規則會搭配運作，以確保您的所有受管理使用者僅獲得指定它們應該具有的 Office 365 授權。

附註：

- DRA 不會管理僅線上使用者帳戶的 Office 365 授權。為了讓 DRA 管理具有 Office 365 授權的使用者，這些使用者必須與 Active Directory 同步。
- 如果您選擇使用 DRA 來管理您的 Office 365 授權，DRA 會在下一次授權更新工作執行時，覆寫在 DRA 外部所做的任何 Office 365 授權手動變更。
- 如果您在確定 Office 365 授權規則已正確設定之前就啟用 Office 365 授權更新工作，在授權更新工作執行之後，您的指定授權可能會不正確。

建立及導入主目錄規則

當您管理大量的使用者帳戶時，建立及維護這些主目錄和共享可能需要大量時間，且可能會是安全性錯誤的來源。每次建立、重新命名或刪除使用者時，都需要額外維護。主目錄規則可協助您管理主目錄和主目錄共享維護。

DRA可讓您自動化使用者主目錄的建立和維護。例如，您可以輕易地設定 DRA，讓管理伺服器在您建立使用者帳戶時建立主目錄。在此情況下，如果您在建立使用者帳戶時指定主目錄路徑，則伺服器會自動針對每個指定的路徑建立主目錄。如果您未指定路徑，則伺服器不會建立主目錄。

DRA 在建立使用者主目錄或在允許的父路徑中設定使用者的主目錄規則期間，支援分散式檔案系統 (DFS) 路徑。您可以在 Netapp Filer 和 DFS 路徑或分割區上，建立、重新命名及刪除主目錄。

設定主目錄規則

若要設定主目錄、共享及磁碟區磁碟配額規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。每個規則會根據您管理相關聯使用者帳戶的方式，自動管理主目錄、共享及磁碟區磁碟配額。

若要設定主目錄規則，請導覽至**規則和自動化管理**>**設定主目錄規則**>

- 主目錄
- 主目錄共享
- 主目錄磁碟區磁碟配額

管理伺服器需求

針對您需要建立主目錄共享的每部電腦，管理伺服器服務帳戶或存取帳戶應該是該電腦的管理員，或是對應網域中「管理員」群組的成員。

DRA 管理及儲存主目錄所在的每個磁碟機上，必須有管理共享 (例如 C$ 或 D$) 存在。DRA 會使用管理共享來執行一些主目錄和主目錄共享自動化任務。如果這些共享不存在，DRA 就無法提供主目錄和主目錄共享自動化。

針對 NetApp Filer 設定主目錄允許的路徑

若要針對 NetApp Filer 設定允許的父路徑：

1. 導覽至**規則和自動化管理**>**設定主目錄規則**。
2. 在**允許的父路徑**文字方塊中，輸入下表中其中一個允許的路徑：

共享類型	允許的路徑
Windows	(*FileName**adminshare:**volumerootpath**directorypath*)
非 Windows	(*non-windows**share*)

3. 按一下**新增**。
4. 針對您想要套用主目錄規則的每個允許的父路徑重複步驟 1-3。

瞭解主目錄規則

為了與適當的Microsoft Windows安全性規則保持一致，DRA僅在目錄層級建立存取控制限制。同時在共享名稱層級和檔案或目錄物件層級放置存取控制限制時，通常會導致管理員和使用者的存取規劃混淆。

當您變更主目錄共享的存取控制限制時，DRA 不會變更該目錄的現有安全性。在此情況下，您必須確定使用者帳戶具有它們自己的主目錄的適當存取。

主目錄自動化和規則

DRA會藉由在您修改使用者帳戶時管理主目錄，來自動化主目錄維護任務。DRA可以在建立、複製、修改、重新命名或刪除使用者帳戶時，執行不同的動作。

若要成功執行您的主目錄規則，請考量下列指導方針：

- 確保指定的路徑使用正確格式。
  - 若要為單一主目錄指定路徑，請使用下表中其中一個範本：

共享類型	路徑範本
Windows	*computer**share*\. 例如，如果您想要讓 DRA 在 server01 電腦上的 Home Share 資料夾中自動建立主目錄，請輸入 \\server01\Home Share\
非 Windows	*non-windows**share*

  - 若要標準化對應主目錄共享之根目錄上的主目錄管理，請使用通用命名慣例語法，例如 *伺服器名稱*\C:*主目錄的路徑*。
  - 若要為巢狀主目錄指定路徑，請使用下表中其中一個範本：

共享類型	路徑範本
Windows	*computer**share**first directory**second directory*\ 例如，如果您想要讓DRA在server01電腦上Home Share 資料夾下方的現有 JSmit\Home directory 中自動建立主目錄，請輸入 \\server01\Home Share\JSmith\Home。
非 Windows	*non-windows**share**first directory**second directory*\

附註： DRA 也支援下列格式：*computer**share**username* and *computer**share**%username%*。在每個情況下，DRA 會自動針對相關聯的使用者帳戶建立主目錄。

- 當您定義規則或自動化觸發以管理 NetApp Filer 上的主目錄時，必須針對目錄規格使用不同的格式。
  - 如果您使用 NetApp Filer，請以下列格式指定父目錄：
    *FilerName**adminshare*:*volumerootpat*h*directorypath*
  - adminshare 變數是隱藏的共享，對應至 NetApp Filer 上的根磁碟區，例如 *c$*。例如，如果 NetApp Filer (名稱為 usfiler) 上共享的本機路徑是 c$\vol\vol0\mydirectory，您可以為 NetApp Filer 指定根路徑 \\usfiler\c:\vol\vol0\mydirectory。
- 若要在您建立使用者主目錄或為使用者設定主目錄規則時指定 DFS 路徑，請使用 *server**root**<link>* format，其中 root 可以是管理的網域或獨立根目錄，格式如下：*FilerName**adminshare*:*volumerootpath**directorypath*。
- 建立共享目錄以儲存此使用者帳戶的主目錄。
- 確定 DRA 可以存取在路徑中參考的電腦或共享。

當建立使用者帳戶時建立主目錄

這個規則可讓DRA自動為新的使用者帳戶建立主目錄。當DRA建立主目錄時，管理伺服器會使用在「建立使用者精靈」之**主目錄**欄位中指定的路徑。您可以在稍後透過使用者內容視窗的「設定檔」索引標籤來修改此路徑，DRA會將主目錄移至新位置。如果您未指定這些欄位的值，DRA不會為該使用者帳戶建立主目錄。

DRA 會根據選取的**主目錄許可**選項，設定新目錄的安全性。這些選項可讓您控制所有主目錄的一般存取。

例如，對於在其中建立使用者主目錄的共享，您可以指定「管理員」群組的成員擁有完整控制，而「服務台」群組的成員擁有讀取存取權。然後，當 DRA建立使用者主目錄時，新的主目錄可以繼承父目錄的這些權限。因此，「管理員」群組的成員擁有所有使用者主目錄的完整控制，而「服務台」群組的成員擁有所有使用者主目錄的讀取存取權。

如果指定的主目錄已存在，DRA 不會建立主目錄，也不會修改現有目錄許可。

當重新命名使用者帳戶時重新命名主目錄

此規則可讓 DRA 自動執行下列動作：

- 當您指定新的主目錄路徑時建立主目錄
- 當您變更主目錄路徑時移動主目錄內容
- 當您重新命名使用者帳戶時重新命名主目錄

當您重新命名使用者帳戶時，DRA 會根據新的帳戶名稱，重新命名現有主目錄。如果現有主目錄目前正在使用中，DRA 會使用新的名稱來建立新的主目錄，而且不會變更現有主目錄。

如果先前的主目錄和新的主目錄名稱及位置都相同，您可以重新命名主目錄。但是，如果目錄重新命名失敗，DRA 會建立新的主目錄、將先前主目錄的內容移至新的主目錄，然後刪除現有主目錄。

當您變更主目錄路徑時，DRA 會嘗試建立指定的主目錄，並且將先前主目錄的內容移至新位置。您也可以設定「主目錄」規則以建立主目錄，不需要從現有主目錄移動內容。DRA 也會從先前目錄將指定的 ACL 套用至新目錄。如果指定的主目錄已存在，DRA不會建立這個新目錄，也不會修改現有目錄許可。如果先前的主目錄未鎖定，DRA 會將它刪除。

當DRA無法重新命名主目錄時，DRA會嘗試使用新名稱建立新的主目錄，然後從先前的主目錄將內容複製到新的主目錄。然後DRA會嘗試刪除先前的主目錄。您可以設定DRA不要從先前的主目錄將內容複製到新的主目錄，並且手動從先前的主目錄將內容移至新的主目錄，以避免例如複製已開啟檔案的疑慮。

當刪除先前的主目錄時，DRA 需要明確許可以便從先前的主目錄刪除唯讀檔案和子目錄。您可以對 DRA 提供許可，以明確地從先前的主目錄刪除唯讀檔案和子目錄。

允許主目錄共享的父目錄或路徑

DRA 可讓您針對檔案伺服器上的主目錄共享，指定允許的父目錄或路徑。如果您有許多的目錄或檔案伺服器要指定，可以將這些路徑輸出到CSV檔案，然後使用DRA主控台，從CSV檔案將路徑新增至 DRA。DRA 會使用在允許的父路徑欄位中輸入的資訊以確保：

- 當助理管理員刪除使用者帳戶和使用者帳戶主目錄時，DRA 不會刪除檔案伺服器上的父目錄。
- 當您重新命名使用者帳戶或變更使用者帳戶的主目錄路徑時，DRA 會將主目錄移至檔案伺服器上的有效父目錄或路徑。

當刪除使用者帳戶時刪除主目錄

此規則可讓 DRA 在您刪除相關聯的使用者帳戶時，自動刪除主目錄。如果您啟用資源回收筒，在您從資源回收筒刪除使用者帳戶之前，DRA 不會刪除主目錄。當刪除主目錄時，DRA 需要明確許可以便從先前的主目錄刪除唯讀檔案和子目錄。您可以對 DRA 提供許可，以明確地從先前的主目錄刪除唯讀檔案和子目錄。

主目錄共享自動化和規則

DRA會藉由在您修改使用者帳戶或管理主目錄時管理主目錄共享，以自動化主目錄共享維護任務。DRA 可以在建立、複製、修改、重新命名或刪除使用者帳戶時，執行不同的動作。

為了與適當的Microsoft Windows安全性規則保持一致，DRA不會在共享名稱層級建立存取控制限制。相反地，DRA 只會在目錄層級建立存取控制限制。同時在共享名稱層級和檔案或目錄物件層級放置存取控制限制時，通常會導致管理員和使用者的存取規劃混淆。

附註： 指定的位置必須在主目錄上面一個層級有通用主目錄共享，例如 HOMEDIRS。

例如，下列路徑有效：*HOUSERV1\HOMEDIRS\%username%*

下列路徑無效：*HOUSERV1\%username%*

指定主目錄共享名稱

當定義主目錄共享自動化規則時，您可以為每個自動建立的主目錄共享指定字首和字尾。藉由指定字首和字尾，您可以針對主目錄共享強制執行命名慣例。

例如，您啟用建立主目錄和建立主目錄共享自動化規則。針對主目錄共享，您可以指定底線字首和貨幣符號字尾。當您建立名稱為 TomS 的使用者時，變會將它的新目錄對應至 U 磁碟機，並且指定 \\HOUSERV1\HOMEDIRS\%username% 作為目錄路徑。在此範例中，DRA會建立名為 _TomS$ 的網路共享，指向 \\HOUSERV1\HOMEDIRS\TomS directory。

為新的使用者帳戶建立主目錄共享

當 DRA 建立主目錄共享時，管理伺服器會使用在「建立使用者精靈」之**主目錄**欄位中指定的路徑。您稍後可以透過使用者內容視窗的「設定檔」索引標籤，修改此路徑。

DRA 會藉由將指定的字首和字尾 (如果有的話) 新增至使用者名稱，來建立共享名稱。如果您使用完整使用者帳戶名稱，DRA 可能無法新增指定的共享字首和字尾。字首和字尾以及許可的連線數目是根據您選取的主目錄共享建立選項。

為複製的使用者帳戶建立主目錄共享

如果從新建立的使用者帳戶名稱所產生的主目錄共享名稱已存在，DRA 會刪除現有共享並且將新共享建立至指定的主目錄。

當複製使用者帳戶時，必須有現有使用者帳戶的共享名稱存在。當您複製使用者帳戶時，DRA 也會複製主目錄資訊，並且為新的使用者自定該資訊。

修改主目錄共享內容

當您變更主目錄位置時，DRA 會刪除現有共享並且將新共享建立至新的主目錄。如果原始主目錄是空白的，DRA 會刪除原始目錄。

針對已重新命名的使用者帳戶重新命名主目錄共享

當您重新命名使用者帳戶時，DRA 會刪除現有主目錄共享，並且根據新的帳戶名稱建立新的共享。新的共享會指向現有主目錄。

針對已刪除的使用者帳戶刪除主目錄共享

當您永久刪除使用者帳戶時，DRA 會刪除主目錄共享。

主目錄磁碟區磁碟配額管理規則

DRA 可讓您管理主目錄磁碟區的磁碟配額。您可以在原生網域 (其中主目錄位於 Microsoft Windows 電腦上) 中執行此規則。當您執行此規則時，應該指定至少 25MB 的磁碟配額，以便具有足夠的空間。

啟用密碼產生

此功能可讓您針對DRA產生的密碼指定規則設定。DRA不會對使用者建立的密碼強制執行這些設定。當設定「密碼規則」內容時，密碼長度必須有至少 6 個字元且不超過 127 個字元。除了密碼長度之外，所有值都可以設為零。

若要設定「密碼產生規則」，請導覽至**規則和自動化管理**>**設定密碼產生規則**，然後選取**啟用密碼規則**核取方塊。按一下**密碼設定**然後設定「密碼規則」內容。

規則任務

若要刪除、啟用或停用規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。

若要執行其中一個動作，請導覽至**規則和自動化管理**>**規則**。在右窗格中以滑鼠右鍵按一下您想要刪除、啟用或停用的規則，然後選取想要的動作。

導入內建規則

若要導入內建規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。如需關於內建規則的詳細資訊，請參閱瞭解內建規則。

附註： 在讓內建規則與 AA 和 ActiveView 產生關聯之前，請先驗證 AA 已指定給該 ActiveView。

若要執行內建規則：

1. 導覽至**規則和自動化管理**>**規則**。
2. 在「任務」功能表上，按一下**新增規則**，然後選取您想要建立的內建規則類型。
3. 在每個精靈視窗上，指定適當的值，然後按**下一步**。例如，您可以讓此新規則與特定 ActiveView 產生關聯，讓 DRA 對該 ActiveView 所包含的物件強制執行此規則。
4. 檢閱摘要，然後按一下**完成**。

導入自定規則

若要執行自定規則，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。

若要成功執行自定規則，您必須撰寫程序檔，在特定操作 (管理任務) 期間執行。在自定規則程序檔中，您可以定義每當動作違反規則時顯示的錯誤訊息。您也可以透過「建立規則精靈」指定預設錯誤訊息。

如需關於撰寫自定規則、檢視管理操作的清單，或使用引數陣列的詳細資訊，請參閱 SDK。如需詳細資訊，請參閱 撰寫自定規則程序檔或可執行檔。

附註：

- 在讓自定規則與 AA 和 ActiveView 產生關聯之前，請先確定 AA 已指定給該 ActiveView。
- 如果自定規則程序檔或可執行檔的路徑包含空格，請在路徑前後指定引號 (")。

若要執行自定規則：

1. 撰寫規則程序檔或可執行檔。
2. 使用已獲得指定管理的網域中內建「管理規則和自動化觸發」角色的帳戶，登入 DRA 用戶端電腦。
3. 啟動「委託和組態」主控台。
4. 連接至主要管理伺服器。
5. 在左窗格中，展開**規則和自動化管理**。
6. 按一下**規則**。
7. 在「任務」功能表上，按一下**新增規則 > 建立自定規則**。
8. 在每個精靈視窗上，指定適當的值，然後按**下一步**。例如，您可以讓此新規則與特定 ActiveView 產生關聯，讓 DRA 對該 ActiveView 所包含的物件強制執行此規則。
9. 檢閱摘要，然後按一下**完成**。

修改規則內容

若要修改規則的所有內容，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。

若要修改規則內容：

1. 導覽至**規則和自動化管理**>**規則**。

2 以滑鼠右鍵按一下您想要修改的規則，然後選取內容。

3 修改此規則的適當內容和設定。

撰寫自定規則程序檔或可執行檔

如需關於撰寫自定規則程序檔或可執行檔的詳細資訊，請參閱 SDK。

若要存取 SDK：

1 請確定您已在電腦上安裝 SDK。安裝程式會在「目錄和資源管理員」程式群組中建立 SDK 的捷徑。如需詳細資訊，請參閱 安裝 DRA 管理伺服器 中的安裝核對清單。

2 按一下「目錄和資源管理員」程式群組中的 SDK 捷徑。

如需關於 SDK 的詳細資訊，請參閱 DRA 文件網站上的《「DRA REST 服務指南」》。

5.1.6 委託及設定用戶端規則

自動命名規則包含 Exchange 規則中的三個規則組態，這些組態是「委託和組態」用戶端獨佔的，意思是它是用戶端規則。

自動命名規則可讓您為信箱的特定內容指定自動化命名規則。這些選項可讓您建立命名慣例，並且快速地針對顯示名稱、目錄名稱及別名內容產生標準值。Exchange可讓您針對數個自動化命名選項指定替代字串，例如 %First 和 %Last。

當 Exchange 產生目錄名稱或別名時，它會檢查產生的值是否是唯一的。如果產生的值非唯一，則 Exchange 會附加連字號 (-) 和兩位數數字，從 -01 開始，讓值成為唯一的值。當 Exchange 產生顯示名稱時，它不會檢查值是否是唯一的。

Exchange 針對自動命名和 Proxy 產生規則支援下列替代字串：

%First	**表示相關聯使用者帳戶「名字」內容的值。**
%Last	表示相關聯使用者帳戶「姓氏」內容的值。
%Initials	表示相關聯使用者帳戶「姓名首字母」內容的值。
%Alias	表示「別名」信箱內容的值。
%DirNam	表示「目錄名稱」信箱內容的值。產生 Microsoft Exchange 信箱的電子郵件地址時，Exchange 不支援 Proxy 產生字串，該字串會指定 %DirName 變數。
%個別人員	表示相關聯使用者帳戶「使用者名稱」內容的值。

您也可以在百分比符號 (%) 與替代字串名稱之間指定數字，以表示該值包含的字元數。例如，%2First 表示使用者帳戶之名字內容的前兩個字元。

每個自動命名規則或 Proxy 產生規則可以包含一或多個替代字串。您也可以在每個規則中指定字元作為特定替代字串的字首或字尾，例如句點號空格 (.)，後面接續著 %Initials 替代字串。如果替代字串的內容為空白，Exchange 不會包含該內容的字尾。

例如，請針對顯示名稱內容考量下列自動命名規則：

```
%First %1Initials. %Last
```

如果名字內容是 Susan，姓名首字母內容是 May，姓氏內容是 Smith，則 Exchange 會將顯示名稱內容設為 Susan M. Smith。

如果**名字**內容是 Michael，**姓名首字母**內容是空白，**姓氏**內容是 Jones，則 Exchange 會將**顯示名稱**內容設為 Michael Jones。

指定自動化信箱命名規則

若要指定自動化信箱命名選項，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限，且您的授權必須支援 Exchange 產品。

若要指定自動化信箱命名規則：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**>**別名命名**。
2. 指定適當的名稱產生資訊。
3. 選取**在信箱更新期間強制執行別名命名規則**。
4. 按一下**「確定」**。

指定資源命名規則

若要指定資源命名選項，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限，且您的授權必須支援 Exchange 產品。

若要指定資源命名規則：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**>**資源命名**。
2. 指定適當的資源名稱產生資訊。
3. 選取**在信箱更新期間強制執行資源命名規則**。
4. 按一下**「確定」**。

指定歸檔命名規則

若要指定歸檔命名選項，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限，且您的授權必須支援 Exchange 產品。

若要指定歸檔命名規則：

1. 導覽至**規則和自動化管理**>**設定 Exchange 規則**>**歸檔命名**。
2. 指定使用者帳戶的適當歸檔名稱產生資訊。
3. 選取**在信箱更新期間強制執行歸檔命名規則**。
4. 按一下**「確定」**。

5.2 任務觸發自動化前與後

自動化觸發是一項規則，讓程序檔或可執行檔與一或多個操作產生關聯。您可以透過程序檔或可執行檔自動化現有工作流程，並且建立DRA與其它資料存庫之間的資訊橋接。自動化觸發可讓您延伸DRA所提供的功能和安全性。

當您定義自動化觸發時，您會設定規則參數、哪些操作應該與觸發相關聯、要執行哪些程序檔或可執行檔，以及 (如果適用) 哪些 ActiveView 或 AA 應該與此觸發相關聯。這些規則會決定管理伺服器如何套用您的觸發。

您也可以為您的觸發指定復原程序檔或可執行檔。**復原程序檔**可讓您在操作失敗時復原您的變更。

DRA 支援 VBScript 和 PowerShell 程序檔。

5.2.1 管理伺服器如何自動化程序

除了 ActiveView 規則型管理以外，DRA 可讓您自動化您的現有工作流程，以及透過自動化觸發自動執行相關任務。自動化現有工作流程可以協助您簡化企業運作，同時提供更好又更快的服務。

當管理伺服器執行與您的自動化觸發相關聯的操作時，伺服器也會執行觸發程序檔或可執行檔。如果您的觸發是任務前觸發，伺服器會在執行操作之前執行程序檔或可執行檔。如果您的觸發是任務後觸發，伺服器會在執行操作之後執行程序檔或可執行檔。此程序稱為交易。**交易**代表管理伺服器所執行之每個任務或操作的完整執行週期。交易包含完成操作所需的動作，以及管理伺服器在操作失敗時應該執行的任何復原動作。

管理伺服器會在每次自動化觸發執行時，將觸發狀態輸入到稽核記錄中。這些記錄項目會記錄傳回碼、相關聯的操作、執行的物件以及觸發程序檔是否成功。

警告： 自動化觸發是使用管理伺服器服務帳戶來執行的。因為服務帳戶具有管理員許可，所以規則和自動化觸發具有所有企業資料的完整存取權。若要定義自動化觸發，您必須擁有適當的權限，例如內建「管理規則和自動化觸發」角色中所包含的權限。這些自動化觸發會在服務帳戶安全性內容內執行。因此，與內建「管理規則和自動化觸發」角色相關聯的 AA 可以取得比您預期還要多的權限。

5.2.2 導入自動化觸發

若要執行自動化觸發，您必須先撰寫觸發程序檔或可執行檔，並且擁有適當的能力，例如內建「管理規則和自動化觸發」角色中所包含的權限。

若要成功執行自定觸發，您必須撰寫程序檔，在特定操作 (管理任務) 期間執行。您可以指定 DRA 在操作執行之前 (任務前) 或之後 (任務後) 套用觸發。在觸發程序檔中，您可以定義每當觸發失敗時顯示的錯誤訊息。您也可以透過「建立自動化觸發精靈」指定預設錯誤訊息。

如需關於撰寫自定觸發、檢視管理操作的清單，或使用引數陣列的詳細資訊，請參閱 *SDK*。

附註：

- 在讓自定自動化觸發與 AA 和 ActiveView 產生關聯之前，請先確定 AA 已指定給該 ActiveView。
- 如果自定規則程序檔或可執行檔的路徑包含空格，請在路徑前後指定引號 (")。

若要執行自動化觸發：

1. 撰寫觸發程序檔或可執行檔。
2. 使用已獲得指定管理的網域中內建**管理規則和自動化觸發**角色的帳戶，登入 DRA 用戶端電腦。
3. 啟動「委託和組態」主控台。
4. 連接至主要管理伺服器。
5. 在左窗格中，展開**規則和自動化管理**。
6. 按一下**自動化觸發**。
7. 在「任務」功能表上，按一下**新增觸發**。
8. 在每個精靈視窗上，指定適當的值，然後按**下一步**。例如，您可以讓此新觸發與特定 ActiveView 產生關聯，讓 DRA 在 AA 管理 ActiveView 所包含的物件時套用此觸發。
9. 檢閱摘要，然後按一下**完成**。

5.3 自動化工作流程

使用自動化工作流程，您可以藉由建立自定工作流程表單 (會在工作流程執行時執行，或是在自動化工作流程伺服器中所建立的具名工作流程事件觸發時執行)，來自動化 IT 程序。當您建立工作流程表單時，您定義可以檢視表單的「管理員」群組。表單提交或工作流程程序執行，是取決於當建立工作流程表單時委託給所包含群組的權限。

工作流程表單在建立或修改之後會儲存至Web伺服器。登入至此伺服器Web主控台的助理管理員，會根據您設定表單的方式，具有表單的存取。表單一般來說可供具有 Web 伺服器身分證明的所有使用者使用。您藉由新增「助理管理員」群組然後對其它使用者隱藏表單，來限制特定表單的存取。提交表單的能力需要下列其中一個權限：

- 建立工作流程事件和修改所有內容
- 啟動工作流程

啟動工作流程表單： 工作流程是在自動化工作流程伺服器中建立，必須透過Web主控台與DRA整合。若要儲存新表單，您必須在表單內容中設定**啟動特定工作流程**或**依事件觸發工作流程**選項。關於這些選項的詳細資訊提供如下：

- **啟動特定工作流程：** 此選項會列出在DRA之工作流程伺服器生產中的所有可用工作流程。若要讓工作流程填入此清單，工作流程必須建立在自動化工作流程伺服器的 DRA_Workflows 資料夾中。
- **依事件觸發工作流程：** 此選項是用於以預先定義的觸發來執行工作流程。具有觸發的工作流程也會建立在自動化工作流程伺服器中。

附註： 只有以「啟動特定工作流程」設定的工作流程表單將具有執行歷程，可以在**管理**>**要求**下方的主要搜尋窗格中查詢。

您可以修改現有表單或建立新表單。若要建立新工作流程表單或修改現有表單，請導覽至**自定**>**工作流程**。

當您建立新表單時，遵循以下基本步驟：

1. 提交表單時設定要執行*指定工作流程*的表單，或由預先定義的*具名事件*觸發時設定要執行的表單。
2. 選擇包含在工作流程程序中的「助理管理員」群組，然後啟用「一般」索引標籤中的**表單已隱藏**選項，以限制這些使用者的表單存取。
3. 將任何必要內容欄位或額外內容頁面新增至表單。
4. 如果適用，建立自訂處理程式以進一步定義工作流程程序以及其執行方式。

   附註： 在新工作流程表單初始儲存之前，不會針對表單公開自訂處理程式選項。您在**表單內容**中存取、建立及修改自訂處理程式。

如需關於自定工作流程表單的詳細資訊，請參閱自定工作流程表單。

6 稽核與報告

稽核使用者動作是安全性執行最重要的層面。為了讓您檢閱及報告助理管理員 (AA) 動作，DRA 會在管理伺服器電腦上的記錄歸檔中，記錄所有使用者操作。DRA 提供清楚且全面的報告，其中包含稽核事件前後的值，讓您可以確實看到變更的項目。

6.1 活動稽核

事件記錄中的稽核活動可以協助您隔離、診斷及解決您環境中的問題。本節提供的資訊可協助您啟用及瞭解事件記錄，以及如何與記錄歸檔搭配運作。

6.1.1 原生 Windows 事件記錄

為了讓您檢閱及報告助理管理員動作，DRA 會在管理伺服器電腦上的記錄歸檔中，記錄所有使用者操作。使用者操作包括變更定義的所有嘗試，例如更新使用者帳戶、刪除群組或重新定義 ActiveView。DRA 也會記錄特定內部操作，例如管理伺服器初始化和相關伺服器資訊。除了記錄這些稽核事件之外，DRA 也會記錄事件的前後值，讓您可以確實看到變更的項目。

DRA 會使用 **NetIQLogArchiveData** 資料夾 (稱為**記錄歸檔**) 以安全地儲存歸檔記錄資料。DRA 會在一段時間之後歸檔記錄，然後透過稱為清理的程序刪除較舊的資料，為較新的資料騰出空間。

DRA 會使用儲存在記錄歸檔中的稽核事件來顯示「活動詳細資料」報告，例如顯示在指定時間期間已對物件進行哪些變更。您也可以設定 DRA 從這些記錄歸檔檔案將資訊輸出到 SQL Server 資料庫，NetIQ Reporting Center 會用來顯示「管理」報告。

DRA 一律會將稽核事件寫入至記錄歸檔。您也可以啟用或停用讓 DRA 將事件寫入至 Windows 事件記錄。

針對 DRA 啟用及停用 Windows 事件記錄稽核

當您安裝 DRA 時，稽核事件預設不會記錄在 Windows 事件記錄中。您可以藉由修改登錄機碼來啟用此類型的記錄。

警告： 編輯您的 Windows 登錄時請小心謹慎。如果您的登錄中有錯誤，您的電腦可能會變得無法運作。如果發生錯誤，您可以將登錄還原至您上次成功啟動電腦時的狀態。如需詳細資訊，請參閱 Windows 登錄編輯器的說明。

若要啟用事件稽核：

1. 按一下**「開始」>「執行」**。
2. 在**開啟**欄位中輸入 regedit，然後按一下**確定**。
3. 展開下列登錄機碼：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\。
4. 按一下**編輯 > 新增 > DWORD 值**。
5. 輸入 IsNTAuditEnabled 作為機碼名稱。

6 按一下**編輯 > 修改**。

7 在**值資料**欄位中輸入 1，然後按一下**確定**。

8 關閉登錄編輯器。

若要停用事件稽核：

1 按一下**「開始」>「執行」**。

2 在**開啟**欄位中輸入 regedit，然後按一下**確定**。

3 展開下列登錄機碼：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\。

4 選取 IsNTAuditEnabled 機碼。

5 按一下**編輯 > 修改**。

6 在**值資料**欄位中輸入 0，然後按一下**確定**。

7 關閉登錄編輯器。

確定稽核完整性

為了確定所有使用者動作都已稽核，DRA 會在產品無法驗證記錄活動時，提供替代記錄方法。當您安裝 DRA 時，AuditFailsFilePath 機碼和路徑會新增至您的登錄，以確保下列動作：

- 如果DRA偵測到稽核事件不再記錄在記錄歸檔中，DRA會在管理伺服器的本機檔案中記錄稽核事件。
- 如果 DRA 無法將稽核事件寫入至本機檔案，DRA 會將稽核事件寫入至 Windows 事件記錄。
- 如果 DRA 無法將稽核事件寫入至 Windows 事件記錄，產品會將稽核事件寫入至 DRA 記錄。
- 如果 DRA 偵測到未記錄稽核事件，它會封鎖進一步的使用者操作。

若要在記錄歸檔無法使用時啟用寫入操作，您也必須為 AllowOperationsOnAuditFailure 機碼設定登錄機碼值。

警告： 編輯您的 Windows 登錄時請小心謹慎。如果您的登錄中有錯誤，您的電腦可能會變得無法運作。如果發生錯誤，您可以將登錄還原至您上次成功啟動電腦時的狀態。如需詳細資訊，請參閱 Windows 登錄編輯器的說明。

若要啟用寫入操作：

1 按一下**「開始」>「執行」**。

2 在**開啟**欄位中輸入 regedit，然後按一下**確定**。

3 展開下列登錄機碼：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\。

4 按一下**編輯 > 新增 > DWORD 值**。

5 輸入 AllowOperationsOnAuditFailure 作為機碼名稱。

6 按一下**編輯 > 修改**。

7 在**值資料**欄位中輸入 736458265。

8 在**基本**欄位中選取**十進位**，然後按一下**確定**。

9 關閉登錄編輯器。

6.1.2 瞭解記錄歸檔

DRA會在管理伺服器的記錄歸檔中記錄使用者活動資料。DRA會建立每日記錄歸檔分割區，以儲存當天收集及標準化的資料。DRA會使用管理伺服器上本機時間的日期(*YYYYMMDD*)，作為每日記錄歸檔分割區的命名慣例。

如果您已啟用「管理包告收集器」，DRA會將記錄歸檔資料輸出至SQL Server資料庫，作為DRA管理報告的來源。

DRA 一開始預設會將記錄資料無限期保留在記錄歸檔中。記錄歸檔大小會達到大小上限，這個上限是在安裝時根據可用硬碟空間所決定的。當記錄歸檔超過此大小上限時，系統就不會儲存新的稽核事件。您可以針對資料保留設定時間限制，DRA 會透過稱為清理的程序移除最舊的資料，為較新的資料騰出空間。請在啟用清理之前，確定已準備好備份策略。您可以使用「記錄歸檔組態」公用程式來設定記錄歸檔保留期間。如需詳細資訊，請參閱 修改記錄歸檔清理設定。

使用記錄歸檔檢視器公用程式

您可以使用「記錄歸檔檢視器」公用程式來檢視儲存在記錄歸檔檔案中的資料。您可以選擇與 DRA 一併安裝的 NetIQ DRA Log Archive Resource Kit (LARK)，提供「記錄歸檔檢視器」公用程式。如需詳細資訊，請參閱 NetIQ DRA Log Archive Resource Kit 技術參考。

備份記錄歸檔檔案

記錄歸檔檔案是記錄區塊的集合。因為記錄歸檔檔案是位於實體資料庫外部的壓縮二進位檔案，所以您不需要使用 Microsoft SQL Server Management Studio 來備份記錄歸檔。如果您已準備好自動化檔案備份系統，您的記錄歸檔檔案就會像其它檔案一樣自動備份。

規劃備份策略時請記住下列最佳實務：

- 每天都會建立單一分割區，其中包含當天的事件資料。當您啟用清理時，「記錄歸檔服務」預設每 90 天會自動清理這些分割區中的資料。備份策略應該將清理排程納入考量以決定備份的頻率。當清理記錄歸檔分割區時，DRA 會刪除二進位檔案。您無法擷取已清理的資料。您必須從備份還原已清理的資料。如需詳細資訊，請參閱 修改記錄歸檔清理設定。
- 您應該只在分割區關閉之後才進行備份。在正常狀況下，分割區會在隔天午夜的 2 小時內關閉。
- 將分割區資料夾及其所有子資料夾視為一個單位來進行備份及還原。在進行分割區備份時備份 VolumeInfo.xml 檔案。
- 如果您想要還原報告的記錄歸檔分割區，請確定已保留備份的記錄歸檔或者可以還原為其原始格式。
- 當設定您的程序以備份記錄歸檔檔案時，NetIQ 建議您同時排除位於主要記錄歸檔資料夾中的 index_data 和 CubeExport 子資料夾。這些子資料夾包含暫存資料，不應該進行備份。

修改記錄歸檔清理設定

當您安裝 DRA 時，記錄歸檔清理依預設為停用。當您為您的記錄歸檔檔案建立定期備份程序時，應該啟用記錄歸檔清理以節省磁碟空間。您使用「記錄歸檔組態」公用程式來修改記錄歸檔分割區清理前的天數。

若要變更記錄歸檔分割區在進行清理之前的天數：

1. 請使用「本機管理員」群組成員的帳戶登入管理伺服器。
2. 在「NetIQ Security Manager > 組態」程式群組中啟動**記錄歸檔組態**。

3 按一下**記錄歸檔伺服器設定**。

4 *如果您想要啟用分割區清理*，請將**分割區清理已啟用**欄位的值設為 True。

5 在**清理前的天數**欄位中，輸入您想要在清理前保留記錄歸檔分割區的天數。

6 按一下「**套用**」。

7 按一下「**是**」。

8 按一下「**關閉**」。

9 找到<*LogArchiveData 的路徑*>\<*分割區名稱*> 資料夾，然後

如果值為	
已選取	按一下確認訊息上的**是**以重新啟動 NetIQ Security Manager 記錄歸檔服務。 **附註：** 如果您修改任何記錄歸檔設定，則必須重新啟動記錄歸檔服務才能讓變更生效。
未勾選	按一下確認訊息上的**否**。請參閱若要啟用 DRA 記錄歸檔伺服器以清理未歸檔的資料：。

如果未勾選指定分割區內檔案或資料夾上的「File is ready for archiving」屬性，您必須編輯 CONFIG檔案以啟用記錄歸檔清理。若要瞭解為何要或不要勾選此屬性，請參閱**額外資訊**一節，位於您要如何為 DRA 記錄歸檔資料設定資料保留期間？知識庫文章。

若要啟用 DRA 記錄歸檔伺服器以清理未歸檔的資料：

1 以本機管理員群組成員的身分登入每個 DRA 伺服器視窗主控台本機。

2 使用文字編輯器開啟 C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config 檔案，並且找出 <Property name="GroomUnarchivedData" value="false" /> 行。

3 將 "false" 變更為 "true" 並且儲存檔案。

4 重新啟動 NetIQ DRA 記錄歸檔服務。

附註： 如果您修改任何記錄歸檔設定，則必須重新啟動記錄歸檔服務才能讓變更生效。

6.2 報告

本節提供瞭解及啟用 DRA 報告、報告資料收集、ActiveView 分析器收集和報告以及存取內建報告的相關資訊。

DRA 會停用您授權不支援的功能和報告。您也必須擁有執行及檢視報告的適當權限。因此，您可能沒有某些報告的存取權。

一旦您透過ARM主控台和「委託和組態」主控台安裝DRA，即可使用「活動詳細資料」報告，提供網路變更的最新詳細資料。

- 第 6.2.1 節「管理資料收集以進行報告」(第 101 頁)
- 第 6.2.2 節「內建報告」(第 102 頁)

6.2.1 管理資料收集以進行報告

DRA 報告提供兩個產生報告的方法，可讓您查看環境中最新的變更，以及收集和檢閱網域中的使用者帳戶、群組及資源定義。

活動詳細資料報告

透過 ARM 主控台和「委託和組態」主控台存取，這些報告提供您網域中物件的即時變更資訊。

DRA 管理報告

透過 NetIQ Reporting Center (Reporting Center) 存取，這些報告提供您管理的網域中物件的活動、組態及摘要資訊。某些報告提供資料的圖形表示。

例如，您可以使用「活動詳細資料」報告，檢視指定時間期間對物件所做之變更的清單。您也可以使用「管理」報告檢視圖表，該圖表顯示指定時間期間每個管理的網域中的事件數。報告也可讓您檢視 DRA 安全性模型的相關詳細資料，例如 ActiveView 和 AA 群組定義。

DRA 管理報告可以安裝及設定為選擇性功能，並且在 Reporting Center 中檢視。當您啟用及設定資料收集時，DRA 會收集稽核事件的相關資訊，並且以您定義的排程，將該資訊輸出至 SQL Server 資料庫。當您連接至 Reporting Center 中的此資料庫時，您可以存取超過 60 個內建報告：

- 活動報告，顯示誰在何時做了什麼
- 組態報告，顯示 AD 或 DRA 在指定時間點的狀態
- 摘要報告，顯示活動量

如需關於設定管理報告之資料收集的詳細資訊，請參閱Reporting Configuration (報告組態)。

檢視收集器狀態

您可以在「收集器狀態」索引標籤上檢視每個資料收集器的詳細資料。

若要檢視收集器的狀態：

1. 展開**組態管理**，然後按一下**更新報告服務組態**。
2. 在「收集器狀態」索引標籤上，按一下每個項目以檢視資料收集的額外資訊，例如上次收集資料的時機以及上次資料收集是否成功。
3. 如果您在「伺服器」清單中未看到任何資料，請按一下**重新整理**。

啟用報告和資料收集

安裝 DRA 報告元件之後，啟用及設定報告資料收集以存取 Reporting Center 報告。

若要啟用報告和資料收集：

1. 導覽至**組態管理**>**更新報告服務組態**。
2. 在 SQL Server 索引標籤上，選取**啟用 DRA 報告支援**。
3. 按一下「伺服器名稱」欄位中的**瀏覽**，然後選取安裝 SQL Server 所在的電腦。
4. 在「身分證明」索引標籤上，指定要用於 SQL Server 互動的適當身分證明。
5. 如果這是可用於建立資料庫及初始化綱要的相同帳戶，請選取使用上述身分證明以建立資料庫及初始化資料庫綱要核取方塊。

6 如果您想要指定不同的帳戶來建立資料庫，請在「管理員身分證明」索引標籤上指定使用者帳戶和密碼。

7 按一下**「確定」**。

如需關於設定特定收集器的詳細資訊，請參閱Reporting Configuration (報告組態)。

6.2.2 內建報告

內建報告可讓您對物件變更、物件清單及物件詳細資料產生報告。參考本節中的主題以深入瞭解如何存取這些報告。

報告物件變更

您可以藉由產生「活動詳細資料」報告，檢視網域中物件的即時變更資訊。例如，您可以檢視指定時間期間對物件所做之變更的清單。您也可以輸出及列印「活動詳細資料」報告。

若要報告物件變更：

1 尋找符合您的準則的物件。

2 以滑鼠右鍵按一下物件，然後選取**報告 > 對 objectName 所做的變更**或**報告 > objectName 所做的變更**。

3 選取開始和結束日期以指定您想要檢視的變更。

4 *如果您想要變更顯示的列數*，請在預設值 250 上面輸入值。

附註： 顯示的列數會套用至您的環境中的每個管理伺服器。如果您在報告中包含 3 個管理伺服器，並且使用顯示 250 列的預設值，則在報告中最多可以顯示 750 列。

---

5 *如果您想要在報告中僅包含特定管理伺服器*，請選取**將查詢限制為這些DRA伺服器**，然後輸入您想要報告包含的伺服器名稱。以逗號分隔多個伺服器名稱。

6 按一下**「確定」**。

報告物件清單

您可以從物件清單輸出或列印資料。您可以使用此功能快速且輕易地報告及散佈您受管理物件的一般資訊。

當您輸出物件清單時可以指定檔案位置、名稱及格式。DRA支援HTML、CSV及XML格式，因此您可以將此資訊輸出至資料庫應用程式或將清單結果張貼至網頁

附註： 您也可以選取清單中的多個項目，然後將這些項目複製到文字應用程式，例如「記事本」。

若要報告物件清單：

1 尋找符合您的準則的物件。

2 若要輸出此物件清單，請按一下「檔案」功能表上的**輸出清單**。

3 若要列印此物件清單，請按一下「檔案」功能表上的**列印清單**。

4 指定適當資訊以儲存或列印此清單。

報告物件詳細資料

您可以從列出物件屬性 (例如群組成員資格) 的詳細資料索引標籤，輸出或列印資料。您可以使用此功能快速且輕易地報告及散佈特定物件經常需要的詳細資料。

當您輸出物件詳細資料索引標籤時，您可以指定檔案位置、名稱及格式。DRA支援HTML、CSV及XML格式，因此您可以將此資訊輸出至資料庫應用程式或將清單結果張貼至網頁。

若要報告物件詳細資料：

1. 尋找符合您的準則的物件。
2. 在「檢視」功能表上，按一下**詳細資料**。
3. 在詳細資料窗格中，選取適當的索引標籤。
4. 若要輸出這些物件詳細資料，請按一下「檔案」功能表上的**輸出詳細資料清單**。
5. 若要列印這些物件詳細資料，請按一下「檔案」功能表上的**列印詳細資料清單**。
6. 指定適當資訊以儲存或列印此清單。

7 其他 功能

DRA 中的暫時群組指定、動態群組、事件戳記及 BitLocker 復原密碼和額外功能，您可以在您的企業環境中採用。

7.1 暫時群組指定

DRA 可讓您建立暫時群組指定，為授權使用者提供資源的暫時存取。助理管理員可以使用暫時群組指定，在特定時間期間將使用者指定給目標群組。在時間期間結束時，DRA 會自動從群組移除使用者。

「管理暫時群組指定」角色會授與 AA 可以建立及管理暫時群組指定的權限。

使用下列權限來委託暫時群組指定的建立和管理：

- 建立暫時群組指定
- 檢視暫時群組指定
- 刪除/修改暫時群組指定
- 將物件新增至群組
- 從群組移除物件

目標群組和目標使用者也必須在相同 ActiveView 中。

附註：

- 助理管理員只能在主要管理伺服器上建立、修改及刪除暫時群組指定。它們無法在次要管理伺服器上管理暫時群組指定。
- DRA 會在 MMS 複寫期間，從主要管理伺服器將暫時群組指定複寫至次要管理伺服器。
- 您無法為已經是目標群組成員的使用者建立暫時群組指定。如果您嘗試為已經是目標群組成員的使用者建立暫時群組指定，DRA 會顯示警告訊息，而且不會讓您為該使用者建立暫時群組指定。
- 如果您為不是目標群組成員的使用者建立暫時群組指定，DRA 會在暫時群組指定過期時從群組移除使用者。

如需建立及使用暫時群組指定的詳細資訊，請參閱《*使用者指南*》。

7.2 DRA 動態群組

動態群組是一個其成員資格變更根據您在群組內容中設定之已定義準則組的群組。您可以讓任何群組成為動態的，或是從已設定動態過濾器的任何群組移除動態過濾器。此功能也提供將群組成員新增至靜態清單或排除清單的能力。這些清單中的群組成員不會受到動態準則的影響。

如果您將動態群組還原回一般群組，「靜態成員清單」中的任何成員會新增至群組成員資格，且會忽略排除的成員和動態過濾器。您可以讓現有群組成為動態，或者在「委託和組態」主控台與 Web 主控台中建立新的動態群組。

若要讓群組成為動態：

1. 在適當的主控台中找到群組。
   - 委託和組態：移至**我的所有受管理物件**>**立即尋找**。

     附註： 若要啟用「查詢產生器」，請按一下**瀏覽**然後選取網域、容器或 OU。

   - Web 主控台：移至**管理**>**搜尋**。
2. 開啟群組的「內容」，然後在「動態成員過濾器」索引標籤中選取**讓群組成為動態**。
3. 新增想要的 LDAP 和虛擬屬性以過濾群組成員資格。
4. 將任何想要的靜態或排除的成員新增至動態群組，然後套用您的變更。

若要建立新的動態群組：

- **委託和組態：**以滑鼠右鍵按一下「我的所有受管理物件」中的網域或子節點，然後選取**新增**>**動態群組**。
- **Web 主控台：**移至**管理**>**建立**>**新增動態群組**。

7.3 事件戳記的運作方式

當您為物件類型設定屬性，且DRA執行其中一個受支援的操作時，該屬性會以DRA特定資訊進行更新(戳記)，包括誰執行操作。這樣會導致 AD 針對該屬性變更產生一個稽核事件。

舉例來說，假設您選取 extensionAttribute1 屬性作為您的使用者屬性，且您已設定 AD DS 稽核。每當 AA 更新使用者時，DRA 將會以「事件戳記」資料來更新 extensionAttribute1 屬性。這表示除了 AA 更新之每個屬性的 AD DS 事件以外 (例如，描述和名稱等)，extensionAttribute1 屬性還有額外的 AD DS 事件。

這些事件都包含「關連 ID」，對於更新使用者時變更的每個已變更屬性都相同。這就是應用程式讓「事件戳記」資料與更新的其它屬性產生關聯的方式。

7.3.1 AD DS 事件

每當 DRA 執行受支援的操作時，您將會在 Windows 安全性事件記錄檔中看到諸如此類的事件。

LDAP 顯示名稱：	**extensionAttribute1**
語法 (OID)：2.5.5.12	2.5.5.12
值：	<dra-event **user**="DRDOM300\drauseradmin" **sid**="S-1-5-21-53918190-1560392134-2889063332-1914" **tid**="E0E257E6B4D24744A9B0FE3F86EC7038" **SubjectUserSid**="S-1-5-21-4224976940-2944197837-1672139851-500" **ObjectDN**="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/>+a+02ROO+bJbhyPbR4leJpKWCGTp/KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=

事件值包含兩個部分。第一個部分是 XML 字串，其中包含「事件戳記」資料。第二個部分是資料的簽名，可用來驗證資料是否確實是由 DRA 產生。若要驗證簽名，應用程式必須具有簽名的公用金鑰。

XML 字串包含下列資訊：

使用者	執行操作的助理管理員
Sid	執行操作之助理管理員的 SID
Tid	DRA 會稽核交易 ID 以確定每個事件都是唯一的
SubjectUserSid	實際更新 AD 之 DRA 服務帳戶或存取帳戶的 SID
ObjectDN	已修改之物件的可辨識名稱

7.3.2 支援操作

使用者	◆ 建立 ◆ 重新命名 ◆ 修改 ◆ 複製品
群組	◆ 建立 ◆ 重新命名 ◆ 修改 ◆ 複製品
聯絡人	◆ 建立 ◆ 重新命名 ◆ 修改 ◆ 複製品
電腦	◆ 建立 ◆ 啟用 ◆ 停用 ◆ 重新命名 ◆ 修改
組織單位	◆ 建立 ◆ 重新命名 ◆ 複製品

7.4 BitLocker 復原密碼

Microsoft BitLocker 會將其復原密碼儲存在 Active Directory 中。使用 DRA BitLocker 復原功能，您可以將能力委託給助理管理員，以尋找及復原使用者遺失的 BitLocker 密碼。

重要： 在使用 BitLocker 復原密碼功能之前，請確定您的電腦已指定至網域且 BitLocker 已開啟。

7.4.1 檢視及複製 BitLocker 復原密碼

如果電腦的 BitLocker 密碼遺失，可以使用 Active Directory 中電腦內容的「復原密碼」金鑰來重設。複製密碼金鑰並且提供給使用者。

若要檢視及複製復原密碼：

1. 啟動**委託和組態**主控台，然後展開樹狀結構檢視結構。
2. 在**帳戶和資源管理**節點中，導覽至**我的所有受管理物件 > 網域 > 電腦**。
3. 在電腦清單中，以滑鼠右鍵按一下必要的電腦，然後選取**內容**。
4. 按一下 **BitLocker 復原密碼**索引標籤以檢視 BitLocker 復原密碼。
5. 以滑鼠右鍵按一下 BitLocker 復原密碼，按一下**複製**，然後將文字貼上至必要的文字檔或試算表。

7.4.2 尋找復原密碼

如果電腦的名稱已變更，必須使用「密碼 ID」的前 8 個字元在網域中搜尋「復原密碼」。

若要使用「密碼 ID」尋找復原密碼：

1. 啟動**委託和組態**主控台，然後展開樹狀結構檢視結構。
2. 在**帳戶和資源管理**節點中，導覽至**我的所有受管理物件**，以滑鼠右鍵按一下**管理的網域**，然後按一下**尋找 BitLocker 復原密碼**。

   若要尋找復原密碼的前 8 個字元，請參閱檢視及複製 BitLocker 復原密碼。
3. 在**尋找 BitLocker 復原密碼**頁面中，將複製的字元貼上到搜尋欄位，然後按一下**搜尋**。

7.5 ActiveView 分析器

ActiveView 分析器可協助您診斷 ActiveView 問題。例如，您可以檢查 ActiveView 處理的異常，包括在操作執行時很長的處理時間或未使用的 ActiveView 處理。ActiveView 分析器也會簡化尋找重複的 ActiveView。

在執行資料收集及檢視報告之後，您可能會發現必須修改 ActiveView 規則。

7.5.1 啟動 ActiveView 資料收集

使用 ActiveView 分析器，您可以在 ActiveView 上從助理管理員 (AA) 在上面所執行的動作收集資料。然後可以在 Analyzer 報告中檢視此資料。若要收集資料，您必須指定 AA 收集資料然後啟動 ActiveView 收集。

附註： 您想要其收集資料的助理管理員，必須連接到 Analyzer 執行所在的相同 DRA 伺服器。

若要啟動 ActiveView 收集：

1. 啟動 Web 主控台，並且以管理員身分證明登入。
2. 導覽至**管理員**> **ActiveView 分析器**。

3 在 ActiveView 分析器頁面中，指定下列項目：

3a **助理管理員：** 使用「搜尋」功能來尋找您想要其收集資料的助理管理員，並且新增。

3b **檢視內容：** (選擇性) 使用「檢視內容」功能，在啟動收集之前檢視或修改 AA 的內容。

3c **收集期間：** 指定收集分析器資料所需的總時數。超過指定時間之後，資料收集就會停止，並且會在 Mongo 資料庫中建立索引。

4 按一下**開始收集**以收集 ActiveView 資料。

5 (選擇性) 按一下**停止收集**以停止錄製助理管理員在 ActiveView 上的操作。系統會在 Mongo 資料庫中建立索引。

您可以在排程期間結束之前手動停止資料收集，而且仍然可以產生報告。

重要： 如果您停止收集並且變更助理管理員，或重新啟動相同助理管理員的資料收集，ActiveView 分析器會清除 Mongo 資料庫中的現有資料。您在資料庫中一次只能有一個助理管理員的 Analyzer 資料。

7.5.2 產生 Analyzer 報告

在產生分析器報告之前，請確定您已停止收集資料，並且可在 Mongo 資料庫中取得索引。

若要產生分析器報告：

1 導覽至**管理員**> **ActiveView 分析器**。

2 在 ActiveView 分析器頁面中會顯示助理管理員所執行操作的清單，且您可以從下列項目中選擇：

- **執行的操作：** 選取您要收集其分析器資料的操作。
- **時間最長的操作：** 選取您要檢視多少個執行時間最長的操作。

3 按一下**產生報告**以產生具有 ActiveView 操作詳細資料的分析報告，以納入相符項目、不相符項目和期間。

您可以使用報告來分析哪些規則耗費更多時間執行操作，然後決定是否應該修改任何規則，或是從個別的 ActiveView 中將其刪除。

7.5.3 清除分析的資料

「清除」動作可協助您藉由刪除重複和未使用的資料，以釋放 Mongo 資料庫中的空間。

若要從 Mongo 資料庫清除所有現有的 ActiveView 分析資料，請按一下**清除資料**。

7.6 資源回收筒

您可以針對每個 Microsoft Windows 網域或那些網域內的物件來啟用或停用資源回收筒，以控制您整個企業的帳戶管理。如果您啟用資源回收筒然後刪除使用者帳戶、群組、動態通訊群組、動態群組、資源信箱、聯絡人或電腦帳戶，則管理伺服器會停用選取的帳戶，並且將其移至資源回收筒容器。一旦 DRA 將帳戶移至資源回收筒，帳戶就不會在它所屬的 ActiveView 中顯示。如果您在停用資源回收筒時刪除使用者帳戶、群組、聯絡人或電腦帳戶，則管理伺服器會永久刪除選取的帳戶。您可以停用其中包含先前已刪除帳戶的資源回收筒。但是，一旦停用資源回收筒，就再也無法在「資源回收筒」節點中取得這些帳戶。

7.6.1 指定資源回收筒權限

若要允許助理管理員從「我的所有受管理物件」節點以及「資源回收筒」永久刪除帳戶，請從下列清單指定相關權限：

- 永久刪除使用者帳戶
- 永久刪除群組
- 永久刪除電腦
- 永久刪除聯絡人
- 永久刪除動態通訊群組
- 永久刪除動態群組
- 永久刪除資源信箱

如果多個管理伺服器管理相同 Microsoft Windows 網域中的不同子樹狀結構，則無論管理該帳戶的管理伺服器為何，您皆可使用資源回收筒來檢視此網域中任何已刪除的帳戶。

7.6.2 使用資源回收筒

使用資源回收筒來永久刪除帳戶、還原帳戶或檢視已刪除帳戶的內容。您也可以搜尋特定帳戶，以及追蹤刪除的帳戶已在資源回收筒中多少天。「資源回收筒」索引標籤也會包含在所選取網域的「內容」視窗中。您可以從此索引標籤，針對整個網域或特定物件停用或啟用資源回收筒，以及排程資源回收筒清除。

使用**全部還原**或**清空資源回收筒**選項，以快速且輕易地還原或刪除這些帳戶。

當您還原帳戶時，DRA 會恢復帳戶，包括所有許可、權限委託、規則指定、群組成員資格及 ActiveView 成員資格。如果您永久刪除帳戶，DRA 會從 Active Directory 移除此帳戶。

為了確保安全的刪除帳戶，只有具有下列權限的 AA 可以從資源回收筒永久刪除帳戶：

- 永久刪除使用者帳戶
- 從資源回收筒刪除使用者
- 永久刪除群組帳戶
- 從資源回收筒刪除群組
- 永久刪除電腦帳戶
- 從資源回收筒刪除電腦
- 永久刪除聯絡人帳戶
- 從資源回收筒刪除聯絡人
- 永久刪除動態通訊群組
- 從資源回收筒刪除動態通訊群組
- 永久刪除動態群組
- 從資源回收筒刪除動態群組
- 永久刪除資源信箱
- 從資源回收筒刪除資源信箱
- 檢視資源回收筒物件

若要從資源回收筒還原帳戶，AA 必須在包含帳戶的 OU 中具有下列權限：

- 從資源回收筒還原使用者
- 從資源回收筒還原群組
- 從資源回收筒還原動態通訊群組
- 從資源回收筒還原動態群組
- 從資源回收筒還原資源信箱
- 從資源回收筒還原電腦
- 從資源回收筒還原聯絡人
- 檢視資源回收筒物件

附註：

- 如果您將 AA帳戶刪除到資源回收筒，DRA 會繼續顯示 ActiveView 和此帳戶的角色指定。DRA 不是顯示已刪除 AA 帳戶的名稱，而是顯示安全性識別碼 (SID)。您可以在永久刪除 AA 帳戶之前，移除這些指定。
- DRA 會在您從資源回收筒刪除使用者帳戶之後，刪除主目錄。
- 如果您刪除具有 Office 365 授權的使用者，該使用者帳戶會移至資源回收筒且授權會遭到移除。如果您稍後還原使用者帳戶，Office 365 授權也會還原。

---

8 用戶端自訂

您可以自定委託和組態和ARM用戶端與Web主控台。前者需要實體或遠端存取和帳戶身分證明。後者需要伺服器 URL 和帳戶身分證明以便從網頁瀏覽器登入。

8.1 委託和組態和 ARM 用戶端

本節包含的資訊可協助您自定「委託和組態」和「帳戶和資源管理」用戶端，包括瞭解如何建立自定內容頁面、如何在 DRA 中建立可以在網路中用戶端和伺服器電腦上執行的自定工具，以及如何自定使用者介面的組態。

8.1.1 自定內容頁

您可以藉由導入自定內容，來自定及延伸「委託和組態」和ARM主控台。自定內容可讓您將專屬帳戶和 OU 內容 (例如 Active Directory 綱要延伸和虛擬屬性) 新增至特定精靈和內容視窗。這些延伸可讓您自定 DRA 以符合您的特定需求。使用「委託和組態」主控台中的「新增自定頁面」精靈，您可以快速且輕易地建立自定頁面以延伸適當的使用者介面。

如果您的AA需要獨特的能力以安全地管理自定頁面，您也可以建立及委託自定權限。例如，您可能想要將使用者帳戶管理限制為僅限自定頁面上的內容。如需詳細資訊，請參閱 導入自定權限。

自定內容頁面的運作方式

使用者介面延伸是 DRA 在適當精靈和內容視窗中顯示的自定頁面。您可以設定自定頁面，在「委託和組態」主控台和「帳戶和資源管理」主控台公開 Active Directory 屬性、綱要延伸及虛擬屬性。

當您選取任何支援的 Active Directory 屬性、綱要延伸或虛擬屬性時，您可以下列方式使用自定頁面：

- 限制 AA 管理妥善定義且受控制的內容組。此內容組可以包含*標準內容*和綱要延伸。標準內容是預設透過「帳戶和資源管理」主控台公開的 Active Directory 屬性。
- 公開由 DRA 管理之標準內容以外的 Active Directory 屬性。
- 延伸「帳戶和資源管理」主控台和「委託和組態」主控台以包含專屬內容。

您也可以設定 DRA 顯示及套用這些內容的方式。例如，您可以定義具有預設內容值的使用者介面控制項。

DRA 會將自定頁面套用至您的企業中適用的所有受管理物件。例如，如果您建立自定頁面以將 Active Directory 綱要延伸新增至「群組內容」視窗，DRA 會將此頁面上的內容套用至支援指定綱要延伸之網域中的每個受管理群組。每個自定頁面需要唯一的內容組。您無法將 Active Directory 屬性新增至一個以上的自定頁面。

您無法停用現有使用者介面中的個別視窗或索引標籤。AA 可以使用預設使用者介面或自定頁面來選取內容值。DRA 會套用內容的最新選取值。

DRA 會提供自定內容的完整稽核追蹤。DRA 會將下列資料記錄到應用程式事件記錄：

- 對自定頁面的變更

  重要： 您必須手動設定 Windows 應用程式記錄稽核。請參閱「我要如何重新啟用 DRA 以將事件寫入 DRA 8.5 及更新版本中的應用程式事件記錄？」

- 建立及刪除自定頁面
- 公開自定頁面上包含的綱要延伸、Active Directory 屬性及虛擬屬性

您也可以執行變更活動報告以監控自定內容的組態變更。

從主要管理伺服器執行及修改自定頁面。在同步期間，DRA 會跨多主機組複寫自定頁面組態。如需詳細資訊，請參閱 設定多主機組。

支援的自定頁面

您建立的每個自定頁面可讓您選取一組 Active Directory 內容、綱要延伸或虛擬屬性，並且將這些內容公開為自定索引標籤。您可以建立以下類型的自定頁面：

自定使用者頁面

可讓您在下列視窗中顯示自定索引標籤：

- 使用者內容視窗
- 建立使用者精靈
- 複製使用者精靈

自定群組頁面

可讓您在下列視窗中顯示自定索引標籤：

- 群組內容視窗
- 建立群組精靈
- 複製群組精靈

自定電腦頁面

可讓您在下列視窗中顯示自定索引標籤：

- 電腦內容視窗
- 建立電腦精靈

自定聯絡人頁面

可讓您在下列視窗中顯示自定索引標籤：

- 聯絡人內容視窗
- 建立聯絡人精靈
- 複製聯絡人精靈

自定 OU 頁面

可讓您在下列視窗中顯示自定索引標籤：

- OU 內容視窗

- 建立 OU 精靈
- 複製 OU 精靈

自定資源信箱頁面

可讓您在下列視窗中顯示自定索引標籤：

- 資源信箱內容視窗
- 建立資源信箱精靈
- 複製資源信箱精靈

自定動態通訊群組頁面

可讓您在下列視窗中顯示自定索引標籤：

- 動態通訊群組內容視窗
- 建立動態通訊群組精靈
- 複製動態通訊群組精靈

支援的自定內容控制項

當您將 Active Directory 屬性、綱要延伸或虛擬屬性新增至自定頁面時，您也會設定使用者介面控制項，AA 會使用該控制項來輸入內容值。例如，您可以下列方式指定內容值：

- 定義特定值範圍
- 設定預設內容值
- 指出內容是否為必要

您也可以設定使用者介面控制項，以顯示專屬資訊或指示。例如，如果您針對員工識別碼定義特定範圍，您可以設定文字方塊控制項標籤以顯示**指定員工識別碼 (001 到 100)**。

每個使用者介面控制項提供單一 Active Directory 屬性、綱要延伸或虛擬屬性的支援。根據內容類型來設定下列使用者介面控制項：

Active Directory 屬性的類型	**支援的使用者介面控制項**
布林值	核取方塊
日期	行事曆控制項
整數	文字方塊 (預設) 選取項目清單
字串	文字方塊 (預設) 選取項目清單 物件選擇器
多值字串	選取項目清單

使用自定頁面

您可以從「使用者介面延伸」節點建立自定頁面。一旦建立頁面，您可以新增或移除 AD 屬性內容，以及停用或刪除頁面。針對您想要設定的每個自定，建立自定頁面並且將適當權限或角色指定給 AA。當您開始使用自定頁面時，請考量下列最佳實務：

1. 為了確保 DRA 能夠辨識您的 Active Directory 屬性、綱要延伸屬性或虛擬屬性，請重新啟動每個管理伺服器上的 NetIQ 管理服務。
2. 識別您想要建立的自定頁面類型，以及您想要 AA 使用此自定頁面來管理的內容。您可以選取任何 Active Directory 屬性，包括綱要延伸屬性與現有 DRA 精靈和內容視窗中的屬性，或者您建立的任何虛擬屬性。但是，每個自定頁面需要唯一的內容組。您無法將 Active Directory 屬性新增至一個以上的自定頁面。

   自定頁面不會取代現有的使用者介面。如需詳細資訊，請參閱自定內容頁面的運作方式與支援的自定頁面。
3. 決定您要 AA 如何指定這些內容。例如，您可能想要將指定內容限制為三個可能值。您可以為每個內容定義適當的使用者介面控制項。如需詳細資訊，請參閱 支援的自定內容控制項。
4. 判斷您的 AA 是否需要專屬資訊或指示，才能成功管理這些內容。例如，判斷 Active Directory 是否需要內容值的語法，例如可辨識名稱 (DN) 或 LDAP 路徑。
5. 識別這些內容在自定頁面上顯示的順序。您可以隨時變更顯示順序。
6. 決定 DRA 應該如何使用此自定頁面。例如，您可以將使用者自定頁面新增至「新增使用者」精靈和「使用者內容」視窗。
7. 使用「助理管理員」詳細資料窗格上的「指定」索引標籤，來驗證您的 AA 是否具有正確物件組的適當權限。如果您已為此自定頁面建立自定權限，請將這些能力委託給適當的 AA。
8. 判斷您的 AA 是否需要自定權限以便管理此頁面上的內容。例如，如果您將自定頁面新增至「使用者內容」視窗，則委託*修改所有使用者內容*能力可能會給予 AA 太多權限。建立執行您的自定頁面所需的任何自定權限。如需詳細資訊，請參閱 導入自定權限。
9. 使用您對於上述步驟的答案，建立適當的自定頁面。
10. 將您執行之自定內容頁面的相關資訊，散佈給適當的 AA，例如您的服務台。

若要執行內容自定，您必須有「DRA 管理」角色中所包含的權限。如需自定頁面的詳細資訊，請參閱自定內容頁面的運作方式。

建立自定內容頁面

您可以藉由建立不同的自定頁面，來建立不同的自定內容。新的自定頁面預設為啟用。

當您建立自定頁面時，您可以將它停用。停用自定頁面會將它從使用者介面隱藏。如果您建立多個自定頁面，可能想要在自定測試及完成之前停用頁面。

附註： 電腦帳戶會從使用者帳戶繼承 Active Directory 屬性。如果您延伸 Active Directory 綱要以包含使用者帳戶的額外屬性，您可以在建立自定頁面時選取這些屬性來管理電腦帳戶。

若要建立自定內容頁面：

1. 導覽至**組態管理**>**使用者介面延伸**節點。
2. 在「任務」功能表上，按一下**新增**，然後針對您想要建立的自定頁面按一下適當功能表項目。
3. 在「一般」索引標籤上，輸入此自定頁面的名稱，然後按一下**確定**。如果您想要停用此頁面，請清除**已啟用**核取方塊。

4 針對您想要納入此自定頁面的每個內容，完成下列步驟：

4a 在「內容」索引標籤上，按一下**新增**。

4b 若要選取內容，按一下**瀏覽**。

4c 在**控制項標籤**欄位中，輸入 DRA 應該使用作為使用者介面控制項標籤的內容名稱。確定控制項標籤是使用者易記的，並且有高度描述性。您也可以包含指示、有效值範圍及語法範例。

4d 從**控制項類型**功能表選取適當的使用者介面控制項。

4e 選取您想要 DRA 在「帳戶和資源管理」主控台的哪個位置顯示此自定頁面。

4f 若要指定額外屬性 (例如長度下限或預設值)，請按一下**進階**。

4g 按一下**「確定」**。

5 若要變更 DRA 在自定頁面上顯示這些內容的順序，請選取適當內容，然後按一下**上移**或**下移**。

6 按一下**「確定」**。

修改自定內容

您可以藉由修改自定內容來變更自定頁面。

若要修改自定內容：

1 導覽至**組態管理**>**使用者介面延伸**節點。

2 在清單窗格中，選取想要的自定頁面。

3 在「任務」功能表上，按一下**內容**。

4 修改此自定頁面的適當內容和設定。

5 按一下**「確定」**。

識別使用自定頁面管理的 Active Directory 屬性

您可以快速地識別哪些 Active Directory 內容、綱要延伸或虛擬屬性是使用特定自定頁面進行管理的。

若要識別使用自定頁面管理的 Active Directory 內容：

1 導覽至**組態管理**>**使用者介面延伸**節點。

2 在清單窗格中，選取想要的自定頁面。

3 在詳細資料窗格中，按一下**內容**索引標籤。若要檢視詳細資料窗格，請按一下「檢視」功能表上的**詳細資料**。

4 若要確認 DRA 如何顯示及套用內容，請從清單選取適當的 Active Directory 屬性、綱要延伸或虛擬屬性，然後按一下**內容**圖示。

啟用、停用及刪除自定頁面

當您啟用自定頁面時，DRA 會將此自定頁面新增至相關聯的精靈和視窗。若要指定由哪些精靈和視窗顯示自定頁面，請修改自定頁面內容。

附註： 為了確保每個自定頁面公開唯一的內容組，DRA 不會啟用包含已在其它自定頁面公開之內容的自定頁面。

當您停用自定頁面時，DRA會從相關聯的精靈和視窗移除自定頁面。DRA不會刪除自定頁面。若要確保自定頁面永遠不會在使用者介面中顯示，請刪除自定頁面。

當您刪除自定頁面時，DRA 會從相關聯的精靈和視窗移除自定頁面。您無法還原已刪除的自定頁面。若要從使用者介面暫時移除自定頁面，請停用自定頁面。

若要啟用、停用或刪除自定頁面，請導覽至**組態管理**>**使用者介面延伸**節點，然後在「任務」功能表中或按一下滑鼠右鍵以選取想要的動作。

指令行介面

CLI 可讓您使用指令或批次檔案來存取及套用強大的管理產品權限。您可以使用 CLI 來發出一個指令，對多個物件執行變更。

例如，如果您需要將 200 名員工的主目錄重新定位至新伺服器，則可以使用 CLI 來輸入以下單一指令來變更全部 200 個使用者帳戶：

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE
HOMEDIR:\\HOU2\USERS\@Target()
```

此指令會指示 DRA 將 HOU_SALES 和 HOU_MIS 群組中 200 個使用者帳戶的主目錄欄位皆變更為 \\HOU2\USERS*user_id*。若要使用原生 Microsoft Windows 管理工具來完成這個任務，您需要執行最少 200 個個別動作。

附註： CLI 工具將在未來版本中遭到淘汰，因為有越來越多功能新增至 PowerShell。

8.1.2 自定工具

自定工具可用來叫用要在網路中用戶端和伺服器電腦上執行的任何應用程式，方法是選取在 DRA 中受管理的任何 Active Directory 帳戶。

DRA 支援兩種類型的自定工具：

- 啟動通用桌面公用程式 (例如 Microsoft Office) 的自定工具
- 您建立並散佈至每個 DRA 用戶端電腦的自定工具

您可以建立自定工具，從 DRA 用戶端安裝所在的所有電腦啟動防毒掃描。您也可以建立自定工具，啟動需要 DRA 定期更新程序檔的外部應用程式或工具。這些定期更新可能會是組態或商務規則中的變更。接著在定期更新之後，DRA從主要管理伺服器將自定工具複寫至次要管理伺服器和DRA用戶端電腦。

若要瞭解自定工具如何在伺服器多主機組中進行複寫，請參閱File Replication (檔案複寫)。

建立自定工具

您可以藉由關聯至選取的 Active Directory 物件或在該建立自定工具精靈中顯示的所有 Active Directory物件，以在DRA主要伺服器中建立自定工具。相同的自定工具會透過檔案複寫，複寫到MMS中的次要伺服器以及複寫到 DRA 用戶端。

新的自定工具會視需要建立功能表或子功能表，以針對 DRA 中相關聯的 Active Directory 物件叫用操作。

您可以將能力委託給助理管理員以建立及執行自定工具，以及存取及執行應用程式。

當建立自定工具時，您必須輸入參數，如下所示：

一般索引標籤

1. **名稱：**工具的任何必要客戶名稱。
2. **功能表和子功能表：**若要為新自定工具建立功能表項目，請在功能表和子功能表結構欄位中輸入功能表標題。當您建立自定工具及選取物件時，DRA 會使用您在「任務」功能表、「捷徑」功能表及 DRA 工具列中指定的功能表和子功能表結構，以顯示自定工具功能表項目。

   *範例功能表和子功能表結構：*輸入功能表項目名稱、反斜線 (\) 字元，然後輸入子功能表項目名稱。

   *具備快速鍵：*在功能表項目名稱前面輸入 & 符號 (&) 字元。

   a. 範例：SendEmail\ApproveAction ---- SendEmail 是功能表而 ApproveAction 是子功能表，其中 ApproveAction 中的第一個字母「A」是啟用的快速鍵。
3. **已啟用：**核取此方塊以啟動自訂工具。
4. **描述：**您可以新增任何必要的描述值。
5. **備註：**您可以新增自定工具的任何必要備註。

支援的物件索引標籤

選取建立的自定工具應該產生關聯的必要 AD 物件或所有 AD 物件。

目前支援的自定工具選項包括：管理的網域、容器、使用者、聯絡人、群組、電腦、組織單位及已發佈印表機。

附註： 其它新引入的物件，例如資源信箱、動態群組及 Exchange 動態群組，不支援自定工具。

應用程式設定索引標籤

應用程式的位置：您需要提供應用程式安裝所在的路徑/位置，方法是複製及貼上確切的應用程式路徑或是使用插入選項。

您也可以使用 DRA 變數、環境變數及登錄值，在「應用程式的位置」欄位中指定外部應用程式的位置。若要使用這些變數，請按一下插入，然後選取您想要使用的變數。

在您插入變數之後，輸入反斜線 (\) 字元，然後指定應用程式的剩餘路徑，包括應用程式可執行檔名稱。

範例:

- *範例 1：*若要指定自定工具將會執行之外部應用程式的位置，請選取環境變數 {%PROGRAMFILES%}，然後在「應用程式的位置」欄位中指定應用程式的剩餘路徑：{%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe

  ---

  附註： DRA 會提供 Office 安裝目錄登錄值作為範例。若要指定登錄機碼 (包含路徑作為值)，請使用下列語法：{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}

- *範例 2：*若要指定自定工具將會執行之自定程序檔案的位置，請選取 DRA 變數 {DRA_Replicated_Files_Path},，然後在「應用程式的位置」欄位中指定程序檔案的剩餘路徑：{DRA_Replicated_Files_Path}\cscript.vbs ;，其中 {DRA_Replicated_Files_Path} 是複寫的檔案路徑，或是管理伺服器中的 {DRAInstallDir}\FileTransfer\Replicate 資料夾。

附註： 在建立自定工具之前，使用檔案複寫功能，將程序檔案上傳至主要管理伺服器。檔案複寫功能會將程序檔案上傳至主要管理伺服器中的 {DRAInstallDir}\FileTransfer\Replicate 資料夾。

- *範例 3：*若要指定自定工具將會執行之 DRA 公用程式的位置，請選取 DRA 變數 {DRA_Application_Path}，然後在「應用程式的位置」欄位中指定公用程式的剩餘路徑：{DRA_Application_Path}\DRADiagnosticUtil.exe，其中 {DRA_Application_Path} 是 DRA 安裝所在的位置。
- *範例 4：*只要複製貼上應用程式的位置與具有副檔名的應用程式檔案名稱。

傳遞至應用程式的參數：若要定義傳遞至外部應用程式的參數，在「參數」中複製及貼上或輸入一或多個要傳遞至應用程式欄位的參數。DRA 會提供您可以在「參數」中用來傳遞至應用程式欄位的參數。若要使用這些參數，請按一下「插入」然後選取您想要使用的參數。提供物件內容作為參數時，請確定 AA 具有物件內容的必要讀取許可，以及執行自定工具所需的*執行自定工具*權限。

範例:

- *範例 1：*若要將群組名稱和網域名稱作為參數傳遞至外部應用程式或程序檔，請選取 Object Property Name 和 Domain Property Name 參數，並且在「傳遞至應用程式的參數」欄位中指定參數名稱："{Object.Name}" "{Domain.$McsName}"
- *範例 2：*若要傳遞應用程式「C:\Windows\SysWOW64\cmd.exe」的輸入參數】「ipconfig」，只要在該欄位中輸入 "{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}" 即可。

應用程式執行所在的目錄：這是應用程式需要在用戶端或伺服器機器中執行所在的位置。您必須傳遞應用程式應該執行所在的路徑。您也可以透過我們針對「應用程式的位置」欄位傳遞參數的相同方式，來使用「插入」選項。此索引標籤中的其它參數對於說明其使用是隱含的。

8.1.3 自定使用者介面

您可以使用數個選項來自定設定「委託和組態」主控台的方式。這些選項大部分都會提供在應用程式之不同功能窗格中隱藏、顯示或重新設定功能的能力。您也可以隱藏或顯示工具列、自定應用程式標題以及新增、移除或重新排序欄。這些自定選項都位於**檢視**功能表中。

修改主控台標題

您可以修改在「委託和組態」主控台與「帳戶和資源管理」主控台之標題列中顯示的資訊。為了方便和明確，您可以新增用來啟動主控台的使用者名稱以及連接主控台的管理伺服器。在您需要使用不同身分證明連接至多個管理伺服器的複雜環境中，此功能可協助您快速地辨別您需要使用的主控台。

若要修改主控台標題列：

1. 啟動「委託和組態」主控台。
2. 按一下**檢視>選項**。
3. 選取「視窗標題」索引標籤。
4. 指定適當的選項，然後按一下**確定**。如需詳細資訊，請按一下 **?** 圖示。

自定清單欄

您可以選取 DRA 在清單欄中顯示哪些物件內容。這個彈性功能可讓您自定使用者介面，例如搜尋結果的清單，以便更加符合管理您的企業的特定需求。例如，您可以設定欄顯示使用者登入名稱或群組類型，讓您快速且有效率地尋找及排序您需要的資料。

若要自定清單欄：

1. 選取適當的節點。例如，若要選擇在檢視受管理物件上的搜尋結果時要顯示哪些欄，請選取**我的所有受管理物件**。
2. 在「檢視」功能表上，按一下**選擇欄**。
3. 從此節點可用內容的清單中，選取您想要顯示的物件內容。
4. 若要變更欄順序，請選取欄，然後按一下**上移**或**下移**。
5. 若要指定欄寬度，請選取欄，然後在提供的欄位中輸入適當的像素。
6. 按一下**「確定」**。

8.2 Web 用戶端

在 Web 用戶端中，您可以自定物件內容、自動化工作流程表單及使用者介面品牌。當正確執行時，內容和工作流程自定會協助自動化助理管理員對於物件管理和自動化工作流程提交的任務。

8.2.1 自定內容頁

您可以依據物件類型，自定您的助理管理員在其 Active Directory 管理角色中使用的物件內容表單。這包含建立及自定新物件頁面，這些頁面是根據內建至 DRA 的物件類型。您也可以修改內建物件類型的內容。

內容物件會清楚地在 Web 主控台的「內容頁面」清單中定義，因此您可以輕易地識別哪些物件頁面是內建的、哪些內建頁面是自定的，以及哪些頁面不是內建的而且是由管理員建立的。

自定物件內容頁面

您可以藉由新增或移除頁面、修改現有頁面和欄位以及建立內容屬性的自訂處理程式，來自定物件內容表單。當您建立自訂處理程式時，它們會在內容欄位變更或管理員回應執行查詢的提示時自動執行，取決於自訂處理程式的設定方式。

「內容頁面」中的物件清單為每個物件類型提供兩個操作類型，「建立物件」和「編輯內容」。這些是您的助理管理員在Web用戶端中執行的主體操作，且您的自定可以改善管理員在管理DRA中的Active Directory 物件時的效率及體驗。

若要自定 Web 主控台中的物件內容頁面：

1. 以 DRA 管理員身分登入 Web 主控台。
2. 導覽至**自定 > 內容頁面**。
3. 在「內容頁面」清單中選取物件和操作類型 (建立或編輯)。
4. 按一下**編輯**按鈕。
5. 藉由執行下列一或多個動作，來自定物件內容，然後套用您的變更：
   - 新增新的內容頁面：**新增頁面**

- 選取內容頁面並自定頁面：
  - 重新排序頁面中的組態欄位：
  - 編輯欄位或子欄位：
  - 新增一或多個欄位： 或**新增欄位**
  - 移除一或多個欄位：
- 藉由使用程序檔、訊息方塊或查詢 (LDAP、DRA 或 REST) 來建立內容的自訂處理程式

  如需使用自訂處理程式的詳細資訊，請參閱新增自訂處理程式。

建立新的物件內容頁面

若要建立新的物件內容頁面：

1. 以 DRA 管理員身分登入 Web 主控台。
2. 導覽至**自定 > 內容頁面**。
3. 在「任務」下方按一下**建立新動作**。
4. 藉由定義物件內容的名稱、圖示、物件類型及操作組態，來建立初始物件內容。
5. 視需要自定新表單。請參閱自定物件內容頁面。

8.2.2 自定工作流程表單

工作流程表單在建立或修改時，會儲存至 Web 伺服器，並且可以在 Web 主控台的**自定**>**工作流程**頁面中存取。這些表單是用來提交在「工作流程自動化」伺服器中建立的自動化工作流程。您可以自定表單，以便在助理管理員使用表單來執行物件管理任務時進一步自動化及改善表單的可用性。

您可以新增及修改現有表單內容和自訂處理程式。在「自動化工作流程」表單中新增及自定內容的介面行為，與它在自定物件內容時的介面行為相同。請參閱以下主題以取得關於新增及修改內容、新增自訂處理程式及瞭解自動化工作流程的詳細資訊。

- 自定內容頁 (Web 用戶端)
- 新增自訂處理程式
- 自動化工作流程

新增自訂處理程式

自訂處理程式是在 DRA 中用於內容屬性以進行彼此的互動來完成工作流程任務，以及用於工作流程、內容或建立表單中的「載入和提交」自定。

內容自訂處理程式的一些範例，包括查詢其它欄位的值、更新值、切換欄位的唯讀狀態，以及根據設定的變數來顯示或隱藏欄位。

「表單載入處理程式」可讓使用者藉由典型的執行某些控制項初始化，來自定表單。「表單提交處理程式」可讓使用者執行一些驗證，並且在某些項目不正確時取消提交。

DRA 也會透過您可以從自訂處理程式建立和驗證程序中選擇的一些可選取 JavaScript (JS) 巨集，來簡化自訂處理程式的建立。

建立自訂處理程式的基本步驟：

以下步驟從預先選取的自訂處理程式頁面開始。若要進入該位置，您要透過內容欄位上的編輯按鈕 存取物件內容自訂處理程式。您要從工作流程表單上的「表單內容」存取「表單載入」和「表單提交」處理程式，或者建立物件頁面。

1 按一下適用的自訂處理程式索引標籤，並且啟用頁面 。

- 自訂處理程式
- 表單載入處理程式
- 表單提交處理程式

2 從下拉式功能表選擇自訂處理程式，然後選取執行時間。一般來說，您會使用「執行時間」的第二個或第三個選項。

附註： 您通常只需要一個自訂處理程式，但是您可以藉由在程序檔中設定流程控制項以將處理程式連結在一併，來使用一個以上的處理程式。

---

3 您需要設定您新增至頁面的 每個自訂處理程式。組態選項會因處理程式類型而異，但是所有處理程式都是從 JavaScript 執行。

您可以建立您自己的 Vanilla JavaScript 項目，或是使用內建巨集。

- **LDAP 或 REST 查詢處理程式：**
  1. 如果您希望您的查詢是根據靜態值，請定義**連線資訊**和**查詢參數**。

     如果您希望您的查詢是動態的，請在必要欄位中輸入預留位置文字。這是執行程序檔的必要項目。程序檔將會覆寫假的值。

     附註： 您也可以設定 REST 查詢的標題和 Cookie。

     ---

  2. 在「查詢前動作」中，選取巨集類型：**全域**、**查詢**或**表單欄位**。
  3. 從下拉式清單選取巨集，然後插入巨集 (**</> 插入巨集**)。
  4. 視需要插入其它巨集，然後提供需要的值以完成程序檔。

     舉例來說，在「查詢前動作」中我們會使用程序檔來驗證當提交表單時，使用者輸入的群組名稱尚未存在於 Active Directory 中。

     我們需要使用由使用者輸入的名稱來建立 LDAP 查詢。我們會使用 Field() 巨集來存取「名稱」欄位的值，並且建立查詢字串，我們隨後會使用 Filter() 巨集將該字串設為查詢過濾器。

     ```
     Filter() = '(&(objectCategory=group)(objectClass=group)(name=' + Field(name) + '))';
     ```

  5. 遵循上述範例，我們會在「查詢後動作」中檢查由查詢傳回的結果。結果是以符合查詢之物件的陣列形式傳回，因此我們只需要檢查陣列的長度是否大於 0。

     當找到相符的群組時，我們會使用 Cancel() 巨集來取消表單提交，將要顯示給使用者的選擇性訊息傳遞給巨集。

     ```
     if (QueryResults().length > 0) { Cancel('A group with that name already exists, please enter a unique name.');}
     ```

- **程序檔:** 插入自定 JavaScript 程式碼或使用巨集來建立程序檔。
- **DRA 查詢：** 針對查詢參數，定義以JSON格式表示的承載。然後以上述適用於LDAP和REST查詢的類似方式來使用巨集。

- **訊息方塊處理程式：** 在定義訊息方塊本身的內容之後，以上述適用於LDAP和REST查詢的類似方式來使用巨集，但是並非是「查詢前動作」和「查詢後動作」，而是針對「顯示動作之前」和「關閉動作之後」來撰寫巨集程序檔。

4 按一下**測試處理程式**以在儲存表單之前驗證您的程序檔。

這樣會產生「測試結果摘要」，您可以在其中檢視執行結果。

附註： 如果處理程式是依據目前的表單狀態 (例如，欄位具有值)，它就無法成功執行，因為在編輯表單時未載入任何資料。在這些情況下，處理程式需要藉由儲存自定、導覽至適當的表單然後填入必要的資料，以便在表單編輯器的外部進行測試。

8.2.3 自定使用者介面品牌

您可以使用您自己的標題和標誌影像，自定DRAWeb主控台的標題列。位置緊接在DRA產品名稱右側。因為此位置也用於最上層導覽，所以會在登入後由最上層 DRA 導覽連結隱藏。但是，瀏覽器索引標籤會繼續顯示自定標題。

若要在 DRA 中自定標題品牌：

1 以 DRA 管理員身分登入 Web 主控台。

2 導覽至**自定 > 品牌**。

3 如果您新增公司標誌，請將標誌影像儲存在 Web 伺服器上的 components\lib\img 中。

4 適當地為品牌自定頁面上的三個欄位新增必要資訊，然後儲存您的變更。

9 工具和公用程式

這些章節討論隨著 DRA 一併提供的診斷公用程式、刪除的物件公用程式、狀態檢查公用程式及資源回收筒公用程式。

9.1 診斷公用程式

「診斷公用程式」會從您的管理伺服器蒐集資訊，協助診對 DRA 的問題。使用此公用程式以將記錄檔案提供給技術支援代表。「診斷公用程式」提供精靈介面，會引導您進行設定記錄層級和收集診斷資訊。

您可以從任何管理伺服器電腦存取「診斷公用程式」。但是，您應該在遇到問題的管理伺服器上執行「診斷公用程式」。

若要存取「診斷公用程式」，請使用 DRA 管理員帳戶登入管理伺服器電腦，然後執行 Program Files (x86)\NetIQ\DRA 資料夾中的 DRADiagnosticUtil.exe。

如需使用此公用程式的詳細資訊，請聯絡技術支援。

9.2 刪除的物件公用程式

此公用程式可讓您在網域存取帳戶並非管理員時，針對特定網域啟用遞增的帳戶快取重新整理支援。如果網域存取帳戶沒有網域中「刪除的物件」容器的讀取許可，DRA 就無法執行遞增的帳戶快取重新整理。

您可以使用此公用程式來執行下列任務：

- 驗證指定的使用者帳戶或群組具有指定網域中「刪除的物件」容器的讀取許可
- 委託或移除指定使用者帳戶或群組的讀取許可
- 委託或移除使用者帳戶的同步化目錄服務資料使用者權限
- 顯示「刪除的物件」容器的安全性設定

您可以從您的管理伺服器的 Program Files (x86)\NetIQ\DRA 資料夾執行「刪除的物件公用程式」檔案 (DraDelObjsUtil.exe)。

9.2.1 刪除的物件公用程式的必要許可

若要使用此公用程式，您必須具有下列許可：

如果想要 ...	您需要此許可...
驗證帳戶許可	「刪除的物件」容器的讀取許可存取
委託「刪除的物件」容器的讀取許可	「刪除的物件」容器所在網域的管理員許可
委託同步化目錄服務資料使用者權限	「刪除的物件」容器所在網域的管理員許可
移除先前委託的許可	「刪除的物件」容器所在網域的管理員許可

顯示「刪除的物件」容器的安全性設定	「刪除的物件」容器的讀取許可存取

9.2.2 刪除的物件公用程式的語法

DRADELOBJSUTIL /DOMAIN:*DOMAINNAME* [/DC:*COMPUTERNAME*] {/DELEGATE:*ACCOUNTNAME* | /VERIFY:*ACCOUNTNAME* | /REMOVE:*ACCOUNTNAME* | /DISPLAY [/RIGHT]}

9.2.3 刪除的物件公用程式的選項

您可以指定下列選項：

/DOMAIN:*domain*	指定「刪除的物件」容器所在之網域的 NETBIOS 或 DNS 名稱。
/SERVER:*computername*	針對指定的網域指定網域控制器的名稱或 IP 位址。
/DELEGATE:*accountname*	將許可委託給指定使用者帳戶或群組。
/REMOVE:*accountname*	移除先前委託給指定使用者帳戶或群組的許可。
/VERIFY:*accountname*	驗證指定使用者帳戶或群組的許可。
/DISPLAY	顯示指定網域中「刪除的物件」容器的安全性設定
/RIGHT	確定指定使用者帳戶或群組具有同步化目錄服務資料使用者權限。您可以使用此選項來委託或驗證此權限。同步化目錄服務資料使用者權限可讓帳戶讀取 Active Directory 中的所有物件和內容。

附註：

- 如果您想要指定的使用者帳戶或群組名稱包含空格，請以引號括住帳戶名稱。例如，如果您想要指定 Houston IT 群組，請輸入「Houston IT」。
- 當指定群組時，針對該群組使用 Windows 2000 以前版本名稱。

9.2.4 刪除的物件公用程式的範例

下列範例示範通用案例的範例指令。

範例 1

若要確認 MYCOMPANY\JSmith 使用者帳戶是否具有 hou.mycompany.com 網域中「刪除的物件」容器的讀取許可，請輸入：

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

範例 2

若要將 MYCOMPANY 網域中「刪除的物件」容器的讀取許可委託給 MYCOMPANY\DraAdmins 群組，請輸入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

範例 3

若要將 MYCOMPANY 網域中「刪除的物件」容器的讀取許可和同步化目錄服務資料使用者權限委託給 MYCOMPANY\JSmith 使用者帳戶，請輸入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

範例 4

若要使用HQDC網域控制器來顯示hou.mycompany.com網域中「刪除的物件」容器的安全性設定，請輸入：

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

範例 5

若要從 MYCOMPANY\DraAdmins 群組移除 MYCOMPANY 網域中「刪除的物件」容器的讀取許可，請輸入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

9.3 狀態檢查公用程式

DRA狀態檢查公用程式是獨立的應用程式，隨附於DRA安裝套件。您可以在安裝後以及升級前後使用「狀態檢查公用程式」來確認、驗證及通知DRA伺服器、DRA網站和DRA用戶端的元件和程序的狀態。您也可以使用它來安裝或更新產品授權、在產品升級之前備份AD LDS例項、檢視檢查的描述，以及修正問題或者識別修正問題需要採取的動作，然後重新驗證。

「狀態檢查公用程式」可以在執行 NetIQAdminInstallationKit.msi 安裝程式之後，在 DRA 程式資料夾中存取。

您隨時可以藉由執行 NetIQ.DRA.HealthCheckUI.exe 檔案來執行「狀態檢查公用程式」。當應用程式開啟時，您可以選擇執行特定操作、對特定元件執行檢查，或者對所有元件執行檢查。請參閱以下項目以瞭解使用「狀態檢查公用程式」時的實用功能：

功能	使用者動作
全選或取消全選	使用「檔案」功能表選項上的工具列以**選取**或**取消選取**所有檢查項目，或選取個別核取方塊以執行特定檢查。
執行選取的檢查	使用「檔案」功能表選項上的此工具列，以執行選取的檢查 (所有或特定)。
儲存或寫入結果	使用「檔案」功能表選項上的此工具列，以針對執行的檢查建立詳細報告並儲存。
執行此檢查	選取項目標題以查看檢查的描述，然後按一下此工具列圖示以執行檢查。例如，若要執行下列其中一個操作： ◆ 安裝或更新產品授權 (授權驗證) ◆ 備份 AD LDS 例項 (AD LDS 例項備份)
修正此問題	選取項目標題，然後在檢查失敗時使用此工具列選項。如果再次執行檢查依然未修正問題，描述應該包含您可以採取來解決問題的資訊或動作。

9.4 資源回收筒公用程式

此公用程式可讓您在管理網域的子樹狀結構時啟用資源回收筒支援。如果網域存取帳戶沒有指定網域中隱藏 NetIQRecycleBin 容器的許可，DRA 無法將刪除的帳戶移至資源回收筒。

附註： 在使用此公用程式以啟用資源回收筒之後，執行完整帳戶快取重新整理以確定管理伺服器套用此變更。

您可以使用此公用程式來執行下列任務：

- 驗證指定的使用者帳戶具有指定網域中 NetIQRecycleBin 容器的讀取許可
- 將讀取許可委託給指定的帳戶
- 顯示 NetIQRecycleBin 容器的安全性設定

9.4.1 資源回收筒公用程式的必要許可

若要使用此公用程式，您必須具有下列許可：

如果想要 ...	您需要此許可...
驗證帳戶許可	NetIQRecycleBin 容器的讀取許可存取
委託 NetIQRecycleBin 容器的讀取許可	指定網域中的管理員許可
顯示 NetIQRecycleBin 容器的安全性設定	NetIQRecycleBin 容器的讀取許可存取

9.4.2 資源回收筒公用程式的語法

DRARECYCLEBINUTIL /DOMAIN:*DOMAINNAME* [/DC:*COMPUTERNAME*] {/DELEGATE:*ACCOUNTNAME* | /VERIFY:*ACCOUNTNAME* | /DISPLAY}

9.4.3 資源回收筒公用程式的選項

下列選項可讓您設定「資源回收筒公用程式」：

/DOMAIN:domain	指定資源回收筒所在之網域的 NETBIOS 或 DNS 名稱。
/SERVER:*computername*	針對指定的網域指定網域控制器的名稱或 IP 位址。
/DELEGATE:*accountname*	將許可委託給指定的帳戶。
/VERIFY:*accountname*	驗證指定帳戶的許可。

/DISPLAY	顯示指定網域中 NetIQRecycleBin 容器的安全性設定。

9.4.4 資源回收筒公用程式的範例

下列範例示範通用案例的範例指令。

範例 1

若要確認MYCOMPANY\JSmith使用者帳戶是否具有hou.mycompany.com網域中NetIQRecycleBin容器的讀取許可，請輸入：

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

範例 2

若要將 MYCOMPANY 網域中 NetIQRecycleBin容器的讀取許可委託給 MYCOMPANY\DraAdmins 群組，請輸入：

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

範例 3

若要使用HQDC網域控制器來顯示hou.mycompany.com網域中NetIQRecycleBin容器的安全性設定，請輸入：

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```