NetIQ Directory and Resource Administrator

安裝指南

2021 年 6 月

法律聲明

如需法律聲明、商標、免責聲明、擔保聲明、出口與其他使用限制、美國政府限制的權利、專利政策與 FIPS 法規遵循的相關資訊，請參閱 https://www.microfocus.com/about/legal/。

目錄

關於本指南

*安裝指南*提供 NetIQ Directory and Resource Administrator (DRA) 及其整合式元件的規劃、安裝、授權和組態資訊。

本手冊引導您進行安裝程序，並協助您在安裝及配置 DRA 時，做出正確的決策。

適用對象

本手冊為安裝 DRA 的所有人員提供資訊。

其他文件

本指南為 NetIQ Directory and Resource Administrator 文件集的一部分。如需本指南的最新版本和其他 DRA 文件資源，請造訪 DRA 文件網站 (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html)。

聯絡資訊

我們想瞭解您對本手冊和本產品隨附的其他文件的想法和建議。您可以使用線上文件任一頁面底部的 **comment on this topic** (新增有關此主題的備註) 連結，或者傳送電子郵件至 Documentation-Feedback@microfocus.com。

如果遇到具體的產品問題，請在 https://www.microfocus.com/support-and-services/ 上聯絡 Micro Focus 客戶服務中心。

入門

在安裝和配置 NetIQ 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 何謂 Directory and Resource Administrator

NetIQ Directory and Resource Administrator (DRA) 為 Microsoft Active Directory (AD) 提供安全有效率的特權身分管理。DRA 的「最低權限」精細委託，可僅讓管理員和使用者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 Microsoft Exchange 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 Microsoft Active Directory、Windows、Exchange 和 Azure Active Directory 環境。

- **支援 Azure 和內部部署 Active Directory、Exchange 和商務用 Skype：**可讓管理員管理 Azure 和內部部署 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，PCI DSS、FISMA、HIPAA 和 NERC CIP) 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。

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，以及用於自動化工作流程程序的 Workflow Automation 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
進階管理員	DRA 報告中心設定 (NRC) PowerShell *(選擇性)* CLI *(選擇性)* DRA ADSI 提供者 *(選擇性)*	任何 DRA 伺服器
服務台臨時管理員	Web 主控台	任何 DRA 伺服器

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。

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、Azure Active Directory 等)。
- **帳戶和資源管理 :** 可讓 DRA 助理管理員從委託和組態主控台檢視和管理連接網域和服務的委託物件。

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。

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：

- Active Directory 物件的資源報告
- Active Directory 物件資料報告
- Active Directory 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。

Workflow Automation 引擎

DRA 與 Workflow Automation 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 Workflow Automation 引擎的詳細資訊，請參閱 DRA 文件網站。

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
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
Skype Online
Exchange Online
授權
Active Directory
Azure Managed Tenant

II 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。

3 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。

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	8 CPU/ 核心 2.0 GHz	16 GB	120 GB
DRA Web 主控台	2 CPU/ 核心 2.0 GHz	8 GB	100 GB
DRA 報告	4 CPU/ 核心 2.0 GHz	16 GB	100 GB
DRA 工作流程伺服器	4 CPU/ 核心 2.0 GHz	16 GB	120 GB

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

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

元件表：

- 「DRA 管理伺服器」(第 18 頁)
- 「DRA REST 伺服器」(第 19 頁)
- 「Web 主控台 (IIS)」(第 20 頁)
- 「DRA 委託和管理主控台」(第 20 頁)
- 「工作流程伺服器」(第 20 頁)

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* .
TCP 50000 *	雙向	DRA 管理伺服器	屬性複寫和 DRA 伺服器 -AD LDS 通訊。(LDAP)
TCP 50001 *	雙向	DRA 管理伺服器	SSL 屬性複寫 (AD LDS)
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)

通訊協定和連接埠	方向	目的地	用法
TCP 80	向外	Microsoft Exchange Server	所有內部部署 Exchange 伺服器 2013 及更新版本所需 (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)
TCP 443、5986、5985	向外	Microsoft PowerShell	原生 PowerShell Cmdlet (HTTPS) 和 PowerShell 遠端
TCP 5984	Localhost	DRA 管理伺服器	對複寫服務的 IIS 存取，以支援臨時群組指派
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。
TCP 8443	雙向	Change Guardian 伺服器	整合的變更歷程
TCP 8898	雙向	DRA 管理伺服器	DRA 伺服器之間的 DRA 複寫服務通訊，用於臨時群組指派
TCP 636	向外	Microsoft Active Directory 網域控制器	Active Directory 物件管理 (LDAP SSL)。

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 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	針對 DRA Web 主控台與 DRA PowerShell 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* (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* (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)

通訊協定和連接埠	方向	目的地	用法
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 Workflow Automation 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

支援的平台

如需所支援軟體平台的最新資訊，請參閱 Directory and Resource Administrator 產品頁面。

受管理系統	先決條件
Azure Active Directory	若要啟用 Azure 管理，您必須安裝下列 PowerShell 模組： ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 版或更新版本 ◆ AzureRM.Profile 5.8.2 版或更新版本 ◆ Exchange Online PowerShell 2 1.0.1 版或更新版本 需要 PowerShell 5.1 或最新模組才能安裝新 Azure PowerShell 模組。
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
商務用 Skype	◆ Microsoft 商務用 Skype 2015
變更歷程	◆ Change Guardian 5.1 或更新版本
資料庫	◆ Microsoft SQL Server 2016
網頁瀏覽器	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
自動化工作流程	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019

DRA 管理伺服器和 Web 主控台需求

DRA 元件需要下列軟體和帳戶：

軟體要求

元件	先決條件
安裝目標 **作業系統**	**NetIQ 管理伺服器作業系統：** ◆ Microsoft Windows Server 2012 R2、2016、2019 **附註：**伺服器也必須是受支援的 Microsoft 內部部署 Active Directory 網域的成員。 **DRA 介面：** ◆ Microsoft Windows Server 2012 R2、2016、2019
安裝程式	◆ Microsoft .Net Framework 4.8 和更新版本
管理伺服器	**Directory and Resource Administrator：** ◆ Microsoft .Net Framework 4.8 和更新版本 ◆ Microsoft Visual C++ 2015-2019 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 Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services 應用程式要求路由 **附註：**DRA REST 端點和服務會與管理伺服器一起安裝。 **Microsoft Office 365/Exchange Online 管理：** ◆ 適用於 Windows PowerShell 的 Windows Azure Active Directory 模組 ◆ Windows PowerShell 模組 ◆ Exchange Online PowerShell 第 2 版模組 ◆ 啟用 WinRM 進行用戶端上 Exchange Online 任務的基本驗證。 如需詳細資訊，請參閱 支援的平台。

元件	先決條件
使用者介面	**DRA 介面：** ◆ Microsoft .NET Framework 4.8 ◆ Microsoft Visual C++ 2015-2019 可轉散發套件 (x64 和 x86)
PowerShell 延伸功能	◆ Microsoft .NET Framework 4.8 ◆ PowerShell 5.1 或更新版本
DRA Web 主控台	**Web 伺服器：** ◆ Microsoft .Net Framework 4.x > WCF 服務 > HTTP 啟動 ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft Internet Information Services URL Rewrite Module ◆ Microsoft Internet Information Services 應用程式要求路由

伺服器領域

元件	作業系統
DRA 伺服器	◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

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	◆ 適用於「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)
		◆ 如果在使用 STIG 方法的伺服器上安裝 DRA，則必須為 DRA 服務帳戶使用者選取下列「帳戶」索引標籤 > **帳戶選項**之一：
		  ◆ Kerberos AES 128 位元加密
		  ◆ Kerberos AES 256 位元加密
		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。
		◆ 如需針對 DRA 設定群組管理的服務帳戶的詳細資訊，請參閱：*《DRA 管理員指南》*的「設定群組管理服務帳戶的 DRA 服務」。

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 助理管理員帳戶	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。僅在您使用複雜用戶端或「委託和組態」主控台時需要。 **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：使用 ADSI 編輯器，針對下列子系物件類型，以最高網域層級授予網域存取帳戶下列 Active Directory 許可：

- 「完整」控制 builtInDomain 物件
- 「完整」控制電腦物件
- 「完整」控制連接點物件
- 完整控制聯絡人物件
- 完整控制容器物件
- 「完整」控制群組物件
- 「完整」控制 InetOrgPerson 物件
- 「完整」控制 MsExchDynamicDistributionList 物件
- 「完整」控制 MsExchSystemObjectsContainer 物件
- 「完整」控制 msDS-GroupManagedServiceAccount 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 publicFolder 物件
- 「完整」控制共用資料夾物件
- 「完整」控制使用者物件

針對此物件和所有子系物件，以最高網域層級授予網域存取帳戶下列 Active Directory 許可：

- 允許建立電腦物件
- 允許建立聯絡人物件
- 允許建立容器物件
- 允許建立群組物件
- 允許建立 MsExchDynamicDistributionList 物件
- 允許建立 msDS-GroupManagedServiceAccount 物件
- 允許建立組織單位物件
- 允許建立 publicFolders 物件
- 允許建立共用資料夾物件
- 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 MsExchDynamicDistributionList 物件
- 允許刪除 msDS-GroupManagedServiceAccount 物件

- 允許刪除組織單位物件
- 允許刪除 publicFolders 物件
- 允許刪除共用資料夾物件
- 允許刪除使用者物件

附註：

- 依預設，部分 Active Directory 中的內建容器物件不會從網域最高層級繼承許可。基於此原因，這些物件需要啟用繼承或設定特定託管許可。
- 如果您使用最小特權帳戶作為存取帳戶，則請確保帳戶在 Active Directory 中獲得指定其自身的「重設密碼」權限，以在 DRA 中成功重設密碼。

Exchange 存取帳戶：若要管理內部部署 Microsoft Exchange 物件，請將「組織管理」角色指派給 Exchange 存取帳戶，並將 Exchange 存取帳戶指派給「帳戶操作員」群組。

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

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

- 分發群組
- 郵件收件人
- 郵件收件人建立
- 安全性群組建立和成員資格
- (選用) 商務用 Skype 管理員

  如果您想要管理商務用 Skype Online，請將商務用 Skype 管理員權限指派給 Azure 租用戶存取帳戶。
- 使用者管理員

NetIQ 管理服務帳戶許可：

- 本機管理員
- 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。
- **資源管理**：若要管理受管理 Active Directory 網域中的已發佈資源，必須授予網域存取帳戶對該資源的本機管理許可。

DRA 安裝之後：管理所需的網域之前，您必須執行下列指令：

- 若要從 DRA 安裝資料夾將許可委託給「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>*

- 若要從 DRA 安裝資料夾將許可委託給「NetIQReceyleBin OU」：

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

遠端存取 SAM：指派網域控制器或由 DRA 管理的成員伺服器以啟用下方 GPO 中所列的帳戶，讓這些帳戶可以對安全性帳戶管理員 (SAM) 的資料庫進行遠端查詢。組態需要包含 DRA 服務帳戶。

網路存取：限制允許對 SAM 進行遠端通話的用戶端

若要存取此設定，請執行下列動作：

1. 開啟網域控制器上的「群組規則管理」主控台。
2. 展開節點樹狀結構中的 **Domains** > **[domain controller]** > **Group Policy Objects** (網域 > [網域控制器] > 群組規則物件)。
3. 在 **Default Domain Controllers Policy** (預設網域控制器規則) 上按一下滑鼠右鍵，然後選取 **Edit** (編輯) 以開啟此規則的 GPO 編輯器。
4. 展開 GPO 編輯器的節點樹狀結構中的 **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** (電腦組態 > 規則 > Windows 設定 > 安全性設定 > 本機規則)。
5. 按兩下規則窗格中的 **Network access: Restrict clients allowed to make remote calls to SAM** (網路存取：限制允許對 SAM 進行遠端通話的用戶端)，然後選取 **Define this policy setting** (定義此規則設定)。
6. 按一下遠端存取的 **Edit Security** (編輯安全性) 並啟用 **Allow** (允許)。如果尚未將 DRA 服務帳戶包含作為使用者或管理群組的一部份，請加以新增。
7. 套用變更。這會將安全性描述子 O:BAG:BAD:(A;;RC;;;BA) 新增至規則設定。

如需更多資訊，請參閱知識庫文章 7023292。

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 R2、2016、2019

元件	先決條件
NetIQ Reporting Center (3.3 版)	**資料庫：** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ 管理 SQL 代理程式工作的網域管理員需要 Microsoft SQL Server Integration Services 的安全性權限，否則可能無法處理一些 NRC 報告。 **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:** ◆ 需要執行 NRC 安裝程式 ◆ 在 DRA 主要伺服器上也需要，用於 DRA 報告服務組態 **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。 **通訊安全性協定：** ◆ SQL Server 必須支援 TLS 1.2。如需詳細資訊，請參閱 Microsoft SQL Server 的 TLS 1.2 支援。 ◆ SQL Server 要求 DRA 伺服器上必須安裝可支援 TLS 的更新驅動程式。建議的驅動程式是最新的 Microsoft® SQL Server® 2012 原生用戶端 - QFE ◆ 在 SQL Server 和 DRA 管理伺服器的作業系統中，都必須支援相同的 TLS 協定版本。例如，僅啟用 TLS 1.2。
DRA 報告	**資料庫：** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

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，您可以使用健康情況檢查公用程式來安裝購買的授權。試用授權金鑰 (TrialLicense.lic) 也包含在安裝套件中，可讓您在 30 天內管理不限數量的使用者帳戶和信箱。

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)。

4 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。

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。

DRA 伺服器套件具備下列功能：

- **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。具備下列功能：
  - **記錄歸檔資源套件：**可讓您檢視稽核資訊。
  - **DRA SDK：**提供 ADSI 範例指令碼，協助您建立自己的指令碼。
  - **暫時群組指定：**提供元件，來啟用臨時群組指派的同步。
- **使用者介面：**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。
  - **ADSI 提供者：**可讓您建立自己的規則指令碼。
  - **指令行介面：**可讓您執行 DRA 作業。
  - **委託和組態：**啟用對 DRA 組態和管理功能的系統管理員存取權。同時，可讓您精細指定受管理資源和任務的存取權給助理管理員。
  - **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。
  - **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。

如需在多部電腦上安裝特定 DRA 主控台和指令行用戶端的相關資訊，請參閱安裝 DRA 用戶端。

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 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。
安裝 DRA	按一下 **Install DRA** (安裝 DRA) 和 **Next** (下一步) 來查看安裝選項。 **附註：**若要稍後安裝，請導覽至安裝媒體的解壓縮位置 (檢視安裝套件)，然後執行 Setup.exe。
預設安裝	選擇要安裝的元件，然後接受預設安裝位置 C:\Program Files (x86)\NetIQ\DRA，或指定其他安裝位置。元件選項： **管理伺服器** ◆ 記錄歸檔資源套件 (選擇性) ◆ DRA SDK ◆ 暫時群組指定 **使用者介面** ◆ ADSI 提供者 (選擇性) ◆ 指令行介面 (選用) ◆ 委託和組態 ◆ PowerShell 延伸功能 ◆ Web 主控台
驗證必要條件	**Prerequisites List** (必要條件清單) 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。
指定記錄位置	指定 DRA 儲存所有記錄檔的位置。 **附註：**委託與組態主控台記錄和 ADSI 記錄都儲存在使用者設定檔資料夾。
選取伺服器操作模式	選取 **Primary Administration Server** (主要管理伺服器) 安裝多主機組的第一部 DRA 管理伺服器 (部署中只會有一部主要伺服器)，或選取 **Secondary Administration Server** (次要管理伺服器) 將新的 DRA 管理伺服器加入現有的多主機組。 如需多主機組的相關資訊，請參閱 *《DRA 管理員指南》*中的「「設定多主機組」」。

步驟	詳細資料
指定安裝帳戶和身分證明	◆ DRA 服務帳戶 ◆ AD LDS 群組 ◆ DRA 管理員 帳戶 詳細相關資訊請參閱：DRA 管理伺服器和 Web 主控台需求。
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。
指定 DRA 複製資料庫位置	◆ 指定 DRA 複製資料庫和複寫服務連接埠的檔案位置。 ◆ 指定您要用於透過 IIS 與資料庫進行安全通訊的 SSL 證書，然後指定 IIS 複寫連接埠。
指定 REST 服務 SSL 證書	選取要用於 REST 服務的 SSL 證書，並指定 REST 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**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。 如需詳細資訊，請參閱 *《DRA 管理員指南》* 中的 「健康情況檢查公用程式」。

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：

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*。

安裝 Workflow Automation 並設定其設定

若要管理 DRA 中的 Workflow Automation 要求，您需要完成下列動作：

- 安裝和設定 Workflow Automation 和 DRA 介面卡。

  如需相關資訊，請參閱 *《Workflow Automation 管理員指南》*和 *《DRA 的 Workflow Automation 介面卡參考》*。

- 設定 Workflow Automation 與 DRA 的整合。

  如需相關資訊，請參閱 *《DRA 管理員指南》*中的 「「設定 Workflow Automation 伺服器」」。

- 在 DRA 中委託 Workflow Automation 能力。

  如需相關資訊，請參閱 *《DRA 管理員指南》*中的 「「委託 Workflow Automation 伺服器能力」」。

上面參考的文件位於 DRA 文件網站。

安裝 DRA 報告

DRA 報告需要您從 NetIQ DRA 安裝套件安裝 DRAReportingSetup.exe 檔案。

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 產品安裝程式必要條件的要求。
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。

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。 如需 NetIQ Reporting Center 的詳細資訊，請參閱文件網站上的 *《報告中心指南》*。
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。

5 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 運作方式的相關資訊，請參閱 *《DRA 管理員指南》* 中的 「設定多主機組」。

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。
- 判斷有多少個助理管理員依賴每一個 MMS。如果大多數助理管理員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。
- 判斷哪些助理管理員需要 「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：
  - 檢閱哪些助理管理員與內建助理管理員群組相關聯。
  - 檢閱哪些助理管理員與內建 ActiveViews 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助理管理員。
- 判斷哪些助理管理員需要連接至主要管理伺服器。一旦您升級主要管理伺服器，這些助理管理員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助理管理員。

- 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。

重要：

- 如果您之前的 DRA 版本已安裝帳戶和資源管理 (ARM) 主控台，該 ARM 主控台會在升級過程中遭移除。
- 當您從 DRA 9.x 版升級 DRA 伺服器時，任何受管理的租用戶都會從 DRA 移除。若要繼續使用這些使用 Azure 的租用戶，您需要在升級後新增這些租用戶。如需新增租用戶的相關資訊，請參閱 *《DRA 管理員指南》*中的「建立 Azure 應用程式和新增 Azure 租用戶」。
- 由於 DRA 10.1 不支援 Exchange 2010，從 DRA 9.x 升級時 Exchange 會遭到停用。若要在升級之後繼續執行 Exchange 作業，請在委託和組態主控台將 **Enable Exchange Policy** (啟用 Exchange Policy) 選項停用後再重新啟用。變更都必須「套用」才能重設規則。

  如需此規則組態的相關資訊，請參閱 *《DRA 管理指南》*中的 「「啟用 Microsoft Exchange」」。

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 (助理管理員用戶端電腦)。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。
將 gMSA 轉換為 DRA 使用者帳戶	*選用：*如果您對 DRA 服務帳戶使用群組管理的服務帳戶 (gMSA)，請在升級之前將 gMSA 帳戶變更為 DRA 使用者帳戶。升級後，您需要將帳戶變更回 gMSA。

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。

升級前主題：

- 「使用本機管理伺服器來專門執行先前的 DRA 版本」(第 37 頁)
- 「同步化前一個 DRA 版本伺服器集」(第 38 頁)
- 「備份管理伺服器登錄」(第 38 頁)

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，可讓助理管理員在整個升級過程中使用先前的 DRA 版本，直到您對完成部署感到滿意為止。

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。
- 您必須支援大量助理管理員，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

在本機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，並確保助理管理員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站點的助理管理員使用先前的 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，可讓助理管理員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. 開啟「委託和組態主控台」，然後展開 **Configuration Management** (組態管理)。
3. 按一下 **Administration servers** (管理伺服器)。
4. 在右窗格中，為此伺服器集選取適當的主要管理伺服器。
5. 按一下 **Properties** (內容)。
6. 在 Synchronization schedule (同步化排程) 索引標籤上，按一下 **Refresh Now** (立即重新整理)。
7. 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\Mission Critical Software\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)。

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)。

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。

您可以將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。

重要：當您將 DRA 伺服器從 DRA 9.x 版升級至 DRA 10.x 版時，DRA 升級安裝會進行下列變更：

- 將 UCH 和 Workflow Automation 伺服器使用者組態從 Web 主控台移至委託和組態主控台
- 從伺服器移除舊的 Web 元件。
- 移除任何受管理租用戶。

  如需新增租用戶的相關資訊，請參閱 *《DRA 管理員指南》* 中的 「「設定 Azure 租用戶」」。
- 如果您已在較舊的版本安裝帳戶和資源管理主控台，當您升級至 DRA 10.x 版時，該帳戶和資源管理主控台會遭到移除。
- MMS 升級過程中，會先升級主要伺服器，然後是次要伺服器。若要成功複寫次要伺服器中的臨時群組指派，請手動執行 **Multi-master synchronization schedule** (多主機同步排程) 或等候其排程執行。
- 由於 DRA 10 不支援 Exchange 2010，從 DRA 9.x 升級時 Exchange 會遭到停用。若要在升級之後繼續執行 Exchange 作業，請在委託和組態主控台將 **Enable Exchange Policy** (啟用 Exchange Policy) 選項停用後再重新啟用。變更都必須 「套用」才能重設規則。

  如需此規則組態的相關資訊，請參閱 *《DRA 管理指南》* 中的 「「啟用 Microsoft Exchange」」。

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。

步驟	詳細資料
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。如需更多資訊，請參閱升級主要管理伺服器。
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。如需更多資訊，請參閱安裝目前 DRA 版本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。如需資訊，請參閱 部署 DRA 使用者介面
升級次要伺服器	升級 MMS 中的次要管理伺服器。如需更多資訊，請參閱升級次要管理伺服器。
升級 DRA 報告	升級 DRA 報告。如需更多資訊，請參閱升級報告。
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。
新增 Azure 租用戶 *(升級後)*	*(選擇性，升級後)* 如果您在升級前有管理任何 Azure 租用戶，這些租用戶在升級期間會遭到移除。您需要再次新增這些租用戶，並從 「委託和組態主控台」執行完整帳戶快取重新整理。如需詳細資訊，請參閱 *《DRA 管理員指南》* 中的 「「設定 Azure 租用戶」」。
更新 Web 主控台組態 *(升級後)*	*(條件式、升級後)* 如果您在升級前具有下列其中一個 Web 主控台組態，則需要在升級安裝完成後更新： • 啟用預設伺服器連接 • 已修改的組態檔案 如需詳細資訊，請參閱 更新 Web 主控台組態 - 安裝後。

伺服器升級主題：

- 「升級主要管理伺服器」 (第 40 頁)
- 「安裝目前 DRA 版本的本機次要管理伺服器」 (第 41 頁)
- 「部署 DRA 使用者介面」 (第 41 頁)
- 「升級次要管理伺服器」 (第 42 頁)
- 「更新 Web 主控台組態 - 安裝後」 (第 42 頁)

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：如需更多升級考量和指示，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助理管理員。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，讓助理管理員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，可讓助理管理員在整個升級過程中使用目前的 DRA 版本和先前的 DRA 版本，直到您對完成部署感到滿意為止。

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。
- 您必須支援大量助理管理員，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助理管理員使用先前的 DRA 版本和目前的 DRA 版本，直到升級完成。此外，助理管理員不會經歷停機時間，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助理管理員，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、ADSI 提供者、PowerShell 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。

您可以讓助理管理員安裝 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 主控台部署給多個助理管理員。

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助理管理員用戶端電腦，請考慮部署 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助理管理員安裝適當的使用者介面，例如 Web 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助理管理員。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，讓助理管理員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，且所有助理管理員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。

更新 Web 主控台組態 - 安裝後

執行下面的其中一個或兩個動作：升級後安裝 (如果其適用於您的 DRA 環境)：

預設 DRA 伺服器連接

從 DRA 10.1 開始，DRA REST 服務元件已與 DRA 伺服器合併。如果您在從 DRA 10.0.x 或更早版本升級之前設定預設 DRA 伺服器連接，則需要在升級後檢閱這些設定，因為現在只有一個連接組態：DRA 伺服器連接。您可以在 Web 主控台的 **Administration (管理)** > **Configuration (組態)** > **DRA Server Connection (DRA 伺服器連接)** 存取此設定。

您還可以在升級後於 web.config 檔案中更新這些設定，而此檔案位於 DRA Web 主控台伺服器的 C:\inetpub\wwwroot\DRAClient\rest 中，如下所示：

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Web 主控台登入組態

從 DRA 10.0.x 或更早版本升級時，如果在沒有 DRA 伺服器的情況下安裝 DRA REST 服務，則解除安裝 DRA REST 服務是升級的必要條件。升級前修改的檔案副本放在伺服器上的 C:\ProgramData\NetIQ\DRA\Backup\。您可以使用這些檔案作為參考，以在升級後更新任何相關檔案。

升級 Workflow Automation

若要在非叢集 64 位元環境上執行本機升級，只需要在現有 Workflow Automation 電腦上執行 Workflow Automation 安裝程式即可。不需要停止任何可能正在執行的 Workflow Automation 服務。

升級之後，必須解除安裝並重新安裝 Workflow Automation 安裝程式的任何未內建 Workflow Automation 介面卡。

如需升級工作流程自動化的詳細資訊，請參閱 *《Workflow Automation 管理員指南》*中的「「從舊版升級」」。

升級報告

升級 DRA 報告之前，請確定環境符合 NRC 3.3 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 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。
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*》。

III 產品組態

如果您是第一次安裝 Directory and Resource Administrator，本章描述必要的組態步驟和程序。

6 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
套用 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。
開啟委託和組態	使用 DRA 服務帳戶，登入已安裝「委託和組態主控台」的電腦。開啟主控台。
將第一個管理的網域新增至 DRA	將第一個管理的網域新增至 DRA。 **附註：**在初始「完整帳戶重新整理」完成之後，您就可以開始委託權限。
新增管理的網域和子樹狀結構	*選用：*將管理的網域和子樹狀結構新增至 DRA。如需管理的網域的相關資訊，請參閱新增管理的網域。
進行 DCOM 設定	*選用：*進行 DCOM 設定。如需 DCOM 設定的相關資訊，請參閱進行 DCOM 設定。
設定網域控制器和管理伺服器	請為每一個網域控制器和每一部管理伺服器設定執行「委託和組態」主控台的用戶端電腦。如需詳細資訊，請參閱 設定網域控制器和管理伺服器。
設定 gMSA 的 DRA 服務	*選擇性：*設定群組受管理服務帳戶 (gMSA) 的 DRA 服務。如需詳細資訊，請參閱 設定群組受管理服務帳戶的 DRA 服務。

7 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，即可使用健康情況檢查公用程式來安裝購買的授權。如有需要，安裝套件中也提供試用授權金鑰檔案 (TrialLicense.lic)，可讓您在 30 天內管理不限數量的使用者帳戶和信箱。

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。

8 新增管理的網域

安裝管理伺服器之後，您可以新增管理的網域、伺服器或工作站。新增第一個管理的網域時，您必須使用 DRA 服務帳戶登入已安裝「委託和組態主控台」的電腦。您在網域內也必須具有「管理權限」，例如授予「網域管理員」群組的權限。安裝第一個管理的網域之後，若要新增管理的網域和電腦，您必須具有適當的權限，例如內建「設定伺服器和網域」角色所包含的權限。

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。如需修改帳戶快取重新整理排程的相關資訊，請參閱 *《DRA 管理員指南》*中的「「設定快取」」。

---

9 新增管理的子樹狀結構

安裝管理伺服器之後，您可以從特定的 Microsoft Windows 網域新增受管理的或遺漏的子樹狀結構。這些功能可從 **Configuration Management** > **Managed Domains** (組態管理 > 受管理網域) 節點在 「委託和組態」主控台執行。安裝管理伺服器之後，若要新增管理的子樹狀結構，您必須具有適當的權限，例如內建 「設定伺服器和網域」角色所包含的權限。若要確保指定的存取帳戶具有許可來管理此子樹狀結構和執行遞增帳戶快取重新整理，請使用 「刪除的物件」公用程式來驗證和委託適當的許可。

如需使用此公用程式的相關資訊，請參閱 *《DRA 管理員指南》* 中的 「「刪除的物件公用程式」」。

如需設定存取帳戶的相關資訊，請參閱 *《DRA 管理員指南》* 中的 「「指定網域存取帳戶」」。

附註：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。如需修改帳戶快取重新整理排程的相關資訊，請參閱 *《DRA 管理員指南》* 中的 「「設定快取」」。

---

10 進行 DCOM 設定

如果您先前沒有允許安裝程式為您設定 DCOM，請在主要管理伺服器上進行 DCOM 設定。

如果您在 DRA 安裝過程中選擇不設定分散式 COM，請更新 Distributed COM Users 群組的成員資格來包含所有使用 DRA 的使用者帳戶。此成員資格應包含 DRA 服務帳戶、所有助理管理員，以及用於管理 DRA REST、DRA 主機和 DRA 管理服務的帳戶。

設定 Distributed COM Users 群組：

1. 以 DRA 管理員身分登入 DRA 管理電腦。
2. 啟動 「委託和組態」主控台。如果主控台未自動連接至管理伺服器，請手動建立連接。

   附註：如果 Distributed COM Users 群組未包含任何助理管理員帳戶，您可能無法連接至管理伺服器。在此情況下，請使用 「Active Directory 使用者和電腦」嵌入式管理單元來設定 Distributed COM Users 群組。如需使用 「Active Directory 使用者和電腦」嵌入式管理單元的相關資訊，請造訪 Microsoft 網站。

   ---
3. 在左窗格中，展開 **Account and Resource Management** (帳戶和資源管理)。
4. 展開 **All My Managed Objects** (我的所有受管理物件)。
5. 針對您有網域控制器的每一個網域，展開其網域節點。
6. 按一下 **Builtin** (內建) 容器。
7. 搜尋 Distributed COM Users 群組。
8. 在搜尋結果清單中，按一下 **Distributed COM Users** 群組。
9. 在下方窗格中按一下 **Members** (成員)，然後按一下 **Add Members** (新增成員)。
10. 新增將使用 DRA 的使用者和群組。務必將 DRA 服務帳戶新增至此群組。
11. 按一下 **「OK」** (確定)。

11 設定網域控制器和管理伺服器

在設定執行「委託和組態」主控台的用戶端電腦之後，請設定每一個網域控制器和每一部管理伺服器。

設定網域控制器和管理伺服器：

1. 從「開始」功能表，移至 **Control Panel** > **System and Security** (控制台 > 系統及安全性)。
2. 開啟 Administrative Tools (系統管理工具)，然後開啟 Component Services (元件服務)。
3. 展開 **Component Services** > **Computers** > **My Computer** > **DCOM Config** (元件服務 > 電腦 > 我的電腦 > DCOM 設定)。
4. 在管理伺服器上選取 **MCS OnePoint Administration Service**。
5. 在 Action (執行) 功能表上，按一下 **Properties** (內容)。
6. 在 General (一般) 索引標籤的 Authentication Level (驗證等級) 區域中，選取 **Packet** (封包)。
7. 在 Security (安全性) 索引標籤的 Access Permissions (存取權限) 區域中，選取 **Customize** (自訂)，然後按一下 **Edit** (編輯)。
8. 請確定有 Distributed COM Users 群組。若沒有，請新增。如果有 Everyone 群組，請移除。
9. 請確定 Distributed COM Users 群組具有「本機存取」和「遠端存取」許可。
10. 在 Security (安全性) 索引標籤的 Activation Permissions (啟用權限) 區域中，選取 **Customize** (自訂)，然後按一下 **Edit** (編輯)。
11. 請確定有 Distributed COM Users 群組。若沒有，請新增。如果有 Everyone 群組，請移除。
12. 請確定 Distributed COM Users 群組具有下列許可：
    - 本機啟動
    - 遠端啟動
    - 本機啟用
    - 遠端啟用
13. 套用變更。

12 設定群組受管理服務帳戶的 DRA 服務

如有需要，您可以將群組管理的服務帳戶 (gMSA) 用於 DRA 服務。如需使用 gMSA 的相關資訊，請參考 Microsoft 參考資料*群組受管理服務帳戶綜覽*。本節說明如何在將帳戶新增至 Active Directory 之後，針對 gMSA 設定 DRA。

重要：安裝 DRA 時，請不要使用 gMSA 作為服務帳戶。

若要為 gMSA 設定 DRA 主要管理伺服器：

1. 將 gMSA 新增為下列群組的成員：
   - DRA 伺服器上的本機管理員群組
   - DRA 受管理網域中的 AD LDS 群組
2. 針對下方每個服務，將服務內容中的登入帳戶變更為 gMSA：
   - NetIQ 管理服務
   - NetIQ DRA 稽核服務
   - NetIQ DRA 快取 DB 服務

     NetIQ DRA 快取服務
   - NetIQ DRA 核心服務
   - NetIQ DRA 記錄歸檔
   - NetIQ DRA 複寫服務
   - NetIQ DRA REST 服務
   - NetIQ DRA Skype 服務
3. 重新啟動所有服務。

若要為 gMSA 設定 DRA 次要管理伺服器：

1. 安裝次要伺服器。
2. 在主要伺服器上，將**設定伺服器和網域**角色指定給次要伺服器服務帳戶的**管理伺服器和受管理的網域** ActiveView。
3. 在主要伺服器上，新增次要伺服器並指定次要伺服器服務帳戶。
4. 將 gMSA 新增到 DRA 次要管理伺服器上的本機管理群組。
5. 在次要伺服器上，將所有 DRA 服務的登入帳戶變更為 gMSA，然後重新啟動 DRA 服務