

---

# Directory and Resource Administrator

安裝指南

2018 年 7 月

## 法律聲明

© 2007-2018 Micro Focus 或其關係企業版權所有。

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。

<b>關於本指南</b>	<b>5</b>
<b>1 入門</b>	<b>7</b>
何謂 Directory and Resource Administrator	7
了解 Directory and Administrator 元件	8
DRA 管理伺服器	8
委託和組態主控台	8
帳戶和資源管理主控台	8
Web 主控台	9
報告元件	9
工作流程引擎	9
產品架構	10
<b>2 產品安裝與升級</b>	<b>11</b>
規劃部署	11
經過測試的資源建議	11
必要的連接埠和通訊協定	11
支援的平台	14
DRA 管理伺服器需求	15
DRA Web 主控台和延伸功能需求	19
報告需求	20
授權需求	21
產品安裝	21
安裝 DRA 管理伺服器	21
產品升級	25
規劃 DRA 升級	25
升級前任務	26
升級 DRA 管理伺服器	28
升級 DRA REST 延伸功能	31
升級未封裝內容	31
<b>3 產品組態</b>	<b>33</b>
組態核對清單	33
安裝或升級授權	33
新增管理的網域	33
新增管理的子樹狀結構	34
進行 DCOM 設定	34
設定 Distributed COM Users 群組	34
設定網域控制器和管理伺服器	35



# 關於本指南

*安裝指南*提供 Directory and Resource Administrator (DRA) 的規劃、安裝、授權和組態資訊，以及其整合式組件。

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 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：	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
美國和加拿大：	1-888-323-6768
電子郵件：	<a href="mailto:info@netiq.com">info@netiq.com</a>
網站：	<a href="http://www.netiq.com">www.netiq.com</a>

## 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：	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
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：	<a href="mailto:support@netiq.com">support@netiq.com</a>
網站：	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## 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](mailto: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。

## 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。

Exchange Administrator (ExA) 延伸 DRA 的強大功能，提供 Microsoft Exchange 無接縫管理。ExA 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 和 ExA 共同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。

# 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
服務台臨時管理員	Web 主控台	任何已安裝 DRA REST 的 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：**可讓您精細指定受管理資源和任務的存取權給助理管理員。
- ◆ **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)。

## 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。



## Web 主控台

「Web 主控台」是 Web 型使用者介面，可讓 DRA Assistant Administrator 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。

管理員可以自訂「Web 主控台」的外觀和用法，以包含自訂的企業品牌和自訂的物件內容，還可以設定與 Change Guardian 伺服器整合，以便於 DRA 之外進行變更稽核。

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...

## 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。

## 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，Assistant Administrator 可以在主控台設定工作流程伺服器，並執行自訂的工作流程自動化表單，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 \(https://www.netiq.com/documentation/directory-and-resource-administrator-92/\)](https://www.netiq.com/documentation/directory-and-resource-administrator-92/)。

# 產品架構



# 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。

## 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	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

### 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

## 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、DRA 用戶端	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 ( <a href="http://go.microsoft.com/fwlink/?LinkID=46088">http://go.microsoft.com/fwlink/?LinkID=46088</a> ) (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)
TCP 443、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	DR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 <a href="http://go.microsoft.com/fwlink/?LinkID=46088">使用分散式 COM 搭配防火牆 (http://go.microsoft.com/fwlink/?LinkID=46088)</a> (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 <a href="http://go.microsoft.com/fwlink/?LinkID=46088">使用分散式 COM 搭配防火牆 (http://go.microsoft.com/fwlink/?LinkID=46088)</a> (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)
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

## 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	<ul style="list-style-type: none"><li>◆ Microsoft Server 2012</li><li>◆ Microsoft Server 2012 R2</li><li>◆ Microsoft Server 2016</li></ul>
Microsoft Exchange	<ul style="list-style-type: none"><li>◆ Microsoft Exchange 2010 SP3 (公用資料夾除外)</li><li>◆ Microsoft Exchange 2013</li><li>◆ Microsoft Exchange 2016</li><li>◆ Microsoft Skype Online</li></ul>

受管理系統	先決條件
Microsoft Office 365	<ul style="list-style-type: none"> <li>◆ Microsoft Exchange Online</li> <li>◆ Microsoft Skype Online</li> <li>◆ 適用於 Windows PowerShell 的 Windows Azure Active Directory 模組 <a href="https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell">https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell</a></li> <li>◆ 商務用 Skype Online、Windows PowerShell 模組 <a href="https://www.microsoft.com/en-us/download/details.aspx?id=39366">https://www.microsoft.com/en-us/download/details.aspx?id=39366</a></li> </ul>
商務用 Skype	<ul style="list-style-type: none"> <li>◆ Microsoft 商務用 Skype 2015</li> </ul>
變更歷程	<ul style="list-style-type: none"> <li>◆ Change Guardian 5.0、5.1</li> </ul>
網頁瀏覽器	<ul style="list-style-type: none"> <li>◆ Microsoft Internet Explorer 11、Edge</li> <li>◆ Google Chrome</li> <li>◆ Mozilla Firefox</li> </ul>

## 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	<b>NetIQ 管理伺服器作業系統：</b>
作業系統	<ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2012、2012 R2、2016</li> <li>◆ Microsoft Windows 2008 R2 僅支援升級。</li> </ul> <p><b>附註：</b> 伺服器也必須是受支援的 Microsoft Windows Server 原生網域的成員。</p> <p><b>Windows DRA 介面：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2012、2012 R2、2016</li> <li>◆ Microsoft Windows 8.1 (x86 &amp; x64)、10 (x86 &amp; x64)</li> </ul>
安裝程式	<ul style="list-style-type: none"> <li>◆ Microsoft .Net Framework 4.5.2 和更新版本</li> </ul>

元件	先決條件
管理伺服器	<p><b>Directory and Resource Administrator :</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft .Net Framework 4.5.2 和更新版本</li> <li>◆ 以下之一： <ul style="list-style-type: none"> <li>◆ Microsoft Visual C++ 2015 (Update 3) 可轉散發套件 (x64 和 x86)</li> <li>◆ Microsoft Visual C++ 2017 (Update 3) 可轉散發套件 (x64 和 x86)</li> </ul> </li> <li>◆ Microsoft Message Queuing</li> <li>◆ Microsoft Active Directory 輕量型目錄服務角色</li> <li>◆ 已啟動的遠端登錄服務</li> </ul> <p><b>Microsoft Office 365/Exchange Online 管理：</b></p> <ul style="list-style-type: none"> <li>◆ 適用於 Windows PowerShell 的 Windows Azure Active Directory 模組</li> <li>◆ 適用於 IT 專業人員的 Microsoft Online Services 登入小幫手</li> <li>◆ 商務用 Skype Online、Windows PowerShell 模組</li> </ul> <p>如需詳細資訊，請參閱<a href="#">支援的平台</a>。</p>
舊版 Web 元件	<p><b>Web 伺服器：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Internet Information Services (IIS) 版本 8.0、8.5、10</li> </ul> <p><b>Microsoft IIS 元件：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Active Service Pages (ASP)</li> <li>◆ Microsoft Active Service Pages .NET (ASP .NET)</li> <li>◆ Microsoft IIS 安全性角色服務</li> </ul> <p><b>Windows DRA 介面：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 4.5.2</li> <li>◆ Microsoft Visual C++ 2015 (Update 3) 可轉散發套件 (x86)</li> </ul>

## 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
<b>DRA 服務帳戶</b>	執行 NetIQ 管理服務所需的許可權	<ul style="list-style-type: none"> <li>◆ 「Distributed COM Users」許可權</li> <li>◆ AD LDS 管理員群組的成員</li> <li>◆ 帳戶操作員群組</li> <li>◆ 記錄歸檔群組 (OnePointOp ConfigAdms &amp; OnePointOp)</li> </ul> <p><b>附註：</b> 如需設定最低權限網域存取帳戶的相關資訊，請參閱：<a href="#">最低權限 DRA 存取帳戶</a>。</p>
<b>DRA 管理員</b>	佈建給內建DRA管理員角色的使用者帳戶或群組	<ul style="list-style-type: none"> <li>◆ 網域本機安全性群組或網域使用者帳戶</li> <li>◆ 管理的網域或受信任的網域的成員 <ul style="list-style-type: none"> <li>◆ 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。</li> </ul> </li> </ul>
<b>DRA Assistant Admin 帳戶</b>	透過 DRA 來委託權限的帳戶	<ul style="list-style-type: none"> <li>◆ 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。</li> </ul> <p><b>附註：</b> 在安裝期間可設定 DRA 來替您管理這方面。</p>

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

將下列具有「此物件和所有子物件」範圍的權限指定給網域服務帳戶：

- ◆ 允許建立電腦物件

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

**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。

## 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： <ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2016、Microsoft Windows 10 (含 Microsoft IIS 10)</li> <li>◆ Microsoft Windows Server 2012、2012 R2 (含 Microsoft IIS 8.0、8.5)</li> </ul>
DRA 主機服務	<ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 4.5.2</li> <li>◆ DRA 管理伺服器</li> </ul>
DRA REST 端點和服務	<ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 4.5.2</li> </ul>
PowerShell 延伸功能	<ul style="list-style-type: none"> <li>◆ Microsoft .NET Framework 4.5.2</li> <li>◆ PowerShell 4.0</li> </ul>

元件	先決條件
DRA Web 主控台	<p><b>Web 伺服器:</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Internet Information Server 8.0、8.5、10</li> <li>◆ Microsoft Internet Information Services WCF (啟用)</li> </ul> <p><b>Microsoft IIS 元件 :</b></p> <ul style="list-style-type: none"> <li>◆ 網路伺服器 <ul style="list-style-type: none"> <li>◆ 通用 HTTP 功能 <ul style="list-style-type: none"> <li>◆ 靜態內容</li> <li>◆ 預設文件</li> <li>◆ 目錄瀏覽器</li> <li>◆ HTTP 錯誤</li> </ul> </li> <li>◆ 應用程式開發 <ul style="list-style-type: none"> <li>◆ ASP</li> </ul> </li> <li>◆ 狀態及診斷 <ul style="list-style-type: none"> <li>◆ HTTP 記錄</li> <li>◆ 申請監視器</li> </ul> </li> <li>◆ 安全性 <ul style="list-style-type: none"> <li>◆ 基本驗證</li> </ul> </li> <li>◆ 效能 <ul style="list-style-type: none"> <li>◆ 靜態內容壓縮</li> </ul> </li> </ul> </li> <li>◆ Web 伺服器管理工具</li> </ul>

## 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	<p><b>作業系統：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Windows Server 2012、2012 R2、2016</li> </ul>

元件	先決條件
<b>NetIQ Reporting Center (3.2 版)</b>	<p><b>資料庫：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft SQL Server 2012、2014、2016</li> <li>◆ Microsoft SQL Server Reporting Services</li> </ul> <p><b>Web 伺服器：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft Internet Information Server 8.0、8.5、10</li> <li>◆ Microsoft IIS 元件： <ul style="list-style-type: none"> <li>◆ ASP .NET 4.0</li> </ul> </li> </ul> <p><b>Microsoft .NET Framework 3.5:</b></p> <p>連接至 DRA Reporting 的每一部 DRA Administration 伺服器，另外還需要 .NET Framework 3.5。</p> <p><b>附註：</b> 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。</p>
<b>DRA 報告</b>	<p><b>資料庫：</b></p> <ul style="list-style-type: none"> <li>◆ Microsoft SQL Server Integration Services</li> <li>◆ Microsoft SQL Server Agent</li> </ul>

## 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」來安裝試用授權金鑰 (License1.lic)，此可允許您管理無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)。

## 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。

#### 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。

步驟	詳細資料
複製和執行 NetIQ 管理員安裝套件	<p>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。</p> <p><b>附註：</b> 必要的話，安裝套件會在目標伺服器上安裝 .NET Framework。</p>
執行 DRA 安裝	<p>啟動 DRA 安裝。</p> <p><b>附註：</b> 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。</p>
選取 NetIQ 管理伺服器元件和安裝目標	<p>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：</p> <p><b>NetIQ 管理伺服器</b></p> <ul style="list-style-type: none"> <li>◆ 記錄歸檔資源套件</li> <li>◆ NetIQ DRA SDK</li> </ul> <p><b>舊版 Web 元件</b></p> <p><b>使用者介面</b></p> <ul style="list-style-type: none"> <li>◆ 帳戶和資源管理</li> <li>◆ DRA ADSI 提供者</li> <li>◆ 指令行介面</li> <li>◆ 委託和組態</li> </ul>
驗證必要條件	<p><b>Prerequisites</b> (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。</p>
接受 EULA 授權合約	<p>接受最終使用者授權合約的條款。</p>
選取伺服器操作模式	<p>選取 <b>Primary</b> (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 <b>Secondary</b>，(次要) 將新的 DRA 管理伺服器加入現有的多主機組。</p> <p>如需關於多主機組的詳細資訊，請參閱「配置多主機組？」(《Directory and Resource Administrator 管理員指南》)。</p>
指定安裝帳戶和身分證明	<ul style="list-style-type: none"> <li>◆ DRA 服務帳戶</li> <li>◆ AD LDS 群組</li> <li>◆ DRA 管理員</li> </ul> <p>詳細相關資訊請參閱：<a href="#">DRA 管理伺服器需求</a>。</p>
設定 DCOM 許可	<p>可讓 DRA 設定「分散式 COM」存取給已驗證的使用者。</p>
設定連接埠	<p>如需預設連接埠的相關資訊，請參閱<a href="#">必要的連接埠和通訊協定</a>。</p>
指定儲存位置	<p>指定本端檔案位置供 DRA 儲存稽核和快取資料。</p>
驗證安裝組態	<p>在按一下<b>安裝</b>來繼續安裝之前，您可以先在安裝摘要頁面驗證組態。</p>
安裝之後驗證	<p>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。</p>

## 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：

<b>NetIQDRAUserConsole.mst</b>	安裝帳戶和資源管理主控台
<b>NetIQDRACLI.mst</b>	安裝指令行介面
<b>NetIQDRAADSI.mst</b>	安裝 DRA ADSI 提供者
<b>NetIQDRAClients.mst</b>	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*。

---

## 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 <code>NetIQAdminInstallationKit.msi</code> 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 <b>Run as administrator</b> (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 <b>Select Components</b> (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	<b>Prerequisites</b> (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 <a href="#">DRA 管理伺服器需求</a> 。
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 <b>Install</b> (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《[Aegis 管理員指南](#)》。

## 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 NetIQAdminNstallationKit.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 <b>Select Components</b> (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	<b>Prerequisites</b> (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。  <b>重要：</b> 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 <b>Configuration Database Installation - SQL Server Logon</b> (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。

## 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「Directory and Resource Administrator 管理員指南」(Directory and Resource Administrator 管理員指南)中的 *Managing a Multi-Master Set* (管理多主機組)。

## 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 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。

## 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 <b>AD LDS 例項備份</b> 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介面 (AA 用戶端電腦)。如需詳細資訊，請參閱 <a href="#">規劃 DRA 升級</a> 。
使用次要伺服器來專門執行先前的 DRA 版本	<i>選用</i> ：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：** 如果您打算回存 AD LDS 例項備份，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：NetIQDRASecureStoragexxxx。
- 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，選擇 **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)。

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 <a href="#">升級前任務</a> 。
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) 若要将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 and 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 and 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。

## 升級 DRA 報告元件

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[DRA文件](#)網站上的《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	<i>條件式：</i> 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。  <i>附註：</i> 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 [DRA 文件網站上的 NetIQ Reporting Center 報告指南](#)。

## 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 Administrator 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。您也可以不在安裝之外，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



# 3 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。

## 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 <a href="#">授權需求</a> 。
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。 <b>附註：</b> 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	<i>選用</i> ：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 <a href="#">新增管理的網域</a> 。
進行 DCOM 設定	<i>選用</i> ：進行 DCOM 設定。如需 DCOM 設定的相關資訊，請參閱 <a href="#">進行 DCOM 設定</a> 。

## 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。

## 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《「Directory and Resource Administrator 管理員指南」》中的 [配置快取](#)。

---

## 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 網域新增管理的子樹狀結構。您可以透過「委託和組態」主控台的 **Advanced Configuration (進階組態)** 節點，以新增您要管理的任何子樹狀結構。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《「Directory and Resource Administrator 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《「Directory and Resource Administrator 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《「Directory Resource Administrator 管理員指南」》中的 *配置快取*。

---

## 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。

### 設定 Distributed COM Users 群組

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。此成員資格應該包含 DRA 服務帳戶和所有助理管理員。

**設定 Distributed COM Users 群組：**

- 1 以 DRA 管理員身分登入 DRA 用戶端電腦。
- 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)。

## 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 **Start** (開始) 功能表，移至 **Settings > System and Security > Control Panel** (設定 > 系統及安全性 > 控制台)。
- 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 > MyComputer > DCOMConfig** (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。