NetIQ Directory and Resource Administrator 10.2

安装指南

2022 年 5 月

法律声明

有关法律声明、商标、免责声明、担保、出口和其他使用限制、美国政府权限、专利政策以及 FIPS 合规性的信息，请参见 https://www.microfocus.com/en-us/legal/。

目录

关于本指南

本*安装指南*将介绍 Directory and Resource Administrator (DRA) 及其集成组件的计划、安装、许可和配置信息。

本指南将指导您完成安装过程，帮您正确安装和配置 DRA。

适用对象

本指南可以为所有要安装 DRA 的人员提供相关安装信息。

其他文档

本指南是 Directory and Resource Administrator 文档集的一部分。有关本指南的最新版本和其他 DRA 文档资源，请访问 DRA 文档网站。

联系信息

我们希望收到您对本手册和本产品中包含的其他文档的意见和建议。您可以使用联机文档任一页面底部的 **comment on this topic** （评论该主题）链接，或者发送电子邮件至 Documentation-Feedback@microfocus.com。

如果遇到特定的产品问题，请通过 https://www.microfocus.com/support-and-services/ 联系 Micro Focus 客户关怀部门。

入门

安装和配置 Directory and Resource Administrator™ (DRA) 所有组件前，应了解 DRA 对企业的基本影响原则，以及产品结构中 DRA 组件的角色。

1 Directory and Resource Administrator 是什么

Directory and Resource Administrator 提供安全高效的 Microsoft Active Directory (AD) 特权身份管理。 DRA 执行 “ 最小特权 ” 细粒度委托，这样管理员和用户将只接收完成他们自己特定任务所需的许可权限。 DRA 强制遵守策略，提供详细的活动审计和报告，通过 IT 流程自动化简化完成重复任务。所有这些功能都有助于保护客户的 AD 和 Exchange 环境，杜绝多种风险的威胁，包括特权升级、错误、恶意活动以及监管方面的不合规性，同时通过向用户、业务管理者和 Help Desk 人员授予自助功能来减轻管理员的负担。

DRA 还扩展了 Microsoft Exchange 的强大功能，以提供对 Exchange 对象的无缝管理。DRA 通过一个通用的用户界面，根据策略来管理整个 Microsoft Exchange 环境中的邮箱、公共文件夹及通讯组列表。

DRA 提供控制和管理 Microsoft Active Directory、 Windows、 Exchange 和 Azure Active Directory 环境所需的解决方案。

- **支持 Azure 和本地 Active Directory、 Exchange 及 Skype for Business：**提供对 Azure 和本地 Active Directory、本地 Exchange Server、本地 Skype for Business、以及 Exchange Online 的一般性管理。
- **细粒度用户和管理特权访问控制：**专利活动视图 (ActiveView) 技术仅委派完成特定任务所需的特权，防止特权升级。
- **可自定义的 Web 控制台：**直观的方法方便非技术人员轻松安全地通过有限 （及指派的） 功能和访问权限执行管理任务。
- **深度活动审计和报告：**提供产品内所执行所有活动的综合性审计记录。安全存储长期数据并向审计方 （如 PCI DSS、 FISMA、 HIPAA 和 NERC CIP） 展示控制对 AD 的访问的流程均已到位。
- **IT 流程自动化：**自动执行多种任务工作流程，如供应和取回、用户和邮箱操作、策略实施和受控自助任务；提高业务效率，减少手动及重复性管理工作。
- **操作完整性：**通过为管理员提供细粒度访问控制及管理系统和资源访问权限，阻止那些对系统和服务的性能及可用性产生影响的恶意或错误篡改。
- **严格执行流程：**保持关键变革管理流程的健全，使其得以提高生产率、减少错误、节省时间并改进管理效率。
- **与 Change Guardian 集成：**增强对 DRA 和 Workflow Automation 之外 Active Directory 内生成的事件的审计

2 了解目录和管理员组件

将一直用于管理特权访问的 DRA 组件包括：主次服务器、管理员控制台、报告组件以及用于自动化工作流程的 Workflow Automation 引擎。

下表定义了每种类型的 DRA 用户使用的典型用户界面和管理服务器：

DRA 用户类型	用户界面	管理服务器
DRA 管理员 （维护产品配置的人）	Delegation and Configuration （委托和配置）控制台	主服务器
高级管理员	DRA Reporting Center 安装程序 (NRC) PowerShell *（可选）* CLI *（可选）* DRA ADSI 提供程序 *（可选）*	任何 DRA 服务器
Help Desk 临时管理员	Web 控制台	任何 DRA 服务器

DRA 管理服务器

DRA 管理服务器存储配置数据 （环境相关数据、委托访问及策略）、执行操作员和自动化任务并审计系统范围内的活动。在支持多个控制台和 API 级别客户端的同时，服务器还经过特别设计，通过多主集合 (MMS) 横向扩展模型为冗余和地理隔离提供高可用性。在此模型中，每个 DRA 环境将需要一个主 DRA 管理服务器，该服务器将与一些其他次 DRA 管理服务器同步。

我们强烈建议您不要在 Active Directory 域控制器上安装管理服务器。对于 DRA 管理的每个域，请确保至少有一个域控制器与管理服务器位于相同站点。默认情况下，管理服务器访问最近的域控制器进行所有读取与写入操作；当执行站点特定的任务时，例如重设置口令，可以指定站点特定域控制器来处理操作。最佳实践是考虑设置一个专用次管理服务器用于报告、批处理和自动化工作负载。

Delegation and Configuration （委托和配置）控制台

Delegation and Configuration （委托和配置）控制台是一个可安装的用户界面，系统管理员可通过此界面访问 DRA 配置和管理功能。

- **委托管理：**让您能够精确指定和指派受管资源及任务的访问权限给助理管理员。
- **策略和自动化管理：**使您能够定义和实施策略，确保标准和环境约定合规性。

- **配置管理：**使您能够更新 DRA 系统设置和选项、添加自定义及配置受管服务 （Active Directory、 Exchange、 Azure Active Directory 等）。
- **帐户和资源管理：**可让 DRA 助理管理员通过 Delegation and Configuration （委托和配置）控制台查看和管理所连接域和服务的委托对象。

Web 控制台

Web 控制台是一个基于 Web 的用户界面，助理管理员可通过此界面快速轻松地查看和管理所连接域和服务的委托对象。管理员可以自定义 Web 控制台的外观和使用，使其包含自定义企业品牌和自定义对象属性。

报告组件

DRA 报告提供内置、可自定义的 DRA 管理模板以及 DRA 受管域和系统的细节：

- Active Directory 对象的资源报告
- Active Directory 对象数据报告
- Active Directory 摘要报告
- DRA 配置报告
- Exchange 配置报告
- Office 365 Exchange Online 报告
- 详尽的活动趋势报告 （按月、域和峰值）
- 汇总的 DRA 活动报告

可通过 SQL Server Reporting Service 计划和发布 DRA 报告，以便于分发给利益相关者。

Workflow Automation 引擎

DRA 与 Workflow Automation 引擎集成以通过 Web 控制台自动执行工作流程任务，在 Web 控制台中，助理管理员可以配置工作流程服务器并执行自定义工作流程自动化表单，然后查看这些工作流程的状态。有关 Workflow Automation 引擎的更多信息，请参见 DRA 文档网站。

产品架构


本地网络
DRA 服务器
Web 服务器(IIS)
报告
工作流引擎
主站点
主站点
邮件服务器
公共文件夹
Active Directory
受管域
受信任域
受管服务
Skype for Business
受管资源
计算机
打印机
DRA管理服务器
主/次（高可用性）
托管网站
报告
工作流引擎
DRA 客户端
Web 控制台
Delegation and Configuration (委托和配置）控制台
PowerShell 命令行
REST 客户端
显示链接
远程站点
远程环境
Active Directory
Exchange
受管服务
受管资源
远程 DRA 环境
DRA 次管理服务器
DRA 客户端
Azure
Office 365
Skype Online
Exchange Online
许可
Active Directory
Azure 受管租户

II 产品安装和升级

本章概述建议的硬件、软件以及 Directory and Resource Administrator 的帐户要求。本章还会指导您完成安装过程，并通过核对清单检查安装的每个组件。

3 计划部署

计划 Directory and Resource Administrator 部署时，使用此部分内容评估硬件和软件环境的兼容性，并注意要为部署配置的必要端口和协议。

经过测试的资源建议

此部分提供了建议的基础资源大小信息。结果可能因可用硬件、特定环境、所处理数据的特定类型及其他因素而异。可能存在着功能更强大且可以处理更大负载的大型硬件配置。如有问题，请咨询 NetIQ 咨询服务。

在有约一百万个 Active Directory 对象的环境中执行：

组件	CPU	内存	储存
DRA 管理服务器	8 核 CPU/ 核频率 2.0 GHz	16 GB	120 GB
DRA Web 控制台	2 核 CPU/ 核频率 2.0 GHz	8 GB	100 GB
DRA 报告	4 核 CPU/ 核频率 2.0 GHz	16 GB	100 GB
DRA 工作流程服务器	4 核 CPU/ 核频率 2.0 GHz	16 GB	120 GB

虚拟环境资源供应

DRA 保持大内存段活动的时间有所延长。为虚拟环境供应资源时，应考虑下列建议：

- 将储存分配为 "Thick Provisioned" （密集置备）

- 将内存预留设置为 Reserve All Guest Memory(All Locked) （预留所有 Guest 内存 （全部锁定））
- 确保分页文件足够大，能够覆盖虚拟层潜在扩大的内存重新分配

所需端口和协议

此部分提供 DRA 通信端口和协议。

- 可配置端口标有一个星号 *
- 需要证书的端口标有两个星号 **

组件表：

- DRA 管理服务器 （第 18 页）
- DRA REST 服务器 （第 20 页）
- Web 控制台 (IIS) （第 20 页）
- DRA 委托和管理控制台 （第 20 页）
- 工作流程服务器 （第 21 页）

DRA 管理服务器

协议和端口	方向	目标	用法
TCP 135	双向	DRA 管理服务器	端点映射器，DRA 通信的基本要求；使管理服务器在 MMS 中能找到彼此
TCP 445	双向	DRA 管理服务器	委托模型复制； MMS 同步 (SMB) 期间的文件复制
动态 TCP 端口范围 *	双向	Microsoft Active Directory 域控制器	默认情况下，DRA 动态分配 TCP 端口范围，即 1024 至 65535。但您可以使用 “组件服务 ” 配置此范围。有关更多信息，请参见 *Using Distributed COM with Firewalls* （与防火墙一起使用分布式 COM）。
TCP 50000 *	双向	DRA 管理服务器	属性复制和 DRA 服务器 - AD LDS 通信。(LDAP)
TCP 50001 *	双向	DRA 管理服务器	SSL 属性复制 (AD LDS)
TCP/UDP 389	出站	Microsoft Active Directory 域控制器	Active Directory 对象管理 (LDAP)
	出站	Microsoft Exchange Server	邮箱管理 (LDAP)

协议和端口	方向	目标	用法
TCP/UDP 53	出站	Microsoft Active Directory 域控制器	名称解析
TCP/UDP 88	出站	Microsoft Active Directory 域控制器	允许从 DRA 服务器到域控制器的身份鉴定 (Kerberos)
TCP 80	出站	Microsoft Exchange Server	为所有本地 Exchange Server 2013 及更高版本所需 (HTTP)
	出站	Microsoft Office 365	远程 PowerShell 访问 (HTTP)
TCP 443	出站	Microsoft Office 365, Change Guardian	Graph API 访问以及 Change Guardian 集成 (HTTPS)
TCP 443, 5986, 5985	出站	Microsoft PowerShell	本机 PowerShell cmdlet (HTTPS) 和 PowerShell 远程处理
TCP 5984	Localhost	DRA 管理服务器	IIS 访问复制服务以支持临时组指派
TCP 8092 * **	出站	工作流程服务器	工作流程状态和触发 (HTTPS)
TCP 50101 *	入站	DRA 客户端	右键单击更改历史记录报告转到 UI 审计报告。可在安装期间配置。
TCP 8989	Localhost	日志存档服务	日志存档通信 （不需要通过防火墙打开）
TCP 50102	双向	DRA 核心服务	日志存档服务
TCP 50103	Localhost	DRA 超速缓存数据库服务	DRA 服务器上的超速缓存服务通信（不需要通过防火墙打开）
TCP 1433	出站	Microsoft SQL Server	报告数据集合
UDP 1434	出站	Microsoft SQL Server	SQL Server 浏览器服务使用此端口识别命名实例的端口。
TCP 8443	双向	Change Guardian 服务器	统一的更改历史记录
TCP 8898	双向	DRA 管理服务器	用于临时组指派的 DRA 服务器之间的 DRA 复制服务通信
TCP 636	出站	Microsoft Active Directory 域控制器	Active Directory 对象管理 (LDAP SSL)。

DRA REST 服务器

协议和端口	方向	目标	用法
TCP 8755 * **	入站	IIS 服务器、 DRA PowerShell cmdlet	执行 DRA 基于 REST 的工作流程活动 (ActivityBroker)
TCP 135	出站	Microsoft Active Directory 域控制器	使用服务连接点 (SCP) 的自动发现
TCP 443	出站	Microsoft AD 域控制器	使用服务连接点 (SCP) 的自动发现

Web 控制台 (IIS)

协议和端口	方向	目标	用法
TCP 8755 * **	出站	DRA REST 服务	用于 Web 控制台和 DRA PowerShell 之间的通信
TCP 443	入站	客户端浏览器	打开 DRA 网站
TCP 443 **	出站	Advanced Authentication 服务器	Advanced Authentication

DRA 委托和管理控制台

协议和端口	方向	目标	用法
TCP 135	出站	Microsoft Active Directory 域控制器	使用 SCP 自动发现
动态 TCP 端口范围 *	出站	DRA 管理服务器	DRA 适配器工作流程活动。默认情况下， DCOM 动态分配 TCP 端口范围，即 1024 至 65535。但您可以使用 “ 组件服务 ” 配置此范围。有关更多信息，请参见 *Using Distributed COM with Firewalls*（与防火墙一起使用分布式 COM） (DCOM)
TCP 50102	出站	DRA 核心服务	更改历史记录报告生成

工作流程服务器

协议和端口	方向	目标	用法
TCP 8755	出站	DRA 管理服务器	执行 DRA 基于 REST 的工作流程活动 (ActivityBroker)
动态 TCP 端口范围 *	出站	DRA 管理服务器	DRA 适配器工作流程活动。默认情况下， DCOM 动态分配 TCP 端口范围，即 1024 至 65535。但您可以使用 “ 组件服务 ” 配置此范围。有关更多信息，请参见 *Using Distributed COM with Firewalls*（与防火墙一起使用分布式 COM） (DCOM)
TCP 1433	出站	Microsoft SQL Server	工作流程数据储存
TCP 8091	入站	操作控制台和配置控制台	工作流程 BSL API (TCP)
TCP 8092 **	入站	DRA 管理服务器	工作流程 BSL API (HTTP) 和 (HTTPS)
TCP 2219	Localhost	命名空间提供程序	命名空间提供程序用于运行适配器
TCP 9900	Localhost	Correlation Engine	Correlation Engine 用于与 Workflow Automation 引擎和命名空间提供程序通信
TCP 10117	Localhost	资源管理命名空间提供程序	由资源管理命名空间提供程序使用

支持的平台

有关支持的软件平台的最新信息，请参见 Directory and Resource Administrator 产品页面。

管理的系统	先决条件
Azure Active Directory	要启用 Azure 管理，您必须安装以下 PowerShell 模块： ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 或更高版本 ◆ AzureRM.Profile 5.8.2 或更高版本 ◆ Exchange Online PowerShell V2.0.3 或更高版本 安装新的 Azure PowerShell 模块需要 PowerShell 5.1 或最新模块。
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Server 2022 ◆ Azure Active Directory

管理的系统	先决条件
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online O365
Skype for Business	◆ Microsoft Skype for Business 2015
更改历史记录	◆ Change Guardian 6.0 或更高版本
数据库	◆ Microsoft SQL Server 2016
Web 浏览器	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019 ◆ Microsoft Server 2022

DRA 管理服务器和 Web 控制台要求

DRA 组件需要以下软件和帐户：

- 软件要求 （第 22 页）
- 服务器域 （第 24 页）
- 帐户要求 （第 24 页）
- 最小特权 DRA 访问帐户 （第 25 页）

软件要求

组件	先决条件
安装目标 **操作系统**	**NetIQ 管理服务器操作系统：** ◆ Microsoft Windows Server 2012 R2、 2016、 2019、 2022 **注释：**服务器还必须是所支持的 Microsoft 本地 Active Directory 域的成员。 **DRA 界面：** ◆ Microsoft Windows Server 2012 R2、 2016、 2019、 2022 ◆ Microsoft Windows 10、 11

组件	先决条件
安装程序	◆ Microsoft .Net Framework 4.8 及更高版本
管理服务器	**Directory and Resource Administrator：** ◆ Microsoft .Net Framework 4.8 及更高版本 ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages （x64 和 x86） ◆ Microsoft 讯息队列 ◆ Microsoft Active Directory 轻型目录服务角色 ◆ 已启动远程注册表服务 ◆ Microsoft Internet 信息服务 ◆ Microsoft Internet 信息服务 URL 重写模块 ◆ Microsoft Internet 信息服务应用程序请求路由 **注释：**NetIQ DRA REST Service 与管理服务器一同安装。 **Microsoft Office 365/Exchange Online 管理：** ◆ 适用于 Windows PowerShell 的 Windows Azure Active Directory 模块 ◆ Windows PowerShell 模块 ◆ Exchange Online PowerShell V2.0.3 或更高版本 ◆ 针对 Exchange Online 任务客户端的基本鉴定启用 WinRM。 有关更多信息，请参见支持的平台。
用户界面	**DRA 界面：** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015-2019 Redistributable Packages （x64 和 x86）
PowerShell 扩展	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 或更高版本
DRA Web 控制台	**Web 服务器：** ◆ Microsoft .Net Framework 4.x > WCF 服务 > HTTP 激活 ◆ Microsoft Internet 信息服务 8.5、 10 ◆ Microsoft Internet 信息服务 URL 重写模块 ◆ Microsoft Internet 信息服务应用程序请求路由 **Web 服务器 (IIS) 组件：** ◆ Web 服务器 > Security （安全性） > URL Authorization （URL 授权）

服务器域

组件	操作系统
DRA 服务器	◆ Microsoft Windows Server 2022 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

帐户要求

帐户	说明	许可权限
AD LDS 组	需要将 DRA 服务帐户添加到此组以便访问 AD LDS	◆ 域本地安全组

DRA 服务帐户	运行 NetIQ 管理服务所需的许可权限	◆ 针对 “ 分布式 COM 用户 ” 许可权限
		◆ AD LDS Admin 组成员
		◆ 帐户操作员组
		◆ 日志存档组 （OnePointOp ConfgAdms 和 OnePointOp）
		◆ 如果在服务器上使用 STIG 方法安装 DRA，则必须针对 DRA 服务帐户用户选择以下任意 “ 帐户 ” 选项卡 > **Account options** （帐户选项）之一：
		  ◆ Kerberos AES 128 位加密
		  ◆ Kerberos AES 256 位加密
		注释：
		◆ 有关设置最小特权域访问帐户的更多信息，请参见：最小特权 DRA 访问帐户。
		◆ 有关为 DRA 设置组托管服务帐户的更多信息，请参见 *《DRA 管理员指南》* 中的 “ 为组托管服务帐户配置 DRA 服务 ”。

DRA 管理员	供应到内置 DRA Admin 角色中的用户帐户或组	◆ 域本地安全组或域用户帐户 ◆ 受管域或受信任域的成员 ◆ 如果指定来自受信任域的帐户，确保管理服务器计算机可以鉴定此帐户。

帐户	说明	许可权限
DRA 助理 Admin 帐户	将通过 DRA 委托权利的帐户	◆ 将所有 DRA 助理 Admin 帐户添加到“分布式 COM 用户”组，以便它们可以从远程客户端连接到 DRA 服务器。仅在使用胖客户端或 Delegation and Configuration （委托和配置）控制台时才需要此操作。 **注释：**可配置 DRA 在安装期间对此进行管理。

最小特权 DRA 访问帐户

下面是指定的帐户所需的许可权限和特权，以及您需要运行的配置命令。

域访问帐户：使用 ADSI 编辑器，可以在域顶层为以下后代对象类型向域访问帐户授予以下 Active Directory 许可权限：

- 对 builtInDomain 对象的完全控制
- 对计算机对象的完全控制
- 对连接点对象的完全控制
- 对联系人对象的完全控制
- 对容器对象的完全控制
- 对组对象的完全控制
- 对 InetOrgPerson 对象的完全控制
- 对 MsExchDynamicDistributionList 对象的完全控制
- 对 MsExchSystemObjectsContainer 对象的完全控制
- 对 msDS-GroupManagedServiceAccount 对象的完全控制
- 对组织单元对象的完全控制
- 对打印机对象的完全控制
- 对 publicFolder 对象的完全控制
- 对共享文件夹对象的完全控制
- 对用户对象的完全控制

注释：如果未针对 Exchange Online 扩展受管域的 Active Directory 纲要，则不会列出以下对象：

- MsExchDynamicDistributionList 对象
- MsExchSystemObjectsContainer objects
- publicFolder 对象

在域顶层向域访问帐户授予对此对象和所有后代对象的以下 Active Directory 许可权限：

- 允许创建计算机对象
- 允许创建联系人对象
- 允许创建容器对象
- 允许创建组对象
- 允许创建 MsExchDynamicDistributionList 对象
- 允许创建 msDS-GroupManagedServiceAccount 对象
- 允许创建组织单元对象
- 允许创建 publicFolders 对象
- 允许创建共享文件夹对象
- 允许创建用户对象
- 允许创建打印机对象
- 允许删除计算机对象
- 允许删除联系人对象
- 允许删除容器
- 允许删除组对象
- 允许删除 InetOrgPerson 对象
- 允许删除 MsExchDynamicDistributionList 对象
- 允许删除 msDS-GroupManagedServiceAccount 对象
- 允许删除组织单元对象
- 允许删除 publicFolders 对象
- 允许删除共享文件夹对象
- 允许删除用户对象
- 允许删除打印机对象

注释：

- 默认情况下， Active Directory 中的某些内置容器对象不继承域顶层的许可权限。因此，这些对象将需要启用继承或设置显式许可权限。
- 如果您将最少的特权帐户用作访问帐户，请确保帐户在 Active Directory 中为自己指派 “ 重设置口令 ” 许可权限，以便在 DRA 中成功重设置口令。

Exchange 访问帐户：要管理本地 Microsoft Exchange 对象，请将组织管理角色指派给 Exchange 访问帐户，并将 Exchange 访问帐户指派给 “ 帐户操作员 ” 组。

Skype 访问帐户：确保此帐户是启用了 Skype 的用户并且至少是下列任意角色的成员：

- CSAdministrator 角色
- CSUserAdministrator 和 CSArchiving 角色

公共文件夹访问帐户：向公共文件夹访问帐户指派下列 Active Directory 许可权限：

- 公共文件夹管理
- 启用电子邮件的公共文件夹

Azure 租户：基本鉴定需要 Azure 租户访问帐户和 Azure 应用程序的 Azure Active Directory 许可权限。基于证书的鉴定需要 Azure 应用程序的 Azure Active Directory 许可权限。默认情况下，DRA 会自动创建鉴定所需的自我签名证书。

Azure 应用程序：Azure 应用程序需要以下角色和许可权限：

角色：

- 用户管理员
- Exchange Administrator

许可权限：

- 读取和写入所有用户的完整个人资料
- 读取和写入所有组
- 读取目录数据
- 将 Exchange Online 作为访问 Exchange Online 资源的应用程序进行管理
- 读取和写入所有应用程序
- Exchange 收件人管理员

Azure 租户访问帐户：Azure 租户访问帐户需要以下许可权限：

- 分发组
- 邮件收件人
- 邮件收件人创建
- 安全组创建和成员资格
- （可选） Skype for Business 管理员

  如果要管理 Skype for Business Online，请将 Skype for Business 管理员权限指派给 Azure 租户访问帐户。
- 用户管理员
- 特权鉴定管理员

NetIQ 管理服务帐户许可权限：

- 本地管理员
- 授予最小特权覆盖帐户对供应了用户主目录的共享文件夹或 DFS 文件夹的“完全许可权限”。
- **资源管理**：要管理托管的 Active Directory 域中已发布的资源，必须为域访问帐户授予对这些资源的本地管理许可权限。

安装 DRA 之后：在管理所需域之前，您必须运行以下命令：

- 将许可权限委托给 DRA 安装文件夹中的“ 已删除对象容器 ”（注意：必须由域管理员执行此命令）：

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

- 将许可权限委托给 DRA 安装文件夹中的 "NetIQReceyleBin OU"：

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

远程访问 SAM：指派由 DRA 管理的域控制器或成员服务器以启用以下 GPO 设置中列出的帐户，以便它们可以对安全帐户管理器 (SAM) 数据库进行远程查询。配置需要包括 DRA 服务帐户。

网络访问 : 限制允许对 SAM 进行远程调用的客户端

要访问此设置，请执行以下操作：

1. 打开域控制器上的组策略管理控制台。
2. 在节点树中展开**域** > **[域控制器]** > **组策略对象**。
3. 右键单击**默认域控制器策略**，然后选择**编辑**以为此策略打开 GPO 编辑器。
4. 在 GPO 编辑器的节点树中展开**计算机配置** > **策略** > **Windows 设置** > **安全设置** > **本地策略**。
5. 在策略窗格中双击**网络访问 : 限制允许对 SAM 进行远程调用的客户端**，然后选择**定义此策略设置**。
6. 单击**编辑安全设置**，然后启用**允许**进行远程访问。如果 DRA 服务帐户尚未作为用户或管理员组的一部分包括在内，则添加该帐户。
7. 应用更改。这会将安全描述符 O:BAG:BAD:(A;;RC;;;BA) 添加到策略设置中。

有关更多信息，请参见知识库文章 7023292。

报告要求

DRA 报告要求包括：

软件要求

组件	先决条件
安装目标	**操作系统：** • Microsoft Windows Server 2012 R2、 2016、 2019、 2022

组件	先决条件
NetIQ Reporting Center （3.3 版）	**数据库：** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ 管理 SQL 代理作业的域管理员需要 Microsoft SQL Server Integration Services 的安全权限，否则某些 NRC 报告可能无法处理。 **Web 服务器：** ◆ Microsoft Internet 信息服务 8.5、 10 ◆ Microsoft IIS 组件： ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5：** ◆ 运行 NRC 安装程序所需 ◆ 在 DRA 主服务器上进行 DRA Reporting 服务配置也需要 **注释：**在 SQL Server 计算机上安装 NetIQ Reporting Center (NRC) 时，安装 NRC 前，可能需要手动安装 .NET Framework 3.5。 **通信安全协议：** ◆ SQL Server 必须支持 TLS 1.2。有关更多信息，请参阅 TLS 1.2 support for Microsoft SQL Server （Microsoft SQL Server 的 TLS 1.2 支持）。 ◆ SQL Server 必须在 DRA 服务器上安装更新的支持 TLS 的驱动程序。建议的驱动程序是最新版 Microsoft® SQL Server® 2012 Native Client - QFE ◆ SQL Server 和 DRA 管理服务器的操作系统必须支持相同的 TLS 协议版本。例如，仅启用了 TLS 1.2。
DRA 报告	**数据库：** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server Agent

许可要求

许可证决定了可以使用的产品和功能。 DRA 要求在管理服务器上安装一个许可证密钥。

安装管理服务器后，可以使用 “ 运行状况检查实用程序 ” 安装所购买的许可证。安装包中还包括试用许可证密钥 (TrialLicense.lic)，使您可以在 30 天内管理数量不受限制的用户帐户和邮箱。有关 DRA 许可证的详细信息，请参阅安装和升级许可证。

有关许可证定义和限制的其他信息，请参见产品 “ 最终用户许可协议 (EULA)”。

4 产品安装

本章将指导您安装 Directory and Resource Administrator。有关计划安装或升级的更多信息，请参见 计划部署。

安装 DRA 管理服务器

您可以在环境中将 DRA 管理服务器安装为主节点或次要节点。主次管理服务器的要求是相同的，但每个 DRA 部署必须包含一个主管理服务器。

DRA 服务器包具有以下功能：

- **管理服务器：**存储配置数据 （环境、委托访问及策略）、执行操作员和自动化任务并审计系统范围内的活动。它具有以下特性：
  - **日志存档资源包：**使您能够查看审计信息。
  - **DRA SDK：**提供 ADSI 示例脚本并帮助您创建自己的脚本。
  - **临时组指派：**提供组件，以启用临时组指派的同步。
- **用户界面：**主要由助理管理员使用的 Web 客户端界面，但也包含自定义选项。
  - **ADSI 提供程序：**使您能够创建自己的策略脚本。
  - **命令行界面：**使您能够执行 DRA 操作。
  - **委托和配置：**允许系统管理员访问 DRA 配置和管理功能。此外，还让您能够精确指定和指派受管资源及任务的访问权限给助理管理员。
  - **PowerShell 扩展：**提供允许非 DRA 客户端使用 PowerShell cmdlet 请求 DRA 操作的 PowerShell 模块。
  - **Web 控制台：**主要由助理管理员使用的 Web 客户端界面，但也包含自定义选项。

有关在多台计算机上安装特定 DRA 控制台和命令行客户端的信息，请参见安装 DRA 客户端。

交互式安装核对清单：

步骤	细节
登录目标服务器	登录目标 Microsoft Windows 服务器，准备通过具有本地管理特权的帐户进行安装。

步骤	细节
复制并运行 Admin 安装包	执行 DRA 安装包 (NetIQAdminInstallationKit.msi) 将 DRA 安装媒体解压缩到本地文件系统。 **注释：**如需要，安装包将在目标服务器上安装 .Net 框架。
安装 DRA	单击 **Install DRA** （安装 DRA），然后单击 **Next** （下一步）以查看安装选项。 **注释：**要稍后运行安装，请导航到解压缩安装媒体的位置 （查看安装包），然后执行 Setup.exe。
默认安装	选择要安装的组件，接受默认安装位置 C:\Program Files (x86)\NetIQ\DRA 或指定其他安装位置。组件选项： **管理服务器** ◆ 日志存档资源包 (可选) ◆ DRA SDK ◆ 临时组指派 **用户界面** ◆ ADSI 提供程序 (可选) ◆ 命令行接口 （可选） ◆ 委托和配置 ◆ PowerShell 扩展 ◆ Web 控制台
校验是否符合先决条件	先决条件列表对话框将基于所选安装组件显示所需软件列表。安装程序将指导您逐步安装任何缺失的必备软件，以便让您成功完成安装 DRA。
接受 EULA 许可证协议	接受最终用户许可证协议条款。
指定日志位置	指定 DRA 存储所有日志文件的位置。 **注释：**Delegation and Configuration （委托和配置）控制台日志和 ADSI 日志存储在用户配置文件文件夹中。
选择服务器操作模式	选择 **Primary Administration Server** （主管理服务器）安装多主集合中的第一个 DRA 管理服务器 （部署中将只有一个主服务器）或选择 **Secondary Administration Server** （次管理服务器）向现有多主集合添加一个新的 DRA 管理服务器。 有关多主集合的更多信息，请参见 *《DRA Resource 管理员指南》*中的 “ 配置多主集合 ”。
指定安装帐户和身份凭证	◆ DRA 服务帐户 ◆ AD LDS 组 ◆ DRA 管理员 帐户 有关更多信息，请参见：DRA 管理服务器和 Web 控制台要求。

步骤	细节
配置 DCOM 许可权限	启用 DRA 为鉴定用户配置“分布式 COM”访问权限。
配置端口	有关默认端口的更多信息，请参见所需端口和协议。
指定储存位置	指定 DRA 将用于储存审计和超速缓存数据的本地文件位置。
指定 DRA 复制数据库位置	◆ 指定 DRA 复制数据库的文件位置和复制服务端口。 ◆ 指定要用于通过 IIS 与数据库进行安全通信的 SSL 证书，然后指定 IIS 复制端口。 **注释：** IIS Replication Web Site SSL Certificate （IIS 复制网站 SSL 证书）字段列出 WebHosting 存储区和个人存储区中的证书。
指定 REST 服务 SSL 证书	选择将用于 REST 服务的 SSL 证书，并指定 REST 服务端口。 **注释：** REST Service SSL Certificate （REST 服务 SSL 证书）字段列出 WebHosting 存储区和个人存储区的证书。
指定 Web 控制台 SSL 证书	指定将用于 HTTPS 绑定的 SSL 证书。
校验安装配置	单击安装继续安装前，可校验安装摘要页面上的配置。
安装后校验	安装完成后，运行状况检查实用程序将运行，校验安装并更新产品许可证。 有关更多信息，请参见 *《DRA 管理员指南》*中的“运行状况检查实用程序”。

安装 DRA 客户端

您可以通过在安装目标位置执行带相应 .mst 软件包的 DRAInstaller.msi 来安装特定 DRA 控制台和命令行客户端：

NetIQDRACLI.mst	安装命令行界面
NetIQDRAADSI.mst	安装 DRA ADSI 提供程序
NetIQDRAClients.mst	安装所有 DRA 用户界面

要将特定 DRA 客户端部署至企业内的多个计算机，配置组策略对象以安装特定 .MST 软件包。

1. 启动 Active Directory 用户和计算机并创建一个组策略对象。
2. 将 DRAInstaller.msi 软件包添加到此组策略对象。
3. 确保此组策略对象具有下列任意属性：
   - 组中每个用户帐户都具备相应计算机的高级用户许可权限。
   - 启用“始终以提升的权限进行安装”策略设置。
4. 向此组策略对象添加用户界面 .mst 文件。
5. 分发组策略。

注释：有关组策略的更多信息，请参见 Microsoft Windows 帮助。要在企业内轻松安全地测试和部署组策略，使用*组策略管理员*。

安装 Workflow Automation 和配置设置

要管理 DRA 中的 Workflow Automation 请求，您需要完成以下工作：

- 安装和配置 Workflow Automation 和 DRA 适配器。

  有关信息，请参见 *《Workflow Automation 管理员指南》*和 *《DRA Workflow Automation 适配器参考》*。
- 配置 Workflow Automation 与 DRA 集成。

  有关信息，请参见 *《DRA 管理员指南》*中的“配置 Workflow Automation 服务器”。
- 在 DRA 中委派 Workflow Automation 权限。

  有关信息，请参见 *《DRA 管理员指南》*中“委派 Workflow Automation 服务器配置权限”。

上述文档可在 DRA 文档网站中找到。

安装 DRA Reporting

DRA Reporting 要求您安装 NetIQ DRA 安装包中的 DRAReportingSetup.exe 文件。

步骤	细节
登录目标服务器	登录目标 Microsoft Windows 服务器，准备通过具有本地管理特权的帐户进行安装。确保此帐户拥有对 SQL Server 的本地和域管理特权，以及系统管理员特权。
复制并运行 NetIQ Admin 安装包	将 DRA 安装包 NetIQAdminInstallationKit.msi 复制到目标服务器，并通过双击文件或从命令行调用来执行该文件。安装包会将 DRA 安装媒体解压缩到本地文件系统的自定义位置。此外，如有需要，安装包还会在目标服务器上安装 .Net Framework，来满足 DRA 产品安装程序先决条件的要求。
执行 DRA Reporting 安装	导航到解压缩安装媒体的位置并执行 DRAReportingSetup.exe 为 DRA 报告集成安装管理组件。
校验和安装先决条件	先决条件对话框将基于所选安装组件显示所需软件列表。安装程序将指导您逐步安装任何缺失的必备软件，以便让您成功完成安装 DRA。 有关 NetIQ Reporting Center 的信息，请参见文档网站中的 *Reporting Center Guide*（《Reporting Center 指南》）。
接受 EULA 许可证协议	接受最终用户许可证协议条款完成安装运行。

5 产品升级

本章介绍帮助您分阶段控制升级或迁移分布式环境的过程。

本章假设您的环境包含多个管理服务器，一些服务器位于远程站点上。此配置称为多主集合 (MMS)。一个 MMS 包含一个主管理服务器和一个或多个相关的次管理服务器。有关 MMS 运行方式的更多信息，请参见 *《DRA 管理员指南》* 中的 " 配置多主集合 "。

计划 DRA 升级

执行 NetIQAdminInstallationKit.msi 解压缩 DRA 安装媒体并安装和运行 " 运行状况检查 " 实用程序。

确保开始升级过程前，已计划 DRA 部署。计划部署时，考虑下列原则：

- 在生产环境中进行升级前，先在实验环境中测试升级过程。通过测试，您可以识别和解决意外问题，无需担心影响日常管理任务。
- 回顾 所需端口和协议。
- 确定依赖每个 MMS 的助理管理员数量。如果大多数助理管理员依赖于特定服务器或服务器集，首先在非峰值时间段升级这些服务器。
- 确定哪些助理管理员需要 Delegation and Configuration （委托和配置）控制台。您可以使用以下任意方法获得此信息：
  - 查看哪些助理管理员与内置助理管理员组相关。
  - 查看哪些助理管理员与内置活动视图相关。
  - 使用 Directory and Resource Administrator Reporting 生成安全模型报告，例如活动视图助理 Admin 细节和助理 Admin 组报告。

  通知这些助理管理员您针对用户界面的升级计划。
- 确定哪些助理管理员需要连接主管理服务器。升级主管理服务器后，这些助理管理员应升级其客户端计算机。

  通知这些助理管理员您针对管理服务器及用户界面的升级计划。

- 确定升级流程开始前是否需要执行任何委托、配置或策略更改。根据环境的不同，可按站点做此决定。
- 协调客户端计算机升级以及管理服务器升级，确保停机时间最短。注意：DRA 不支持在同一管理服务器或客户端计算机上同时运行之前的 DRA 版本和当前 DRA 版本。

升级前任务

开始升级安装前，按照下面的升级前步骤为每个服务器集做好升级准备。

步骤	细节
备份 AD LDS 实例	打开运行状况检查实用程序并运行 **AD LDS 实例备份**检查，创建当前 AD LDS 实例备份。
制定部署计划	制定针对管理服务器和用户界面 （助理管理员客户端计算机）升级的部署计划。有关更多信息，请参见计划 DRA 升级。
指定专用次服务器来运行之前的 DRA 版本	*可选：*升级站点时指定专用的次管理服务器来运行之前的 DRA 版本。
按要求更改此 MMS	对此 MMS 的委托、配置或策略设置执行任何必要更改。使用主管理服务器可修改这些设置。
同步 MMS	同步服务器集，使每个管理服务器都包含最新配置和安全性设置。
备份主服务器注册表	备份主管理服务器的注册表。备份之前的注册表设置可以让您轻松恢复之前的配置和安全设置。
将 gMSA 转换为 DRA 用户帐户	*可选：*如果您将组托管服务帐户 (gMSA) 用作 DRA 服务帐户，请在升级之前将 gMSA 帐户更改为 DRA 用户帐户。升级后，您需要将帐户更改回 gMSA。

注释：如果需要恢复 AD LDS 实例，请执行下列操作：

1. 在 “ 计算机管理 ”>“ 服务 ” 中停止当前 AD LDS 实例。标题变为：NetIQDRASecureStoragexxxxx。
2. 用**备份** adamnts.dit 文件替换**当前** adamnts.dit 文件，如下所示：
   - 当前文件位置：%ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/
   - 备份文件位置：%ProgramData%/NetIQ/ADLDS/
3. 重启动 AD LDS 实例。

升级前主题：

- 指定本地管理服务器来运行之前的 DRA 版本 （第 37 页）
- 同步之前的 DRA 版本服务器集 （第 37 页）
- 备份管理服务器注册表 （第 38 页）

指定本地管理服务器来运行之前的 DRA 版本

指定一个或多个次管理服务器在升级期间在站点本地运行之前的 DRA 版本可以将停机时间以及远程站点连接开销降到最低。此步骤是可选步骤，此步骤将允许助理管理员在升级过程中使用之前的 DRA 版本，直至部署完成。

如果有下列一个或多个升级需求，请考虑此选项：

- 需要尽量缩短停机时间或永不停机。
- 必须支持大量助理管理员并且无法立即升级所有客户端计算机。
- 希望升级主管理服务器后能继续支持访问之前版本的 DRA。
- 您的环境包含一个跨多个站点的 MMS。

您可以安装新的次管理服务器或指定一个现有次服务器运行之前的 DRA 版本。如果想要升级此服务器，则该服务器应该是您升级的最后一个服务器。否则，成功完成升级后从此服务器完全卸装 DRA。

设置新的次服务器

在本地站点安装新的次管理服务器可帮助避免产生连接远程站点的开销，并确保助理管理员可以继续使用之前的 DRA 版本，不会出现中断。如果您的环境包含跨多个站点的 MMS，应考虑此选项。例如，如果 MMS 包含一个位于伦敦站点的主管理服务器和一个位于东京站点的次管理服务器，请考虑在伦敦站点安装一个次服务器并将其添加到相应的 MMS 中。这个额外的服务器将允许伦敦站点的助理管理员使用之前的 DRA 版本，直至升级完成。

使用现有次服务器

您可以将现有次管理服务器用作之前 DRA 版本的专用服务器。如果没有计划升级指定站点的次管理服务器，则应考虑此选项。如果无法将现有次服务器指定为专用，可考虑为此安装一个新的管理服务器。指定一个或多个次服务器运行之前的 DRA 版本将允许助理管理员在升级完成前继续使用之前的 DRA 版本，无中断。此选项最适合用于使用中央管理模型的较大型环境。

同步之前的 DRA 版本服务器集

备份之前的 DRA 版本注册表或开始升级过程前，确保已同步服务器集，保证每个管理服务器都包含最新配置和安全设置。

注释：确保已对此 MMS 的委托、配置或策略设置执行所有必要更改。使用主管理服务器可修改这些设置。升级主管理服务器后，不能与运行之前 DRA 版本的任何管理服务器同步委托、配置或策略设置。

要同步现有服务器集：

1. 以内置 Admin 身份登录主管理服务器。
2. 打开 Delegation and Configuration （委托和配置）控制台，然后展开 **Configuration Management** （配置管理）。

3 单击管理服务器。

4 在右侧窗格中，选择此服务器集的相应主管理服务器。

5 单击属性。

6 在同步日程表选项卡中，单击立即刷新。

7 校验是否已成功完成同步，并校验是否所有次管理服务器均可用。

备份管理服务器注册表

备份管理服务器注册表可确保您可以返回到之前的配置。例如，如果您必须完全卸装当前 DRA 版本并使用之前的 DRA 版本，拥有之前的注册表设置备份将方便您轻松恢复之前的配置和安全设置。

但是，编辑注册表时需谨慎。如果注册表中有错误，管理服务器可能无法如预期般奏效。如果升级过程中出现错误，您可以使用注册表设置备份来恢复注册表。有关更多信息，请参见 *Registry Editor Help* （注册表编辑帮助）。

重要：恢复注册表时， DRA 服务器版本、 Windows OS 名称和受管域配置必须完全相同。

重要：升级前，备份托管 DRA 的计算机的 Windows OS，或创建计算机的虚拟机快照图像。

要备份管理服务器注册表：

1 运行 regedit.exe。

2 右键单击 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint 节点，并选择导出。

3 指定保存注册表项的文件名称和位置并单击保存。

升级 DRA 管理服务器

下面的核对清单将指导您完成整个升级过程。使用此流程升级环境中的每个服务器集。如果尚未进行此操作，使用运行状况检查实用程序创建当前 AD LDS 实例的备份。

警告：在升级该 MMS 的主管理服务器前，不要升级次管理服务器。

您可以将此升级过程分为几个阶段，一次升级一个 MMS。此升级过程还允许您在同一 MMS 中临时包含运行之前 DRA 版本的次服务器和运行当前 DRA 版本的次服务器。 DRA 支持运行之前 DRA 版本的管理服务器与运行当前 DRA 版本的服务器同步。但是， DRA 不支持在同一管理服务器或客户端计算机上同时运行之前的 DRA 版本和当前 DRA 版本。

重要：要成功复制次服务器上的临时组指派，请手动运行 **Multi-master synchronization schedule** （多主同步安排）或等待其计划的运行。

步骤	细节
运行运行状况检查实用程序	安装独立的 DRA 运行状况检查实用程序并使用服务帐户运行该实用程序。修复所有问题。
执行测试升级	在实验环境中执行测试升级，确定潜在问题并将停机时间缩短至最短。
确定升级顺序	确定升级服务器集的顺序。
为每个 MMS 做好升级准备	为每个 MMS 做好升级准备。有关更多信息，请参见 升级前任务。
升级主服务器	升级相应 MMS 中的主管理服务器。有关信息，请参见升级主管理服务器。
安装新的次服务器	*（可选）*要将远程站点的停机时间缩短到最短，请安装运行最新版 DRA 的本地次管理服务器。有关信息，请参见安装运行当前 DRA 版本的本地次管理服务器。
部署用户界面	部署针对助理管理员的用户界面。有关信息，请参见部署 DRA 用户界面
升级次服务器	升级 MMS 中的次管理服务器。有关信息，请参见升级次管理服务器。
升级 DRA Reporting	升级 DRA Reporting。有关信息，请参见升级 Reporting。
运行运行状况检查实用程序	运行作为升级一部分而安装的运行状况检查实用程序。修复所有问题。
添加 Azure 租户 *（升级后）*	*（可选，升级后）*如果您在升级前管理任何 Azure 租户，则在升级期间会去除这些租户。您将需要再次添加这些租户，然后从 Delegation and Configuration （委托和配置）控制台运行完整的帐户超速缓存刷新。有关更多信息，请参见 *《DRA 管理员指南》*中的 “ 配置 Azure 租户 ”。
更新 Web 控制台配置 *（升级后）*	*（有条件的，升级后）*如果您在升级前有以下任意 Web 控制台配置，则需要在升级安装完成后进行更新： • 已启用默认服务器连接 • 已修改配置文件 有关更多信息，请参见更新 Web 控制台配置 - 安装后。

服务器升级主题：

升级主管理服务器

MMS 准备好后，升级主管理服务器。升级完主管理服务器前，不要升级客户端计算机中的用户界面。有关更多信息，请参见部署 DRA 用户界面。

注释：有关更多的升级注意事项和说明，请参见 *Directory and Resource Administrator 发行说明*。

升级前，通知您的助理管理员您计划开始升级的时间。如果指定一个次管理服务器运行之前的 DRA 版本，那么请标记此服务器，这样助理管理员便可以在升级期间继续使用之前的 DRA 版本。

注释：升级主管理服务器后，不能与运行之前 DRA 版本的次管理服务器同步此服务器的委托、配置或策略设置。

安装运行当前 DRA 版本的本地次管理服务器

安装新的次管理服务器在本地站点运行当前 DRA 版本可以帮助您将远程站点连接开销降至最低，并缩短总体停机时间，实现更快部署用户界面。此步骤是可选步骤，此步骤将允许助理管理员在升级过程中使用当前 DRA 版本和之前的 DRA 版本，直至部署完成。

如果有下列一个或多个升级需求，请考虑此选项：

- 需要尽量缩短停机时间或永不停机。
- 必须支持大量助理管理员并且无法立即升级所有客户端计算机。
- 希望升级主管理服务器后能继续支持访问之前版本的 DRA。
- 您的环境包含一个跨多个站点的 MMS。

例如，如果 MMS 包含一个位于伦敦站点的主管理服务器和一个位于东京站点的次管理服务器，请考虑在东京站点安装一个次服务器并将其添加到相应的 MMS 中。此新增服务器可以更好地平衡东京站点每天的管理负载，允许任意站点的助理管理员使用之前的 DRA 版本和当前 DRA 版本，直至升级完成。此外，因为您可以立即部署当前 DRA 用户界面，所以您的助理管理员不会经历停机。有关升级用户界面的更多信息，请参见部署 DRA 用户界面。

部署 DRA 用户界面

通常您应在升级主管理服务器和一个次管理服务器后部署当前 DRA 用户界面。但是，对于必须使用主管理服务器的助理管理员来说，要通过安装 Delegation and Configuration （委托和配置）控制台确保先升级了它们的客户端计算机。有关更多信息，请参见计划 DRA 升级。

如果经常通过 CLI、 ADSI 提供程序、 PowerShell 执行批处理，或经常生成报告，可考虑在专用次管理服务器上安装这些用户界面以维持 MMS 恰当的负载平衡。

您可以让助理管理员安装 DRA 用户界面或通过组策略部署这些界面。您还可以向多个助理管理员轻松快速部署 Web 控制台。

注释：不能在同一 DRA 服务器上并行运行多个版本的 DRA 组件。如果计划逐步升级助理管理员客户端计算机，可考虑部署 Web 控制台以确保可立即访问运行当前 DRA 版本的管理服务器。

升级次管理服务器

升级次管理服务器时，可根据管理需要，按需要升级每个服务器。另外，请考虑计划升级和部署 DRA 用户界面的方式。有关更多信息，请参见部署 DRA 用户界面。

例如，典型的升级路径可能包含下列步骤：

1. 升级一个次管理服务器。
2. 指示使用此服务器的助理管理员安装相应的用户界面，例如 Web 控制台。
3. 重复上面的步骤 1 和 2，直至完全升级 MMS。

升级前，通知您的助理管理员您计划开始升级的时间。如果指定一个次管理服务器运行之前的 DRA 版本，那么请标记此服务器，这样助理管理员便可以在升级期间继续使用之前的 DRA 版本。完成此 MMS 的升级过程并且所有助理管理员客户端计算机都运行升级的用户界面后，使运行之前 DRA 版本的所有剩余服务器变成脱机状态。

更新 Web 控制台配置 - 安装后

如果以下两个操作适用于您的 DRA 环境，升级安装后执行任意操作或这两个操作：

默认 DRA 服务器连接

从 DRA 10.1 开始， DRA REST 服务组件与 DRA 服务器合并。如果您在从 DRA 10.0.x 或更早版本升级之前配置了默认的 DRA 服务器连接，则需要在升级后查看这些设置，因为现在只有一个连接配置，即 DRA 服务器连接。您可以在 Web 控制台的**系统管理** > **配置** > **DRA 服务器连接**中访问此配置。

您还可以升级后在 DRA Web 控制台服务器的 C:\inetpub\wwwroot\DRAClient\rest 的 web.config 文件中更新这些设置：

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

Web 控制台登录配置

当从 DRA 10.0.x 或更早的版本升级时，如果在没有 DRA 服务器的情况下安装 DRA REST 服务，则卸载 DRA REST 服务是升级的先决条件。升级前修改的文件副本将保存到服务器的 C:\ProgramData\NetIQ\DRA\Backup\。升级后您可以参考这些文件以更新所有相关文件。

升级 Workflow Automation

要在非群集 64 位环境中进行就地升级，只需在现有 Workflow Automation 计算机上运行 Workflow Automation 安装程序即可。无需停止任何可能正在运行的 Workflow Automation 服务。

升级后，必须卸载并重新安装未内置到 Workflow Automation 安装程序的所有 Workflow Automation 适配器。

有关升级 Workflow Automation 的更多详细信息，请参见 *《Workflow Automation 管理员指南》* 中的 “ 从之前的版本升级 ”。

升级 Reporting

升级 DRA 报告前，确保您的环境满足针对 NRC 3.3 的最低要求。有关安装要求和升级注意事项的更多信息，请参见 *NetIQ Reporting Center 报告指南*。

步骤	细节
禁用 DRA 报告支持	要确保报告收集器在升级过程中不运行，在 Delegation and Configuration （委托和配置）控制台的 “ 报告服务配置 ” 窗口中禁用 DRA 报告支持。
通过适用的身份凭证登录 SQL 实例服务器	使用管理员账户登录已安装报告数据库 SQL 实例的 Microsoft Windows Server。确保此帐户拥有对 SQL Server 的本地管理特权，以及系统管理员特权。
运行 DRA 报告安装程序	运行 DRAReportingSetup.exe。（在安装包中）并按安装向导中的说明进行操作。
启用 DRA 报告支持	在主管理服务器上，启用 Delegation and Configuration （委托和配置）控制台中的报告。

如果您的环境使用 SSRS 集成，则需要重新部署报告。有关重新部署报告的更多信息，请参见文档网站中的 *Reporting Center Guide* （《Reporting Center 指南》）。

产品配置

本章介绍首次安装 Directory and Resource Administrator 时所需进行的配置步骤和过程。

6 配置核对清单

使用下列核对清单完成配置，以便开始使用。

步骤	细节
应用 DRA 许可证	使用运行状况检查实用程序应用 DRA 许可证。有关 DRA 许可证的更多信息，请参见许可要求。
打开 **Delegation and Configuration** （委托和配置）	使用 DRA 服务帐户，登录安装了 Delegation and Configuration （委托和配置）控制台的计算机。打开控制台。
将第一个受管域添加到 DRA	将第一个受管域添加到 DRA。 **注释：**初始的完全帐户刷新完成后，即可开始委托权利。
添加受管域和子树	*可选：*将其他受管域和子树添加到 DRA。有关受管域的更多信息，请参见添加受管域。
配置 DCOM 设置	*可选：*配置 DCOM 设置。有关 DCOM 设置的更多信息，请参见配置 DCOM 设置。
配置域控制器和管理服务器	为每个域控制器和每个管理服务器配置运行 Delegation and Configuration （委托和配置）控制台的客户端计算机。有关更多信息，请参见配置域控制器和管理服务器。
为 gMSA 配置 DRA 服务	*可选：*为组托管服务帐户 (gMSA) 配置 DRA 服务。有关更多信息，请参见为组托管服务帐户配置 DRA 服务。

7 安装或升级许可证

DRA 要求许可证密钥文件。此文件包含许可证信息，安装在管理服务器上。安装管理服务器后，使用“运行状况检查实用程序”安装所购买的许可证。如果需要，安装包中还提供了试用许可证密钥文件 (TrialLicense.lic)，使您可以在 30 天内管理数量不受限制的用户帐户和邮箱。

要升级现有许可证或试用许可证，打开 Delegation and Configuration （委托和配置）控制台，导航到 **Configuration Management** （配置管理） > **Update License** （更新许可证）。升级许可证时，升级每个管理服务器上的许可证文件。

8 添加受管域

安装完管理服务器后，您可以添加受管域、服务器或工作站。添加第一个受管域时，必须使用 DRA 服务帐户登录安装了 Delegation and Configuration （委托和配置）控制台的计算机。您还必须拥有域的管理权限，例如授予域管理员组的权限。要在安装了第一个受管域后添加受管域和计算机，您必须具备相应权限，例如包含在内置配置服务器和域角色中的那些权限。

注释：添加完受管域后，确保这些域的帐户超速缓存刷新计划是正确的。有关修改帐户超速缓存刷新计划的更多信息，请参见 *《DRA 管理员指南》*中的“ 配置超速缓存 ”。

---

9 添加受管子树

安装管理服务器后，您可以添加来自特定 Microsoft Windows 域的受管或缺失的子树。可在 Delegation and Configuration （委托和配置）控制台的 **Configuration Management** （配置管理）> **Managed Domains** （受管域）节点中执行这些功能。要在安装了管理服务器后添加受管子树，您必须具备相应权限，例如包含在内置配置服务器和域角色中的那些权限。要确保特定访问帐户拥有管理此子树及执行增量帐户超速缓存刷新的许可权限，使用“已删除对象”实用程序校验和委托相应许可权限。

有关使用此实用程序的更多信息，请参见 *《DRA 管理员指南》*中的“已删除对象实用程序”。

有关设置访问帐户的更多信息，请参见 *《DRA 管理员指南》*中的“指定域访问帐户”。

注释：添加完受管子树后，确保相应域的帐户超速缓存刷新计划是正确的。有关修改帐户超速缓存刷新计划的更多信息，请参见 *《DRA 管理员指南》*中的“配置超速缓存”。

---

10 配置 DCOM 设置

如果您不允许安装程序为您配置 DCOM，请在主管理服务器上配置 DCOM 设置。

如果选择不在 DRA 安装过程中配置分布式 COM，您应该更新分布式 COM 用户组的成员资格，以包含使用 DRA 的所有用户帐户。此成员资格应包括 DRA 服务帐户、所有助理 Admin 以及用于管理 DRA REST、 DRA 主机和 DRA Admin 服务的帐户。

要配置分布式 COM 用户组：

1. 以 DRA 管理员身份登录 DRA 管理计算机。
2. 选择 Delegation and Configuration （委托和配置）控制台。如果控制台没有自动连接管理服务器，手动建立连接。

   注释：如果分布式 COM 用户组不包含任何辅助 Admin 帐户，您可能无法连接管理服务器。如果是这种情况，使用 Active Directory 用户和计算机咬接模块配置分布式 COM 用户组。有关使用 Active Directory 用户和计算机咬接模块的更多信息，请参见 Microsoft 网站。

   ---

3. 在左侧窗格中，展开**帐户和资源管理**。
4. 展开**我的所有受管对象**。
5. 展开具有域控制器的每个域的节点。
6. 单击**内置**容器。
7. 搜索分布式 COM 用户组。
8. 在搜索结果列表中，单击**分布式 COM 用户**组。
9. 单击下方窗格中的**成员**，然后单击**添加成员**。
10. 添加将使用 DRA 的用户和组。确保将 DRA 服务帐户添加到此组中。
11. 单击**确定**。

11 配置域控制器和管理服务器

配置运行 Delegation and Configuration （委托和配置）控制台的客户端计算机后，您应配置每个域控制器和每个管理服务器。

要配置域控制器和管理服务器：

1. 在“开始”菜单中，转到**控制面板** > **系统和安全**。
2. 打开“管理工具”，然后打开“组件服务”。
3. 展开**组件服务** > **计算机** > **我的计算机** > **DCOM 配置**。
4. 选择管理服务器的 **MCS OnePoint 管理服务**。
5. 在操作菜单中，单击**属性**。
6. 在鉴定级别区域的常规选项卡中，选择**包**。
7. 在访问许可权限区域的安全选项卡中，选择**自定义**，然后单击**编辑**。
8. 确保存在“分布式 COM 用户”组。如果没有，请添加。如果存在“每个人”组，将其去除。
9. 确保分布式 COM 用户组拥有本地和远程访问许可权限。
10. 在起动和激活许可权限区域的安全选项卡中，选择**自定义**，然后单击**编辑**。
11. 确保存在“分布式 COM 用户”组。如果没有，请添加。如果存在“每个人”组，将其去除。
12. 确保分布式 COM 用户组拥有下列许可权限：
    - 本地起动
    - 远程起动
    - 本地激活
    - 远程激活
13. 应用更改。

12 为组托管服务帐户配置 DRA 服务

如果需要，可以将组托管服务帐户 (gMSA) 用于 DRA 服务。有关使用 gMSA 的更多信息，请参见 Microsoft 参考 *Group Managed Service Accounts Overview* （组托管服务帐户概述）。本节介绍在将帐户添加到 Active Directory 后，如何为 gMSA 配置 DRA。

重要：安装 DRA 时，请勿将 gMSA 用作服务帐户。

为 gMSA 配置 DRA 主管理服务器：

1. 将 gMSA 添加为以下组的成员：
   - DRA 服务器上的本地管理员组
   - DRA 受管域中的 AD LDS 组
2. 将以下每个服务的服务属性中的登录帐户更改为 gMSA：
   - NetIQ 管理服务
   - NetIQ DRA 审计服务
   - NetIQ DRA 超速缓存服务
   - NetIQ DRA 核心服务
   - NetIQ DRA 日志存档
   - NetIQ DRA 复制服务
   - NetIQ DRA Rest 服务
   - NetIQ DRA Skype 服务
3. 重启动所有服务。
4. 通过运行以下命令将 Audit all objects （审计所有对象）角色委托给 gMSA：

```
Add-DRAAssignments -Identifier "All Objects" -Users "CN=<gMSA_name>,
CN=Managed Service Accounts, DC=MyDomain, DC=corp" -Roles "Audit All
Objects"
```

要为 gMSA 配置 DRA 次管理服务器：

1. 安装次服务器。
2. 在主服务器上，将 **Configure Servers and Domains** （配置服务器和域）角色指派给次服务器服务帐户的 **Administration Servers and Managed Domains** （管理服务器和受管域）活动视图。
3. 在主服务器上，添加新的次服务器并指定次服务器服务帐户。
4. 将 gMSA 添加到 DRA 次管理服务器上的本地管理员组。
5. 在次服务器上，将所有 DRA 服务的登录帐户更改为 gMSA，然后重启动 DRA 服务