Directory and Resource Administrator

安装指南

2018 年 7 月

法律声明

关于本指南 **5**

1 入门 **7**

Directory and Resource Administrator 是什么 . . . 7
了解 Directory and Administrator 组件 . . . 8
DRA 管理服务器 . . . 8
委托和配置控制台 . . . 8
帐户和资源管理控制台 . . . 8
Web 控制台 . . . 9
报告组件 . . . 9
工作流程引擎 . . . 9
产品架构 . . . 10

2 产品安装和升级 **11**

计划部署 . . . 11
经过测试的资源建议 . . . 11
所需端口和协议 . . . 11
支持的平台 . . . 14
DRA 管理服务器要求 . . . 15
DRA Web 控制台和扩展要求 . . . 19
报告要求 . . . 20
许可要求 . . . 21
产品安装 . . . 21
安装 DRA 管理服务器 . . . 21
产品升级 . . . 25
计划 DRA 升级 . . . 25
升级前任务 . . . 26
升级 DRA 管理服务器 . . . 28
升级 DRA REST 扩展 . . . 30
升级自定义内容 . . . 31

3 产品配置 **33**

配置核对清单 . . . 33
安装或升级许可证 . . . 33
添加受管域 . . . 33
添加受管子树 . . . 34
配置 DCOM 设置 . . . 34
配置分布式 COM 用户组 . . . 34
配置域控制器和管理服务器 . . . 35

关于本指南

*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。有关支持此版本的出版物的完整列表，请访问文档网站 (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)。

与销售支持联系

若对产品、定价和功能有疑问，请与本地合作伙伴联系。如果无法与合作伙伴联系，请与我们的销售支持团队联系。

全球：	www.netiq.com/about_netiq/officelocations.asp
美国和加拿大：	1-888-323-6768
电子邮件：	info@netiq.com
网站：	www.netiq.com

联系技术支持

有关具体的产品问题，请与我们的技术支持团队联系。

全球：	www.netiq.com/support/contactinfo.asp
北美和南美：	1-713-418-5555
欧洲、中东和非洲：	+353 (0) 91-782 677
电子邮件：	support@netiq.com
网站：	www.netiq.com/support

联系文档支持

我们的目标是提供满足您的需要的文档。如果您有任何关于改进文档的建议，请单击HTML版文档任何页面底部的**评论该主题**。您还可以发送电子邮件至Documentation-Feedback@netiq.com。我们会重视您的意见，欢迎您提供建议。

联系在线用户社区

NetIQ 在线社区 NetIQ Communities 是让您可与同行及 NetIQ 专家沟通的协作网络。NetIQ Communities 上提供了更多即时信息、实用资源的有用链接，以及联系 NetIQ 专家的途径，有助于确保您掌握必要的知识，以充分发挥所依赖的 IT 投资的潜力。有关详细信息，请访问 http://community.netiq.com。

1 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。

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。

Exchange Administrator (ExA) 进一步扩展 DRA 的强大功能，提供对 Microsoft Exchange 的无缝管理。ExA 通过一个通用的用户界面，根据策略来管理邮箱、公共文件夹及跨 Microsoft Exchange 环境的通讯组列表。

DRA 和 ExA 可共同提供控制和管理 Active Directory、Microsoft Windows、Microsoft Exchange 和 Microsoft Office 365 环境所需的解决方案。

- **支持 Active Directory、Office 365、Exchange 以及 Skype for Business：** 提供对 Active Directory、本地 Exchange Server、本地 Skype for Business、Exchange Online 以及 Skype for Business Online 的一般性管理。
- **细粒度用户和管理特权访问控制：** 专利 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 和工作流程自动化之外 Active Directory 内生成的事件的审计。

了解 Directory and Administrator 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 Aegis 工作流程引擎。

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）	委托和配置控制台	主服务器
	DRA 报告中心安装 (NRC) CLI *（可选）* DRA ADSI 提供程序 *（可选）*	次服务器
Help Desk 临时管理员	帐户和资源管理控制台	次服务器
Help Desk 临时管理员	Web 控制台	安装了 DRA REST 的所有 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。

委托和配置控制台

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：** 使您能够精确指定并向助理管理员指派受管资源以及任务的访问权限。
- **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、Office 365 等）。

帐户和资源管理控制台

帐户和资源管理控制台是一个可安装的用户界面，DRA 助理管理员可通过此界面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，可通过此界面快速轻松访问DRA辅助管理员，从而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，也可以配置与 Change Guardian 服务器集成，从而能够对发生于 DRA 以外的更改进行审计。

DRA 管理员可以创建和修改自动化工作流程表单，在触发后运行例程自动化任务。

统一的更改历史记录是 Web 控制台的另一功能，该功能实现与更改历史记录服务器集成，便于审计 DRA 以外对 AD 对象所作的更改。更改历史记录报告选项包括下列内容：

- 已更改...
- ...进行的更改
- ...创建的邮箱
- 用户、组和联系人电子邮件地址的创建者为...
- 用户、组和联系人电子邮件地址的删除者为...
- ...创建的虚拟属性
- ...移动的选项

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：

- AD 对象资源报告
- AD 对象数据报告
- AD 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。

工作流程引擎

DRA与Aegis工作流程引擎集成以通过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。有关工作流程引擎的更多信息，请参见 DRA 文档网站 (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)。

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
委托和配置控制台
帐户管理控制台
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
Exchange Online
Skype Online
许可

2 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。

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	4 核 CPU（64 位）/核频率 2.0 GHz	16 GB	100 GB
DRA Web 控制台	2 核 CPU（64 位）/核频率 2.0 GHz	8 GB	100 GB
DRA 报告	4 核 CPU（64 位）/核频率 2.0 GHz	16 GB	100 GB
DRA 工作流程服务器	4 核 CPU（64 位）/核频率 2.0 GHz	16 GB	100 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"
- 将内存预留设置为 Reserve All Guest Memory(All Locked)（预留所有来宾内存（锁定所有））
- 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 **

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，DRA 客户端	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 (http://go.microsoft.com/fwlink/?LinkID=46088)（与防火墙一起使用分布式 COM）(DCOM)
TCP 50000 *	双向	DRA 管理服务器	属性复制和 DRA 服务器 - ADAM 通信。(LDAP)
TCP 50001 *	双向	DRA 管理服务器	SSL 属性复制 (ADAM)
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)
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 2010 至 2013 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 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

协议和端口	方向	目标	用法
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

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 11192 * **	出站	DRA 主机服务	用于DRAREST服务与DRA管理服务间的通信
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DRAWeb控制台、DRAPowerShell和DRA 主机服务间的通信
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 (http://go.microsoft.com/fwlink/?LinkID=46088)（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 (http://go.microsoft.com/fwlink/?LinkID=46088)（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)
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 用于与工作流程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 NetIQ 网站上的 Directory and Resource Administrator 页面： https://www.netiq.com/support

管理的系统	先决条件
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3（除公共文件夹） ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online

管理的系统	先决条件
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ 适用于 Windows PowerShell 的 Windows Azure Active Directory 模块 https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype for Business Online，Windows PowerShell 模块 https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype for Business	◆ Microsoft Skype for Business 2015
更改历史记录	◆ Change Guardian 5.0, 5.1
Web 浏览器	◆ Microsoft Internet Explorer 11, Edge ◆ Google Chrome ◆ Mozilla Firefox

DRA 管理服务器要求

DRA 对软件和帐户有下列服务器要求：

软件要求：

组件	先决条件
安装目标	**NetIQ 管理服务器操作系统：**
操作系统	◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ 仅支持 Microsoft Windows 2008 R2 升级。 **注释：** 服务器必须是所支持的 Microsoft Windows Server 本机域的成员。 **Windows DRA 接口：** ◆ Microsoft Windows Server 2012, 2012 R2, 2016 ◆ Microsoft Windows 8.1（x86 和 x64）、10（x86 和 x64）
安装程序	◆ Microsoft .Net Framework 4.5.2 及更高版本

组件	先决条件
管理服务器	**Directory and Resource Administrator：** ◆ Microsoft .Net Framework 4.5.2 及更高版本 ◆ 以下版本之一： ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Packages（x64 和 x86） ◆ Microsoft Visual C++ 2017 (Update 3) 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 Office 365/Exchange Online 管理：** ◆ 适用于 Windows PowerShell 的 Windows Azure Active Directory 模块 ◆ 适用于 IT 专业人员的 Microsoft Online Services 登录助手 ◆ Skype for Business Online，Windows PowerShell 模块 有关更多信息，请参见支持的平台。
旧 Web 组件	**Web 服务器：** ◆ Microsoft Internet Information Services (IIS) 版本 8.0、8.5、10 **Microsoft IIS 组件：** ◆ Microsoft Active Service Pages (ASP) ◆ Microsoft Active Service Pages .NET (ASP .Net) ◆ Microsoft IIS 安全角色服务 **Windows DRA 接口：** ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015 (Update 3) Redistributable Package (x86)

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

帐户	说明	许可权限
DRA 服务帐户	运行 NetIQ 管理服务所需的许可权限	◆ “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（OnePointOpConfgAdms 和 OnePointOp） **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。
DRA 管理员	供应到内置DRAAdmin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。
DRA助理Admin帐户	将通过 DRA 委托权利的帐户	◆ 将所有 DRA 辅助 Admin 帐户添加到“分布式 COM 用户”组，这样它们可以从远程客户端连接到 DRA 服务器。 **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： 向域访问帐户指派下列 Active Directory 许可权限：

- 对用户对象的完全控制
- 对计算机对象的完全控制
- 对组对象的完全控制
- 对联系人对象的完全控制
- 对组织单元对象的完全控制
- 对 Inetorgperson 对象的完全控制
- 对打印机对象的完全控制
- 对内置域对象的完全控制
- 对容器对象的完全控制
- 对 MsExchSystemObjectContainer 对象的完全控制
- 对动态分发组的完全控制
- 对公共文件夹的完全控制

向域服务帐户指定下列范围为“此对象及所有子对象”的特权：

- 允许创建计算机对象
- 允许删除计算机对象
- 允许创建联系人对象

- 允许删除联系人对象
- 允许创建组对象
- 允许删除组对象
- 允许删除 InetOrgPerson 对象
- 允许创建组织单元对象
- 允许删除组织单元对象
- 允许创建用户对象
- 允许删除用户对象
- 允许创建动态分发组
- 允许删除动态分发组
- 允许创建服务连接点
- 允许删除服务连接点
- 允许创建容器
- 允许删除容器
- 允许创建公共文件夹
- 允许删除公共文件夹

Office 365 租户访问帐户： 向 Office 365 租户访问帐户指派下列 Active Directory 许可权限：

- Office 365 中的用户管理管理员
- Exchange Online 中的收件人管理

Exchange 访问帐户： 向Exchange访问帐户指派**Organizational Management**（组织管理）角色来管理 Exchange 2010。

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

安装 DRA 之后：

- 在 DRA 安装文件夹下运行下列命令，向“已删除对象容器”委派许可权限（注意：必须由域管理员执行此命令）：

  DraDelObjsUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*Account Name*>
- 在 DRA 安装文件夹下运行下列命令，向 "NetIQReceyleBin OU" 委派许可权限（注意：只能在添加了将由 DRA 管理的相应域之后才能执行此操作）：

  DraRecycleBinUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*AccountName*>
- 向 DRA 将管理资源（如打印机、服务、事件日志、设备等）的每个计算机上的“本地管理员”组添加最小特权覆盖帐户。

- 授予最小特权覆盖帐户对供应了主目录的共享文件夹或 DFS 文件夹的“完全许可权限”。
- 向“组织管理”角色添加最小特权覆盖帐户以管理 Exchange 对象。

DRA Web 控制台和扩展要求

Web 控制台和 REST 扩展要求包括：

软件要求：

组件	先决条件
安装目标	**操作系统：** ◆ 安装了 Microsoft IIS 10 的 Microsoft Windows Server 2016、Microsoft Windows 10 ◆ 安装了 Microsoft IIS 8.0、8.5 的 Microsoft Windows Server 2012、2012 R2
DRA 主机服务	◆ Microsoft .Net Framework 4.5.2 ◆ DRA 管理服务器
DRA REST 端点和服务	◆ Microsoft .Net Framework 4.5.2
PowerShell 扩展	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

组件	先决条件
DRA Web 控制台	**Web 服务器：** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft Internet Information Service WCF （激活） **Microsoft IIS 组件：** ◆ Web 服务器 ◆ 通用 HTTP 功能 ◆ 静态内容 ◆ 默认文档 ◆ 目录浏览器 ◆ HTTP 错误 ◆ 应用程序开发 ◆ ASP ◆ 运行状况和诊断 ◆ HTTP 日志记录 ◆ 请求监视程序 ◆ 安全性 ◆ 基本鉴定 ◆ 性能 ◆ 静态内容压缩 ◆ Web 服务器管理工具

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, 2012 R2, 2016

组件	先决条件
NetIQ Reporting Center（3.2 版）	**数据库：** ◆ Microsoft SQL Server 2012, 2014, 2016 ◆ Microsoft SQL Server Reporting Service **Web 服务器：** ◆ Microsoft Internet Information Server 8.0, 8.5, 10 ◆ Microsoft IIS 组件： ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5：** 每个连接到 DRA 报告的 DRA 管理服务器都需要 .NET Framework 3.5。 **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。
DRA 报告	**数据库：** ◆ Microsoft SQL Server Integration Service ◆ Microsofte SQL Server 代理

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，您可以使用运行状况检查实用程序安装试用许可证密钥 (License1.lic)，该许可证密钥允许您在 30 天内管理数量不受限制的用户帐户和邮箱。

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

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。

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 NetIQ 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。
执行 DRA 安装	起动 DRA 安装。 **注释：** 要稍后运行安装，导航到解压缩安装媒体的位置并执行 Setup.exe。
选择 NetIQ 管理服务器组件和安装目标	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： **NetIQ 管理服务器** ◆ 日志存档资源包 ◆ NetIQ DRA SDK **旧 Web 组件** **用户界面** ◆ 帐户和资源管理 ◆ DRA ADSI 提供程序 ◆ 命令行界面 ◆ 委托和配置
校验是否符合先决条件	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成功安装 DRA 所必需的、先决条件中所缺失的软件。
接受 EULA 许可证协议	接受最终用户许可证协议条款。
选择服务器操作模式	选择主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）或选择次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“配置多主集合”（位于 *Directory and Resource Administrator 管理员指南*）。
指定安装帐户和身份凭证	◆ DRA 服务帐户 ◆ AD LDS 组 ◆ DRA 管理员 有关更多信息，请参见：DRA 管理服务器要求。
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。
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。

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：

NetIQDRAUserConsole.mst	安装帐户和资源管理控制台
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，例如 NetIQDRAUserConsole.mst。
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 DRA REST 扩展

DRA REST 扩展软件包有四种功能：

- **NetIQ DRA 主机服务：** 用于与 DRA 管理服务通信的网关。此服务必须运行于安装了 DRA 管理服务的计算机上。
- **DRA REST 服务和端点：** 提供方便 DRA Web 控制台与非 DRA 客户端请求 DRA 操作的 RESTful 接口。此服务必须运行于安装了 DRA 控制台或 DRA 管理服务的计算机上。
- **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。
- **DRA 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。

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。
安装 SSL 证书	如果 Windows Server 中尚未安装 SSL 证书，您应在运行安装前先安装证书。
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。

步骤	细节
执行DRAREST扩展安装程序	DRA安装包解压缩安装媒体完成后，系统将提示您起动DRA安装。导航到解压缩安装媒体的位置，右键单击 DRARESTExtensionsInstaller.exe 文件并选择**以管理员身份运行**。
接受 EULA 许可证协议	接受最终用户许可证协议条款。
选择组件并 指定安装的目标位置	在安装**选择组件**对话框中，安装所有选项：DRA 主机服务、DRA REST 端点和服务、PowerShell 扩展及 DRA Web 控制台。 接受默认安装位置 C:\Program Files (x86)\NetIQ\DRA Extensions 或指定其他安装位置。
校验是否符合先决条件	**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成功安装 DRA 所必需的、先决条件中所缺失的软件。
指定要以其身份运行的服务帐户	默认情况下，显示DRA服务器的现有服务帐户。指定服务帐户口令。有关为DRA管理服务器设置服务帐户的更多信息，请参见 DRA 管理服务器要求。
指定 REST 服务 SSL 证书	选择将用于 REST 服务的 SSL 证书，并指定 REST 和主机服务端口。
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。

安装工作流程服务器

有关安装工作流程服务器的信息，请参见 Aegis 管理员指南。

安装 DRA 报告

DRA 报告需要您安装两个来自 NetIQ DRA 安装包的可执行文件：NRCSetup.exe 和 DRAReportingSetup.exe。

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 框架，来满足 DRA 产品安装程序先决条件。
执行 NetIQ Reporting Center (NRC) 安装	DRA 安装包解压缩安装媒体完成后，导航到解压缩安装媒体的位置并执行 NRCSetup.exe。
选择 NetIQ Reporting Center 组件	在安装**选择组件**对话框中，使用默认的 "NetIQ Reporting Center" 组件安装四个 NRC 组件。
指定安装目标位置	接受默认安装位置 C:\Program Files (x86)\NetIQ\Reporting Center 或指定其他安装位置。

步骤	细节
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成功安装 DRA 所必需的、先决条件中所缺失的软件。 **重要：** 安装 NRC 前，必须在报告服务器上手动安装 .NET Framework 3.5。
接受 EULA 许可证协议	接受最终用户许可证协议条款。
安装配置数据库	使用 **Configuration Database Installation - SQL Server Logon**（配置数据库安装 - SQL Server 登录）对话框中的默认设置或提供 SQL 鉴定来完成 NRC 安装。如果 SQL Server 安装使用默认实例，实例字段应留空。
执行 DRA 报告安装	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。
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。

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 *Directory and Resource Administrator 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AA数量。如果大多数AA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 AA 需要委托和配置控制台。您可以使用以下任意方法获得此信息：
  - 查看哪些 AA 与内置 AA 组相关。
  - 查看哪些 AA 与内置 ActiveView 相关。
  - 使用 Directory and Resource Administrator 报告生成安全模型报告，例如 ActiveView 助理 Admin 细节和助理 Admin 组报告。

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

  通知这些 AA 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（AA 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

注释： 如果需要恢复 AD LDS 实例备份，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。

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AA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 AA 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AA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AA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AA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. 启动 MMC 界面。
3. 在左侧窗格中，展开**配置管理**。
4. 单击**管理服务器**。
5. 在右侧窗格中，选择此服务器集的相应主管理服务器。
6. 单击**属性**。
7. 在同步日程表选项卡中，单击**立即刷新**。
8. 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\MissionCritical 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。

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。

在DRA9.2或更高版本中，工作流程自动化服务器配置储存在ADLDS中，而不是在注册表中。从DRA 9.1或更早版本更新到DRA9.2或更高版本时，注册表配置自动移动到ADLDS并复制到所有次服务器。

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。

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。
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，安装一个运行最新版本 DRA 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。
升级次服务器	升级 MMS 中的次管理服务器。
升级 DRA 报告	升级 DRA 报告。
升级 REST 扩展	运行 DRA REST 扩展安装程序。
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。

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 AA 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： 有关更多详细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AA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 AA 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AA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 AA 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AA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AA不会停机。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AA来说，要通过安装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 或 ADSI 提供程序执行批处理，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AA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AA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DRA组件版本。如果计划逐步升级AA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. 让使用此服务器的 AA 安装相应的用户界面，例如帐户和资源管理控制台。
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AA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AA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AA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。

升级 DRA 报告组件

升级 DRA 报告前，确保您的环境满足针对 NRC 3.2 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 DRA 文档网站中的 *Reporting Center 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“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。
运行 NRC 安装程序	*（有条件）：*如果NRCWeb服务安装在另一台计算机上，则登录安装Web服务的计算机并运行 NRCSetup.exe 来升级 NRC Web 服务。 **注释：** 如果配置数据库安装在单独的服务器上，则需要先进行升级
在客户端计算机上运行 NRC 安装程序	在所有 NRC 客户端计算机上运行 NRCSetup.exe。
启用 DRA 报告支持	在主管理服务器上，启用“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DRA文档网站中的 *NetIQ Reporting Center 报告指南*。

升级 DRA REST 扩展

要将 Web 控制台和 REST 扩展升级到 Directory and Resource Administrator 9.2，您当前正在使用的 DRA 必须是 9.0.1 或更新版本。有关要求信息，请参见 DRA Web 控制台和扩展要求。

要升级 DRA Web 控制台和扩展：

1. 下载 DRA 安装包后，导航到解压缩安装媒体的位置，右键单击 DRARESTExtensionsInstaller.exe 文件并选择**以管理员身份运行**。
2. 按照安装向导中的说明进行操作，直至安装完成，单击**完成**。

有关安装向导中各步骤的更详细信息，请参见新安装步骤：安装 DRA REST 扩展。

升级自定义内容

升级到新版本DRA后，您想要保留Web服务器上的Web控制台的所有自定义设置。为方便保留，DRA 在 DRA REST 扩展安装程序中内置了一个自定义升级实用程序。此实用程序在您运行 DRARESTExtensionsInstaller.exe时自动运行，从而升级Web服务器上的REST扩展。您也可以在安装之外，从 DRA 安装目录手动重新运行此实用程序。

此自定义升级实用程序的一部分进程会在升级开始前备份自定义。在升级过程中，实用程序将创建因升级而产生的所有更改的日志文件，还会包含无法自动更新的所有自定义项目的警告。

作为最佳实践，我们建议您在升级后查看该日志。如有需要，您可以从备份文件夹复制自定义，回滚到升级前自定义。自定义升级实用程序打开时，可以定义升级自定义的文件夹路径，或者您可以使用自动填充的默认路径。

下面列出的是升级自定义和自定义备份的默认路径：

- 默认自定义文件夹路径：C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom
- 默认的备份文件夹：
  $CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup

3 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。

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**委托和配置**	使用 DRA 服务帐户，登录安装了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。

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 NetIQ 公司为您提供的试用版许可证密钥文件 (TrialLicense.lic)。

要升级现有许可证或试用许可证，打开委托和配置控制台，导航到**配置管理** > **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。

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 *Directory and Resource Administrator 管理员指南*中的“配置超速缓存
”。

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 域的受管子树。您可以在委托和配置控制台中添加任何想通过高级配置节点管理的缺少的子树。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 *Directory and Resource Administrator 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 *Directory and Resource Administrator 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 *Directory and Resource Administrator 管理员指南*中的“配置超速缓存”。

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。

配置分布式 COM 用户组

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。此成员资格应包含 DRA 服务帐户和所有辅助 Admin。

要配置分布式 COM 用户组：

1. 以 DRA 管理员身份登录 DRA 客户端计算机。
2. 选择委托和配置控制台。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**。

配置域控制器和管理服务器

配置运行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**设置 > 系统和安全 > 控制面板**。
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。