法律声明

目录

关于本指南

本*管理员指南*提供有关 Directory and Resource Administrator (DRA) 产品的概念信息。此指南定义了术语和各种相关概念，同时提供了许多配置和操作任务的逐步指导。

适用对象

本书提供的信息适用于负责了解管理概念及实施安全的分布式管理模型的人员。

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 (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html)。

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 以及 Skype for Business：**提供对 Azure 和本地 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。

2 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）	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。

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。

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

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

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)
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

协议和端口	方向	目标	用法
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 11192 * **	出站	DRA 主机服务	用于 DRA REST 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 DRA Web 控制台、 DRA PowerShell 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*（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)

协议和端口	方向	目标	用法
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 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： ◆ Skype for Business Online https://www.microsoft.com/en-us/download/details.aspx?id=39366 ◆ Azure Active Directory V2 (AzureAD) 2.0.2.4 或更高版本 ◆ AzureRM.Profile 5.8.2 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 Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online
Skype for Business	◆ Microsoft Skype for Business 2015
更改历史记录	◆ Change Guardian 5.1 或更高版本
数据库	◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server 2017 ◆ Microsoft SQL Server 2019
Web 浏览器	◆ Microsoft Internet Explorer 11 ◆ Google Chrome ◆ Mozilla Firefox

管理的系统	先决条件
工作流程自动化	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016

DRA 管理服务器、 Web 控制台和 REST 扩展要求

DRA 组件需要以下软件和帐户：

- 软件要求 （第 28 页）
- 服务器域 （第 30 页）
- 帐户要求 （第 31 页）
- 最小特权 DRA 访问帐户 （第 32 页）

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 R2、 2016、 2019 **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 ◆ Microsoft Windows 8.1 （x86 和 x64）、 10 （x86 和 x64）
安装程序	◆ Microsoft .Net Framework 4.6.2 及更高版本

组件	先决条件
管理服务器	**Directory and Resource Administrator：** ◆ Microsoft .Net Framework 4.6.2 及更高版本 ◆ Microsoft Visual C++ 2013 Redistributable Packages (x64) 和 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 Internet 信息服务 URL 重写模块 ◆ Microsoft Internet 信息服务应用程序请求路由 **Microsoft Office 365/Exchange Online 管理：** ◆ 适用于 Windows PowerShell 的 Windows Azure Active Directory 模块 ◆ Skype for Business Online， Windows PowerShell 模块 有关更多信息，请参见支持的平台。
用户界面	**DRA 界面：** ◆ Microsoft .Net Framework 4.6.2 ◆ Microsoft Visual C++ 2017 (Update 3) Redistributable Packages（x64 和 x86）
DRA 主机服务	◆ Microsoft .Net Framework 4.6.2 ◆ DRA 管理服务器
DRA REST 端点和服务	◆ Microsoft .Net Framework 4.6.2
PowerShell 扩展	◆ Microsoft .Net Framework 4.6.2 ◆ PowerShell 5.1 或更高版本

组件	先决条件
DRA Web 控制台	**Web 服务器：** ◆ Microsoft .Net Framework 4.x > WCF 服务 > HTTP 激活 ◆ Microsoft Internet Information Server 8.0, 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 **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

服务器域

组件	操作系统
DRA 服务器	◆ 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）：
		  ◆ 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 “ 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。
DRA 助理 Admin 帐户	将通过 DRA 委托权限的帐户	◆ 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

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 MsExchDynamicDistiributionList 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

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。
- 如果未将 REST 服务器与 DRA 管理服务器安装在同一服务器上，则正在运行的 REST 服务帐户必须对 Active Directory 中的 REST 服务器具有完全控制权限。例如，设置对 CN=DRARestServer,CN=System,DC=myDomain,DC=com 的完全控制

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 租户访问帐户：向 Azure 租户访问帐户指派下列 Azure Active Directory 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

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：添加所需的域或由 DRA 管理所需的域后，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。

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

组件	先决条件
NetIQ Reporting Center （3.2 版）	**数据库：** ◆ Microsoft SQL Server 2016、 2017、 2019 ◆ 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：** ◆ 运行 NRC 安装程序所需 ◆ 在 DRA 主服务器上进行 DRA Reporting Service 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。
DRA 报告	**数据库：** ◆ Microsoft SQL Server Integration Service ◆ 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)”。

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。
- **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。
- **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。
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。

步骤	细节
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 ◆ DRA SDK **REST 服务** **用户界面** ◆ ADSI 提供程序 ◆ 命令行界面 ◆ 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。
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。 有关多主集合的信息，请参见 *《Directory and Resource Administrator 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 有关更多信息，请参见：DRA 管理服务器、 Web 控制台和 REST 扩展要求。
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。
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。

步骤	细节
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*。

安装工作流程服务器

有关安装工作流程服务器的信息，请参见 *Workflow Automation Administrator Guide* （《工作流程自动化管理员指南》）。

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 ActiveView 相关。
  - 使用 Directory and Resource Administrator Reporting 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。

重要：

- 如果您以前的 DRA 版本已安装 Account and Resource Management （ARM，帐户和资源管理）控制台，则在升级过程中将去除 ARM 控制台。

- 从 DRA 9.x 版本升级 DRA 服务器时，将从 DRA 中去除所有受管租户。要继续通过 Azure 使用这些租户，需要在升级后添加租户。有关添加租户的信息，请参见 *《DRA 管理员指南》*中的 “ 创建 Azure 应用程序并添加 Azure 租户 ”。
- 由于 DRA 10 不支持 Exchange 2010，因此从 DRA 9.x 升级时，将禁用 Exchange。要在升级后继续执行 Exchange 操作，请在 Delegation and Configuration （委托和配置）控制台中禁用并重新启用 **Enable Exchange Policy** （启用 Exchange 策略）选项。需要 “ 应用 ” 这两项更改才能重设置策略。

  有关此策略配置的信息，请参见 *《DRA 管理员指南》*中的 “ 启用 Microsoft Exchange”。

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：*如果您使用组托管服务帐户 (gMSA) 作为 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，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 43 页）
- 同步之前的 DRA 版本服务器集 （第 43 页）
- 备份管理服务器注册表 （第 44 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：将 DRA 服务器从 DRA 9.x 版本升级到 DRA 10.x 版本时，DRA 升级安装会进行以下更改：

- 将 UCH 和工作流程自动化服务器用户配置从 Web 控制台移动到 Delegation and Configuration （委托和配置）控制台
- 从服务器中去除旧的 Web 组件。
- 去除任何受管租户。

  有关添加租户的信息，请参见 *《DRA 管理员指南》*中的 " 管理租户 "。
- 如果您在较早版本中安装了 Account and Resource Management （帐户和资源管理）控制台，在升级到 DRA 10.x 版本时，将去除 Account and Resource Management （帐户和资源管理）控制台。
- 在 MMS 升级期间，首先升级主服务器，然后再升级次服务器。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。
- 由于 DRA 10 不支持 Exchange 2010，因此从 DRA 9.x 升级时，将禁用 Exchange。要在升级后继续执行 Exchange 操作，请在 Delegation and Configuration （委托和配置）控制台中禁用并重新启用 **Enable Exchange Policy** （启用 Exchange 策略）选项。需要 " 应用 " 这两项更改才能重设置策略。

  有关此策略配置的信息，请参见*启用 Microsoft Exchange*。

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。

步骤	细节
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“管理租户”。

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。

如果经常通过命令行界面、 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。

升级 Reporting

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 *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》）。

III 组件和进程配置

本章提供有关首次配置 DRA 的信息，包括服务器和服务器自定义、控制台和控制台自定义、Azure 管理、公共文件夹管理以及连接到服务器。

6 初步配置

本节介绍首次安装 Directory and Resource Administrator 时所需进行的配置步骤。

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
安装 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。
配置 DRA 服务器和功能	配置 MMS、 Clone Exceptions （克隆例外项）、 File Replication （文件复制）、 Event Stamping （事件标记）、超速缓存、 AD LDS、动态组、回收站、报告、统一的更改历史记录和工作流程服务器。
配置 Delegation and Configuration （委托和配置）客户端	配置如何在 Delegation and Configuration （委托和配置）客户端中访问和显示项目。
配置 Web 客户端	配置自动注销、证书、服务器连接和鉴定组件

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，请打开 Delegation and Configuration （委托和配置）控制台，然后导航到 **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。

您可以通过 Delegation and Configuration （委托和配置）控制台查看产品许可证。要查看产品许可证，请导航到文件菜单 > **DRA Properties** （DRA 属性） > **License** （许可证）。

配置 DRA 服务器和功能

使用 DRA 管理 Active Directory 任务的最小特权访问权限需要配置许多组件和过程。其中包括常规和客户端组件配置。本节介绍需要为 DRA 配置的常规组件和过程的相关信息。

- 配置多主集合 （第 52 页）
- 管理 Clone Exceptions （克隆例外项）（第 54 页）

- 文件复制 （第 55 页）
- 事件标记 （第 57 页）
- Azure Sync （第 57 页）
- 为组启用多个管理员 （第 58 页）
- 加密通信 （第 58 页）
- 定义虚拟属性 （第 58 页）
- 配置超速缓存 （第 60 页）
- 启用 Active Directory 打印机集合 （第 62 页）
- AD LDS （第 62 页）
- 动态组 （第 62 页）
- 配置回收站 （第 62 页）
- 报告配置 （第 63 页）
- 统一的更改历史记录 （第 65 页）
- 委托工作流程自动化服务器配置权限 （第 65 页）
- 配置工作流程自动化服务器 （第 66 页）
- 委托 LDAP 搜索权限 （第 67 页）

配置多主集合

MMS 环境使用多个管理服务器管理同一组域和成员服务器。一个 MMS 包含一个主管理服务器和多个次管理服务器。

管理服务器的默认模式为主服务器。在将次服务器添加到 MMS 环境时，请记住次管理服务器只能属于一个服务器集。

要确保集合中的每个服务器都管理相同的数据，请定期将次服务器与主管理服务器同步。要减少维护，请对域林中的所有管理服务器使用相同的服务帐户。

重要：

- 安装次服务器时，在安装程序中选择**次管理服务器**。
- 新的 DRA 次服务器版本必须与 DRA 主服务器版本相同，以确保主服务器中的所有功能在次服务器中均可用。

添加次管理服务器

您可以将次管理服务器添加到 Delegation and Configuration （委托和配置）客户端中的现有 MMS。要添加次服务器，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

注释：要成功添加新的次服务器，必须先在管理服务器计算机上安装 Directory and Resource Administrator 产品。有关更多信息，请参见安装 DRA 管理服务器。

要添加次管理服务器，请右键单击 Configuration Management （配置管理）节点中的 **Administration Servers** （管理服务器），然后选择 **Add Secondary Server** （添加次服务器）。

升级次管理服务器

您可以将次管理服务器升级为主管理服务器。将次管理服务器升级为主管理服务器时，现有主管理服务器将成为服务器集中的次管理服务器。要升级次管理服务器，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。在升级次管理服务器之前，请同步 MMS 以使其具有最新配置。

有关同步 MMS 的信息，请参见安排同步。

注释：新升级的主服务器只能连接到升级过程中可用的次服务器。如果次服务器在升级过程中变得不可用，请联系技术支持。

要升级次管理服务器：

1. 导航到 **Configuration Management** （配置管理） > **Administration Servers** （管理服务器）节点。
2. 在右侧窗格中，选择要升级的次管理服务器。
3. 在“任务”菜单上，单击 **Advanced** （高级） > **Promote Server** （升级服务器）。

重要：如果次服务器的服务帐户与主服务器不同，或次服务器安装在与主服务器不同的域（受信任域 / 不可信域）中，并且您升级次服务器，请确保在升级次服务器之前委托以下角色：**Audit All Objects** （审计所有对象）、**Configure Servers and Domains** （配置服务器和域）以及 **Generate UI Reports** （生成用户界面报告）。然后校验 MMS 同步是否成功。

降级主管理服务器

您可以将主管理服务器降级为次管理服务器。要降级主管理服务器，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

要降级主管理服务器：

1. 导航到 **Configuration Management** （配置管理） > **Administration Servers** （管理服务器）节点。
2. 在右侧窗格中，选择要降级的主管理服务器。
3. 在“任务”菜单上，单击 **Advanced** （高级） > **Demote Server** （降级服务器）。
4. 指定要指派为新主管理服务器的计算机，然后单击**确定**。

安排同步

同步将确保 MMS 中的所有管理服务器使用相同的配置数据。您可以随时手动同步服务器，但默认日程表设置为每 4 小时同步一次 MMS。您可以修改此日程表以根据企业需要进行定制。

要修改同步日程表或手动同步 MMS 服务器，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

要访问同步日程表或手动同步，请导航到 **Configuration Management** （配置管理） > **Administration Servers** （管理服务器），然后使用所选服务器上的任务菜单或右键单击选项。同步日程表位于选定服务器的 " 属性 " 中。

了解同步选项

对于同步 MMS 服务器，基本上有四种不同的选项：

- 选择主服务器并同步所有次服务器 Synchronize All Servers （同步所有服务器）
- 选择次服务器并仅同步该服务器
- 独立配置主服务器和次服务器的同步日程表
- 配置所有服务器的同步日程表。在主服务器同步日程表中选择以下设置时，将启用此选项：

  Configure secondary Administration servers when refreshing the primary Administration server （刷新主管理服务器时配置次管理服务器）

注释：如果取消选中此选项，配置文件将按主服务器日程表复制到次服务器上，但此时次服务器不会装载这些配置文件；它们将根据次服务器上配置的日程表进行装载。如果服务器位于不同的时区，这将非常有用。例如，您可以将所有服务器配置为在午夜刷新其配置，即使由于时区的原因可能是不同的时间。

管理 Clone Exceptions （克隆例外项）

使用 Clone Exceptions （克隆例外项），您可以定义在克隆其中一个对象时不会复制的用户、组、联系人和计算机的属性。

通过相应的权限，您可以管理 Clone Exceptions （克隆例外项）。 Manage Clone Exceptions （管理克隆例外项）角色将授予查看、创建和删除 Clone Exceptions （克隆例外项）的权限。

要查看或删除现有克隆例外项或创建新克隆例外项，请导航到 **Configuration Management** （配置管理） > **Clone Exceptions** （克隆例外项） > 任务或右键单击菜单。

文件复制

创建自定义工具时，可能需要先在 DRA Delegation and Configuration （委托和配置）控制台计算机上安装自定义工具使用的支持文件，然后自定义工具才能运行。您可以使用 DRA 的 File Replication （文件复制）功能快速轻松地将自定义工具支持文件从主管理服务器复制到 MMS 中的次管理服务器以及 DRA 客户端计算机。 File Replication （文件复制）还可用于将触发器脚本从主服务器复制到次服务器。

您可以同时使用自定义工具和 File Replication （文件复制），以确保 DRA 客户端计算机可以访问自定义工具文件。 DRA 将自定义工具文件复制到次管理服务器，以确保连接到次管理服务器的 DRA 客户端计算机可以访问自定义工具。

在 MMS 同步过程中， DRA 会将主管理服务器上的自定义工具文件复制到次管理服务器。当 DRA 客户端计算机连接到管理服务器时， DRA 会将自定义工具文件下载到 DRA 客户端计算机。

注释：DRA 会将自定义工具文件下载到 DRA 客户端计算机上的以下位置：

{DRAInstallDir}\{MMS ID}\Download

MMSID 是 DRA 下载自定义工具文件的多主集合的标识。

上载用于复制的自定义工具文件

将文件上载到主管理服务器时，指定要上载和在 MMS 集中的主管理服务器和所有次管理服务器之间复制的文件。 DRA 允许您上载库文件、脚本文件和可执行文件。

“ 复制文件 ” 角色允许您在 MMS 和 DRA 客户端计算机中将文件从主管理服务器复制到次管理服务器。“ 复制文件 ” 角色包含以下权限：

- **从服务器删除文件：**此权限允许 DRA 删除主管理服务器、次管理服务器和 DRA 客户端计算机上不再存在的文件。
- **设置文件信息：**此权限允许 DRA 更新次管理服务器上文件的文件信息。
- **将文件上载到服务器：**此权限允许 DRA 将文件从 DRA 客户端计算机上载到主管理服务器。

注释：您可以使用 Delegation and Configuration （委托和配置）控制台中的 File Replication （文件复制）用户界面，一次仅上载一个文件以进行复制。

要将自定义工具文件上载到主管理服务器：

1. 导航到 **Configuration Management** （配置管理） > **File Replication** （文件复制）。
2. 在 “ 任务 ” 菜单上，单击 **Upload File** （上载文件）。
3. 要搜索并选择要上载的文件，请单击 **Browse** （浏览）。
4. *要将所选文件下载到所有 DRA 客户端计算机*，请选中 **Download to all client computers** （下载到所有客户端计算机）复选框。
5. *如果要注册 COM 库*，请选中 **Register COM library** （注册 COM 库）复选框。

6 单击确定。

注释：

- DRA 会将脚本文件或需要复制到其他次管理服务器的支持文件上载到主管理服务器的 *{DRAInstallDir}*\FileTransfer\Replicate 文件夹中。
  {DRAInstallDir}\FileTransfer\Replicate 文件夹也称为 *{DRA_Replicated_Files_Path}*。
- DRA 会将脚本文件或需要复制到 DRA 客户端计算机的支持文件上载到主管理服务器的 *{DRAInstallDir}*\FileTransfer\Download 文件夹中。
- 在下次安排好的同步或手动同步期间，上载到主管理服务器的自定义工具文件将分发给次管理服务器。

在管理服务器之间复制多个文件

如果要在 MMS 中的主管理服务器和次管理服务器之间上载和复制多个文件，则可以手动上载这些文件以进行复制，方法是将文件复制到位于以下位置的主管理服务器复制目录：

{DRAInstallDir}\FileTransfer\Replicate

安装 DRA 时创建复制目录。

管理服务器可自动识别复制目录中的文件，并在下次安排好的同步期间在管理服务器之间复制文件。同步后， DRA 会在 Delegation and Configuration （委托和配置）控制台的 File Replication （文件复制）窗口中显示上载的文件。

注释：如果要复制的文件包含必须注册的 COM 库，则无法手动将文件复制到管理服务器复制目录。您必须使用 Delegation and Configuration （委托和配置）控制台上载每个文件并注册 COM 库。

将多个文件复制到 DRA 客户端计算机

如果要在主管理服务器和 DRA 客户端计算机之间复制多个文件，则可以将这些文件复制到主管理服务器上的客户端复制目录，该目录位于以下位置：

{DRAInstallDir}\FileTransfer\Download

安装 DRA 时创建客户端复制目录。

管理服务器可自动识别 Download 文件夹中的文件，并在下次安排好的同步期间将文件复制到次管理服务器。同步后， DRA 会在 Delegation and Configuration （委托和配置）控制台的 File Replication （文件复制）窗口中显示上载的文件。 DRA 客户端计算机在复制后首次连接到管理服务器时， DRA 会将复制的文件下载到 DRA 客户端计算机。

注释：如果要复制的文件包含必须注册的 COM 库，则无法将文件复制到管理服务器下载目录。您必须使用 Delegation and Configuration （委托和配置）控制台上载每个文件并注册 COM 库。

事件标记

启用 AD 域服务审计时， DRA 事件将记录为由 DRA 服务帐户或域访问帐户 （如果已配置）生成。 Event Stamping （事件标记）通过生成一个额外的 AD DS 事件以标识执行操作的助理管理员，从而使此功能更进一步。

要生成这些事件，您必须在 DRA 管理服务器上配置 AD DS 审计并启用 Event Stamping （事件标记）。启用 Event Stamping （事件标记）后，您将能够查看助理管理员在 Change Guardian 事件报告中所做的更改。

- 要配置 AD DS 审计，请参见 Microsoft 参考 *AD DS Auditing Step-by-Step Guide* （AD DS 审计逐步指南）
- 要配置 Change Guardian 集成，请参见配置统一的更改历史记录服务器。
- 要启用 Event Stamping （事件标记），请以 DRA 管理员身份打开 Delegation and Configuration （委托和配置）控制台，然后执行以下操作：

  1. 导航到 **Configuration Management** （配置管理） > **Update Administration Server Options** （更新管理服务器选项） > **Event Stamping** （事件标记）。
  2. 选择对象类型，然后单击 **Update** （更新）。
  3. 选择要用于该对象类型的 Event Stamping （事件标记）的属性。

     DRA 当前支持用户、组、联系人、计算机和组织单元的 Event Stamping （事件标记）。

     DRA 还要求每个受管域的 AD 纲要中都存在属性。如果在配置 Event Stamping （事件标记）后添加受管域，则应注意这一点。如果要添加不包含所选属性的受管域，则不会使用 Event Stamping （事件标记）数据审计该域中的操作。

     DRA 将修改这些属性，因此您应选择 DRA 或环境中任何其他应用程序未使用的属性。

有关 Event Stamping （事件标记）的更多信息，请参见 Event Stamping （事件标记）如何工作。

Azure Sync

Azure Sync 使您能够实施无效字符和字符长度策略以防止目录同步失败。选择此选项将确保与 Azure Active Directory 同步的任何属性都将限制无效字符并实施字符长度限制。

要启用 Azure Sync：

1. 在左侧窗格中，单击 **Configuration Management** （配置管理）。
2. 在右侧窗格的 Common Tasks （常见任务）下，单击 **Update Administration Server Options** （更新管理服务器选项）。
3. 在 Azure Sync 选项卡上，选择 **Enforce online mailbox policies for invalid characters and character length** （针对无效字符和字符长度实施联机邮箱策略）。

为组启用多个管理员

当您启用支持多个管理员管理一个组时，系统将使用两个默认属性之一来储存组管理员。运行 Microsoft Exchange 时的属性是 msExchCoManagedByLink 属性。未运行 Microsoft Exchange 时的默认属性是 nonSecurityMember 属性。后一个选项可以修改。但是，如果您需要更改此设置，我们建议您联系技术支持以确定相应的属性。

要为组启用多管理员支持：

1. 在左侧窗格中，单击 **Configuration Management** （配置管理）。
2. 在右侧窗格的 Common Tasks （常见任务）下，单击 **Update Administration Server Options** （更新管理服务器选项）。
3. 在 Enable Support for Group Multiple Managers （启用组多管理员支持）选项卡上，选中 **Enable support for group's multiple managers** （启用组多管理员支持）复选框。

加密通信

此功能允许您启用或禁用 Delegation and Configuration （委托和配置）客户端与管理服务器之间使用加密通信。默认情况下， DRA 会加密帐户口令。此功能不会对 Web 客户端或 PowerShell 通信进行加密，此加密由服务器证书单独处理。

使用加密通信会影响性能。默认情况下禁用加密通信。如果启用此选项，则会在用户界面和管理服务器之间的通信期间对数据进行加密。DRA 使用 Microsoft 标准加密进行远程过程调用 (RPC)。

要启用加密通信，请导航到 **Configuration Management** （配置管理） > **Update Administration Server Options** （更新管理服务器选项） > **General** （常规）选项卡，然后选中 **Encrypted Communications** （加密通信）复选框。

注释：要加密管理服务器和用户界面之间的所有通信，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

定义虚拟属性

使用虚拟属性，您可以创建新属性，并将这些属性与用户、组、动态分发组、联系人、计算机和 OU 相关联。虚拟属性允许您创建新属性，而无需扩展 Active Directory 纲要。

使用虚拟属性，您可以向 Active Directory 中的对象添加新属性。您只能在主管理服务器上创建、启用、禁用、关联和取消关联虚拟属性。 DRA 会储存您在 AD LDS 中创建的虚拟属性。在 MMS 同步过程中， DRA 会将主管理服务器上的虚拟属性复制到次管理服务器。

通过相应的权限，您可以管理虚拟属性。 Manage Virtual Attributes （管理虚拟属性）角色将授予创建、启用、关联、解除关联、禁用和查看虚拟属性的权限。

创建虚拟属性

您需要具备 *Create Virtual Attributes* （创建虚拟属性）权限以创建虚拟属性，并且需要具备 *View Virtual Attributes* （查看虚拟属性）权限以查看虚拟属性。

要创建虚拟属性，请导航到 **Configuration Management** （配置管理） > **Virtual Attributes** （虚拟属性） > **Managed Attributes** （受管属性）节点，然后单击 " 任务 " 菜单中的 **New Virtual Attribute** （新建虚拟属性）。

将虚拟属性与对象关联

您只能将启用的虚拟属性与 Active Directory 对象关联。将虚拟属性与对象关联后，虚拟属性可作为对象属性的一部分使用。

要通过 DRA 用户界面公开虚拟属性，需要创建自定义属性页。

要将虚拟属性与对象关联，请导航到 **Configuration Management** （配置管理） > **Virtual Attributes** （虚拟属性） > **Managed Attributes** （受管属性）节点，右键单击要使用的虚拟属性，然后选择 **Associate** （关联） > （对象类型）。

注释：

- 您只能将虚拟属性与用户、组、动态分发组、计算机、联系人和 OU 关联。
- 将虚拟属性与对象关联时， DRA 会自动创建两个默认的自定义权限。助理管理员需要这些自定义权限来管理虚拟属性。

解除关联虚拟属性

您可以解除虚拟属性与 Active Directory 对象的关联。您创建的任何新对象都不会将解除关联的虚拟属性显示为对象属性的一部分。

要解除虚拟属性与 Active Directory 对象的关联，请导航到 **Configuration Management** （配置管理） > **Virtual Attributes** （虚拟属性） > **Managed Classes** （受管类） > （对象类型）节点。右键单击虚拟属性，然后选择 **Disassociate** （解除关联）。

禁用虚拟属性

如果虚拟属性与 Active Directory 对象没有关联，则可以禁用虚拟属性。禁用虚拟属性时，管理员无法查看虚拟属性或将虚拟属性与对象关联。

要禁用虚拟属性，请导航到 **Configuration Management** （配置管理） > **Managed Attributes** （受管属性）。右键单击列表窗格中的所需属性，然后选择 **Disable** （禁用）。

配置超速缓存

管理服务器将构建并维护一个**帐户超速缓存**，其中包含受管域的 Active Directory 部分。在管理用户帐户、组、联系人和计算机帐户时， DRA 将使用帐户超速缓存来提高性能。

要安排超速缓存刷新时间或查看超速缓存状态，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

注释：要在包含受管子树的域中执行增量帐户超速缓存刷新，请确保服务帐户对 Deleted Objects （已删除对象）容器以及子树域中的所有对象具有读取访问权限。您可以使用 Deleted Objects Utility （已删除对象实用程序）来校验和委托相应的许可权限。

完全和增量刷新

增量帐户超速缓存刷新仅更新自上次刷新以来更改的数据。增量刷新提供了一种简化的方法来跟上不断变化的 Active Directory。使用增量刷新可快速更新帐户超速缓存，同时对企业产生的影响最小。

重要：Microsoft Server 将连接到 WinRM/WinRS 会话的并发用户数量限制为五个，将每个用户的壳层数量限制为五个，以确保针对 DRA 次服务器，同一用户帐户限制为五个壳层。

增量刷新会更新以下数据：

- 新建和克隆的对象
- 已删除和已移动的对象
- 组成员资格
- 已修改对象的所有超速缓存对象属性

完全帐户超速缓存刷新将重建指定域的 DRA 帐户超速缓存。

注释：正在运行完全帐户超速缓存刷新时， DRA 用户将无法使用该域。

执行完全帐户超速缓存刷新

要刷新帐户超速缓存，您必须具备相应权限，例如内置 “Configure Servers and Domains” （配置服务器和域）角色中所包含的权限。

要立即执行完全帐户超速缓存刷新：

1. 导航到 **Configuration Management** （配置管理） > **Managed Domains** （受管域）。
2. 右键单击所需的域，然后选择**属性**。
3. 单击 **Full refresh** （完全刷新）选项卡中的 **Refresh Now** （立即刷新）。

默认安排的时间

刷新帐户超速缓存的频率取决于企业更改的频率。使用增量刷新经常更新帐户超速缓存，以确保 DRA 具有关于 Active Directory 的最新信息。

默认情况下，管理服务器在以下时间执行增量帐户超速缓存刷新：

域类型	默认安排的刷新时间
受管域	每 5 分钟
受信任域	每小时

您无法安排 FACR ；但是， DRA 在以下情况下会运行自动 FACR：

- 首次配置受管域后。
- 将 DRA 从以前版本升级到新的完整版本后。
- 安装 DRA 服务包后。

执行完全帐户超速缓存刷新可能需要几分钟。

注意事项

您必须定期刷新帐户超速缓存以确保 DRA 具有最新信息。在执行或安排帐户超速缓存刷新之前，请查看以下注意事项：

- 要执行增量帐户超速缓存刷新，管理服务器服务帐户或访问帐户必须具有对受管域或受信任域的 Active Directory 中已删除对象的访问许可权限。
- 当 DRA 执行帐户超速缓存刷新时，管理服务器不包括来自受信任域的域本地安全组。由于超速缓存不包含这些组，因此 DRA 不允许您将域本地安全组从受信任域添加到受管成员服务器上的本地组。
- 如果从帐户超速缓存刷新中省略受信任域，则管理服务器也会从域配置刷新中省略该域。
- 如果在帐户超速缓存刷新中包含先前省略的受信任域，请对受管域执行完全帐户超速缓存刷新。这可确保受管域的管理服务器上的帐户超速缓存正确反映受管域和受信任域中的组成员资格数据。
- 如果将增量帐户超速缓存刷新间隔设置为 **Never** （从不），则管理服务器仅执行完全帐户超速缓存刷新。完全帐户超速缓存刷新可能需要一些时间，在此期间您无法管理此域中的对象。
- DRA 无法自动确定何时通过其他工具（如 Microsoft Directory Service）进行更改。在 DRA 之外执行的操作可能会影响超速缓存信息的准确性。例如，如果使用其他工具将邮箱添加到用户帐户，则在更新帐户超速缓存之前，无法使用 Exchange 管理此邮箱。
- 执行完全帐户超速缓存刷新会删除超速缓存中保留的上次登录统计信息。然后，管理服务器将从所有域控制器收集最新的登录信息。

启用 Active Directory 打印机集合

默认情况下禁用 AD 打印机集合。要启用 AD 打印机集合，请导航到 **Configuration Management**（配置管理） > **Update Administration Server Options** （更新管理服务器选项） > **General** （常规）选项卡，然后选中 Collect Printers （收集打印机）复选框。

AD LDS

您可以将 AD LDS 清理刷新配置为按特定域的日程表运行。默认设置为 " 从不 " 刷新。您还可以查看清理状态并查看与 AD LDS (ADAM) 配置相关的特定信息。

要配置日程表或查看 AD LDS 清理状态，请在 **Account and Resource Management** （帐户和资源管理） > **All My Managed Objects** （我的所有受管对象）节点中右键单击所需的域，然后分别选择**属性** > **Adlds Cleanup Refresh Schedule** （Adlds 清理刷新日程表）或 **Adlds Cleanup status** （Adlds 清理状态）。

要查看 AD LDS (ADAM) 配置信息，请导航到 **Configuration Management** （配置管理） > **Update Server Options** （更新服务器选项） > **ADAM Configuration** （ADAM 配置）。

动态组

动态组根据组属性中配置的一组定义的准则更改其成员资格。在 " 域属性 " 中，您可以将动态组刷新配置为按特定域的日程表运行。默认设置为 " 从不 " 刷新。您还可以查看刷新状态。

要配置日程表或查看动态组刷新状态，请在 **Account and Resource Management** （帐户和资源管理） > **All My Managed Objects** （我的所有受管对象）节点中右键单击所需的域，然后分别选择**属性** > **Dynamic group refresh** （动态组刷新）或 **Dynamic group status** （动态组状态）。

有关动态组的更多信息，请参见 DRA 动态组。

配置回收站

您可以为每个 Microsoft Windows 域或每个域中的对象启用或禁用回收站，并配置何时以及如何进行回收站清理。

有关使用回收站的详细信息，请参见回收站。

启用回收站

您可以为特定 Microsoft Windows 域和这些域中的对象启用回收站。默认情况下， DRA 会为其管理的每个域和所有域的对象启用回收站。您必须是 DRA Admin 或 DRA 配置 Admin 组的成员才能启用回收站。

如果您的环境包括以下配置，请使用回收站实用程序启用此功能：

- DRA 正在管理此域的子树。
- 管理服务器服务或访问帐户无权创建回收站容器、将帐户移至此容器以及修改此容器中的帐户。

您还可以使用回收站实用程序校验管理服务器服务或访问帐户对回收站容器的许可权限。

要启用回收站，请右键单击回收站节点中的相应域，然后选择 **Enable Recycle Bin** （启用回收站）。

禁用回收站

您可以为特定 Microsoft Windows 域和这些域中的对象禁用回收站。如果禁用的回收站包含帐户，则无法查看、永久删除或恢复这些帐户。

您必须是 DRA Admin 或 DRA 配置 Admin 助理管理员组的成员才能禁用回收站。

要禁用回收站，请右键单击回收站节点中的相应域，然后选择 **Disable Recycle Bin** （禁用回收站）。

配置回收站对象和清理

回收站清理的默认设置是每天。您可以将此配置更改为每 x 天清理域回收站。在安排的清理期间，回收站将删除超出为每种对象类型配置的天数的对象。每种类型的默认设置是删除超过 1 天的对象。通过禁用、重新启用和设置每个对象类型的删除对象的期限，您可以自定义回收站清理的行为。

要配置回收站清理，请在 Delegation and Configuration （委托和配置）控制台中选择相应的域，然后转到任务 > 属性 > 回收站选项卡。

报告配置

以下章节将提供有关 DRA Management （DRA 管理）报告和可以启用的报告收集器的概念信息。要访问可以配置收集器的向导，请导航到 **Configuration Management** （配置管理） > **Update Reporting Service Configuration** （更新报告服务配置）。

配置 Active Directory Collector （Active Directory 收集器）

Active Directory Collector （Active Directory 收集器）将从 Active Directory 中为 DRA 中的每个受管用户、组、联系人、计算机、 OU 和动态分发组收集一组指定的属性。这些属性将储存在报告数据库中，用于在 Reporting （报告）控制台中生成报告。

您可以配置 Active Directory Collector （Active Directory 收集器）以指定要收集和储存在报告数据库中的属性。您还可以配置将运行收集器的 DRA 管理服务器。

配置 DRA Collector （DRA 收集器）

DRA Collector （DRA 收集器）将收集有关 DRA 配置的信息，并将该信息储存在报告数据库中，该数据库用于在 Reporting （报告）控制台中生成报告。

要启用 DRA Collector （DRA 收集器），您必须指定将运行收集器的 DRA 管理服务器。作为最佳实践，您应安排 DRA Collector （DRA 收集器）在 Active Directory Collector （Active Directory 收集器）成功运行之后和服务器负载最少时或在正常工作时间以外运行。

配置 Azure Tenant Collector （Azure 租户收集器）

Azure Tenant Collector （Azure 租户收集器）将收集有关同步到 Azure Active Directory 租户的 Azure 用户和组信息，并将该信息储存在报告数据库中，该数据库用于在 Reporting （报告）控制台中生成报告。

要启用 Azure Tenant Collector （Azure 租户收集器），您必须指定将运行收集器的 DRA 管理服务器。

注释：Azure 租户只有在其相应域的 Active Directory Collector （Active Directory 收集器）成功运行收集后，才能成功运行收集。

配置 Management Reports Collector （管理报告收集器）

Management Reports Collector （管理报告收集器）将收集 DRA 审计信息并将该信息储存在报告数据库中，该数据库用于在 Reporting （报告）控制台中生成报告。启用收集器时，可以配置数据库中数据的更新频率，以便在 DRA Reporting 工具中运行查询。

此配置要求 DRA 服务帐户在报告服务器的 SQL Server 中具有 **sysadmin** 许可权限。可配置选项定义如下：

- **Audit Export Data Interval** （审计导出数据间隔）：这是将 DRA 跟踪日志 (LAS) 中的审计数据导出到 SQL Server 中的 "SMCubeDepot" 数据库的时间间隔。
- **Management Report Summarization Interval**（管理报告摘要间隔）：这是将 SMCubeDepot 数据库中的审计数据提取到 DRA Reporting 数据库的时间间隔，可以通过 DRA Reporting 工具查询该数据库。

收集上次登录统计信息

您可以配置 DRA 以从受管域的所有域控制器中收集上次登录统计信息。要启用和安排收集上次登录统计信息，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

默认情况下，禁用上次登录统计信息收集功能。如果要收集上次登录统计数据，则必须启用此功能。启用收集上次登录统计信息后，您可以查看特定用户的上次登录统计信息，或显示上次登录统计信息收集的状态。

要收集上次登录统计信息：

1. 导航到 **Configuration Management** （配置管理） > **Managed Domains** （受管域）。
2. 右键单击所需的域，然后选择**属性**。
3. 单击 **Last logon schedule** （上次登录日程表）选项卡以配置上次登录统计信息收集。

统一的更改历史记录

统一的更改历史记录服务器功能使您能够针对在 DRA 之外进行的更改生成报告。

委托统一的更改历史记录服务器配置权限

要管理统一的更改历史记录服务器，请将统一的更改历史记录服务器管理角色或以下适用的权限指派给助理管理员：

- 删除统一的更改历史记录服务器配置
- 设置统一的更改历史记录配置信息
- 查看统一的更改历史记录配置信息

要委托统一的更改历史记录服务器权限：

1. 单击 Delegation Management （委托管理）节点中的 **Powers** （权限），然后使用搜索对象功能查找并选择所需的 UCH 权限。
2. 右键单击其中一个选定的 UCH 权限，然后选择 **Delegate Roles and Powers** （委托角色和权限）。
3. 搜索要向其委托权限的特定用户、组或助理管理员组。
4. 使用 **Object Selector** （对象选择器）查找并添加所需的对象，然后单击 **Wizard** （向导）中的 **Roles and Powers** （角色和权限）。
5. 单击 **ActiveView**，然后使用 **Object Selector** （对象选择器）查找和添加所需的 ActiveView。
6. 单击 **Next** （下一步），然后单击 **Finish** （完成）以完成委托过程。

配置统一的更改历史记录服务器

要配置统一的更改历史记录服务器：

1. 登录到 Delegation and Configuration （委托和配置）控制台。
2. 展开 **Configuration Management** （配置管理） > **Integration Servers** （集成服务器）。
3. 右键单击 **Unified Change History** （统一的更改历史记录），然后选择 **New Unified Change History Server** （新的统一的更改历史记录服务器）。
4. 在统一的更改历史记录配置中指定 UCH 服务器名称或 IP 地址、端口号、服务器类型和访问帐户细节。
5. 测试服务器连接，然后单击 **Finish** （完成）以保存配置。
6. 根据需要添加其他服务器。

委托工作流程自动化服务器配置权限

要管理工作流程，请将工作流程自动化服务器管理角色或以下适用的权限指派给助理管理员：

- Create Workflow Event and Modify All Properties （创建工作流程事件并修改所有属性）

- Delete Workflow Automation Server Configuration （删除工作流程自动化服务器配置）
- Set Workflow Automation Server Configuration Information （设置工作流程自动化服务器配置信息）
- Start Workflow （启动工作流程）
- View All Workflow Event Properties （查看所有工作流程事件属性）
- View All Workflow Properties （查看所有工作流程属性）
- View Workflow Automation Server Configuration Information （查看工作流程自动化服务器配置信息）

要委托工作流程自动化服务器配置权限：

1. 单击 Delegation Management （委托管理）节点中的 **Powers** （权限），然后使用搜索对象功能查找并选择所需的工作流程权限。
2. 右键单击其中一个选定的工作流程权限，然后选择 **Delegate Roles and Powers** （委托角色和权限）。
3. 搜索要向其委托权限的特定用户、组或助理管理员组。
4. 使用 **Object Selector** （对象选择器）查找并添加所需的对象，然后单击 **Wizard** （向导）中的 **Roles and Powers** （角色和权限）。
5. 单击 **ActiveView**，然后使用 **Object Selector** （对象选择器）查找和添加所需的 ActiveView。
6. 单击 **Next** （下一步），然后单击 **Finish** （完成）以完成委托过程。

配置工作流程自动化服务器

要在 DRA 中使用工作流程自动化，则必须在 Windows Server 上安装工作流程引擎，然后通过 Delegation and Configuration （委托和配置）控制台配置工作流程自动化服务器。

要配置工作流程自动化服务器：

1. 登录到 Delegation and Configuration （委托和配置）控制台。

   有关工作流程自动化权限，请参见委托工作流程自动化服务器配置权限。
2. 展开 **Configuration Management** （配置管理） > **Integration Servers** （集成服务器）。
3. 右键单击 **Workflow Automation** （工作流程自动化），然后选择 **New Workflow Automation Server** （新的工作流程自动化服务器）。
4. 在 **Add Workflow Automation Server** （添加工作流程自动化服务器）向导中指定细节，例如服务器名称、端口、协议和访问帐户。
5. 测试服务器连接，然后单击 **Finish** （完成）以保存配置。

有关安装工作流程引擎的信息，请参见 *Workflow Automation Administrator Guide* （《工作流程自动化管理员指南》）。

委托 LDAP 搜索权限

DRA 使您能够在本地 Active Directory 域中搜索 LDAP 对象，例如 LDAP 服务器的用户、联系人、计算机、组和 OU。 DRA 服务器仍会处理操作，且其为执行搜索的域控制器。使用搜索过滤器可以更有效地进行搜索。此外，您还可以保存搜索查询以供将来使用，可以将其与公众共享，也可以通过将其标记为私用以供自己使用。您可以编辑已保存的查询。 LDAP 高级查询角色授予助理管理员创建和管理 LDAP 搜索查询的权限。使用以下权限委托创建和管理 LDAP 搜索查询：

- Create Private Advanced Query （创建私用高级查询）
- Create Public Advanced Query （创建公共高级查询）
- Delete Public Advanced Query （删除公共高级查询）
- Execute Advanced Query （执行高级查询）
- Execute Save Advanced Query （执行保存高级查询）
- Modify Public Query （修改公共查询）
- View Advanced Query （查看高级查询）

要委托 LDAP 查询权限：

1. 单击 Delegation Management （委托管理）节点中的 **Powers** （权限），然后使用搜索对象功能查找并选择所需的高级 LDAP 查询权限。
2. 右键单击其中一个选定的 LDAP 权限，然后选择 **Delegate Roles and Powers** （委托角色和权限）。
3. 搜索要向其委托权限的特定用户、组或助理管理员组。
4. 使用 **Object Selector** （对象选择器）查找并添加所需的对象，然后单击 **Wizard** （向导）中的 **Roles and Powers** （角色和权限）。
5. 单击 **ActiveView**，然后使用 **Object Selector** （对象选择器）查找和添加所需的 ActiveView。
6. 单击 **Next** （下一步），然后单击 **Finish** （完成）以完成委托过程。

要访问 Web 控制台中的搜索功能，请导航到 **Management （管理） > LDAP Search** （LDAP 搜索）。

为组托管服务帐户配置 DRA 服务

如果需要，您可以针对 DRA 服务使用组托管服务帐户 (gMSA)。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）。本节介绍在先前将帐户添加到 Active Directory 后，如何为组托管服务帐户配置 DRA。

重要：安装 DRA 时，请勿将 gMSA 用作服务帐户。

要配置 gMSA 的 DRA 主管理服务器：

1. 将 gMSA 添加为以下组的成员：
   - DRA 服务器的本地管理员组
   - DRA 受管域的 AD LDS 组
2. 在服务属性中，将以下每个服务的登录帐户更改为 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 主机服务
   - 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。

要配置 gMSA 的 DRA 次管理服务器：

1. 安装次服务器。
2. 在主服务器上，针对次服务器的服务帐户，将 **Configure Servers and Domains** （配置服务器和域）角色指派给 **Administration Servers and Managed Domains** （管理服务器和受管域）ActiveView。
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。

配置 Delegation and Configuration （委托和配置）客户端

Delegation and Configuration （委托和配置）客户端可提供对配置和委托任务的访问权限，从而满足从分布式管理到策略实施的企业管理需求。通过 Delegation and Configuration （委托和配置）控制台，您可以设置有效管理企业所需的安全模型和服务器配置。

要配置 Delegation and Configuration （委托和配置）客户端：

1. 起动 Delegation and Configuration （委托和配置）客户端，然后导航到 **Configuration Management** （配置管理） > **Update Administration Server Options** （更新管理服务器选项）。
2. 单击 **Client Options** （客户端选项）选项卡，然后从显示的配置选项中定义首选设置：
   - 允许用户按 ActiveView 搜索

- 从控制台列表中隐藏仅源对象
- 显示高级 Active Directory 对象
- 显示安全性命令
- 搜索用户时显示资源和共享邮箱
- 当前域的默认用户 UPN 后缀。
- 一次可编辑的最大项目数 （多选）
- 搜索选项
- 回车选项
- Exchange 邮箱储存限制单位

配置 Web 客户端

您可以将 Web 控制台配置为使用智能卡或多因子鉴定进行鉴定，还可以使用您自己的徽标和应用程序标题自定义品牌。

启动 Web 控制台

您可以从运行 Web 浏览器的任何计算机、 iOS 设备或 Android 设备启动 Web 控制台。要启动控制台，请在 Web 浏览器地址字段中指定相应的 URL。例如，如果在 HOUserver 计算机上安装了 Web 组件，请在 Web 浏览器的地址字段中键入 https://HOUserver/draclient。

注释：要在 Web 控制台中显示最新帐户和 Microsoft Exchange 信息，请将 Web 浏览器设置为每次访问时检查超速缓存页的较新版本。

自动注销

您可以定义 Web 控制台在不活动后自动注销的时间增量，或将其设置为永远不会自动注销。

要在 Web 控制台中配置自动注销，请导航到**管理** > **配置** > **自动注销**。

DRA 服务器连接

在 Web 控制台中，可任选一种登录时 DRA 服务器的连接方式。配置完成后，登录到 Web 控制台时，**选项**下拉面板中的连接配置对于管理员和助理管理员均相同。

- 始终使用默认 DRA 服务器位置 （**始终**）

- 从不使用默认 DRA 服务器位置 （从不）
- 仅限于选中时使用默认 DRA 服务器位置 （仅限于选中）

登录时每个选项的行为如下所述：

连接配置	登录屏幕 - 选项	连接选项说明
始终	无	禁用选项配置
从不	使用自动发现	自动查找 DRA 服务器；没有可用的配置选项
	连接到特定 DRA 服务器	用户可配置服务器和端口
	连接到管理特定域的服务器	用户提供受管域并选择连接选项： ◆ 使用自动发现 （在提供的域中） ◆ 此域的主服务器 ◆ 搜索 DRA 服务器 （在提供的域中）
仅限于选中	使用自动发现	自动查找 DRA 服务器；没有可用的配置选项
	连接到默认 DRA 服务器	选择默认服务器并禁用 DRA 服务器配置
	连接到特定 DRA 服务器	用户可配置服务器和端口
	连接到管理特定域的服务器	用户提供受管域并选择连接选项： ◆ 使用自动发现 （在提供的域中） ◆ 此域的主服务器 ◆ 搜索 DRA 服务器 （在提供的域中）

要在 Web 控制台中配置 DRA 服务器连接，请导航到**管理** > **配置** > **DRA 服务器连接**。

REST 服务器连接

REST 服务连接的配置包括设置默认服务器位置和连接超时 （以秒为单位）。在 Web 控制台中，可任选一种登录时 REST 服务的连接方式。配置完成后，登录到 Web 控制台时，**选项**下拉面板中的连接配置对于管理员和助理管理员均相同。

- 始终使用默认 REST 服务位置 （始终）
- 从不使用默认 REST 服务位置 （从不）
- 仅限于选中时使用默认 REST 服务位置 （仅限于选中）

登录时每个选项的行为如下所述：

连接配置	登录屏幕 - 选项	连接选项说明
始终	无	禁用选项配置
从不	使用自动发现	自动查找 REST 服务器；没有可用的配置选项

连接配置	登录屏幕 - 选项	连接选项说明
	连接到特定 REST 服务器	用户可配置服务器和端口
	连接到特定域中的 REST 服务器	用户提供受管域并选择连接选项： • 使用自动发现 （在提供的域中） • 搜索 REST 服务器 （在提供的域中）
仅限于选中	使用自动发现	自动查找 REST 服务器；没有可用的配置选项
	连接到默认 REST 服务器	选择默认 REST 服务器并禁用 REST 服务器配置
	连接到特定 REST 服务器	用户可配置服务器和端口
	连接到特定域中的 REST 服务器	用户提供受管域并选择连接选项： • 使用自动发现 （在提供的域中） • 搜索 REST 服务器 （在提供的域中）

要在 Web 控制台中配置 REST 服务连接，请导航到**管理** > **配置** >**REST 服务连接**。

鉴定

本节包含有关使用 Advanced Authentication 集成配置智能卡鉴定、 Windows 鉴定和多因子鉴定的信息。

- 智能卡鉴定 （第 71 页）
- Windows 鉴定 （第 73 页）
- 使用 Advanced Authentication 进行多因子鉴定 （第 73 页）

智能卡鉴定

要将 Web 控制台配置为基于用户智能卡中的客户端身份凭证接受用户，您必须配置因特网信息服务 (IIS) 和 REST 服务配置文件。

重要：确保智能卡上的证书也安装在 Web 服务器上的根证书存储中，因为 IIS 必须能够找到与卡上证书相匹配的证书。

1 在 Web 服务器上安装鉴定组件。

1a 启动服务器管理器。

1b 单击 **Web 服务器 (IIS)**。

1c 转到 “ 角色服务 ” 部分，然后单击**添加角色服务**。

1d 转到 “ 安全角色服务 ” 节点，然后选择 **Windows 鉴定**和**客户端证书映射鉴定**。

2 在 Web 服务器上启用鉴定。

2a 启动 **IIS 管理器**。

2b 选择您的 Web 服务器。

2c 在 IIS 部分下找到**鉴定**图标，然后双击图标。

2d 启用 “Active Directory 客户端证书鉴定 ” 和 “Windows 鉴定 ”。

3 配置 DRA 客户端。

3a 选择您的 DRA 客户端。

3b 在 IIS 部分下找到**鉴定**图标，然后双击图标。

3c 启用 “Windows 鉴定 ” 并禁用 “ 匿名鉴定 ”。

4 在 DRA 客户端上启用 SSL 和客户端证书。

4a 在 IIS 部分下找到 **SSL 服务**图标，然后双击图标。

4b 选择**需要 SSL**，然后在 “ 客户端证书 ” 下选择**需要**。

提示：如果有选项，请选择**需要 128 位 SSL**。

---

5 配置 REST 服务 Web 应用程序。

5a 选择 REST 服务 Web 应用程序。

5b 在 IIS 部分下找到**鉴定**图标，然后双击图标。

5c 启用 “Windows 鉴定 ” 并禁用 “ 匿名鉴定 ”。

6 在 REST 服务 Web 应用程序上启用 SSL 和客户端证书。

6a 在 IIS 部分下找到 **SSL 服务**图标，然后双击图标。

6b 选择**需要 SSL**，然后在 “ 客户端证书 ” 下选择**需要**。

提示：如果有选项，请选择**需要 128 位 SSL**。

---

7 配置 WCF Web 服务文件。

7a 选择您的 REST 服务 Web 应用程序并切换到 “ 内容视图 ”。

7b 找到 .svc 文件并右键单击。

7c 选择**切换到功能视图**。

7d 在 IIS 部分下找到**鉴定**图标，然后双击图标。

7e 启用 “ 匿名鉴定 ” 并禁用所有其他鉴定方法。

8 编辑 REST 服务配置文件。

8a 使用文本编辑器打开 C:\inetpub\wwwroot\DRAClient\rest\web.config 文件。

8b 找到 <authentication mode="None" /> 行并将其删除。

8c 取消注释以下指定的行：

- 在 <system.serviceModel> 一行下方：

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

- 在 <serviceDebug includeExceptionDetailInFaults="false"/> 一行下方：

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

- 在 <serviceHostingEnvironment multipleSiteBindingsEnabled="true" /> 一行上方：

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

9 保存该文件并重启动 IIS 服务器。

Windows 鉴定

要在 Web 控制台上启用 Windows 鉴定，您必须配置因特网信息服务 (IIS) 和 REST 服务配置文件。

1 打开 “IIS 管理器 ”。

2 在 “ 连接 ” 窗格中，找到并选择 REST 服务 Web 应用程序。

3 在右窗格中，转到 IIS 部分，然后双击**鉴定**。

4 启用 **Windows 鉴定**并禁用所有其他鉴定方法。

5 使用文本编辑器打开 C:\inetpub\wwwroot\DRAClient\rest\web.config 文件并找到 <authentication mode="None" /> 行。

6 将 "None" 更改为 "Windows" 并保存文件。

7 重启动 IIS 服务器。

使用 Advanced Authentication 进行多因子鉴定

Advanced Authentication Framework (AAF) 是我们的首选软件包，可让您超越简单的用户名和口令，以更安全的方式 - 多因子鉴定来保护您的敏感信息。

Advanced Authentication 支持以下安全通信协议：

- TLS 1.2 （默认设置）、 TLS 1.1、 TLS 1.0
- SSL 3.0

多因子鉴定是一种计算机访问控制方法，需要从不同类别的身份凭证中使用多种鉴定方法来校验用户的身份。

有三种类型的鉴定类别或因子：

- *知识*。此类别要求您了解特定信息，例如口令或激活码。
- *拥有*。此类别要求您拥有鉴定设备，例如智能卡或智能电话。
- *身体*。此类别要求您使用身体的一部分 （例如指纹）作为校验方法。

每个鉴定因子至少包含一种鉴定方法。鉴定方法是一种可用于建立用户身份的特定技术，例如使用指纹或需要口令。

如果鉴定过程使用多种鉴定方法 - 例如，如果需要口令和指纹，则可以认为是强鉴定过程。

Advanced Authentication 支持以下鉴定方法：

- LDAP 口令
- 远程鉴定拨入用户服务 (RADIUS)
- 智能电话

提示：智能电话方法要求用户下载 iOS 或 Android APP。有关更多信息，请参见 *Advanced Authentication - Smartphone Applications User Guide* （《Advanced Authentication - 智能电话应用程序用户指南》），该指南可从 NetIQ 文档网站中获取。

使用以下章节中的信息将 Web 控制台配置为使用多因子鉴定。

重要：虽然以下章节中的有些步骤在 Web 控制台中进行，但大多数多因子鉴定配置过程都需要访问 AAF。这些过程假定您已安装 AAF，并且可以访问 AAF 的帮助文档。

将储存库添加到 Advanced Authentication Framework

配置 Web 控制台以使用多因子鉴定的第一步是将包含由 DRA 管理的 DRA 管理员和助理管理员的所有 Active Directory 域添加到 AAF。这些域称为储存库，它们包含要进行鉴定的用户和组的标识属性。

1. 使用管理员级别的用户名和口令登录到 AAF 管理门户。
2. 转到左侧面板，然后单击**储存库**。
3. 单击**添加**。
4. 填写表单。

   提示：**LDAP 类型**为 **AD**。

   提示：在相应字段中键入管理员级别的用户名和口令。
5. 单击**添加服务器**。
6. 在**地址**字段中键入 LDAP 服务器的 IP 地址。
7. 单击**保存**。
8. 对 DRA 管理的所有其他 AD 储存库重复步骤 3 到 7。
9. 对于“储存库”页上列出的每个储存库，单击**立即同步**以将其与 AAF 服务器同步。

创建鉴定链

鉴定链至少包含一种鉴定方法。链中的方法将按照其添加到链中的顺序进行调用。要对用户进行鉴定，用户必须通过链中的所有方法。例如，您可以创建包含 LDAP 口令方法和短信方法的链。当用户尝试使用此链进行鉴定时，必须首先使用其 LDAP 口令进行鉴定，之后用户手机会收到一条包含一次性口令的短信。输入口令后，将完成链中的所有方法，鉴定成功。可以将鉴定链指派给特定用户或组。

要创建鉴定链：

1 使用管理员级别的用户名和口令登录到 AAF 管理门户。

2 转到左侧面板，然后单击**链**。右侧面板将显示当前可用链的列表。

3 单击**添加**。

4 填写表单。所有字段均为必填字段。

重要：按照调用顺序添加方法 - 也就是说，如果您希望用户先输入 LDAP 口令，则先将 LDAP 口令添加到链中。

重要：确保**端点拥有者使用时应用**开关为“关”。

---

5 将**已启用**切换为“开”。

6 在**角色和组**字段中键入要接受鉴定请求的角色或组的名称。

提示：如果要将链应用于所有用户，请在**角色和组**字段中键入 all users，然后从打开的下拉列表中选择 **All Users** （所有用户）。

您选择的任何用户或组都将添加到**角色和组**字段下方。

7 单击**保存**。

创建鉴定事件

鉴定事件由应用程序触发，在本例中是希望对用户进行鉴定的 Web 控制台。必须至少为事件指派一个鉴定链，以便在触发事件时，将调用与事件关联的链中的方法以对用户进行鉴定。

端点是运行触发鉴定事件的软件的实际设备，例如计算机或智能电话。创建事件后， DRA 将使用 AAF 注册端点。

您可以使用“端点白名单”框限制特定端点对事件的访问，或者您可以允许所有端点访问事件。

要创建鉴定事件：

1 使用管理员级别的用户名和口令登录到 AAF 管理门户。

2 转到左侧面板，然后单击**事件**。右侧面板将显示当前可用事件的列表。

3 单击**添加**。

4 填写表单。所有字段均为必填字段。

重要：确保**已启用**开关为“开”。

---

5 如果要限制对特定端点的访问，请转到“端点白名单”部分，并将目标端点从*可用*列表移动到*已使用*列表。

提示：如果*已使用*列表中没有端点，则该事件将对所有端点可用。

启用 Web 控制台

配置链和事件后，以管理员身份登录 Web 控制台并启用 Advanced Authentication。

启用鉴定后，每个用户都需要通过 AAF 进行鉴定，然后才能访问 Web 控制台。

重要：在启用 Web 控制台之前，您必须已注册 Web 控制台将用于对用户进行鉴定的鉴定方法。请参见 *Advanced Authentication Framework User Guide* （《Advanced Authentication Framework 用户指南》）以了解如何注册鉴定方法。

要启用 Advanced Authentication，登录到 Web 控制台并导航到**管理** > **配置** > **Advanced Authentication**。选中**已启用**复选框，并根据为每个字段提供的说明配置表单。

提示：保存配置后，将在 AAF 中创建端点。要查看或编辑端点，请使用管理员级别的用户名和口令登录到 AAF 管理门户，然后单击左窗格中的**端点**。

最后的步骤

1. 使用管理员级别的用户名和口令登录到 AAF 管理门户，然后单击左窗格中的**事件**。
2. 编辑每个 Web 控制台事件：
   - **2a** 打开事件以进行编辑。
   - **2b** 转到“端点白名单”部分，并将在配置 Web 控制台时创建的端点从**可用**列表移动到**已使用**列表。这将确保只有 Web 控制台才能使用这些事件。
3. 单击**保存**。

7 连接受管系统

本节提供有关连接和配置与域和 Microsoft Exchange 组件相关的受管系统的信息，这些组件包括公共文件夹、 Exchange、 Office 365 和 Skype for Business Online。

管理 Active Directory 域

安装管理服务器后，您可以通过 Delegation and Configuration （委托和配置）客户端添加新的受管域和计算机。您还可以添加子树和受信任域，并为其配置域和 Exchange 访问帐户。要添加受管域和计算机，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

注释：添加完受管域后，确保这些域的帐户超速缓存刷新日程表是正确的。

添加受管域和计算机

要添加受管域或计算机：

1. 导航到 **Configuration Management** （配置管理） > **New Managed Domain** （新建受管域）。
2. 通过选择适用的单选按钮并提供域或计算机名称，指定要添加的组件：
   - **Manage a domain** （管理域）
     - 如果要管理域的子树，请参见添加受管子树。
     - 如果添加的是新域、域控制器已启用安全 LDAP 且您希望 DRA 使用 SSL 与域控制器通信，请选择 **This domain is configured for LDAP over SSL** （此域已配置为通过 SSL 的 LDAP）。有关更多信息，请参见配置 DRA 以运行安全 Active Directory。
   - **Manage a computer** （管理计算机）

   完成配置后，请单击 **Next** （下一步）。
3. 在 **Domain access** （域访问）选项卡上，指定您希望 DRA 用于访问此域或计算机的帐户身份凭证。默认情况下， DRA 将使用管理服务器服务帐户。
4. 查看摘要，然后单击**完成**。
5. 要开始管理此域或计算机中的对象，请刷新域配置。

指定域访问帐户

对于每个受管域或子树，您可以指定访问该域要使用的帐户 （而不是管理服务器服务帐户）。此备用帐户称为访问帐户。要配置访问帐户，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

要指定成员服务器的访问帐户，您必须具有管理域成员所在域的许可权限。只有在域成员存在于可通过管理服务器访问的受管域中时，才能管理域成员。

要指定访问帐户：

1. 导航到 **Configuration Management** （配置管理） > **Managed Domains** （受管域）节点。
2. 右键单击要为其指定访问帐户的域或子树，然后单击**属性**。
3. 在 Domain access （域访问）选项卡上，单击 **Use the following account to access this domain** （使用以下帐户访问此域）。
4. 指定并确认此帐户的身份凭证，然后单击**确定**。

有关配置此最低特权帐户的信息，请参见最小特权 DRA 访问帐户。

指定 Exchange 访问帐户

对于 DRA 中的每个域，您可以使用 DRA 域访问帐户或单独的 Exchange 访问帐户管理 Exchange 对象。要配置 Exchange 访问帐户，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

重要：Microsoft Server 将连接到 WinRM/WinRS 会话的并发用户数量限制为五个，将每个用户的壳层数量限制为五个，以确保针对 DRA 次服务器，将同一用户帐户限制为五个壳层。

要指定 Exchange 访问帐户：

1. 导航到 **Configuration Management** （配置管理） > **Managed Domains** （受管域）节点。
2. 右键单击要为其指定访问帐户的域或子树，然后单击**属性**。
3. 在 Exchange access （Exchange 访问）选项卡上，单击 **Use the following account to access all Exchange servers** （使用以下帐户访问所有 Exchange 服务器）。
4. 指定并确认此帐户的身份凭证，然后单击**确定**。

有关配置此最低特权帐户的信息，请参见。

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 域的受管和缺失的子树。要添加受管子树，您必须具备相应权限，例如内置 Configure Servers and Domains （配置服务器和域）角色中所包含的权限。

有关支持的 Microsoft Windows 版本的信息，请参见 DRA 管理服务器、 Web 控制台和 REST 扩展要求。

通过管理 Windows 域的子树，您可以使用 DRA 来保护大型公司域中的部门或分区。

例如，您可以在 SOUTHWEST （西南）域中指定休斯顿子树，从而允许 DRA 仅安全地管理休斯顿 OU 及其子 OU 中包含的对象。这种灵活性允许您管理一个或多个子树，而无需整个域的管理许可权限。

注释：

- 要确保指定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 Deleted Objects Utility （已删除对象实用程序）校验和委托相应许可权限。
- 添加完受管子树后，确保相应域的帐户超速缓存刷新日程表是正确的。

要添加受管子树：

1. 导航到**配置管理** > **新建受管域**。
2. 在 Domain or server （域或服务器）选项卡上，单击 **Manage a domain** （管理域），然后指定要管理的子树的域。
3. 指定要管理的子树的域。
4. 选择 **Manage a subtree of this domain** （管理此域的子树），然后单击 **Next** （下一步）。
5. 在 Subtrees （子树）选项卡上，单击**添加**以指定要管理的子树。您可以指定多个子树。
6. 在 “ 访问帐户 ” 选项卡上，指定您希望 DRA 用于访问此子树的帐户身份凭证。默认情况下， DRA 将使用管理服务器服务帐户。
7. 查看摘要，然后单击**完成**。
8. 要开始管理此子树中的对象，请刷新域配置。

添加受信任域

受信任域允许在整个受管环境中的受管系统上进行用户鉴定。添加受信任域后，您可以指定域和 Exchange 访问帐户、安排超速缓存刷新以及在域的属性中执行其他操作，这一点与受管域相同。

要添加受信任域：

1. 在 **Configuration Management** （配置管理） > **Managed Domains** （受管域）节点中，选择具有关联受信任域的受管域。
2. 单击 Details （细节）窗格中的 **Trusted domains** （受信任域）。必须在 View （视图）菜单中开启 Details （细节）窗格。
3. 右键单击受信任域，然后选择**属性**。
4. 取消选中 **Ignore this trusted domain** （忽略此受信任域），然后应用更改。

注释：添加受信任域将启动完全帐户超速缓存刷新，但是当您单击 **Apply** （应用）时，将通过确认提示通知您。

配置 DRA 以运行安全 Active Directory

安全 Active Directory 是由 DRA 环境所定义，该环境已配置为使用 LDAPS （通过 SSL 的 LDAP）协议运行，可加密 DRA 和 Active Directory 之间的通信，以提供更安全的环境。

从 9.x 版升级到 DRA 10.x 版时，升级后需要启用 LDAPS 以使用安全 Active Directory。检测并连接到 DRA 和 REST 服务器的自动发现功能，也需要针对此功能进行配置。

启用通过 SSL 的 LDAP (LDAPS)

如果您从 9.x 升级到 DRA 10.x，请按照以下步骤继续操作。如果配置的是新安装的 DRA，请参见添加受管域和计算机。

1. 在 DRA Delegation and Configuration （委托和配置）控制台中，导航到 **Configuration Management** （配置管理） > **Managed Domains** （受管域）。
2. 右键单击域并打开属性。
3. 在 General （一般信息）选项卡中，启用 **This domain is configured for LDAP over SSL** （此域已配置为通过 SSL 的 LDAP），然后单击 **OK** （确定）。
4. 重启动 NetIQ 管理服务。

注释：如果您也将自动发现配置为使用安全 Active Directory，完成配置后，可以等待重启动服务。有关更多信息，请参见针对 LDAPS 配置自动发现。

针对 LDAPS 配置自动发现

自动发现是客户端用于自动连接到可用 DRA 环境的机制。

要针对运行安全 Active Directory 的环境配置 DRA，请配置 ClientSSLAllDomains 注册表项：

1. 起动注册表编辑器实用程序。
2. 右键单击 HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions 节点。
3. 选择 **New** （新建） > **DWORD (32-bit) Value** （DWORD （32 位）值）。
4. 将新项命名为 ClientSSLAllDomains。
5. 将注册表项值设置为 1。
6. 添加 ClientSSLAllDomains 注册表项后，请重启动以下服务：
   - World Wide Web 发布服务
   - NetIQ DRA 主机服务
   - NetIQ DRA REST 服务

连接公共文件夹

DRA 可让您管理 Microsoft Exchange 公共文件夹。通过配置“公共文件夹”林域并为助理管理员授予权限，您可以使用 DRA 管理公共文件夹的某些属性。

重要：要管理公共文件夹管理，必须先在 DRA 中启用 Microsoft Exchange 支持并具有相应的权限。

- 有关启用 Microsoft Exchange 的信息，请参见启用 Microsoft Exchange。
- 有关帐户许可权限的信息，请参见最小特权 DRA 访问帐户。

要配置 Exchange 公共文件夹支持：

1. 在 Configuration and Management （配置和管理）节点中右键单击 **Managed Public Folder Forests** （受管公共文件夹林），然后单击 **New Public Folder Forest** （新建公共文件夹林）。
2. 单击 **Forest Domain** （林域），指定公共文件夹对象所在的 Active Directory 林，然后单击下一步。
3. 在 **Domain access** （域访问）中，指定访问帐户。

   重要：如果使用的是次服务器，则 **Use the Primary Administration Server domain access account** （使用主管理服务器域访问帐户）选项将可用。

   ---

4. 在 **Exchange access** （Exchange 访问）中，指定希望 DRA 用于安全访问 Exchange 服务器的帐户。

   重要：如果使用的是次服务器，则 **Use the Primary Administration Server Exchange access account** （使用主管理服务器 Exchange 访问帐户）选项将可用。

   ---

5. 在 **Exchange 服务器**中，选择您希望 DRA 用于管理公共文件夹的 Exchange 服务器。
6. 在 **Summary** （摘要）中，查看帐户细节和 Exchange 服务器细节，然后单击**完成**以完成该过程。

   DRA 服务器在公共文件夹上运行完全帐户超速缓存刷新。超速缓存刷新完成 （这可能需要几分钟时间）后，新的公共文件夹林将显示在控制台中。

注释：您可以从任务菜单或右键单击菜单中去除选定的公共文件夹林域。

查看和修改公共文件夹域属性

要查看或修改公共文件夹域属性：

1. 在 Configuration Management （配置管理）节点中，单击 **Managed Public Folder Forests** （受管公共文件夹林）以查看公共文件夹。
2. 右键单击要查看的公共文件夹帐户，然后选择**属性**。

3 在 Public Folder Forest （公共文件夹林）属性中，可以执行以下操作：

- **常规：**查看公共文件夹帐户细节并更新 Exchange Server （Exchange 服务器）字段，DRA 服务器使用该字段在公共文件夹服务器上执行 Exchange 活动。
- **统计：**查看公共文件夹的数量和已启用邮件的公共文件夹的数量。
- **Incremental Status （增量状态）：**查看或更新增量帐户超速缓存状态。
- **Incremental schedule （增量日程表）：**查看增量超速缓存刷新日程表并重安排超速缓存刷新。
- **Full status （完整状态）：**查看完整帐户超速缓存刷新状态。
- **Full refresh （完全刷新）：**立即执行完全帐户超速缓存刷新。

  NetIQ 建议您仅在公共文件夹超速缓存数据损坏时执行完全刷新。
- **域访问：**查看 DRA 服务帐户细节或覆盖访问帐户。
- **Exchange 访问：**查看或更新 Exchange 服务器的安全访问权限。

委托公共文件夹权限

使用 ActiveView 定义权限并管理公共文件夹委托。您可以指定添加受管对象、选择域和指派权限的规则，然后将这些公共文件夹权限委托给助理管理员。

要创建 ActiveView 并委托公共文件夹权限：

1 在 Delegation Management （委托管理）节点中，单击 ActiveView。

2 在 Create ActiveView > （创建 ActiveView）向导中单击 Next （下一步），从 Add （添加）下拉列表中选择所需规则，然后选择“公共文件夹”作为对象类型。例如，要创建对象匹配规则：选择 Objects that match a rule （与规则匹配的对象），然后选择 Public Folders （公共文件夹）作为对象类型。

3 指定要添加到公共文件夹的 ActiveView 规则，然后单击 Next （下一步）。

4 指定 ActiveView 的名称，然后单击 Finish （完成）。

5 右键单击 ActiveView 并转到 Delegate Administration （委托管理） > Assistant Admins （助理 Admin），然后在 Wizard （向导）的 Add （添加）下拉列表中指定 Admin 类型。

6 搜索要向其委托权限的特定用户、组或助理管理员组。

7 使用 Object Selector （对象选择器）查找并添加所需的对象，然后单击 Wizard （向导）中的 Roles and Powers （角色和权限）。

8 从 Add （添加）下拉列表中选择 Roles （角色），然后搜索并添加公共文件夹管理角色。

9 从 Add （添加）下拉列表中选择“权限”，然后查找并添加要指派给不属于公共文件夹管理角色的助理管理员的任何其他权限。

10 单击 Next （下一步），然后单击 Finish （完成）以完成委托过程。

完成公共文件夹权限的委托后，授权用户将能够使用 Web 控制台对已配置域中的公共文件夹属性执行创建、读取、更新和删除操作。

启用 Microsoft Exchange

启用 Microsoft Exchange 使您能够利用 Exchange 和 Exchange Online 功能，包含 Microsoft Exchange 策略、集成邮箱和已启用邮件的对象管理。您可以针对 Microsoft Exchange Server 2013 及更高版本的每个管理服务器，启用或禁用 Microsoft Exchange 支持。

要启用 Exchange，您需要所需特权，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的特权，并且您的许可证必须支持 Exchange 产品。有关 Microsoft Exchange 要求的更多信息，请参见支持的平台。

要启用 Microsoft Exchange 和 Exchange Online 的支持：

1 在 Delegation and Configuration （委托和配置）控制台中，导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略）。

2 选择 **Enable Exchange Policy** （启用 Exchange 策略），然后单击 **Apply** （应用）。

配置 Azure 租户

使用活动的 Azure 帐户和一个或多个 Azure 租户，您可以配置 DRA 以与 Azure Active Directory 一起使用以管理用户和组对象。这些对象包含 Azure 中创建的用户和组，以及从 DRA 受管域与 Azure 租户同步的用户和组。

需要 Azure PowerShell 模块、 Azure Active Directory 和 Azure 资源管理器配置文件才能管理 Azure 任务。您也需要 Azure Active Directory 中的帐户。有关 Azure 租户访问帐户许可权限的信息，请参见最小特权 DRA 访问帐户。

重要：Delegation and Configuration （委托和配置）控制台不支持对 Azure 对象的操作，例如创建、修改、删除、禁用和启用。

- 委托角色和权限 （第 83 页）
- 创建 Azure 应用程序并添加 Azure 租户 （第 84 页）
- 重设置 Azure 应用程序口令 （第 86 页）

委托角色和权限

您可以使用 DRA 管理员或已委托 "Configure Servers and Domains" （配置服务器和域）角色的助理管理员管理 Azure 租户，且需要 Azure 内置角色才能管理 Azure 对象。

Azure 内置角色

为委托 Azure 对象，指派以下 Azure 角色：

- **Azure Group Administration （Azure 组管理）：**提供管理 Azure 组和 Azure 组成员资格所需的所有权限。
- **Azure User Administration （Azure 用户管理）：**提供管理 Azure 用户所需的所有权限。

Azure 权限

使用以下权限委托创建和管理 Azure 用户和组。

Azure 用户帐户权限：

- Create Azure User and Modify All Properties （创建 Azure 用户和修改所有属性）
- Delete Azure User Account Permanently （永久删除 Azure 用户帐户）
- Manage Sign-In for Azure Users （管理 Azure 用户的登录）
- Manage Sign-In for Azure Users Synced to Azure Tenant （管理同步到 Azure 租户的 Azure 用户的登录）
- Modify All Azure User Properties （修改所有 Azure 用户属性）
- Reset Azure User Account Password （重设置 Azure 用户帐户口令）
- View All Azure User Properties （查看所有 Azure 用户属性）

Azure 组权限：

- Add Object to Azure Group （将对象添加到 Azure 组）
- Create Azure Group and Modify All Properties （创建 Azure 组和修改所有属性）
- Delete Azure Group Account （删除 Azure 组帐户）
- Modify All Azure Group Properties （修改所有 Azure 组属性）
- Remove Object from Azure Group （从 Azure 组中去除对象）
- View All Azure Group Properties （查看所有 Azure 组属性）

要针对 Azure 用户或组管理更细粒度级别的属性，您可以通过选择指定的对象属性创建自定义权限。

支持的 Azure 对象

支持以下 Azure 组类型：

- 分发列表
- 有邮件功能的安全性
- Office 365
- 安全性

注释：不支持在 Azure 中创建的 Guest 用户。

创建 Azure 应用程序并添加 Azure 租户

要管理新的 Azure 租户，请通过在 Delegation and Configuration （委托和配置）控制台中完成 Azure 应用程序添加新租户。 DRA 支持联机和脱机创建 Azure 应用程序，且需要具有以下许可权限的 Azure 应用程序才能管理租户中的对象：

- 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

这些许可权限将自动授予联机和脱机 Azure 应用程序。

要联机创建 Azure 应用程序并添加租户：

1. 在 Delegation and Configuration （委托和配置）控制台中，导航到 **Configuration Management** （配置管理） > **Azure Tenants** （Azure 租户）。
2. 右键单击 **Azure Tenants** （Azure 租户），然后选择 New Azure Tenant （新 Azure 租户）。
3. （可选）指定用于在同步期间将 Active Directory 对象映射到 Azure 的源定位属性。
4. 指定用于访问 Azure 租户的帐户，然后验证身份凭证。

   有关 Azure 租户访问帐户许可权限的信息，请参见最小特权 DRA 访问帐户。
5. 选择 **Allow DRA to create the Azure application** （允许 DRA 创建 Azure 应用程序）选项。
6. 为具有 Azure AD 公司管理员角色的用户帐户指定身份凭证，然后验证身份凭证。
7. 单击 **Finish** （完成）。

   添加 Azure 租户可能需要几分钟时间。租户成功添加后， DRA 会针对租户执行完全帐户超速缓存刷新，添加的租户会显示在 Azure 租户视图窗格中。

要针对 DRA 脱机创建 Azure 应用程序并添加租户：

1. 在 Delegation and Configuration （委托和配置）控制台中，导航到 **Configuration Management** （配置管理） > **Azure Tenants** （Azure 租户）。
2. 右键单击 **Azure Tenants** （Azure 租户），然后选择 **New Azure Tenant** （新 Azure 租户）。
3. （可选）指定用于在同步期间将 Active Directory 对象映射到 Azure 的源定位属性。
4. 指定用于访问 Azure 租户的帐户，然后验证身份凭证。
5. 选择 **Create the Azure application offline** （脱机创建 Azure 应用程序）选项。
6. 在 DRA 管理服务器中，起动 PowerShell 会话，然后导航至 C:\Program Files (x86)\NetIQ\DRA\SupportingFiles
7. 执行 ..\NewDraAzureApplication.ps1 以装载 PowerShell。
8. 执行 New-DRAAzureApplication cmdlet 以提示输入参数。
9. 针对 New-DraAzureApplication 指定以下参数：
   - <name> - 租户向导的应用程序名称。

     重要： Micro Focus 建议您使用 DRA 控制台中指定的名称。
   - （可选） <environment> - 根据使用的租户，指定 AzureCloud、 AzureChinaCloud、AzureGermanyCloud 或 AzureUSGovernment。
10. 在 Credential （身份凭证）对话框中，指定公司管理员身份凭证。

    将生成 Azure 应用程序 ID 和口令。
11. 将应用程序 ID 和口令复制到 DRA 控制台 （租户向导 **DRA Azure Application Credentials** （DRA Azure 应用程序身份凭证）），然后验证身份凭证。

12 单击 **Finish** （完成）。

添加 Azure 租户可能需要几分钟时间。租户成功添加后， DRA 会针对租户执行完全帐户超速缓存刷新，然后，添加的租户会显示在 Azure 租户视图窗格中。

重设置 Azure 应用程序口令

如果您需要联机或脱机 （如果适用）重设置 Azure 口令，请按照以下步骤继续操作。

要使用 Azure 身份凭证针对 DRA 重设置 Azure 应用程序口令：

1 在 Delegation and Configuration （委托和配置）控制台中，导航到 **Configuration Management** （配置管理） > **Azure Tenants** （Azure 租户）。

2 右键单击受管 Azure 租户，然后选择 **Properties** （属性）。

3 单击 " 属性 " 页面中的 **Azure Application** （Azure 应用程序）。

4 选择 **Allow DRA to reset the password using your Azure Credentials** （允许 DRA 使用 Azure 身份凭证重设置口令），然后指定 Azure 身份凭证。

5 应用更改。

要脱机针对 DRA 重设置 Azure 应用程序口令：

1 在 DRA 管理服务器中，起动 PowerShell 会话，然后导航至 C:\Program Files (x86)\NetIQ\DRA\SupportingFiles

2 执行 . .\ResetDraAzureApplicationPassword.ps1 以装载 PowerShell。

3 执行 . .\ResetDraAzureApplicationPassword cmdlet 以提示输入参数。

4 针对 Reset-DRAAzureApplicationPassword 指定以下参数：

- <name> - 租户向导的应用程序名称。

  重要：Micro Focus 建议您使用 DRA 控制台中指定的名称。

- （可选） <environment> - 根据使用的租户，指定 AzureCloud、 AzureChinaCloud、AzureGermanyCloud 或 AzureUSGovernment。

5 在 Credential （身份凭证）对话框中，指定公司管理员身份凭证。

将生成 Azure 应用程序 ID 和口令。

6 将应用程序 ID 和口令复制到 DRA 控制台 （租户向导 **DRA Azure Application Credentials** （DRA Azure 应用程序身份凭证）），然后验证身份凭证。

7 打开 Delegation and Configuration （委托和配置）控制台，然后导航到 **Configuration Management** （配置管理） > **Azure Tenants** （Azure 租户）。

8 右键单击 Azure 租户，然后转到 **Properties** （属性） > **Azure Application** （Azure 应用程序）。

9 使用提供的脚本选项，选择 **Reset the password offline** （脱机重设置口令），然后粘贴脚本生成的 Azure 应用程序口令。

10 应用更改

IV 委托模型

DRA 可让管理员通过提供一组灵活的控件来实现“最小特权”许可权限方案，以便为企业中的特定受管对象授予细粒度权限。通过这些委托，管理员可以确保助理管理员仅获得完成其特定角色和职责所需的许可权限。

8 了解动态委托模型

DRA 可让您在委托模型的环境中管理对企业的管理访问权限。委托模型允许您通过一组动态控件为助理管理员设置“最小特权”访问权限，这些控件可随着企业的变化和发展而进行调整。委托模型提供的管理访问控制更能代表公司的运作方式：

- 借助灵活的范围规则，管理员可以根据业务需要而不是企业结构来定位特定受管对象的许可权限。
- 基于角色的委托可确保一致地授予许可权限并简化供应。
- 可以从单个位置跨域、云租户和受管应用程序管理特权指派。
- 细粒度权限使您能够定制授予助理管理员的特定访问权限。

委托模型控件

管理员使用以下控件通过委托模型供应访问权限：

- **委托：**管理员通过指派角色来供应对用户和组的访问权限，该角色在提供范围的 ActiveView 环境中具有指定的许可权限。
- **ActiveView：**ActiveView 表示由一个或多个规则定义的特定受管对象范围。 ActiveView 中由每个规则标识的受管对象将一起聚合到一个统一的范围中。
- **ActiveView 规则：**规则由基于许多条件 （如对象类型、位置、名称等）与一组受管对象匹配的表达式定义。
- **角色：**角色表示执行特定管理功能所需的一组特定权限 （许可权限）。 DRA 为常见业务功能提供了许多内置角色，您可以定义最适合您组织需求的自定义角色。
- **权限：**权限为受管对象支持的任务定义特定许可权限，例如查看、修改、创建、删除等。修改受管对象的许可权限可以进一步细分为可以更改的特定属性。 DRA 为支持的受管对象提供了广泛的内置功能列表，并可以定义自定义权限以扩展可通过委托模型供应的内容。

DRA 如何处理请求

当管理服务器收到操作请求 （例如更改用户口令）时，它将使用以下过程：

1. 搜索配置为管理操作的目标对象的 ActiveView。
2. 验证指派给请求操作的帐户的权限。
   a. 评估包含请求操作的助理管理员的所有 ActiveView 指派。
   b. 完成该列表后，构建包含目标对象和助理管理员的所有 ActiveView 的列表。
   c. 将权限与请求操作所需的权限进行比较。
3. *如果帐户具有正确的权限*，则管理服务器将允许执行操作。

如果帐户没有正确的权限，则管理服务器将返回错误。

4. 更新 Active Directory。

DRA 如何处理委托指派的示例

以下示例描述 DRA 在处理请求时如何评估委托模型中出现的常见情况：

示例 1：更改用户口令

当助理管理员尝试为 JSmith 用户帐户设置新口令时，管理服务器将查找包含 JSmith 的所有 ActiveView。此搜索将通过通配符规则或通过组成员资格查找直接指定 JSmith 的任何 ActiveView。如果 ActiveView 包含其他 ActiveView，则管理服务器还会搜索这些其他 ActiveView。管理服务器确定助理管理员是否在任何这些 ActiveView 中具有*重设置用户帐户口令*权限。如果助理管理员具有*重设置用户帐户口令*权限，则管理服务器将重设置 JSmith 的口令。如果助理管理员没有此权限，则管理服务器会拒绝该请求。

示例 2：重叠 ActiveView

权限定义了助理管理员可以在受管域或子树中查看、修改或创建的对象的属性。多个 ActiveView 可以包含同一个对象。此配置称为**重叠 ActiveView**。

当 ActiveView 重叠时，您可以在同一对象上累积一组不同的权限。例如，如果一个 ActiveView 允许您将用户帐户添加到域，而另一个 ActiveView 允许您从同一个域中删除用户帐户，则可以在该域中添加或删除用户帐户。通过这种方式，您对给定对象的权限可以累积。

了解 ActiveView 如何重叠非常重要，您可以对 ActiveView 中包含的这些对象具有更多的权限。考虑下图所示的 ActiveView 配置。

白色标签按位置*纽约市*和*休斯顿*识别 ActiveView。黑色标签通过其组织功能*销售*和*营销*识别 ActiveView。单元格显示每个 ActiveView 中包含的组。

NYC_Sales 组和 HOU_Sales 组都呈现在销售 ActiveView 中。如果您在销售 ActiveView 中拥有权限，则可以管理 NYC_Sales 和 HOU_Sales 组的任何成员。如果您在纽约市 ActiveView 中也具有权限，则这些额外的权限适用于 NYC_Marketing 组。这样，当 ActiveView 重叠时，权限便会累积。

重叠的 ActiveView 可以提供强大、灵活的委托模型。但是，此功能也可能会产生意想不到的后果。仔细规划您的 ActiveView，以确保每个助理管理员对每个用户帐户、组、 OU、联系人或资源仅具有您所希望的权限。

多个 ActiveView 中的组

在此示例中， NYC_Sales 组呈现在多个 ActiveView 中。 NYC_Sales 组的成员呈现在纽约市 ActiveView 中，因为组名称与 NYC_* ActiveView 规则匹配。该组也位于销售 ActiveView 中，因为组名称与 *_Sales ActiveView 规则匹配。通过在多个 ActiveView 中包含相同的组，您可以允许不同的助理管理员以不同方式管理相同的对象。

使用多个 ActiveView 中的权限

假设有一个助理管理员 JSmith，他在纽约市 ActiveView 中具有*修改常规用户属性*权限。此第一个权限允许 JSmith 编辑用户属性窗口“常规”选项卡上的所有属性。 JSmith 在销售 ActiveView 中具有*修改用户配置文件属性*权限。此第二个权限允许 JSmith 编辑用户属性窗口“配置文件”选项卡上的所有属性。

下图显示了 JSmith 对每个组的权限。

JSmith 具有以下权限：

- NYC_* ActiveView 中的常规属性
- *_Sales ActiveView 中的配置文件属性

这些重叠 ActiveView 中的权限委托允许 JSmith 修改 NYC_Sales 组的常规和配置文件属性。因此， JSmith 具有代表 NYC_Sales 组的所有 ActiveView 中授予的所有权限。

9 ActiveView

ActiveView 使您能够实现具有以下特点的委托模型：

- 独立于 Active Directory 结构
- 允许您指派权限并定义与现有工作流程相关的策略
- 提供自动化以帮助您进一步集成和自定义您的企业
- 动态响应变化

ActiveView 表示一个或多个受管域中的一组对象。您可以在多个 ActiveView 中包含一个对象。您还可以包含来自多个域或 OU 的许多对象。

内置 ActiveView

内置 ActiveView 是 DRA 提供的默认 ActiveView。这些 ActiveView 表示所有当前对象和安全设置。因此，内置 ActiveView 可以立即访问所有对象和设置以及默认委托模型。您可以使用这些 ActiveView 来管理对象 （如用户帐户和资源），或将默认委托模型应用于您的当前企业配置。

DRA 提供了多个可以代表委托模型的内置 ActiveView。内置 ActiveView 节点包含以下 ActiveView：

所有对象

包括所有受管域中的所有对象。通过此 ActiveView，您可以管理企业的任何方面。将此 ActiveView 指派给管理员或需要整个企业审计权限的助理管理员。

Objects Current User Manages as Windows Administrator （当前用户以 Windows 管理员身份管理的对象）

包括当前受管域中的对象。通过此 ActiveView，您可以管理用户帐户、组、联系人、 OU 和资源。将此 ActiveView 指派给负责受管域中的帐户和资源对象的本机管理员。

Administration Servers and Managed Domains （管理服务器和受管域）

包括管理服务器计算机和受管域。通过此 ActiveView，您可以管理管理服务器的日常维护。将此 ActiveView 指派给助理管理员，其职责包括监控同步状态或执行超速缓存刷新。

DRA Policies and Automation Triggers （DRA 策略和自动化触发器）

包括所有受管域中的所有策略和自动化触发器对象。通过此 ActiveView，您可以管理策略属性和范围以及自动化触发器属性。将此 ActiveView 指派给负责创建和维护公司策略的助理管理员。

DRA Security Objects （DRA 安全对象）

包括所有安全对象。通过此 ActiveView，您可以管理 ActiveView、助理管理员组和角色。将此 ActiveView 指派给负责创建和维护安全模型的助理管理员。

SPA Users from All Managed and Trusted Domains （所有受管域和受信任域中的 SPA 用户）

包括受管域和受信任域中的所有用户帐户。通过此 ActiveView，您可以通过 Secure Password Administrator (SPA) 管理用户口令。

访问内置 ActiveView

访问内置 ActiveView 以审计默认委托模型或管理您自己的安全设置。

要访问内置 ActiveView：

1. 导航到 **Delegation Management** （委托管理） > **Manage ActiveViews** （管理 ActiveView）。
2. 确保搜索字段为空，然后单击 **List items that match my criteria** （列出与我的准则匹配的项目）窗格中的 **Find Now** （立即查找）。
3. 选择相应的 ActiveView。

使用内置 ActiveView

您无法删除、克隆或修改内置 ActiveView。但是，您可以将这些 ActiveView 合并到现有的委托模型中，或使用这些 ActiveView 来设计自己的模型。

您可以通过以下方式使用内置 ActiveView：

- 将各个内置 ActiveView 指派给相应的助理管理员组。该关联允许助理管理员组成员以适当的权限管理相应的对象集。
- 参阅内置 ActiveView 规则和关联，作为设计和实现委托模型的指南。

有关设计动态委托模型的更多信息，请参见了解动态委托模型。

实现自定义 ActiveView

ActiveView 可实时访问一个或多个域或 OU 中的特定对象。您可以在 ActiveView 中添加或去除对象，而无需更改基础域或 OU 结构。

您可以将 ActiveView 视为虚拟域或 OU，或视为关系数据库的 select 语句或数据库视图的结果。 ActiveView 可以包括或排除任何对象集，包含其他 ActiveView，并具有重叠内容。ActiveView 可以包含来自不同域、树和林的对象。您可以配置 ActiveView 以满足任何企业管理需求 .

ActiveView 可以包括以下对象类型：

帐户：

- 用户

- 组
- 计算机
- 联系人
- 动态分发组
- 已发布的打印机
- 已发布的打印机打印作业
- 资源邮箱
- 共享邮箱
- 公共文件夹

目录对象：

- 组织单元
- 域
- 成员服务器

委托对象：

- ActiveView
- 自我管理
- 直属上司
- 受管组

资源：

- 已连接的用户
- 设备
- 事件日志
- 打开的文件
- 打印机
- 打印作业
- 服务
- 共享

Azure 对象：

- Azure 用户
- Azure 组
- Azure 租户

随着企业的变化或发展， ActiveView 会发生变化以包含或排除新对象。因此，您可以使用 ActiveView 来降低模型的复杂性，提供所需的安全性，并为您提供比其他企业组织工具更大的灵活性。

ActiveView 规则

ActiveView 可以由包含或排除对象 （如用户帐户、组、 OU、联系人、资源、计算机、资源邮箱、共享邮箱、动态分发组和 ActiveView）的规则组成。这种灵活性使得 ActiveView 具有动态性。

这些匹配称为**通配符**。例如，您可以定义规则以包含名称与 DOM* 匹配的所有计算机。此通配符规范将搜索名称以字符串 DOM 开头的任何计算机帐户。通配符匹配将使管理具有动态性，因为帐户在与规则匹配时会自动包含在内。因此，在使用通配符时，无需在组织发生变化时重新配置 ActiveView。

另一个示例是基于组成员资格定义 ActiveView。您可以定义规则以包含以字母 NYC 开头的组的所有成员。然后，当成员添加到符合此规则的任何组时，这些成员将自动包含在此 ActiveView 中。随着企业的变化或发展， DRA 将重新应用规则以在相应的 ActiveView 中包含或排除新对象。

10 角色

本节包括 DRA 内置角色说明的列表、如何使用这些角色以及有关创建和管理自定义角色的信息。

有关角色及其一般用法的说明，请参见委托模型控件。

内置角色

内置助理管理员角色可即时访问一组常用权限。您可以使用这些默认角色将权限指派给特定用户帐户或其他组，从而扩展当前的安全配置。

这些角色包含执行常见管理任务所需的权限。例如， DRA 管理角色包含管理对象所需的所有权限。但是，要使用这些权限，角色必须与用户帐户或助理管理员组以及受管 ActiveView 关联。

由于内置角色是默认委托模型的一部分，因此您可以使用内置角色快速委托权限并实现安全性。这些内置角色将处理您可以通过 DRA 用户界面执行的常见任务。下面的列表描述了每个内置角色，并总结了与该角色关联的权限。

Application Servers Administration （应用程序服务器管理）

提供配置、查看和删除应用程序服务器配置所需的权限。

Audit All Objects （审计所有对象）

提供查看整个企业中对象属性、策略和配置所需的所有权限。此角色不允许助理管理员修改属性。将此角色指派给负责审计整个企业的操作的助理管理员。允许助理管理员查看除 Custom Tools （自定义工具）节点以外的所有节点。

Audit Limited Account and Resource Properties （审计受限帐户和资源属性）

提供针对所有对象属性的权限。

Audit Resources （审计资源）

提供查看受管资源属性所需的所有权限。将此角色指派给负责审计资源对象的助理管理员。

Audit Users and Groups （审计用户和组）

提供查看用户帐户和组属性所需的所有权限，但无权修改这些属性。将此角色指派给负责审计帐户属性的助理管理员。

Azure Group Administration （Azure 组管理）

提供管理 Azure 组和 Azure 成员资格所需的所有权限。

Azure User Administration （Azure 用户管理）

提供创建、修改、删除、启用、禁用和查看管理 Azure 用户属性所需的所有权限。将此角色指派给负责管理 Azure 用户的助理管理员。

Built-in Scheduler - Internal Use Only （内置计划程序 - 仅供内部使用）

提供安排 DRA 刷新超速缓存的时间的权限。

Clone User with Mailbox （克隆用户和邮箱）

提供克隆现有用户帐户和帐户邮箱所需的所有权限。将此角色指派给负责管理用户帐户的助理管理员。

注释：要允许助理管理员在克隆任务期间将新用户帐户添加到组，还需指派“管理组成员资格”角色。

Computer Administration （计算机管理）

提供修改计算机属性所需的所有权限。此角色允许助理管理员添加、删除和关闭计算机，以及同步域控制器。将此角色指派给负责管理 ActiveView 中计算机的助理管理员。

Configure Servers and Domains （配置服务器和域）

提供修改管理服务器选项和受管域所需的所有权限。还提供配置和管理 Azure 租户所需的权限。将此角色指派给负责监控和维护管理服务器和管理 Azure 租户的助理管理员。

Contact Administration （联系人管理）

提供创建新联系人、修改联系人属性或删除联系人所需的所有权限。将此角色指派给负责管理联系人的助理管理员。

Create and Delete Computer Accounts （创建和删除计算机帐户）

提供创建和删除计算机帐户所需的所有权限。将此角色指派给负责管理计算机的助理管理员。

Create and Delete Groups （创建和删除组）

提供创建和删除组所需的所有权限。将此角色指派给负责管理组的助理管理员。

Create and Delete Resource Mailbox （创建和删除资源邮箱）

提供创建和删除邮箱所需的所有权限。将此角色指派给负责管理邮箱的助理管理员。

Create and Delete Resources （创建和删除资源）

提供创建和删除共享和计算机帐户以及清除事件日志所需的所有权限。将此角色指派给负责管理资源对象和事件日志的助理管理员。

Create and Delete User Accounts （创建和删除用户帐户）

提供创建和删除用户帐户所需的所有权限。将此角色指派给负责管理用户帐户的助理管理员。

DRA Administration （DRA 管理）

将所有权限提供给助理管理员。此角色将为用户授予在 DRA 中执行所有管理任务的许可权限。此角色等同于管理员的许可权限。与 DRA 管理角色关联的助理管理员可以访问所有 Directory and Resource Administrator 节点。

Dynamic Group Administration （动态组管理）

提供管理 Active Directory 动态组所需的所有权限。

Execute Advanced Queries （执行高级查询）

提供执行保存的高级查询所需的所有权限。将此角色指派给负责执行高级查询的助理管理员。

Group Administration （组管理）

提供管理组和组成员资格以及查看相应用户属性所需的所有权限。将此角色指派给负责管理组或通过组管理的帐户和资源对象的助理管理员。

Help Desk Administration （Help Desk 管理）

提供查看用户帐户属性以及更改口令和口令相关属性所需的所有权限。此角色还允许助理管理员禁用、启用和解除锁定用户帐户。将此角色指派给负责 Help Desk 职责 （确保用户对其帐户具有适当访问权限）的助理管理员。

Mailbox Administration （邮箱管理）

提供管理 Microsoft Exchange 邮箱属性所需的所有权限。如果使用 Microsoft Exchange，请将此角色指派给负责管理 Microsoft Exchange 邮箱的助理管理员。

管理 Active Directory Collector （Active Directory 收集器）、 DRA Collector （DRA 收集器）和 Management Reporting Collector （管理报告收集器）

提供管理用于数据收集的 Active Directory Collector （Active Directory 收集器）、 DRA Collector （DRA 收集器）和 Management Reporting Collector （管理报告收集器）所需的所有权限。将此角色指派给负责管理报告配置的助理管理员。

管理 Active Directory Collector （Active Directory 收集器）、 DRA Collector （DRA 收集器）、 Management Reporting Collector （管理报告收集器）和 Database Configuration （数据库配置）

提供管理用于数据收集的 Active Directory Collector （Active Directory 收集器）、 DRA Collector （DRA 收集器）、 Management Reporting Collector （管理报告收集器）和 Database Configuration （数据库配置）。将此角色指派给负责管理报告和数据库配置的助理管理员。

Manage Advanced Queries （管理高级查询）

提供创建、管理和执行高级查询所需的所有权限。将此角色指派给负责管理高级查询的助理管理员。

Manage and Execute Custom Tools （管理和执行自定义工具）

提供创建、管理和执行自定义工具所需的所有权限。将此角色指派给负责管理自定义工具的助理管理员。

Manage Clone Exceptions （管理克隆例外项）

提供创建和管理克隆例外项所需的所有权限。

Manage Computer Properties （管理计算机属性）

提供管理计算机帐户所有属性所需的所有权限。将此角色指派给负责管理计算机的助理管理员。

Manage Database Configuration （管理数据库配置）

提供管理管理报告的数据库配置所需的所有权限。将此角色指派给负责管理报告数据库配置的助理管理员。

Manage Dynamic Distribution Groups （管理动态分发组）

提供管理 Microsoft Exchange 动态分发组所需的所有权限。

Manage Exchange Mailbox Rights （管理 Exchange 邮箱权限）

提供管理 Microsoft Exchange 邮箱的安全性和权限所需的所有权限。如果使用 Microsoft Exchange，请将此角色指派给负责管理 Microsoft Exchange 邮箱许可权限的助理管理员。

Manage Group Email （管理组电子邮件）

提供查看、启用或禁用组的电子邮件地址所需的所有权限。将此角色指派给负责管理帐户对象的组或电子邮件地址的助理管理员。

Manage Group Membership Security （管理组成员资格安全性）

提供指定可通过 Microsoft Outlook 查看和修改 Microsoft Windows 组成员资格的用户所需的所有权限

Manage Group Memberships （管理组成员资格）

提供在现有组中添加和去除用户帐户或组以及查看用户或计算机帐户的主要组所需的所有权限。将此角色指派给负责管理组或用户帐户的助理管理员。

Manage Group Properties （管理组属性）

提供管理组的所有属性所需的所有权限。将此角色指派给负责管理组的助理管理员。

Manage Mailbox Move Requests （管理邮箱移动请求）

提供管理邮箱移动请求所需的所有权限。

Manage Policies and Automation Triggers （管理策略和自动化触发器）

提供定义策略和自动化触发器所需的所有权限。将此角色指派给负责维护公司策略和自动化工作流程的助理管理员。

Manage Printers and Print Jobs （管理打印机和打印作业）

提供管理打印机、打印队列和打印作业所需的所有权限。要管理与用户帐户关联的打印作业，打印作业和用户帐户必须包含在同一 ActiveView 中。将此角色指派给负责维护打印机和管理打印作业的助理管理员。

Manage Resource Mailbox Properties （管理资源邮箱属性）

提供管理邮箱所有属性所需的所有权限。将此角色指派给负责管理邮箱的助理管理员。

Manage Resources for Managed Users （管理受管用户的资源）

提供管理与特定用户帐户关联的资源所需的所有权限。助理管理员和用户帐户必须包含在同一 ActiveView 中。将此角色指派给负责管理资源对象的助理管理员。

Manage Security Model （管理安全模型）

提供定义管理规则 （包括 ActiveView、助理管理员和角色）所需的所有权限。将此角色指派给负责实施和维护安全模型的助理管理员。

Manage Services （管理服务）

提供管理服务所需的所有权限。将此角色指派给负责管理服务的助理管理员。

Manage Shared Folders （管理共享文件夹）

提供管理共享文件夹所需的所有权限。将此角色指派给负责管理共享文件夹的助理管理员。

Manage Temporary Group Assignments （管理临时组指派）

提供创建和管理临时组指派所需的所有权限。将此角色指派给负责管理组的助理管理员。

Manage UI Reporting （管理用户界面报告）

提供为用户、组、联系人、计算机、组织单元、权限、角色、 ActiveView、容器、已发布的打印机和助理管理员生成和导出 Activity Detail （活动细节）报告所需的所有权限。将此角色指派给负责生成报告的助理管理员。

Manage User Dial in Properties （管理用户拨入属性）

提供修改用户帐户拨入属性所需的所有权限。将此角色指派给负责管理远程访问企业的用户帐户的助理管理员。

Manage User Email （管理用户电子邮件）

提供查看、启用或禁用用户帐户的电子邮件地址所需的所有权限。将此角色指派给负责管理帐户对象的用户帐户或电子邮件地址的助理管理员。

Manage User Password and Unlock Account （管理用户口令和解除锁定帐户）

提供重设置口令、指定口令设置和解除锁定用户帐户所需的所有权限。将此角色指派给负责维护用户帐户访问权限的助理管理员。

Manage User Properties （管理用户属性）

提供管理用户帐户所有属性 （包括 Microsoft Exchange 邮箱属性）所需的所有权限。将此角色指派给负责管理用户帐户的助理管理员。

Manage Virtual Attributes （管理虚拟属性）

提供创建和管理虚拟属性所需的所有权限。将此角色指派给负责管理虚拟属性的助理管理员。

Manage WTS Environment Properties （管理 WTS 环境属性）

提供更改用户帐户的 WTS 环境属性所需的所有权限。将此角色指派给负责维护 WTS 环境或管理用户帐户的助理管理员。

Manage WTS Remote Control Properties （管理 WTS 远程控制属性）

提供更改用户帐户的 WTS 远程控制属性所需的所有权限。将此角色指派给负责维护 WTS 访问权限或管理用户帐户的助理管理员。

Manage WTS Session Properties （管理 WTS 会话属性）

提供更改用户帐户的 WTS 会话属性所需的所有权限。将此角色指派给负责维护 WTS 会话或管理用户帐户的助理管理员。

Manage WTS Terminal Properties （管理 WTS 终端属性）

提供更改用户帐户的 WTS 终端属性所需的所有权限。将此角色指派给负责维护 WTS 终端属性或管理用户帐户的助理管理员。

OU Administration （OU 管理）

提供管理组织单元所需的所有权限。将此角色指派给负责管理 Active Directory 结构的助理管理员。

Public Folder Administration （公共文件夹管理）

提供创建、修改、删除、启用或禁用邮件以及查看公共文件夹属性的权限。您可以将此角色指派给负责管理公共文件夹的所有助理管理员。

Rename Group and Modify Description （重命名组和修改说明）

提供修改组名称和说明所需的所有权限。将此角色指派给负责管理组的助理管理员。

Rename User and Modify Description （重命名用户和修改说明）

提供修改用户帐户的名称和说明所需的所有权限。将此角色指派给负责管理用户帐户的助理管理员。

Replicate Files （复制文件）

提供上载、删除和修改文件信息所需的所有权限。将此角色指派给负责将文件从主管理服务器复制到 MMS 和 DRA 客户端计算机中的其他管理服务器的助理管理员。

Reset Local Administrator Password （重设置本地管理员口令）

提供重设置本地管理员帐户口令和查看计算机管理员名称的所有权限。将此角色指派给负责管理管理员帐户的助理管理员。

Reset Password （重设置口令）

提供重设置和修改口令所需的所有权限。将此角色指派给负责口令管理的助理管理员。

Reset Password and Unlock Account Using SPA （使用 SPA 重设置口令和解除锁定帐户）

提供使用 Secure Password Administrator 重设置口令和解除锁定用户帐户所需的所有权限。

Reset Unified Messaging PIN Properties （重设置统一讯息交换 PIN 属性）

提供重设置用户帐户的统一讯息交换 PIN 属性所需的所有权限。

Resource Administration （资源管理）

提供修改受管资源 （包括与任何用户帐户关联的资源）属性所需的所有权限。将此角色指派给负责管理资源对象的助理管理员。

Resource Mailbox Administration （资源邮箱管理）

提供管理资源邮箱所需的所有权限。

Self Administration （自我管理）

提供修改您自己的用户帐户的基本属性 （如电话号码）所需的所有权限。将此角色指派给助理管理员以允许其管理自己的个人信息。

Shared Mailbox Administration （共享邮箱管理）

提供创建、修改、删除和查看共享邮箱属性所需的所有权限。将此角色指派给负责管理共享邮箱的所有助理管理员。

Start and Stop Resources （启动和停止资源）

提供暂停、启动、继续或停止服务，启动或停止设备或打印机，关闭计算机或同步域控制器所需的所有权限。还提供暂停、继续和启动服务，停止设备或打印队列以及关闭计算机所需的所有权限。将此角色指派给负责管理资源对象的助理管理员。

Transform a User （转换用户）

提供向模板帐户中的组添加或去除用户所需的所有权限，包括在转换用户时修改用户属性的权限。

Unified Change History Server Administration （统一的更改历史记录服务器管理）

提供配置、查看和删除统一的更改历史记录服务器配置所需的权限。

User Administration （用户管理）

提供管理用户帐户、关联的 Microsoft Exchange 邮箱和组成员资格所需的所有权限。将此角色指派给负责管理用户帐户的助理管理员。

查看 Active Directory Collector （Active Directory 收集器）、 DRA Collector （DRA 收集器）、Management Reporting Collector （管理报告收集器）和 Database Configuration （数据库配置）信息

提供查看 AD Collector （AD 收集器）、 DRA Collector （DRA 收集器）、 Management Reporting Collector （管理报告收集器）和数据库配置信息所需的所有权限。

View All Computer Properties （查看所有计算机属性）

提供查看计算机帐户属性所需的所有权限。将此角色指派给负责审计计算机的助理管理员。

View All Group Properties （查看所有组属性）

提供查看组属性所需的所有权限。将此角色指派给负责审计组的助理管理员。

View All Resource Mailbox Properties （查看所有资源邮箱属性）

提供查看资源邮箱属性所需的所有权限。将此角色指派给负责审计资源邮箱的助理管理员。

View All User Properties （查看所有用户属性）

提供查看用户帐户属性所需的所有权限。将此角色指派给负责审计用户帐户的助理管理员。

Workflow Automation Server Administration （工作流程自动化服务器管理）

提供配置、查看和删除工作流程自动化服务器配置所需的权限。

WTS Administration （WTS 管理）

提供在 ActiveView 中管理用户帐户的 Windows Terminal Server (WTS) 属性所需的所有权限。如果您使用 WTS，请将此角色指派给负责维护用户帐户的 WTS 属性的助理管理员。

访问内置角色

访问内置角色以审计默认委托模型或管理您自己的安全设置。

要访问内置角色：

1. 导航到 **Delegation Management** （委托管理） > **Manage Roles** （管理角色）。
2. 确保搜索字段为空，然后单击 **List items that match my criteria** （列出与我的准则匹配的项目）窗格中的 **Find Now** （立即查找）。
3. 选择相应的角色。

使用内置角色

您无法删除或修改内置角色。但是，您可以将内置角色合并到现有的委托模型中，或使用这些角色来设计和实施您自己的模型。

您可以通过以下方式使用内置角色：

- 将内置角色与用户帐户或助理管理员组关联。此关联可为用户或助理管理员组成员提供相应的任务权限。
- 克隆内置角色并将该克隆用作自定义角色的基础。您可以为此新角色添加其他角色或权限，并去除最初内置角色中所包含的权限。

有关设计动态委托模型的更多信息，请参见了解动态委托模型。

创建自定义角色

通过创建角色，您可以快速轻松地委托一组代表管理任务或工作流程的权限。您可以从 Delegation and Configuration （委托和配置）控制台中的 **Delegation Management** （委托管理） > **Roles** （角色）节点创建和管理角色。在此节点中，您可以执行以下操作：

- 创建新角色
- 克隆现有角色
- 修改角色属性
- 删除角色
- 管理角色指派
  - 委托新指派
  - 去除现有指派
  - 查看指派的助理管理员的属性
  - 查看指派的 ActiveView 的属性
- 管理角色和角色中的权限 （角色可以嵌套）
- 生成角色更改报告

执行本节中列出的任何操作的常规工作流程是选择角色节点，然后执行任意下列操作：

- 使用任务或右键单击菜单打开适用的向导或对话框以执行必要的操作。
- 在 **List items that match my criteria** （列出与我的准则匹配的项目）窗格中找到角色对象，然后使用任务或右键单击菜单选择并打开相应的向导或对话框以执行必要的操作。

要执行上述任何操作，您必须具有相应的权限，例如 Manage Security Model （管理安全模型）角色中所包含的权限。

11 权限

权限是“最小特权”管理的初始构建块。为用户指派权限可帮助您实施和维护动态安全模型。您可以在 Delegation and Configuration （委托和配置）控制台中执行这些过程。

内置权限

有超过 390 种内置权限用于管理对象和执行常见的管理任务，您可以在定义角色和进行委托指派时使用这些权限。无法删除内置权限，但可以克隆它们以创建自定义权限。下面列出了一些内置权限的示例：

创建组和修改所有属性

提供创建组和在创建组期间指定所有属性的权限。

删除用户帐户

如果启用了回收站，则提供将用户帐户移动到回收站的权限。如果禁用了回收站，则提供永久删除用户帐户的权限。

修改所有计算机属性

提供修改计算机帐户所有属性的权限。

实施自定义权限

要创建自定义权限，您可以创建新权限或克隆现有权限。您可以使用现有权限作为新权限委托的模板。权限定义了助理管理员可以在受管域或子树中查看、修改或创建的对象的属性。自定义权限可以包括对多个属性的访问权限，例如 *View All User Properties* （查看所有用户属性）权限。

注释：无法克隆所有内置权限。

您可以从 Delegation and Configuration （委托和配置）控制台中的 **Delegation Management** （委托管理） > **Powers** （权限）节点实施自定义权限。在此节点中，您可以执行以下操作：

- 查看所有权限属性
- 创建新权限
- 克隆现有权限
- 修改自定义权限
- 生成权限更改报告

要执行上述操作，您必须具有相应的权限，例如 Manage Security Model （管理安全模型）角色中所包含的权限。

在尝试创建新权限之前，请考虑以下过程。

1. 查看 DRA 提供的权限。
2. 决定是否需要自定义权限。如果适用，您可以克隆现有的自定义权限。
3. 完成相应的向导驱动过程。例如，完成 New Power （新建权限）向导。
4. 查看您的新权限。
5. 如有必要，修改您的新权限。

执行本节中列出的任何操作的常规工作流程是选择**权限**节点，然后执行任意下列操作：

- 使用“任务”或右键单击菜单打开适用的向导或对话框以执行必要的操作。
- 在 **List items that match my criteria** （列出与我的准则匹配的项目）窗格中找到权限对象，然后使用**任务**或右键单击菜单选择并打开适用的向导或对话框以执行必要的操作。

扩展权限

您可以通过扩展权限向该权限添加许可权限或功能。

例如，要允许助理管理员创建用户帐户，您可以指派 *Create User and Modify All Properties* （创建用户和修改所有属性）权限或 *Create User and Modify Limited Properties* （创建用户和修改有限属性）权限。如果您还指派 *Add New User to Group* （将新用户添加到组）权限，则助理管理员可以在使用 Create User （创建用户）向导时将此新用户帐户添加到组中。在这种情况下，*Add New User to Group*（将新用户添加到组）权限将提供其他向导功能。*Add New User to Group* （将新用户添加到组）权限是**扩展权限**。

扩展权限无法自行添加许可权限或功能。要成功委托包含扩展权限的任务，您必须指派扩展权限以及要扩展的权限。

注释：

- 要成功创建组并在 ·ActiveView· 中包含新组，您必须在指定的 ·ActiveView· 中拥有 *Add New Group to ActiveView* （将新组添加到 ActiveView）权限。指定的 ActiveView 还必须包括将包含新组的 OU 或内置容器。
- 要成功克隆组并在 ·ActiveView· 中包含新组，您必须在指定的 ·ActiveView· 中拥有*将克隆组添加到 ·ActiveView* 权限。指定的 ActiveView 还必须包括源组以及将包含新组的 OU 或内置容器。

下表列出了在创建新权限或修改现有权限属性时可配置的一些操作示例：

委托此任务	指派此权限	和此扩展权限
克隆组并在指定的 ActiveView 中包含新组	克隆组和修改所有属性	将克隆组添加到 ActiveView
创建组并在指定的 ActiveView 中包含新组	创建组和修改所有属性	将新组添加到 ActiveView

委托此任务	指派此权限	和此扩展权限
创建已启用邮件的联系人	创建联系人和修改所有属性 创建联系人和修改有限属性	为新联系人启用电子邮件
创建已启用邮件的组	创建组和修改所有属性	为新组启用电子邮件
创建已启用邮件的用户帐户	创建用户和修改所有属性 创建用户和修改有限属性	为新用户启用电子邮件
创建用户帐户并将新帐户添加到特定组	创建用户和修改所有属性 创建用户和修改有限属性	将新用户添加到组

12 委托指派

您可以从 Delegation and Configuration （委托和配置）控制台中的 **Delegation Management** （委托管理） > **Assistant Admin** （助理 Admin）节点管理委托指派。在此节点中，您可以查看指派给助理管理员的权限和角色，以及管理角色和 ActiveView 的指派。您还可以对助理 Admin 组执行以下操作：

- 添加组成员
- 创建组
- 克隆组
- 删除组
- 修改组属性

要查看和管理指派并对助理 Admin 组进行更改，您必须具有相应的权限，例如 Manage Security Model （管理安全模型）角色中所包含的权限。

执行本节中列出的任何操作的常规工作流程是选择**助理 Admin** 节点，然后执行任意下列操作：

- 使用“任务”或右键单击菜单打开适用的向导或对话框以执行必要的操作。
- 在**列出与我的准则匹配的项目**窗格中找到组或助理管理员，然后使用**任务**或右键单击菜单选择并打开适用的向导或对话框以执行必要的操作。

V 策略和流程自动化

本章提供的信息可帮助您了解策略在 DRA 环境中的运作方式以及相关策略选项。此外，本章还解释了在使用 Active Directory 中的对象时，如何使用触发器和自动化的工作流程来自动化流程。

13 了解 DRA 策略

DRA 可让您配置各种策略，以帮助您保护企业安全并防止数据损坏。这些策略在动态安全模型的环境中执行，从而确保策略实施自动跟上不断变化的企业。通过建立策略 （如命名约定、磁盘用量限制和属性验证），您可以实施有助于维护企业数据完整性的规则。

在 DRA 中，您可以快速定义以下企业管理方面的策略规则：

- Microsoft Exchange
- Office 365 许可证
- 用户主目录
- 口令生成

DRA 还将为组、用户帐户和计算机提供内置策略。

要管理或定义策略，您必须具备相应权限，例如 DRA Admin 或 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。为了帮助您管理策略， DRA 提供了 “ 策略细节 ” 报告。此报告提供以下信息：

- 指示策略是否已启用。
- 列出关联的操作
- 列出受此策略管理的对象
- 提供策略范围细节

您可以使用此报告确保正确定义策略。您还可以使用此报告来比较策略属性、捕获冲突并在整个企业中更好地实施策略。

管理服务器如何实施策略

您可以将每个任务或管理操作与一个或多个策略相关联。执行与策略关联的操作时，管理服务器将运行该策略并强制执行指定的规则。如果服务器检测到策略违规，则会返回错误讯息。如果服务器未检测到策略违规，则会完成操作。您可以通过将策略与特定 ActiveView 或助理 Admin 组关联来限制策略的范围。

如果操作与多个策略关联，则管理服务器会按字母顺序强制执行策略。也就是说，无论指定的规则如何，策略 A 都将在策略 B 之前实施。

要确保策略不会相互冲突，请使用以下准则：

- 对策略进行命名，使其按正确顺序执行
- 校验每个策略是否不会干扰其他策略执行的验证或操作
- 在生产环境中实施自定义策略之前，请对其进行彻底测试

每次策略运行时，管理服务器都会在审计日志中输入策略状态。这些日志条目会记录返回代码、关联操作、作用对象以及自定义策略是否成功。

警告：使用管理服务帐户运行策略。由于服务帐户具有管理员许可权限，因此策略可以完全访问所有企业数据。因此，与内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色关联的助理管理员可以获得比预期更多的权限。

内置策略

安装管理服务器时会实施内置策略。使用这些策略时，可能会遇到以下术语：

策略范围

定义 DRA 应用策略的对象或属性。例如，一些策略允许您将策略应用于特定 ActiveView 中的特定助理管理员。一些策略允许您从不同类的对象中进行选择，例如用户帐户或组。

全局策略

对受管域中指定类或类型的所有对象实施策略规则。全局策略不允许您限制策略适用的对象范围。

策略关系

定义联合应用还是单独应用策略。要建立策略关系，请定义应用于同一操作的两个或多个规则，然后选择策略组选项中的成员。如果操作参数或属性与任何规则匹配，则操作成功。

内置策略主题：

- 了解内置策略 （第 118 页）
- 可用策略 （第 119 页）
- 使用内置策略 （第 121 页）

了解内置策略

内置策略提供业务规则以解决常见的安全性和数据完整性问题。这些策略是默认安全模型的一部分，允许您将 DRA 安全功能集成到现有企业配置中。

DRA 提供了两种实施策略的方法。您可以创建自定义策略或从多个内置策略中进行选择。内置策略使您可以轻松应用策略，而无需开发自定义脚本。如果您需要实施自定义策略，则可以调整现有的内置策略以满足您的需求。大多数策略允许您修改错误讯息文本、重命名策略、添加说明以及指定如何应用策略。

安装 DRA 时会启用许多内置策略。默认情况下会实施以下策略。如果您不想实施这些策略，可以禁用或删除它们。

策略名称	默认值	说明
$ComputerNameLengthPolicy	64 15 （Windows 2000 之前）	限制计算机名称或 Windows 2000 之前的计算机名称中的字符数
$GroupNameLengthPolicy	64 20 （Windows 2000 之前）	限制组名称或 Windows 2000 之前的组名称中的字符数
$GroupSizePolicy	5000	限制组中的成员数
$NameUniquenessPolicy	无	确保 Windows 2000 之前和 CN 的名称在所有受管域中都是唯一的
$SpecialGroupsPolicy	无	防止环境中未经检查的权限升级。
$UCPowerConflictPolicy	无	通过使用户克隆和用户创建权限相互排斥来防止权限升级
$UPNUniquenessPolicy	无	确保 UPN 名称在所有受管域中都是唯一的
$UserNameLengthPolicy	64 20 （下层登录名）	限制用户登录名或下层登录名中的字符数

可用策略

DRA 提供了几种可以为您的安全模型自定义的策略。

注释：您可以创建一个策略，该策略需要 DRA 用户界面中当前不可用的属性条目。如果策略需要条目，并且用户界面未提供输入值的字段 （例如新用户帐户的部门），则您将无法创建或管理该对象。要避免此问题，请配置仅需要可从用户界面访问的属性的策略。

Create a Custom Policy （创建自定义策略）

允许您将脚本或可执行文件链接到 DRA 或 Exchange 操作。自定义策略可让您验证您选择的任何操作。

Enforce a Maximum Name Length （实施最大名称长度）

允许您全局实施用户帐户、组、 OU、联系人或计算机的最大名称长度。

策略将检查名称容器 （常用名或 cn）和 Windows 2000 之前的名称 （用户登录名）。

Enforce Maximum Number of Group Members （实施最大组成员数）

允许您对组中的成员数实施全局限制。

Enforce Unique Pre-Windows 2000 Account Names （实施唯一的 Windows 2000 之前的帐户名称）

校验 Windows 2000 之前的名称在所有受管域中是否唯一。在 Microsoft Windows 域中，Windows 2000 之前的名称在域中必须是唯一的。此全局策略将在所有受管域中实施此规则。

Enforce unique User Principal Names (UPNs) （实施唯一的用户主体名称 (UPN)）

校验用户主体名称 (UPN) 在所有受管域中是否唯一。在 Microsoft Windows 域中， UPN 在域中必须是唯一的。此策略将在所有受管域中实施此规则。由于这是一个全局策略，因此 DRA 会提供策略名称、说明和策略关系。

Limit actions on members of special groups （限制对特殊组成员的操作）

阻止您管理管理员组的成员，除非您是该管理员组的成员。默认情况下启用此全局策略。

当您限制对管理员组成员的操作时， Create Policy Wizard（创建策略向导）不需要其他信息。您可以指定自定义错误讯息。由于这是一个全局策略，因此 DRA 会提供策略名称、说明和策略关系。

Prevent assistant administrators from Creating and Cloning Users in Same AV （防止助理管理员在同一 AV 中创建和克隆用户）

防止可能的权限升级。启用此策略后，您可以创建用户帐户或克隆用户帐户，但不能同时拥有这两种权限。此全局策略可确保您无法在同一 ActiveView 中创建和克隆用户帐户。

此策略不需要其他信息。

Set Naming Convention Policy （设置命名约定策略）

允许您建立适用于特定助理管理员、 ActiveView 和对象类 （例如用户帐户或组）的命名约定。

您还可以指定此策略监控的确切名称。

Create a Policy to Validate a Specific Property （创建策略以验证特定属性）

允许您创建策略以验证 OU 或帐户对象的任何属性。您可以指定默认值、属性格式掩码以及有效值和范围。

使用此策略可在创建、克隆或修改特定对象的属性时，通过验证特定条目字段来实施数据完整性。此策略提供了极大的灵活性和强大的功能，可以验证条目、提供默认条目以及限制各种属性字段的条目选择。通过使用此策略，您可以要求在任务完成之前进行正确的输入，从而维护受管域中的数据完整性。

例如，假设您有三个部门：制造、销售和管理。您可以将 DRA 将接受的条目限制为这三个值。您还可以使用此策略实施正确的电话号码格式、提供有效数据的范围或要求输入电子邮件地址字段。要为电话号码指定多个格式掩码，例如 (123)456 7890 以及 456 7890，请将属性格式掩码定义为 (###)### ####,### ####。

Create Policy to Enforce Office 365 Licenses （创建实施 Office 365 许可证的策略）

允许您创建策略以根据 Active Directory 组成员资格指派 Office 365 许可证。当从相关 Active Directory 组中删除成员时，此策略还会强制去除 Office 365 许可证。

如果将未同步到云的用户添加到 Active Directory 组，则会在向该用户指派 Office 365 许可证之前同步该用户。

在创建策略时，您可以指定多个属性和设置，例如策略名称和助理管理员尝试执行违反此策略的操作时显示的错误讯息词句。

Ensure only licenses assigned by DRA policies are enabled on accounts. All other licenses will be removed.（确保只会对帐户启用 DRA 指派的许可证。将去除所有其他许可证。）设置包含在 Tenant Properties（租户属性）页面中，可以对每个租户配置。此设置用于针对 DRA Office 365 许可证策略，配置许可证指派的实施方式：

启用此设置时， DRA 许可证实施将确保只有通过 DRA 策略指派的许可证才能供应给帐户（在 DRA 之外指派的许可证将从指派给许可证策略的帐户去除）。禁用此设置时 （默认）， DRA 许可证实施将仅确保将 Office 365 策略中包含的特定许可证供应给帐户 （帐户从许可证策略中取消指派时，将仅取消供应由该策略指派的许可证）。

使用内置策略

由于内置策略是默认安全模型的一部分，因此您可以使用这些策略来实施当前的安全模型或修改它们以更好地满足您的需求。您可以更改多个内置策略的名称、规则设置、范围、策略关系和错误讯息。您可以启用或禁用每个内置策略。

您还可以轻松创建新策略。

实施自定义策略

自定义策略允许您充分利用默认安全模型的功能和灵活性。通过使用自定义策略，您可以将 DRA 与现有企业组件集成，同时确保实施您的专有规则。您可以使用自定义策略功能来扩展企业策略。

通过将可执行文件或脚本与管理操作相关联，您可以创建和实施自定义策略。例如，与 UserCreate 操作关联的策略脚本可以检查您的人力资源数据库以查看指定的员工是否存在。如果员工存在于人力资源数据库中且没有现有帐户，则该脚本将从数据库中检索员工 ID、名字和姓氏。操作成功完成，用户帐户属性窗口填充相应信息。但是，如果员工已拥有帐户，则操作失败。

脚本将为您提供极大的灵活性和强大的功能。要创建自己的策略脚本，可以使用 Directory and Resource Administrator ADSI 提供程序 （ADSI 提供程序）、软件开发包 (SDK) 和 PowerShell cmdlet。有关创建自己的策略脚本的更多信息，请参见 DRA 文档网站中的 Reference （参考）部分。

限制本机内置安全组

为了提供更安全的环境， DRA 允许您限制授予 Microsoft Windows 内置安全组的权限。修改组成员资格、内置安全组属性或组成员属性的功能可能具有重要的安全隐患。例如，如果您可以更改 Server Operators （服务器操作员）组中用户的口令，则可以以该用户身份登录并执行委托给此内置安全组的权限。

DRA 通过提供策略来检查您对本机内置安全组及其成员的权限，从而防止这一安全问题。此验证可确保您请求的操作不会升级这些权限。启用此策略后，作为内置安全组 （例如 Server Operators （服务器操作员）组）成员的助理管理员只能管理同一组的其他成员。

可以限制的本机内置安全组

您可以使用 DRA 策略限制以下 Microsoft Windows 内置安全组的权限：

- 帐户操作员
- 管理员
- 备份操作员
- 证书发布者
- DNS Admin
- 域 Admin
- 企业 Admin
- 组策略创建者所有者
- 打印操作员
- 纲要 Admin

注释：DRA 通过内部标识符引用内置安全组。因此，即使重命名组， DRA 也支持这些组。此功能可确保 DRA 支持在不同国家 / 地区使用不同名称的内置安全组。例如， DRA 引用具有相同内部标识符的管理员组和 *Administratoren* 组。

限制对本机内置安全组的操作

DRA 使用策略来限制本机内置安全组及其成员可以执行的权限。 $SpecialGroupsPolicy 策略可限制本机内置安全组的成员可以对其他成员或其他本机内置安全组执行的操作。 DRA 默认启用此策略。如果您不想限制对本机内置安全组及其成员的操作，则可以禁用此策略。

启用此策略后， DRA 将使用以下验证测试来确定是否允许对本机内置安全组或其成员执行操作：

- 如果您是 Microsoft Windows 管理员，则可以对具有相应权限的本机内置安全组及其成员执行操作。
- 如果您是内置安全组的成员，只要您具有相应的权限，则可以对同一内置安全组及其成员执行操作。
- 如果您不是内置安全组的成员，则无法修改内置安全组或其成员。

例如，如果您是 Server Operators （服务器操作员）和 Account Operators （帐户操作员）的成员，并且具有相应的权限，则可以对 Server Operators （服务器操作员）组的成员、 Account Operators （帐户操作员）组的成员或两个组的成员执行操作。但是，您无法对作为打印操作员组和 Account Operators （帐户操作员）组成员的用户帐户执行操作。

DRA 限制您对本机内置安全组执行以下操作：

- 克隆组
- 创建组
- 删除组
- 将成员添加到组
- 从组中去除成员
- 将组移动到 OU
- 修改组的属性
- 复制邮箱
- 去除邮箱
- 克隆用户帐户
- 创建用户帐户
- 删除用户帐户
- 将用户帐户移动到 OU
- 修改用户帐户属性

DRA 还限制操作以确保您不会获得对象的权限。例如，当您向组添加用户帐户时， DRA 会检查以确保您不会因为该用户帐户是该组的成员而获得该用户帐户的额外权限。此验证有助于防止权限升级。

管理策略

通过 Policy and Automation Management （策略和自动化管理）节点，您可以访问 Microsoft Exchange 和用户主目录策略，以及内置和自定义策略。使用以下常见任务来提高企业安全性和数据完整性。

配置 Exchange 策略

允许您定义 Microsoft Exchange 配置、邮箱策略、自动命名和代理生成规则。这些规则可以定义在助理管理员创建、修改或删除用户帐户时邮箱的管理方式。

配置用户主目录策略

可用于在助理管理员创建、重命名或删除用户帐户时，自动创建、重命名或删除主目录和主共享。用户主目录策略还允许您为 Microsoft Windows 服务器以及非 Windows 服务器上的用户主目录启用或禁用磁盘配额支持。

配置口令生成策略

允许您定义 DRA 生成的口令的要求。

有关在 DRA 中管理策略的更多详细信息，请参见以下章节：

- Microsoft Exchange 策略 （第 124 页）
- Office 365 许可证策略 （第 125 页）
- 创建和实施用户主目录策略 （第 126 页）
- 启用口令生成 （第 131 页）
- 策略任务 （第 131 页）

Microsoft Exchange 策略

Exchange 提供了多种策略来帮助您更有效地管理 Microsoft Exchange 对象。Microsoft Exchange 策略允许您自动执行邮箱管理、实施别名和邮箱储存的命名约定，并自动生成电子邮件地址。

这些策略可以帮助您简化工作流程并维护数据完整性。例如，您可以指定在创建、修改或删除用户帐户时 Exchange 管理邮箱的方式。要定义和管理 Microsoft Exchange 策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。

指定默认电子邮件地址策略

要指定默认电子邮件地址策略，您必须具备相应的权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限，并且您的许可证必须支持 Exchange 产品。

要指定默认电子邮件地址策略：

1 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略） > **Proxy Generation** （代理生成）。

2 指定 Microsoft Exchange 服务器的域。

   2a 单击**浏览**。

   2b 根据需要指定其他搜索准则，然后单击 **Find Now** （立即查找）。

   2c 选择要配置的域，然后单击**确定**。

3 为所选域指定代理生成规则。

   3a 单击**添加**。

   3b 选择代理类型。例如，单击**因特网地址**。

   3c 接受默认值或键入新的代理生成规则，然后单击**确定**。

   有关代理生成规则支持的替换字符串的更多信息，请参见 Delegation and Configuration （委托和配置）客户端策略

4 单击 **Custom attributes** （自定义属性）以编辑自定义邮箱属性的自定义名称。

   4a 选择属性并单击 **Edit** （编辑）按钮。

   4b 在 Attribute Properties （属性）窗口中，在 **Custom name** （自定义名称）字段中输入属性名称，然后单击**确定**。

5 单击**确定**。

注释：DRA 策略 Admin 应具有 *Manage Custom Tools* （管理自定义工具）的权限，以修改 Microsoft Exchange 策略中的自定义属性。

邮箱规则

邮箱规则允许您指定在助理管理员创建、克隆、修改或删除用户帐户时 Exchange 管理邮箱的方式。邮箱规则将根据助理管理员管理关联用户帐户的方式自动管理 Microsoft Exchange 邮箱。

注释：在 Microsoft Windows 域中启用 **Do not allow Assistant Admins to create a user account without a mailbox** （不允许助理 Admin 创建没有邮箱的用户帐户）选项时，请确保助理管理员有权克隆或创建用户帐户。启用此选项需要助理管理员使用邮箱创建 Windows 用户帐户。

要指定 Microsoft Exchange 邮箱规则，您必须具备相应的权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限，并且您的许可证必须支持 Exchange 产品。

要指定 Exchange 邮箱规则：

1 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略） > **Mailbox Rules** （邮箱规则）。

2 选择在创建或修改用户帐户时希望 Exchange 实施的邮箱策略。

3 单击**确定**。

Office 365 许可证策略

要指定 Office 365 许可证策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。您的许可证还必须支持 Microsoft Exchange 产品。

允许 DRA 管理 Office 365 许可证 （可选）

如果要允许 DRA 管理 Office 365 许可证，则必须执行以下操作：

- 创建许可证强制策略。
- 在租户属性页上启用 **license update schedule** （许可证更新日程表）。

创建实施 Office 365 许可证的策略

要创建用于实施 Office 365 许可证的策略，请单击 Delegation and Configuration （委托和配置）控制台中的 **Policy and Automation Management** （策略和自动化管理）节点，然后选择 **New Policy** （新建策略） > **Create New Policy to Enforce Office 365 Licenses** （创建新策略以实施 Office 365 许可证）。

当实施策略并将用户添加到 Active Directory 中时，DRA 会使用组成员资格自动将 Office 365 许可证指派给用户。

Office 365 许可证更新日程表

除非您还在租户属性页上启用 **License update schedule** （许可证更新日程表），否则在 DRA 之外进行更改时，不会应用您为实施 Office 365 许可证而创建的策略。许可证更新作业可确保指派给用户的 Office 365 许可证与您的 Office 365 许可证策略匹配。

许可证更新作业和 Office 365 许可证策略协同工作，以确保仅为所有受管用户指派其应该拥有的 Office 365 许可证。

注释：

- DRA 不会管理仅限联机使用的用户帐户的 Office 365 许可证。要使 DRA 能够使用 Office 365 许可证管理您的用户，必须将这些用户与 Active Directory 同步。
- 如果选择使用 DRA 管理 Office 365 许可证，则在下次运行许可证更新作业时， DRA 将覆盖在 DRA 之外对 Office 365 许可证所做的任何手动更改。
- 如果在确保正确配置 Office 365 许可证策略之前启用 Office 365 许可证更新作业，则在运行许可证更新作业后，指派的许可证可能不正确。

创建和实施用户主目录策略

当您管理大量用户帐户时，创建和维护这些用户主目录和共享可能需要大量时间，并且可能成为安全错误的来源。每次创建、重命名或删除用户时都可能需要进行额外的维护。用户主目录策略可帮助您管理用户主目录和主共享维护。

DRA 允许您自动创建和维护用户主目录。例如，您可以轻松配置 DRA，以便管理服务器在您创建用户帐户时创建用户主目录。在这种情况下，如果在创建用户帐户时指定用户主目录路径，则服务器会根据指定的路径自动创建用户主目录。如果未指定路径，则服务器不会创建用户主目录。

在创建用户主目录或为允许的父路径中的用户配置用户主目录策略期间， DRA 支持分布式文件系统 (DFS) 路径。您可以在 Netapp Filer 和 DFS 路径或分区上创建、重命名和删除用户主目录。

配置用户主目录策略

要配置用户主目录、共享和卷磁盘配额策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。每个策略都会根据您管理关联用户帐户的方式自动管理用户主目录、共享和卷磁盘配额。

要配置用户主目录策略，请导航到 **Policy and Automation Management**（策略和自动化管理）> **Configure Home Directory Policies** （配置用户主目录策略）。

- 用户主目录
- 主共享
- 主卷磁盘配额

管理服务器要求

对于需要创建主共享的每台计算机，管理服务器服务帐户或访问帐户应是该计算机上的管理员或相应域中管理员组的成员。

DRA 管理和储存用户主目录的每个驱动器必须存在管理共享，例如 C$ 或 D$。DRA 使用管理共享来执行一些用户主目录和主共享自动化任务。如果这些共享不存在，则 DRA 无法提供用户主目录和主共享自动化。

为 NetApp Filer 配置用户主目录允许的路径

要为 NetApp Filer 配置允许的父路径：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Home Directory Policies** （配置用户主目录策略）。
2. 在 **Allowable parent paths** （允许的父路径）文本框中，输入下表中的一个允许的路径：

共享类型	允许的路径
Windows	(*FileName**adminshare:**volumerootpath**directory path*)
非 Windows	(*non-windows**share*)

3. 单击**添加**。
4. 对于要应用用户主目录策略的每个允许的父路径，重复步骤 1 至 3。

了解用户主目录策略

为了与相应的 Microsoft Windows 安全策略保持一致， DRA 仅在目录级别创建访问控制限制。在共享名称级别和文件或目录对象级别设置访问控制限制，通常会导致管理员和用户的访问方案混乱。

当您更改主共享的访问控制限制时， DRA 不会更改该目录的现有安全性。在这种情况下，您必须确保用户帐户对其自己的用户主目录拥有相应的访问权限。

用户主目录自动化和规则

在修改用户帐户时， DRA 会通过管理用户主目录来自动执行用户主目录维护任务。创建、克隆、修改、重命名或删除用户帐户时， DRA 可以执行不同的操作。

要成功实施用户主目录策略，请考虑以下准则：

- 确保指定的路径使用正确的格式。
  - 要指定单个用户主目录的路径，请使用下表中的一个模板：

共享类型	路径模板
Windows	*computer**share*\. 例如，如果您希望 DRA 在 server01 计算机上的 Home Share （主共享）文件夹中自动创建用户主目录，请键入 \\server01\Home Share\
非 Windows	*non-windows**share*

  - 要在相应主共享的根目录上标准化用户主目录管理，请使用 Universal Naming Convention （通用命名约定）语法，例如 *server name**C:*\ *根目录路径*。
  - 要指定嵌套用户主目录的路径，请使用下表中的一个模板：

共享类型	路径模板
Windows	*computer**share**first directory**second directory*\ 例如，如果您希望 DRA 在 server01 计算机上的 Home Share 文件夹下的现有 JSmith\Home directory 中自动创建用户主目录，请键入 \\server01\Home Share\JSmith\Home。
非 Windows	*non-windows**share**first directory**second directory*\

注释： DRA 还支持以下格式：*computer**share**username* 和 *computer**share**%username%*。在每种情况下， DRA 都会自动为关联的用户帐户创建用户主目录。

- 在 NetApp Filer 上定义用于管理用户主目录的策略或自动化触发器时，需要使用不同的目录规范格式。
  - 如果使用的是 NetApp Filer，请按以下格式指定父目录：*FilerName**adminshare:**volumerootpat*h*directorypath*
  - adminshare 变量是映射到 NetApp Filer 上的根卷的隐藏共享，例如 *c$*。例如，如果 NetApp Filer （称为 usfiler）上共享的本地路径为 c$\vol\vol0\mydirectory，则可以为 NetApp Filer 指定 \\usfiler\c:\vol\vol0\mydirectory 根路径。

- 要在创建用户主目录或为用户配置用户主目录策略时指定 DFS 路径，请使用 *server**root*\<*link*> format，其中 root 可以是受管域，也可以是以下格式的独立根目录：*FilerName**adminshare:**volumerootpath**directorypath*。
- 创建共享目录以储存此用户帐户的用户主目录。
- 确保 DRA 可以访问路径中引用的计算机或共享。

创建用户帐户时创建用户主目录

此规则允许 DRA 自动为新用户帐户创建用户主目录。 DRA 创建用户主目录时，管理服务器将使用 Create User Wizard （创建用户向导）中**用户主目录**字段中指定的路径。您可以稍后通过用户属性窗口的“配置文件”选项卡修改此路径， DRA 会将用户主目录移动到新位置。如果未指定这些字段的值，则 DRA 不会为该用户帐户创建用户主目录。

DRA 会根据所选的**用户主目录许可权限**选项设置新目录的安全性。使用这些选项可以控制所有用户主目录的常规访问。

例如，您可以指定管理员组的成员具有完全控制权，而 Help Desk 组的成员对创建用户主目录的共享拥有读取访问权限。然后，当 DRA 创建用户主目录时，新的用户主目录可以从父目录继承这些权限。因此，管理员组的成员可以完全控制所有用户主目录，而 Help Desk 组的成员对所有用户主目录拥有读取访问权限。

如果指定的用户主目录已存在，则 DRA 不会创建用户主目录，也不会修改现有的目录许可权限。

重命名用户帐户时重命名用户主目录

此规则允许 DRA 自动执行以下操作：

- 指定新的用户主目录路径时创建用户主目录
- 更改用户主目录路径时移动用户主目录内容
- 重命名用户帐户时重命名用户主目录

重命名用户帐户时， DRA 会根据新的帐户名重命名现有用户主目录。如果现有用户主目录当前正在使用中，则 DRA 将使用新名称创建新用户主目录，并且不会更改现有用户主目录。

更改用户主目录路径时， DRA 会尝试创建指定的用户主目录，并将先前用户主目录的内容移动到新位置。您还可以配置用户主目录策略以创建用户主目录，而无需移动现有用户主目录中的内容。 DRA 还会将从先前目录中指派的 ACL 应用于新目录。如果指定的用户主目录已存在，则 DRA 不会创建此新目录，也不会修改现有的目录许可权限。如果先前的用户主目录未锁定，则 DRA 会将其删除。

当 DRA 重命名用户主目录失败时， DRA 会尝试使用新名称创建新的用户主目录，并将先前用户主目录中的内容复制到新的用户主目录中。然后， DRA 将尝试删除先前的用户主目录。您可以将 DRA 配置为不将先前用户主目录中的内容复制到新用户主目录，并手动将先前用户主目录中的内容移动到新用户主目录，以避免复制打开的文件等问题。

删除先前的用户主目录时， DRA 需要显式许可权限才能从先前的用户主目录中删除只读文件和子目录。您可以为 DRA 提供从先前用户主目录中显式删除只读文件和子目录的许可权限。

允许主共享的父目录或路径

DRA 允许您为文件服务器上的主共享指定允许的父目录或路径。如果要指定多个目录或文件服务器路径，则可以将这些路径导出到 CSV 文件，并使用 DRA 控制台将 CSV 文件中的路径添加到 DRA。 DRA 使用在允许的父路径字段中输入的信息来确保：

- 当助理管理员删除用户帐户和用户帐户用户主目录时， DRA 不会删除文件服务器上的父目录。
- 重命名用户帐户或更改用户帐户的用户主目录路径时， DRA 会将用户主目录移动到文件服务器上的有效父目录或路径。

删除用户帐户时删除用户主目录

在您删除关联的用户帐户时，此规则允许 DRA 自动删除用户主目录。如果启用了回收站，则在从回收站中删除用户帐户之前， DRA 不会删除用户主目录。删除用户主目录时， DRA 需要显式许可权限才能从先前的用户主目录中删除只读文件和子目录。您可以为 DRA 提供从先前用户主目录中显式删除只读文件和子目录的许可权限。

主共享自动化和规则

当您修改用户帐户或管理用户主目录时， DRA 会通过管理主共享来自动执行主共享维护任务。创建、克隆、修改、重命名或删除用户帐户时， DRA 可以执行不同的操作。

为了与相应的 Microsoft Windows 安全策略保持一致， DRA 不会在共享名称级别创建访问控制限制。相反， DRA 仅在目录级别创建访问控制限制。在共享名称级别和文件或目录对象级别设置访问控制限制，通常会导致管理员和用户的访问方案混乱。

注释：指定的位置必须在用户主目录的上一级具有共同的主共享，例如 HOMEDIRS。

例如，此路径有效：*HOUSERV1**HOMEDIRS**%username%*

此路径无效：*HOUSERV1**%username%*

指定主共享名称

定义主共享自动化规则时，您可以为每个自动创建的主共享指定前缀和后缀。通过指定前缀或后缀，您可以实施主共享的命名约定。

例如，您启用 Create home directory （创建用户主目录）和 Create home share automation rules （创建主共享自动化规则）。对于主共享，您指定下划线前缀和美元符号后缀。创建名为 TomS 的用户时，将其新目录映射到 U 盘并指定 \\HOUSERV1\HOMEDIRS\%username% 作为目录路径。在此示例中， DRA 将创建名为 _TomS$ 的网络共享，该共享指向 \\HOUSERV1\HOMEDIRS\TomS directory。

为新用户帐户创建主共享

DRA 创建主共享时，管理服务器将使用 Create User Wizard （创建用户向导）中用户主目录字段中指定的路径。您可以稍后通过用户属性窗口的“配置文件”选项卡修改此路径。

DRA 通过将指定的前缀和后缀 （如果有）添加到用户名来创建共享名称。如果使用长用户帐户名， DRA 可能无法添加指定的主共享前缀和后缀。前缀和后缀以及允许的连接数基于您选择的主共享创建选项。

为克隆的用户帐户创建主共享

如果从新创建的用户帐户名生成的主共享名称已存在，则 DRA 将删除现有共享并为指定的用户主目录创建新共享。

克隆用户帐户时，当前必须存在现有用户帐户的共享名称。克隆用户帐户时， DRA 还会克隆用户主目录信息并为新用户自定义该信息。

修改主共享属性

更改用户主目录位置时， DRA 将删除现有共享并为新用户主目录创建新共享。如果原始用户主目录为空，则 DRA 将删除原始目录。

为重命名的用户帐户重命名主共享

重命名用户帐户时， DRA 会删除现有的主共享，并根据新帐户名创建新共享。新共享将指向现有用户主目录。

删除已删除用户帐户的主共享

永久删除用户帐户时， DRA 会删除主共享。

主卷磁盘配额管理规则

DRA 允许 您管理主卷的磁盘配额。您可以在用户主目录位于 Microsoft Windows 计算机上的本机域中实施此策略。实施此策略时，应指定至少 25MB 的磁盘配额，以便留出足够的空间。

启用口令生成

此功能可让您指定 DRA 生成的口令的策略设置。 DRA 不会对用户创建的口令实施这些设置。配置口令策略属性时，口令长度必须超过 6 个字符且少于 127 个字符，除口令长度和最大限制以外，所有值都可以设置为零。

要配置口令生成策略，请导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Password Generation Policies** （配置口令生成策略），然后选中 **Enable Password Policy** （启用口令策略）复选框。单击 **Password Settings** （口令设置）并配置 “ 口令策略 ” 属性。

策略任务

要删除、启用或禁用策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。

要执行任意操作，请导航到 **Policy and Automation Management** （策略和自动化管理） > **Policy** （策略）。在右侧窗格中右键单击要删除、启用或禁用的策略，然后选择所需的操作。

实施内置策略

要实施内置策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。有关内置策略的更多信息，请参见了解内置策略。

注释：在将内置策略与助理管理员和 ActiveView 关联之前，请先校验助理管理员是否已指派给该 ActiveView。

要实施内置策略：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Policy** （策略）。
2. 在 " 任务 " 菜单上，单击 **New Policy** （新建策略），然后选择要创建的内置策略的类型。
3. 在每个向导窗口中，指定相应的值，然后单击**下一步**。例如，您可以将此新策略与特定 ActiveView 相关联，从而允许 DRA 对该 ActiveView 包含的对象实施此策略。
4. 查看摘要，然后单击**完成**。

实施自定义策略

要实施自定义策略，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。

要成功实施自定义策略，您必须编写在特定操作 （管理任务）期间运行的脚本。在自定义策略脚本中，您可以定义在操作违反策略时要显示的错误讯息。您还可以通过 Create Policy Wizard （创建策略向导）指定默认错误讯息。

有关编写自定义策略、查看管理操作列表或使用自变量数组的更多信息，请参见 SDK。有关更多信息，请参见编写自定义策略脚本或可执行文件。

注释：

- 在将自定义策略与助理管理员和 ActiveView 关联之前，请先确保助理管理员已指派给该 ActiveView。
- 如果自定义策略脚本或可执行文件的路径包含空格，请为路径加上引号 (")。

要实施自定义策略：

1. 编写策略脚本或可执行文件。
2. 使用在受管域中指派了内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色的帐户登录到 DRA 客户端计算机。
3. 启动 Delegation and Configuration （委托和配置）控制台。
4. 连接到主管理服务器。
5. 在左侧窗格中，展开 **Policy and Automation Management （策略和自动化管理）**。
6. 单击 **Policy** （策略）。
7. 在 " 任务 " 菜单上，单击 **New Policy （新建策略） > Create a Custom Policy （创建自定义策略）**。
8. 在每个向导窗口中，指定相应的值，然后单击**下一步**。例如，您可以将此新策略与特定 ActiveView 相关联，从而允许 DRA 对该 ActiveView 包含的对象实施此策略。
9. 查看摘要，然后单击**完成**。

修改策略属性

要修改策略的所有属性，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。

要修改策略属性：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Policy** （策略）。
2. 右键单击要修改的策略，然后选择**属性**。
3. 修改此策略的相应属性和设置。

编写自定义策略脚本或可执行文件

有关编写自定义策略脚本或可执行文件的更多信息，请参见 SDK。

要访问 SDK：

1. 确保已在计算机上安装 SDK。安装程序会在 Directory and Resource Administrator 程序组中创建 SDK 的快捷方式。有关更多信息，请参见安装 DRA 管理服务器中的安装核对清单。
2. 单击 Directory and Resource Administrator 程序组中的 SDK 快捷方式。

有关 SDK 的更多信息，请参见 DRA 文档网站中的 “DRA REST Services Guide” （《DRA REST 服务指南》）。

Delegation and Configuration （委托和配置）客户端策略

自动命名策略在 Exchange 策略中有三个策略配置，这些配置是 Delegation and Configuration （委托和配置）客户端独有的，这意味着它是客户端策略。

自动命名策略允许您为邮箱的特定属性指定自动命名规则。使用这些选项，您可以建立命名约定并快速生成显示名称、目录名称和别名属性的标准值。 Exchange 允许您为多个自动命名选项指定替换字符串，例如 %First 和 %Last。

当 Exchange 生成目录名称或别名时，会检查生成的值是否唯一。如果生成的值不唯一，则 Exchange 会附加连字符 (-) 和两位数字 （以 -01 开头），以使值唯一。当 Exchange 生成显示名称时，它不会检查该值是否唯一。

Exchange 支持用于自动命名和代理生成策略的以下替换字符串：

%First	**表示关联用户帐户的“名”属性的值。**
%Last	表示关联用户帐户的“姓”属性的值。
%Initials	表示关联用户帐户的“名字的首字母”属性的值。
%Alias	表示“别名”邮箱属性的值。
%DirNam	表示“目录名称”邮箱属性的值。生成 Microsoft Exchange 邮箱的电子邮件地址时， Exchange 不支持指定 %DirName 变量的代理生成字符串。
%UserName	表示关联用户帐户的“用户名”属性的值。

您还可以在百分号 (%) 和替换字符串名称之间指定一个数字，以指示要从该值中包含的字符数。例如， %2First 表示用户帐户的名属性中的前两个字符。

每个自动命名规则或代理生成策略都可以包含一个或多个替换字符串。您还可以将每个规则中的字符指定为特定替换字符串的前缀或后缀，例如句号和空格 (.) （%Initials 替换字符串后面的）。如果替换字符串的属性为空，则 Exchange 不会包含该属性的后缀。

例如，请考虑显示名称属性的以下自动命名规则：

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

如果名属性为 Susan，名字的首字母属性为 May，而姓属性为 Smith，则 Exchange 会将显示名称属性设置为 Susan M. Smith。

如果名属性为 Michael，名字的首字母属性为空，而姓属性为 Jones，则 Exchange 会将显示名称属性设置为 Michael Jones。

指定自动邮箱命名策略

要指定自动邮箱命名选项，您必须具备相应的权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限，并且您的许可证必须支持 Exchange 产品。

要指定自动邮箱命名策略：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略） > **Alias naming** （别名命名）。
2. 指定相应的名称生成信息。
3. 选择 **Enforce alias naming rules during mailbox updates** （在邮箱更新期间实施别名命名规则）。
4. 单击确定。

指定资源命名策略

要指定资源命名选项，您必须具备相应的权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限，并且您的许可证必须支持 Exchange 产品。

要指定资源命名策略：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略） > **Resource naming** （资源命名）。
2. 指定相应的资源名称生成信息。
3. 选择 **Enforce resource naming rules during mailbox updates** （在邮箱更新期间实施资源命名规则）。
4. 单击**确定**。

指定存档命名策略

要指定存档命名选项，您必须具备相应的权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限，并且您的许可证必须支持 Exchange 产品。

要指定存档命名策略：

1. 导航到 **Policy and Automation Management** （策略和自动化管理） > **Configure Exchange Policies** （配置 Exchange 策略） > **Archive naming** （存档命名）。
2. 为用户帐户指定相应的存档名称生成信息。
3. 选择 **Enforce archive naming rules during mailbox updates** （在邮箱更新期间实施存档命名规则）。
4. 单击**确定**。

14 任务前和任务后触发自动化

自动化触发器是将脚本或可执行文件与一个或多个操作相关联的规则。通过脚本或可执行文件，您可以将现有工作流程自动化，并在 DRA 和其他数据储存库之间建立信息桥梁。自动化触发器可让您扩展 DRA 提供的功能和安全性。

定义自动化触发器时，可以设置规则参数、应与触发器关联的操作、要运行的脚本或可执行文件以及 （如果适用）应与此触发器关联的 ActiveView 或助理管理员。这些规则将确定管理服务器如何应用触发器。

您还可以为触发器指定撤消脚本或可执行文件。**撤消脚本**允许您在操作失败时回滚更改。

DRA 支持 VBScript 和 PowerShell 脚本。

管理服务器如何自动执行流程

除了基于 ActiveView 规则的管理之外， DRA 还允许您将现有工作流程自动化，并通过自动化触发器自动运行相关任务。将现有工作流程自动化可帮助您简化企业，同时提供更好、更快的服务。

当管理服务器运行与自动化触发器关联的操作时，服务器还会运行触发器脚本或可执行文件。如果触发器是任务前触发器，则服务器将在运行操作之前运行脚本或可执行文件。如果触发器是任务后触发器，则服务器将在运行操作后运行脚本或可执行文件。此过程称为事务。**事务**表示管理服务器执行的每个任务或操作的完整实现周期。事务包括完成操作所需的操作，以及管理服务器在操作失败时应执行的任何撤消操作。

每次运行自动化触发器时，管理服务器都会在审计日志中输入触发器状态。这些日志条目会记录返回代码、关联操作、作用对象以及触发器脚本是否成功。

警告：使用管理服务器服务帐户运行自动化触发器。由于服务帐户具有管理员许可权限，因此策略和自动化触发器可以完全访问所有企业数据。要定义自动化触发器，您必须具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。这些自动化触发器将在服务帐户安全环境中运行。因此，与内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色关联的助理管理员可以获得比预期更多的权限。

实施自动化触发器

要实施自动化触发器，必须先编写触发器脚本或可执行文件，并具备相应权限，例如内置 Manage Policies and Automation Triggers （管理策略和自动化触发器）角色中所包含的权限。

要成功实施自定义触发器，您必须编写在特定操作 （管理任务）期间运行的脚本。您可以指定 DRA 在操作运行之前 （任务前）还是之后 （任务后）应用触发器。在触发器脚本中，您可以定义在触发器失败时显示的错误讯息。您还可以通过 Create Automation Trigger Wizard （创建自动化触发器向导）指定默认错误讯息。

有关编写自定义触发器、查看管理操作列表或使用自变量数组的更多信息，请参见 *SDK*。

注释：

- 在将自定义自动化触发器与助理管理员和 ActiveView 关联之前，请先确保助理管理员已指派给该 ActiveView。
- 如果自定义触发器脚本或可执行文件的路径包含空格，请为路径加上引号 (")。
- 当前，如果将 **UserSetInfo** 操作用于脚本自动化触发器，并且更改了用户属性 （执行触发器），则直到在用户对象上运行 **Find Now** （立即查找）操作后，更改的属性才会在整个企业中扩散。
- 为特定 ActiveView 实施触发器时，或者换句话说，实施范围有限的触发器时， GetInfo 操作还需要包含该对象类型的属性操作。例如，触发 **UserGetInfo** 操作时，还需要将 **UserProperties** 操作添加到触发操作列表中。

要实施自动化触发器：

1. 编写触发器脚本或可执行文件。
2. 使用在受管域中指派了内置 **Manage Policies and Automation Triggers** （管理策略和自动化触发器）角色的帐户登录到 DRA 客户端计算机。
3. 启动 Delegation and Configuration （委托和配置）控制台。
4. 连接到主管理服务器。
5. 使用文件复制将触发器文件上载到 DRA 主服务器和次服务器。

   文件夹路径必须已存在于受管域中的所有 DRA 服务器上。此路径 （包含文件）将用于 Automation Trigger （自动化触发器）向导的 **Do file path** （执行文件路径）中。
6. 在左侧窗格中，展开 **Policy and Automation Management** （策略和自动化管理）。
7. 单击 **Automation Triggers** （自动化触发器）。
8. 在 “ 任务 ” 菜单上，单击 **New Trigger** （新建触发器）。
9. 在每个向导窗口中，指定相应的值，然后单击下一步。例如，您可以将此新触发器与特定 ActiveView 相关联，从而允许 DRA 在助理管理员管理该 ActiveView 包含的对象时应用此触发器。
10. 查看摘要，然后单击 **Finish** （完成）。

重要：如果通过在 ActiveView 之间添加逗号为触发器配置了多个 ActiveView，则升级到新版本的 DRA 时，这些 ActiveView 在触发器中会分叉，并且触发器将不会执行。要使操作在升级后执行，需要重新配置触发器或需要创建新触发器。

15 自动化工作流程

使用工作流程自动化，您可以通过创建自定义工作流程表单来自动化 IT 流程，这些表单在执行工作流程时或由在工作流程自动化服务器中创建的命名工作流程事件触发时运行。创建工作流程表单时，您可以定义可查看表单的 Admin 组。表单提交或工作流程执行取决于在创建工作流程表单时委托给组的权限。

工作流程表单在创建或修改时将保存到 Web 服务器。登录到此服务器的 Web 控制台的助理管理员可以根据您配置表单的方式访问表单。表单通常可供具有 Web 服务器身份凭证的所有用户使用。通过添加助理 Admin 组，然后对其他用户隐藏该表单，即可限制对此特定表单的访问。提交表单的能力需要以下任意权限：

- Create Workflow Event and Modify All Properties （创建工作流程事件并修改所有属性）
- Start Workflow （启动工作流程）

起动工作流程表单：工作流程在工作流程自动化服务器中创建，必须通过 Delegation and Configuration （委托和配置）控制台与 DRA 集成。要保存新表单，您必须在表单属性中配置**起动特定工作流程**或**按事件触发工作流程**选项。下面提供了有关这些选项的更多信息：

- **起动特定工作流程：**此选项将列出 DRA 工作流程服务器中正在生产的所有可用工作流程。要在此列表中填充工作流程，需要在工作流程自动化服务器的 DRA_Workflows 文件夹中创建工作流程。
- **按事件触发工作流程：**此选项用于执行具有预定义触发器的工作流程。带有触发器的工作流程也在工作流程自动化服务器中创建。

注释：只有使用 " 启动特定工作流程 " 配置的工作流程请求，才会具有可在**任务** > **请求**下的主搜索窗格中查询的执行历史记录。

您可以修改现有请求或创建请求。要创建工作流程请求或修改现有请求，请导航到**任务** > **自定义** > **Workflow (Requests)** （工作流程 （请求））。

按照下列基本步骤创建请求：

1. 配置请求以在提交表单时执行*指定的工作流程*，或配置请求以在由预定义的*命名事件*触发时执行。
2. 选择工作流程中包含的助理 Admin 组或组，并在**常规**选项卡中启用**表单已隐藏**选项，以将表单的访问权限限制为这些用户。
3. 向表单添加任何必需的属性字段或其他属性页。
4. 如果适用，请创建自定义处理程序以进一步定义工作流程及其执行方式。

   注释：在最初保存请求之前，不会为新的工作流程请求公开自定义处理程序选项。您可以在**表单属性**中访问、创建和修改自定义处理程序。

   ---

5. 禁用**表单已隐藏**选项可使用户能够查看表单。

有关配置工作流程自动化服务器的信息，请参见配置工作流程自动化服务器 （第 66 页）。有关自定义工作流程请求，请参见自定义请求表单。

VI 审计和报告

审计用户操作是良好安全实现的最重要方面之一。为了允许您查看和报告助理管理员操作，DRA 会在管理服务器计算机上的日志存档中记录所有用户操作。 DRA 将提供清晰而全面的报告，其中包括审计事件的之前值和之后值，以便您可以确切地看到更改的内容。

16 审计活动

事件日志中的审计活动可以帮助您隔离、诊断和解决环境中的问题。本节提供的信息可帮助您启用和了解事件日志记录以及如何使用日志存档。

本机 Windows 事件日志

为了允许您查看和报告助理管理员操作， DRA 会在管理服务器计算机上的日志存档中记录所有用户操作。用户操作包括更改定义的所有尝试，例如更新用户帐户、删除组或重新定义 ActiveView。 DRA 还会记录特定的内部操作，例如管理服务器初始化和相关的服务器信息。除了记录这些审计事件外， DRA 还会记录事件之前和之后的值，以便您可以确切地看到更改的内容。

DRA 使用称为 **log archive** （日志存档）的文件夹 **NetIQLogArchiveData** 来安全地储存存档的日志数据。 DRA 会随着时间的推移对日志进行存档，然后删除较旧的数据，以通过整理过程为较新的数据腾出空间。

DRA 使用储存在日志存档文件中的审计事件来显示 Activity Detail （活动细节）报告，例如显示在指定时间段内对对象所作的更改。您还可以配置 DRA 将这些日志存档文件中的信息导出到 NetIQ Reporting Center 用于显示管理报告的 SQL Server 数据库。

DRA 始终会将审计事件写入日志存档。您也可以启用或禁用 DRA 将事件写入 Windows 事件日志。

为 DRA 启用和禁用 Windows 事件日志审计

在安装 DRA 时，默认情况下不会在 Windows 事件日志中记录审计事件。您可以通过修改注册表项来启用此类型的日志记录。

警告：编辑 Windows 注册表时需要加倍小心。如果您的注册表中存在错误，则您的计算机可能无法正常运行。如果发生错误，您可以将注册表恢复到上次成功启动计算机时的状态。有关更多信息，请参见 Help for the Windows Registry Editor （Windows 注册表编辑器帮助）。

要启用事件审计：

1. 单击**启动 > 运行**。
2. 在**打开**字段中键入 regedit，然后单击**确定**。
3. 展开以下注册表项：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\。
4. 单击**编辑 > 新建 > DWORD 值**。
5. 输入 IsNTAuditEnabled 作为项名称。
6. 单击**编辑 > 修改**。

7 在 Value data （数值数据）字段中输入 **1**，然后单击**确定**。

8 关闭注册表编辑器。

要禁用事件审计：

1 单击**启动 > 运行**。

2 在**打开**字段中键入 regedit，然后单击**确定**。

3 展开以下注册表项：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\。

4 选择 IsNTAuditEnabled 项。

5 单击**编辑 > 修改**。

6 在 Value data （数值数据）字段中输入 **0**，然后单击**确定**。

7 关闭注册表编辑器。

确保审计完整性

为确保审计所有用户操作， DRA 在产品无法校验日志记录活动时提供备用日志记录方法。安装 DRA 时，会将 AuditFailsFilePath 项和路径添加到注册表中，以确保执行以下操作：

- 如果 DRA 检测到审计事件不再记录到日志存档中，则 DRA 会将审计事件记录到管理服务器上的本地文件中。
- 如果 DRA 无法将审计事件写入本地文件，则 DRA 会将审计事件写入 Windows 事件日志。
- 如果 DRA 无法将审计事件写入 Windows 事件日志，则产品会将审计事件写入 DRA 日志。
- 如果 DRA 检测到未记录审计事件，则会阻止进一步的用户操作。

要在日志存档不可用时启用写入操作，还必须为 AllowOperationsOnAuditFailure 项设置注册表项值。

警告：编辑 Windows 注册表时需要加倍小心。如果您的注册表中存在错误，则您的计算机可能无法正常运行。如果发生错误，您可以将注册表恢复到上次成功启动计算机时的状态。有关更多信息，请参见 Help for the Windows Registry Editor （Windows 注册表编辑器帮助）。

要启用写入操作：

1 单击**启动 > 运行**。

2 在**打开**字段中键入 regedit，然后单击**确定**。

3 展开以下注册表项：HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\。

4 单击**编辑 > 新建 > DWORD 值**。

5 输入 AllowOperationsOnAuditFailure 作为关键字名称。

6 单击**编辑 > 修改**。

7 在 Value data （数值数据）字段中输入 **736458265**。

8 在基准字段中选择十进制，然后单击确定。

9 关闭注册表编辑器。

了解日志存档

DRA 会将用户活动数据记录在管理服务器上的日志存档中。 DRA 将创建每日日志存档分区以储存当天收集和规范化的数据。 DRA 将使用管理服务器上的本地时间日期 (*YYYYMMDD*) 作为每日日志存档分区的命名约定。

如果已启用 “ 管理报告收集器 ”，则 DRA 会将日志存档数据导出到 SQL Server 数据库，作为 DRA Management （DRA 管理）报告的来源。

最初， DRA 默认情况下会无限期地将日志数据保留在日志存档中。日志存档大小可以达到在安装时根据可用硬盘空间确定的最大大小。当日志存档超过此最大大小时，便不会储存新的审计事件。您可以设置数据保留的时间限制，而 DRA 会去除最旧的数据，以通过清理过程为较新的数据腾出空间。在启用清理之前，请确保您已有备份策略。您可以使用日志存档配置实用程序配置日志存档保留期。有关更多信息，请参见修改日志存档清理设置。

使用日志存档查看器实用程序

您可以使用日志存档查看器实用程序查看储存在日志存档文件中的数据。您可以选择随 DRA 一同安装的 NetIQ DRA 日志存档资源包 (LARK) 将提供日志存档查看器实用程序。有关更多信息，请参见 *NetIQ DRA Log Archive Resource Kit Technical Reference* （NetIQ DRA 日志存档资源包技术参考）。

备份日志存档文件

日志存档文件是记录块的集合。由于日志存档文件是位于物理数据库之外的压缩二进制文件，因此您无需使用 Microsoft SQL Server Management Studio 备份日志存档。如果您有自动文件备份系统，则会像任何其他文件一样自动备份日志存档文件。

在计划备份策略时，请记住以下最佳实践：

- 每天创建一个包含当天事件数据的分区。启用清理时，日志存档服务默认情况下会每隔 90 天自动清理这些分区中的数据。备份策略应考虑清理日程表以确定备份的频率。在清理日志存档分区时， DRA 会删除二进制文件。您无法检索已清理的数据。您必须从备份中恢复已清理的数据。有关更多信息，请参见修改日志存档清理设置。
- 只应在分区关闭后备份分区。在正常情况下，分区将在第二天午夜的 2 小时内关闭。
- 将分区文件夹及其所有子文件夹作为一个单元进行备份和恢复。备份 VolumeInfo.xml 文件作为分区备份的一部分。
- 如果要恢复报告的日志存档分区，请确保备份日志存档保留或可以恢复为其原始格式。
- 配置备份日志存档文件的过程时， NetIQ 建议您排除主日志存档文件夹中的 index_data 和 CubeExport 子文件夹。这些子文件夹包含临时数据，不应备份。

修改日志存档清理设置

安装 DRA 时，默认情况下禁用日志存档清理。为日志存档文件建立常规备份过程时，应启用日志存档清理以节省磁盘空间。您可以使用日志存档配置实用程序修改清理日志存档分区之前的天数。

要更改清理日志存档分区之前的天数：

1. 使用属于本地管理员组的帐户登录到管理服务器。
2. 在 NetIQ 管理程序组中，启动 **Log Archive Configuration** （日志存档配置）。
3. 单击 **Log Archive Server Settings** （日志存档服务器设置）。
4. *如果要启用分区清理，*请将 **Partition Grooming Enabled** （已启用分区清理）字段的值设置为 True。
5. 在 **Number of Days before Grooming** （清理前的天数）字段中键入要在清理之前保留日志存档分区的天数。
6. 单击应用。
7. 单击是。
8. 单击关闭。
9. 找到 *NetIQLogArchiveData*\< *分区名称* > 文件夹的路径，通常为：
   C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData

   如果未选中指定分区中文件或文件夹的 File is ready for archiving （可以存档文件）属性（在文件或文件夹属性中），则必须编辑 CONFIG 文件以启用日志存档清理。要了解选中或没有选中此属性的原因，请参见知识库文章 *How do you configure the data retention period for DRA Logarchival Data?* （如何配置 DRA 日志存档数据的数据保留期？）中的 **Additional Information** （其他信息）部分。

如果值是	
选中	在确认讯息上单击是以重启动 NetIQ Security Manager 日志存档服务。 **注释：**如果修改任何日志存档设置，则必须重启动日志存档服务才能使更改生效。
未选中	在确认讯息上单击否。请参见要使 DRA 日志存档服务器能够清理未存档的数据：。

要使 DRA 日志存档服务器能够清理未存档的数据：

1. 以本地管理员组的成员身份在本地登录到每个 DRA 服务器 Windows 控制台。
2. 使用文本编辑器打开 C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config 文件，然后找到 <Property name="GroomUnarchivedData" value="false" /> 行。
3. 将 "false" 更改为 "true" 并保存文件。
4. 重启动 NetIQ DRA 日志存档服务。

注释：如果修改任何日志存档设置，则必须重启动日志存档服务才能使更改生效。

17 报告

本节提供有关了解和启用 DRA Reporting、报告数据收集、 ActiveView Analyzer 收集和报告以及访问内置报告的信息。

DRA 将禁用您的许可证不支持的功能和报告。您还必须具有运行和查看报告的相应权限。因此，您可能无法访问某些报告。

安装 DRA 后， Delegation and Configuration （委托和配置）控制台中将提供 Activity Detail （活动细节）报告，以提供有关网络更改的最新细节。

- 管理报告数据收集 （第 149 页）
- 内置报告 （第 150 页）

管理报告数据收集

DRA Reporting 提供了两种生成报告的方法，使您可以查看环境中的最新更改，以及收集和查看域中的用户帐户、组和资源定义。

Activity Detail （活动细节）报告

这些报告可通过 Delegation and Configuration （委托和配置）控制台进行访问，提供域中对象的实时更改信息。

DRA Management （DRA 管理）报告

这些报告可通过 NetIQ Reporting Center (Reporting Center) 进行访问，提供有关受管域中事件的活动、配置和摘要信息。部分报告以数据的图形表示形式呈现。

例如，您可以通过 Activity Detail （活动细节）报告查看在指定时间段内对对象所做更改或对象所做更改的列表。您还可以使用 “ 管理 ” 报告查看显示每个受管域在指定时间段内的事件数的图表。通过报告，您还可以查看有关 DRA 安全模型的细节，例如 ActiveView 和助理管理员组定义。

DRA Management （DRA 管理）报告可以作为可选功能进行安装和配置，并可在 Reporting Center 中进行查看。启用和配置数据收集时， DRA 会收集有关已审计事件的信息，并按照您定义的日程表将其导出到 SQL Server 数据库。在 Reporting Center 中连接到此数据库时，您可以访问 60 多个内置报告：

- 活动报告，显示谁执行了哪些操作以及执行操作的时间
- 配置报告，显示特定时间点的 AD 或 DRA 状态
- 摘要报告，显示活动量

有关为管理报告配置数据收集的更多信息，请参见报告配置。

查看收集器状态

您可以在 Collectors Status （收集器状态）选项卡上查看每个数据收集器的细节。

要查看收集器的状态：

1. 展开 **Configuration Management** （配置管理），然后单击 **Update Reporting Service Configuration** （更新报告服务配置）。
2. 在 Collectors Status （收集器状态）选项卡上，单击每个条目以查看有关数据收集的其他信息，例如上次收集数据的时间以及上次数据收集是否成功。
3. 如果“服务器”列表中未显示任何数据，请单击**刷新**。

启用报告和数据收集

安装 DRA Reporting 组件后，启用并配置报告数据收集以访问 Reporting Center 报告。

要启用报告和数据收集：

1. 导航到 **Configuration Management** （配置管理） > **Update Reporting Service Configuration** （更新报告服务配置）。
2. 在 "SQL Server" 选项卡上，选择 **Enable DRA Reporting support** （启用 DRA Reporting 支持）。
3. 单击 Server Name （服务器名称）字段中的 **Browse** （浏览），然后选择安装 SQL Server 的计算机。
4. 在 Credentials （身份凭证）选项卡上，指定用于 SQL Server 交互的相应身份凭证。
5. 如果这是可用于创建数据库和初始化纲要的同一帐户，请选中 Use the above credentials for creating a database and initializing the database schema （使用上述身份凭证创建数据库并初始化数据库纲要）复选框。
6. 如果要为创建数据库指定其他帐户，请在 Admin Credentials （Admin 身份凭证）选项卡上指定该用户帐户和口令。
7. 单击**确定**。

有关配置特定收集器的信息，请参见报告配置。

内置报告

内置报告使您能够生成有关对象更改、对象列表和对象细节的报告。这些报告不是 DRA Reporting Service 的一部分，不需要任何配置即可启用内置的更改历史记录报告。请参阅本节中的主题，以了解如何访问这些报告。

注释： DRA 与 Change Guardian 集成时，也可以访问 DRA 之外事件的更改历史记录报告。有关这些报告类型和配置 Change Guardian 服务器的信息，请参见统一的更改历史记录。

报告对象更改

通过生成 Activity Detail （活动细节）报告，您可以查看域中对象的实时更改信息。例如，您可以查看在指定时间段内对对象所做更改或对象所做更改的列表。您还可以导出和打印 Activity Detail （活动细节）报告。

要报告对象更改：

1. 查找与准则匹配的对象。
2. 右键单击对象，然后选择 **Reporting （报告） > 对 objectName 所作的更改**或 **Reporting （报告） > objectName 所作的更改**。
3. 选择开始日期和结束日期以指定要查看的更改。
4. *如果要更改要显示的行数*，请键入超过默认值 250 的数字。

   注释：显示的行数适用于环境中的每个管理服务器。如果在报告中包含 3 个管理服务器并使用默认值 250 行进行显示，则报告中最多可显示 750 行。

5. *如果要在报告中仅包括特定的管理服务器*，请选择 **Restrict query to these DRA servers** （将查询限制为这些 DRA 服务器），然后键入希望报告包含的服务器名称。用逗号分隔多个服务器名称。
6. 单击**确定**。

报告对象列表

您可以从对象列表中导出或打印数据。使用此功能，您可以快速轻松地报告和分发有关受管对象的常规信息。

导出对象列表时，可以指定文件位置、名称和格式。 DRA 支持 HTML、 CSV 和 XML 格式，因此您可以将此信息导出到数据库应用程序或将列表结果张贴到网页

注释：您还可以选择列表中的多个项目，然后将这些项目复制到文本应用程序 （如记事本）。

要报告对象列表：

1. 查找与准则匹配的对象。
2. 要导出此对象列表，请单击 “ 文件 ” 菜单上的 **Export List** （导出列表）。
3. 要打印此对象列表，请单击 “ 文件 ” 菜单上的 **Print List** （打印列表）。
4. 指定相应的信息以保存或打印此列表。

报告对象细节

您可以从列出对象属性的细节选项卡中导出或打印数据，例如组成员资格。使用此功能，您可以快速轻松地报告和分发有关特定对象的常用细节。

导出对象细节选项卡时，可以指定文件位置、名称和格式。 DRA 支持 HTML、 CSV 和 XML 格式，因此您可以将此信息导出到数据库应用程序或将列表结果张贴到网页。

要报告对象细节：

1. 查找与准则匹配的对象。
2. 在“视图”菜单上，单击**细节**。
3. 在细节窗格中，选择相应的选项卡。
4. 要导出这些对象细节，请单击“文件”菜单上的 **Export Details** （导出细节）列表。
5. 要打印这些对象细节，请单击“文件”菜单上的 **Print Details List** （打印细节列表）。
6. 指定相应的信息以保存或打印此列表。

VII 其他功能

临时组指派、动态组、 Event Stamping （事件标记）和 BitLocker 恢复口令是 DRA 中可以在企业环境中使用的其他功能。

18 临时组指派

DRA 允许您创建临时组指派，从而为授权用户提供对资源的临时访问权限。助理管理员可以使用临时组指派在特定时间段内将用户指派到目标组。在该时间段结束时， DRA 会自动从组中去除用户。

Manage Temporary Group Assignments （管理临时组指派）角色将授予助理管理员创建和管理临时组指派的权限。

助理管理员只能针对有权在其中添加或去除成员的组查看临时组指派。

使用以下权限委托创建和管理临时组指派：

- 创建临时组指派
- Delete Temporary Group Assignments （删除临时组指派）
- Modify Temporary Group Assignments （修改临时组指派）
- Reset Temporary Group Assignment State （重设置临时组指派状态）
- View Temporary Group Assignments （查看临时组指派）
- Add Object to Group （将对象添加到组）
- Remove Object from Group （从组中去除对象）

目标组和用户必须属于同一 ActiveView。

注释：

- 您无法为已是目标组成员的用户创建临时组指派。如果您尝试为已是目标组成员的用户创建临时组指派，则 DRA 会显示一条警告讯息，并且不允许您为该用户创建临时组指派。
- 如果为不是目标组成员的用户创建临时组指派，则 DRA 会在临时组指派失效时从该组中去除该用户。

示例：

人力资源经理 Bob 通知 help-desk 管理员 John，公司已针对特定时间段与名为 Joe 的临时雇员签约以完成项目。 John 执行以下操作：

- 创建临时组指派 (TGA)
- 将临时雇员的人力资源组添加到 TGA
- 将 Joe 添加为临时雇员组的成员
- 将 TGA 持续时间设置为一个月 （2019/07/03 到 2019/08/02）

预期结果：

默认情况下， TGA 失效时，将从人力资源组中去除 Joe 的成员资格。除非 John 选择**保留此临时组指派以供将来使用**，否则 TGA 将保持七天的可用状态。

有关创建和使用临时组指派的更多信息，请参见 *《用户指南》*。

19 DRA 动态组

动态组根据组属性中配置的一组定义的准则更改其成员资格。您可以使任何组成为动态组，也可以从已配置动态过滤器的任何组中去除动态过滤器。此功能还提供将组成员添加到静态列表或排除列表的功能。这些列表中的组成员不会受动态准则的影响。

如果将动态组还原为常规组，则静态成员列表中的所有成员都将添加到组成员资格，并且将忽略排除的成员和动态过滤器。您可以使现有组成为动态组，也可以在 Delegation and Configuration （委托和配置）控制台以及 Web 控制台中创建新的动态组。

要使组成为动态组：

1 在适用的控制台中查找该组。

- Delegation and Configuration （委托和配置）：转到 **All My Managed Objects** （我的所有受管对象） > **Find Now** （立即查找）。

  注释：要启用查询生成器，请单击浏览并选择域、容器或 OU。

- Web 控制台：转到管理 > 搜索。

2 打开组的属性，然后在 " 动态成员过滤器 " 选项卡中选择使组成为动态组。

3 添加所需的 LDAP 和虚拟属性以过滤组成员资格。

4 将任何所需的静态或排除成员添加到动态组，然后应用更改。

要创建新的动态组：

- **Delegation and Configuration （委托和配置）：**右键单击 All My Managed Objects （我的所有受管对象）中的域或子节点，然后选择 **New** （新建） > **Dynamic Group** （动态组）。
- **Web 控制台：**转至管理 > 创建 > **Dynamic Group** （动态组）。

20 Event Stamping （事件标记）如何工作

当您为对象类型配置属性，而 DRA 执行其中一个受支持的操作时，将使用 DRA 特定信息（包括执行操作的人员）更新 （标记）该属性。这会导致 AD 为该属性更改生成审计事件。

例如，假设您选择属性 extensionAttribute1 作为用户属性，并且已配置 AD DS 审计。每当助理管理员更新用户时， DRA 将使用 Event Stamping （事件标记）数据更新 extensionAttribute1 属性。这意味着，除了助理管理员更新的每个属性的 AD DS 事件 （例如，说明、名称等）之外，还将为 extensionAttribute1 属性提供额外的 AD DS 事件。

每个事件都包含一个关联 ID，对于更新用户时更改的每个已更改属性，该关联 ID 是相同的。这是应用程序可以将 Event Stamping （事件标记）数据与已更新的其他属性相关联的方式。

AD DS 事件

每次 DRA 执行支持的操作时，您都会在 Windows 安全事件日志中看到此类事件。

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

事件值由两部分组成。第一部分是包含 Event Stamping （事件标记）数据的 XML 字符串。第二部分是数据的签名，可用于验证数据是否实际由 DRA 生成。要验证签名，应用程序必须具有签名的公共密钥。

XML 字符串包含以下信息：

用户	执行操作的助理管理员
Sid	执行操作的助理管理员的 SID
Tid	DRA 审计事务 ID 以确保每个事件都是唯一的
SubjectUserSid	实际更新 AD 对象的 DRA 服务帐户或访问帐户的 SID
ObjectDN	已修改的对象的判别名

支持的操作

用户	◆ 创建 ◆ 重命名 ◆ 修改 ◆ 克隆
组	◆ 创建 ◆ 重命名 ◆ 修改 ◆ 克隆
联系人	◆ 创建 ◆ 重命名 ◆ 修改 ◆ 克隆
计算机	◆ 创建 ◆ 启用 ◆ 禁用 ◆ 重命名 ◆ 修改
组织单元	◆ 创建 ◆ 重命名 ◆ 克隆

21 BitLocker 恢复口令

Microsoft BitLocker 将其恢复口令储存在 Active Directory 中。使用 DRA BitLocker 恢复功能，您可以将权限委托给助理管理员，以便查找和恢复最终用户丢失的 BitLocker 口令。

重要：在使用 BitLocker 恢复口令功能之前，请确保已将计算机指派给域并且已启用 BitLocker。

查看和复制 BitLocker 恢复口令

如果计算机的 BitLocker 口令丢失，可以使用 Active Directory 中计算机属性的“恢复口令”密钥重设置口令。复制口令密钥并将其提供给最终用户。

要查看和复制恢复口令：

1. 起动 **Delegation and Configuration** （委托和配置）控制台，然后展开树视图结构。
2. 在 **Account and Resource Management** （帐户和资源管理）节点中，导航到 **All My Managed Objects** （我的所有受管对象） > **Domain** （域） > **Computers** （计算机）。
3. 在计算机列表中，右键单击所需的计算机，然后选择 **Properties** （属性）。
4. 单击 **BitLocker 恢复口令**选项卡以查看 BitLocker 恢复口令。
5. 右键单击 BitLocker 恢复口令，单击**复制**，然后将文本粘贴到所需的文本文件或电子表格中。

查找恢复口令

如果计算机的名称已更改，则必须使用口令 ID 的前八个字符在域中搜索恢复口令。

要使用口令 ID 查找恢复口令：

1. 起动 **Delegation and Configuration** （委托和配置）控制台，然后展开树视图结构。
2. 在 **Account and Resource Management** （帐户和资源管理）节点中，导航到 **All My Managed Objects** （我的所有受管对象），右键单击 **Managed Domain** （受管域），然后单击 **Find BitLocker Recovery Password** （查找 BitLocker 恢复口令）。

   要查找恢复口令的前八个字符，请参见查看和复制 BitLocker 恢复口令。
3. 在 **Find BitLocker Recovery Password** （查找 BitLocker 恢复口令）页面中，将复制的字符粘贴到搜索字段中，然后单击 **Search** （搜索）。

22 回收站

您可以为每个 Microsoft Windows 域或这些域中的对象启用或禁用回收站，从而控制整个企业中的帐户管理。如果启用回收站，然后删除用户帐户、组、动态分发组、动态组、资源邮箱、联系人或计算机帐户，则管理服务器将禁用所选帐户并将其移至回收站容器。 DRA 将帐户移至回收站后，该帐户不会显示在其所属的 ActiveView 中。如果在禁用回收站时删除用户帐户、组、联系人或计算机帐户，则管理服务器将永久删除所选帐户。您可以禁用包含以前删除的帐户的回收站。但是，一旦禁用回收站，这些帐户在“回收站”节点中将不再可用。

指派回收站权限

要允许助理管理员从“我的所有受管对象”节点以及“回收站”中永久删除帐户，请从以下列表中指派相关的权限：

- 永久删除用户帐户
- 永久删除组
- 永久删除计算机
- 永久删除联系人
- 永久删除动态分发组
- 永久删除动态组
- 永久删除资源邮箱

如果多个管理服务器管理同一 Microsoft Windows 域中的不同子树，您可以使用回收站查看此域中的任何已删除帐户，而无论哪个管理服务器管理该帐户。

使用回收站

使用回收站永久删除帐户、恢复帐户或查看已删除帐户的属性。您还可以搜索特定帐户并跟踪已删除帐户在回收站中的天数。“回收站”选项卡也包含在所选域的“属性”窗口中。在此选项卡中，您可以为整个域或特定对象禁用或启用回收站，以及安排回收站清理。

使用 **Restore All** （全部恢复）或 **Empty Recycle Bin** （清空回收站）选项可以快速轻松地恢复或删除这些帐户。

恢复帐户时， DRA 会复原该帐户，包括所有许可权限、权限委托、策略指派、组成员资格和 ActiveView 成员资格。如果您永久删除帐户， DRA 会从 Active Directory 中去除此帐户。

为确保安全删除帐户，只有具有以下权限的助理管理员才能永久删除回收站中的帐户：

- 永久删除用户帐户
- 从回收站中删除用户
- 永久删除组帐户

- 从回收站中删除组
- 永久删除计算机帐户
- 从回收站中删除计算机
- 永久删除联系人帐户
- 从回收站中删除联系人
- 永久删除动态分发组
- 从回收站删除动态分发组
- 永久删除动态组
- 从回收站删除动态组
- 永久删除资源邮箱
- 从回收站中删除资源邮箱
- 查看所有回收站对象

要从回收站恢复帐户，助理管理员必须在包含该帐户的 OU 中具有以下权限：

- 从回收站恢复用户
- 从回收站恢复组
- 从回收站恢复动态分发组
- 从回收站恢复动态组
- 从回收站恢复资源邮箱
- 从回收站恢复计算机
- 从回收站恢复联系人
- 查看所有回收站对象

注释：

- 如果将助理管理员帐户删除到回收站， DRA 会继续显示此帐户的 ActiveView 和角色指派。 DRA 不会显示已删除的助理管理员帐户的名称，而是显示安全标识符 (SID)。您可以在永久删除助理管理员帐户之前去除这些指派。
- 从回收站删除用户帐户后， DRA 将删除用户主目录。
- 如果删除具有 Office 365 许可证的用户，则该用户帐户将转到回收站并去除许可证。如果稍后恢复用户帐户，则还将恢复 Office 365 许可证。

VIII 客户端自定义

您可以自定义 Delegation and Configuration （委托和配置）客户端和 Web 控制台。前者需要物理或远程访问权限和帐户身份凭证。后者需要服务器 URL 和帐户身份凭证才能从 Web 浏览器登录。

23 Delegation and Configuration （委托和配置）客户端

本节包含的信息可帮助您自定义 Delegation and Configuration （委托和配置）客户端，其中包括了解如何创建自定义属性页、如何在 DRA 中创建可在网络中的客户端和服务器计算机上运行的自定义工具，以及如何自定义用户界面的配置。

自定义属性页

通过实施自定义属性，您可以自定义和扩展 Delegation and Configuration （委托和配置）控制台。通过自定义属性，您可以将专有帐户和 OU 属性 （如 Active Directory 纲要扩展和虚拟属性）添加到特定向导和属性窗口。这些扩展允许您自定义 DRA 以满足您的特定需求。使用 Delegation and Configuration （委托和配置）控制台中的 New Custom Page （新建自定义页面）向导，您可以快速轻松地创建自定义页面以扩展相应的用户界面。

如果您的助理管理员需要独特的权限来安全地管理自定义页面，您还可以创建和委托自定义权限。例如，您可能希望将用户帐户管理仅限于自定义页面上的属性。有关更多信息，请参见实施自定义权限。

自定义属性页的工作方式

User Interface Extensions （用户界面扩展）是 DRA 在相应的向导和属性窗口中显示的自定义页面。您可以配置自定义页面以在 Delegation and Configuration （委托和配置）控制台中公开 Active Directory 属性、纲要扩展和虚拟属性。

选择任何受支持的 Active Directory 属性、纲要扩展或虚拟属性时，可以通过以下方式使用自定义页面：

- 限制助理管理员管理定义明确且受控制的属性集。此属性集可以包括*标准属性*和纲要扩展。标准属性是默认情况下通过 “ 帐户和资源管理 ” 控制台公开的 Active Directory 属性。

- 公开由 DRA 管理的标准属性以外的 Active Directory 属性。
- 扩展 Delegation and Configuration （委托和配置）控制台以包含专有属性。

您还可以配置 DRA 如何显示和应用这些属性。例如，您可以使用默认属性值定义用户界面控件。

DRA 会将自定义页面应用于企业中所有适用的受管对象。例如，如果创建自定义页面以将 Active Directory 纲要扩展添加到 Group Properties （组属性）窗口，则 DRA 会将此页面上的属性应用于支持指定纲要扩展的域中的每个受管组。每个自定义页面都需要一组唯一的属性。您无法将 Active Directory 属性添加到多个自定义页面。

您无法在现有用户界面中禁用单个窗口或选项卡。助理管理员可以使用默认用户界面或自定义页面选择属性值。 DRA 将应用最近选择的属性值。

DRA 会为自定义属性提供完整的审计追踪。 DRA 会将以下数据记录到应用程序事件日志中：

- 对自定义页面的更改

  重要：您必须手动配置 Windows 应用程序日志审计。请参见知识库文章 *How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?* （如何重新启用 DRA 以将事件写入 DRA 8.5 及更高版本中的应用程序事件日志？）

- 创建和删除自定义页面
- 自定义页面上包含的公开纲要扩展、 Active Directory 属性和虚拟属性

您还可以运行更改活动报告以监视自定义属性的配置更改。

从主管理服务器实施和修改自定义页面。在同步期间， DRA 会跨多主集合复制自定义页面配置。有关更多信息，请参见配置多主集合。

支持的自定义页面

您创建的每个自定义页面都允许您选择一组 Active Directory 属性、纲要扩展或虚拟属性，并将这些属性公开为自定义选项卡。可以创建以下类型的自定义页面：

自定义用户页面

可在以下窗口中显示自定义选项卡：

- “用户属性”窗口
- “创建用户”向导
- “克隆用户”向导

自定义组页面

可在以下窗口中显示自定义选项卡：

- “组属性”窗口
- “创建组”向导
- “克隆组”向导

自定义计算机页面

可在以下窗口中显示自定义选项卡：

- “ 计算机属性 ” 窗口
- “ 创建计算机 ” 向导

自定义联系人页面

可在以下窗口中显示自定义选项卡：

- “ 联系人属性 ” 窗口
- “ 创建联系人 ” 向导
- “ 克隆联系人 ” 向导

自定义 OU 页面

可在以下窗口中显示自定义选项卡：

- “OU 属性 ” 窗口
- “ 创建 OU” 向导
- “ 克隆 OU” 向导

自定义资源邮箱页面

可在以下窗口中显示自定义选项卡：

- “ 资源邮箱属性 ” 窗口
- “ 创建资源邮箱 ” 向导
- “ 克隆资源邮箱 ” 向导

自定义动态分发组页面

可在以下窗口中显示自定义选项卡：

- “ 动态分发组属性 ” 窗口
- “ 创建动态分发组 ” 向导
- “ 克隆动态分发组 ” 向导

支持的自定义属性控件

将 Active Directory 属性、纲要扩展或虚拟属性添加到自定义页面时，还可以配置助理管理员输入属性值的用户界面控件。例如，可以通过以下方式指定属性值：

- 定义特定的值范围
- 设置默认属性值
- 指明是否需要属性

还可以配置用户界面控件以显示专有信息或说明。例如，如果为员工标识号定义特定范围，则可以配置文本框控件标签以显示**指定员工标识号 （001 到 100）**。

每个用户界面控件都支持单个 Active Directory 属性、纲要扩展或虚拟属性。根据属性类型配置以下用户界面控件：

Active Directory 属性类型	支持的用户界面控件
布尔	复选框
日期	日历控件
整数	文本框 （默认） 选择列表
字符串	文本框 （默认） 选择列表 对象选择器
多值字符串	选择列表

使用自定义页面

可以从 User Interface Extensions （用户界面扩展）节点创建自定义页面。创建页面后，可以添加或去除 AD 属性，以及禁用或删除页面。对于要配置的每个自定义，请创建自定义页面并为助理管理员指派相应的权限或角色。在开始使用自定义页面时，请考虑以下最佳实践：

1. 要确保 DRA 识别您的 Active Directory 属性、纲要扩展属性或虚拟属性，请在每个管理服务器上重启动 NetIQ 管理服务。
2. 确定要创建的自定义页面的类型以及希望助理管理员使用此自定义页面管理的属性。您可以选择任何 Active Directory 属性，包括纲要扩展属性和现有 DRA 向导和属性窗口中的属性，或您创建的任何虚拟属性。但是，每个自定义页面都需要一组唯一的属性。您无法将 Active Directory 属性添加到多个自定义页面。

   自定义页面不会替换现有的用户界面。有关详细信息，请参见自定义属性页的工作方式和支持的自定义页面。
3. 确定您希望助理管理员如何指定这些属性。例如，您可能希望将指定的属性限制为三个可能的值。您可以为每个属性定义相应的用户界面控件。有关更多信息，请参见支持的自定义属性控件。
4. 确定助理管理员是否需要专有信息或指令才能成功管理这些属性。例如，确定 Active Directory 是否需要属性值的语法，例如判别名 (DN) 或 LDAP 路径。
5. 确定这些属性应在自定义页面上显示的顺序。您可以随时更改显示顺序。
6. 确定 DRA 应如何使用此自定义页面。例如，您可以将用户自定义页面添加到 New User （新建用户）向导和 User Properties （用户属性）窗口。
7. 使用 “ 助理 Admin 细节 ” 窗格上的 “ 指派 ” 选项卡校验助理管理员对正确的对象集是否具有相应的权限。如果已为此自定义页面创建自定义权限，请将这些权限委托给相应的助理管理员。

8. 确定助理管理员是否需要自定义权限来管理此页面上的属性。例如，如果将自定义页面添加到“用户属性”窗口，则委托 *Modify All User Properties* （修改所有用户属性）权限可能会授予助理管理员过多的权限。创建实现自定义页面所需的任何自定义权限。有关更多信息，请参见实施自定义权限。
9. 使用上述步骤中的答案，创建相应的自定义页面。
10. 将有关您实施的自定义属性页的信息分发给相应的助理管理员 （例如 Help Desk）。

要实现属性自定义，您必须具有 DRA 管理角色中包含的权限。有关自定义页面的更多信息，请参见自定义属性页的工作方式。

创建自定义属性页

通过创建不同的自定义页面，可以创建不同的自定义属性。默认情况下会启用新的自定义页面。

创建自定义页面时，可以禁用它。禁用自定义页面会将其隐藏在用户界面中。如果要创建多个自定义页面，则可能需要禁用这些页面，直到测试并完成自定义。

注释：计算机帐户将从用户帐户继承 Active Directory 属性。如果扩展 Active Directory 纲要以包含用户帐户的其他属性，则可以在创建自定义页面以管理计算机帐户时选择这些属性。

要创建自定义属性页：

1 导航到 **Configuration Management** （配置管理） > **User Interface Extensions** （用户界面扩展）节点。

2 在“任务”菜单上，单击**新建**，然后单击要创建的自定义页面的相应菜单项。

3 在“常规”选项卡上，键入此自定义页面的名称，然后单击**确定**。如果要禁用此页面，请清除**已启用**复选框。

4 对于要包含在此自定义页面中的每个属性，请完成以下步骤：

4a 在“属性”选项卡上，单击**添加**。

4b 要选择属性，请单击**浏览**。

4c 在 **Control label** （控件标签）字段中，键入 DRA 应用作用户界面控件标签的属性名称。确保控件标签具有用户友好性和高度描述性。还可以包含指令、有效值范围和语法示例。

4d 从 **Control type** （控件类型）菜单中选择相应的用户界面控件。

4e 在 Delegation and Configuration （委托和配置）控制台中选择希望 DRA 显示此自定义页面的位置。

4f 要指定其他属性，例如最小长度或默认值，请单击**高级**。

4g 单击**确定**。

5 要更改 DRA 在自定义页面上显示这些属性的顺序，请选择相应的属性，然后单击**向上移动**或**向下移动**。

6 单击**确定**。

修改自定义属性

通过修改自定义属性，可以更改自定义页面。

要修改自定义属性：

1. 导航到 **Configuration Management** （配置管理） > **User Interface Extensions** （用户界面扩展）节点。
2. 在列表窗格中，选择所需的自定义页面。
3. 在“任务”菜单上，单击**属性**。
4. 修改此自定义页面的相应属性和设置。
5. 单击**确定**。

识别使用自定义页面管理的 Active Directory 属性

可以快速识别使用特定自定义页面管理的 Active Directory 属性、纲要扩展或虚拟属性。

要识别使用自定义页面管理的 Active Directory 属性：

1. 导航到 **Configuration Management** （配置管理） > **User Interface Extensions** （用户界面扩展）节点。
2. 在列表窗格中，选择所需的自定义页面。
3. 在细节窗格中，单击**属性**选项卡。要查看细节窗格，请单击“视图”菜单上的**细节**。
4. 要校验 DRA 如何显示和应用属性，请从列表中选择相应的 Active Directory 属性、纲要扩展或虚拟属性，然后单击**属性**图标。

启用、禁用和删除自定义页面

启用自定义页面时， DRA 会将此自定义页面添加到关联的向导和窗口。要指定显示自定义页面的向导和窗口，请修改自定义页面属性。

注释：为确保每个自定义页面都公开一组唯一的属性， DRA 不会启用包含在其他自定义页面上公开的属性的自定义页面。

禁用自定义页面时， DRA 会从关联的向导和窗口中去除该自定义页面。 DRA 不会删除自定义页面。要确保自定义页面永远不会显示在用户界面中，请删除自定义页面。

删除自定义页面时， DRA 会从关联的向导和窗口中去除该自定义页面。您无法恢复已删除的自定义页面。要从用户界面临时去除自定义页面，请禁用自定义页面。

要启用、禁用或删除自定义页面，请导航到“**Configuration Management** （配置管理） > **User Interface Extensions** （用户界面扩展）节点，然后在“任务”或右键单击菜单中选择所需的操作。

命令行界面

命令行界面可让您使用命令或批处理文件访问和应用功能强大的管理产品功能。使用命令行界面，您可以发出命令来实现跨多个对象的更改。

例如，如果需要将 200 名员工的用户主目录重定位到新服务器，则可以使用命令行界面输入以下单个命令来更改所有 200 个用户帐户：

EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE HOMEDIR:\\HOU2\USERS\@Target()

此命令指示 DRA 将 HOU_SALES 和 HOU_MIS 组中所有 200 个用户帐户的用户主目录字段更改为 \\HOU2\USERS*user_id*。要使用本机 Microsoft Windows 管理工具完成此任务，至少需要执行 200 个单独的操作。

注释：随着更多功能添加到 PowerShell 中，未来版本中将弃用命令行界面工具。

自定义工具

通过选择在 DRA 中管理的任何 Active Directory 帐户，可以使用自定义工具调用要在网络中的客户端和服务器计算机上运行的任何应用程序。

DRA 支持两种类型的自定义工具：

- 起动常用桌面实用程序 （如 Microsoft Office）的自定义工具
- 您创建并分发到每台 DRA 客户端计算机的自定义工具

您可以创建一个自定义工具，从已安装 DRA 客户端的所有计算机起动防病毒扫描。还可以创建一个自定义工具，用于起动需要 DRA 定期更新脚本的外部应用程序或工具。这些定期更新可以是配置中的更改或业务规则中的更改。随后，在定期更新之后， DRA 会将自定义工具从主管理服务器复制到任何次管理服务器和 DRA 客户端计算机。

要了解如何在服务器多主集合中复制自定义工具，请参见文件复制。

创建自定义工具

通过与所选的 Active Directory 对象或在该创建自定义工具向导中显示的所有 Active Directory 对象关联，您可以在 DRA 主服务器中创建自定义工具。该自定义工具将通过 File Replication （文件复制）复制到 ·MMS· 中的次服务器和 ·DRA· 客户端。

如果需要，新的自定义工具将创建菜单和子菜单，以针对 DRA 中关联的 Active Directory 对象调用操作。

您可以将权限委托给助理管理员，以创建和执行自定义工具，以及访问和运行应用程序。

创建自定义工具时，需要输入参数，如下所示：

“常规”选项卡

1. **名称：**工具所需的任何客户名称。

2. **菜单和子菜单：**要为新的自定义工具创建菜单项，请在 **Menu and Submenu Structure** （菜单和子菜单结构）字段中输入菜单标题。创建自定义工具和选择对象时， DRA 将使用您在“任务”菜单、“快捷方式”菜单和 DRA 工具栏中指定的菜单和子菜单结构显示自定义工具菜单项。

   *示例菜单和子菜单结构：*键入菜单项名称、反斜杠 (\) 字符，然后键入子菜单项名称。

   *使用快捷键：*在菜单项的名称前键入一个与号 (&) 字符。

   a. 示例：SendEmail\ApproveAction ---- SendEmail 是菜单， ApproveAction 是子菜单，ApproveAction 中的第一个字母 "A" 是启用的快捷键。

3. **已启用：**勾选此复选框启用自定义工具。
4. **说明：**可以添加任何所需的说明值。
5. **注释：**可以向自定义工具添加任何所需的注释。

Supported Objects （支持的对象）选项卡

选择所需的 AD 对象或创建的自定义工具应关联的所有 AD 对象。

当前支持的自定义工具选项包括：受管域、容器、用户、联系人、组、计算机、组织单元和 Published Printers （已发布的打印机）。

注释：自定义工具不支持其他新引入的对象，如资源邮箱、动态组和 Exchange 动态组。

Application Settings （应用程序设置）选项卡

Location of the application （应用程序的位置）：您需要通过复制和粘贴确切的应用程序路径或通过**插入**选项提供应用程序安装的路径 / 位置。

此相同路径必须已存在于 MMS 中的所有 DRA 服务器上。如果需要，创建新的自定义工具前，您可以使用**文件复制**将文件上载和复制到 MMS 服务器上可使用的路径。

还可以使用 DRA 变量、环境变量和注册表值在应用程序的“位置”字段中指定外部应用程序的位置。要使用这些变量，请单击**插入**，然后选择要使用的变量。

插入变量后，键入反斜杠 (\) 字符，然后指定应用程序路径的其余部分，包括应用程序可执行文件名。

示例：

- *示例 1：*要指定自定义工具将运行的外部应用程序的位置，请选择环境变量 {%PROGRAMFILES%}，然后在应用程序的“位置”字段中指定应用程序路径的其余部分：{%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe

  ---

  注释：DRA 会提供 Office 安装目录注册表值作为示例。要指定包含路径作为值的注册表项，请使用以下语法：{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}

- *示例 2：*要指定自定义工具将运行的自定义脚本文件的位置，请选择 DRA 变量 {DRA_Replicated_Files_Path}，然后在应用程序的“位置”字段中指定脚本文件路径的其余部分：{DRA_Replicated_Files_Path}\cscript.vbs ； 其中 {DRA_Replicated_Files_Path} 是复制的文件路径或管理服务器中的 {DRAInstallDir}\FileTransfer\Replicate 文件夹。

  注释：在创建自定义工具之前，请使用 File Replication （文件复制）功能将脚本文件上载到主管理服务器。 File Replication （文件复制）功能可将脚本文件上载到主管理服务器中的 {DRAInstallDir}\FileTransfer\Replicate 文件夹。

- *示例 3：*要指定自定义工具将运行的 DRA 实用程序的位置，请选择 DRA 变量 {DRA_Application_Path}，然后在应用程序的“位置”字段中指定该实用程序路径的其余部分：{DRA_Application_Path}\DRADiagnosticUtil.exe ； 其中 {DRA_Application_Path} 是安装 DRA 的位置。
- *示例 4：*只需复制粘贴应用程序的位置以及带扩展名的应用程序文件名。

要传递到应用程序的参数：要定义要传递到外部应用程序的参数，请复制并粘贴或在“参数”中键入要传递到应用程序字段的一个或多个参数。DRA 提供了可在 Parameters to pass to the application （传递至应用程序的参数）字段中使用的参数。要使用这些参数，请单击“插入”，然后选择要使用的参数。提供对象属性作为参数时，请确保助理管理员对对象属性具有所需的读取许可权限，以及 *Execute Custom Tools* （执行自定义工具）权限以运行自定义工具。

示例：

- *示例 1：*要将组名称和域名作为参数传递到外部应用程序或脚本，请选择 Object Property Name （对象属性名称）和 Domain Property Name （域属性名称）参数，然后在“参数”中指定要传递到应用程序字段的参数名称："{Object.Name}" "{Domain.$McsName}"
- *示例 2：*要为应用程序 "C:\Windows\SysWOW64\cmd.exe" 传递输入参数 "ipconfig"，只需在该字段中键入 "{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}"。

Directory where the application will run （运行应用程序的目录）：这是应用程序需要在客户端或服务器计算机中运行的位置。您需要传递应用程序应执行的路径。您也可以使用“插入”选项，方法与传递“应用程序位置”字段的参数相同。此选项卡中的其他参数足以解释其用法。

自定义用户界面

有多个选项可用于自定义 Delegation and Configuration （委托和配置）控制台的配置方式。这些选项中的大多数都可隐藏、显示或重新配置应用程序中不同功能窗格中的功能。您还可以隐藏或显示工具栏、自定义应用程序标题以及添加、去除或重新排序列。所有这些自定义选项都位于视图菜单中。

修改控制台标题

您可以修改 Delegation and Configuration （委托和配置）控制台标题栏中显示的信息。为方便和清楚起见，您可以添加起动控制台的用户名以及控制台所连接的管理服务器。在需要使用不同身份凭证连接到多个管理服务器的复杂环境中，此功能可帮助您快速识别需要使用的控制台。

要修改控制台标题栏：

1. 启动 Delegation and Configuration （委托和配置）控制台。
2. 单击 **View** （查看） > **Options** （选项）。
3. 选择 Window Title （窗口标题）选项卡。
4. 指定相应的选项，然后单击**确定**。有关更多信息，请单击 **?** 图标。

自定义列表列

您可以选择 DRA 在列表列中显示的对象属性。这项灵活的功能可用于自定义用户界面，例如搜索结果列表，以更好地满足管理企业的特定需求。例如，可以设置列以显示用户登录名或组类型，以便快速有效地查找和排序所需的数据。

要自定义列表列：

1. 选择相应节点。例如，要选择在受管对象上查看搜索结果时显示的列，请选择 **All My Managed Objects （我的所有受管对象）**。
2. 在 View （视图）菜单上，单击 **Choose Columns** （选择列）。
3. 从此节点的可用属性列表中，选择要显示的对象属性。
4. 要更改列顺序，请选择一列，然后单击 **Move Up** （向上移动）或 **Move Down** （向下移动）。
5. 要指定列宽，请选择一列，然后在提供的字段中键入相应的像素数。
6. 单击**确定**。

24 Web 客户端

在 Web 客户端中，您可以自定义对象属性、工作流程自动化表单和用户界面品牌化。正确实施后，属性和工作流程自定义将有助于在对象管理和自动化工作流程提交期间自动执行助理管理员任务。

自定义属性页

您可以按对象类型自定义助理管理员在其 Active Directory 管理角色中使用的对象属性表单。这包括创建和自定义基于 DRA 中内置的对象类型的新对象页面。您还可以修改内置对象类型的属性。

属性对象在 Web 控制台的 “ 自定义 ”>“ 属性页面 ” 列表中明确定义，以便轻松识别内置的对象页面、自定义的内置页面以及不是内置并由管理员创建的页面。

自定义对象属性页

通过添加或去除页面、修改现有页面和字段以及为属性特性创建自定义处理程序，即可自定义对象属性表单。每当修改字段的值时，都会执行字段上的自定义处理程序。您还可以配置时间，以便管理员指定是否应在字段失去焦点时或在指定的时间延迟后，立即 （在每次按键时）运行处理程序。

“ 属性页面 ” 中的对象列表可为每种对象类型提供以下操作类型：创建对象和编辑属性。这些是助理管理员在 Web 控制台中执行的主要操作。其通过导航到**管理** > **搜索**或**高级搜索**执行这些操作。他们可以在这里从 “ 创建 ” 下拉菜单中创建对象，或通过 “ 属性 ” 图标编辑在搜索结果表格中选择的现有对象。

要在 Web 控制台中自定义对象属性页：

1. 以 DRA 管理员身份登录到 Web 控制台。
2. 导航到**系统管理** > **自定义** > **属性页面**。
3. 在 “ 属性页面 ” 列表中选择对象和操作类型 （创建对象或编辑对象）。
4. 单击**属性**图标 。
5. 通过执行以下一项或多项操作然后应用更改来自定义对象属性表单：
   - 添加新的属性页：**+ 添加页面**
   - 重新排序和删除属性页
   - 选择一个属性页面并自定义该页面：
     - 对页面中的配置字段进行重新排序：↑ ↓
     - 编辑字段或子字段：

- 添加一个或多个字段：+ 或**插入新字段**
- 去除一个或多个字段：

- 使用脚本、讯息框或查询 （LDAP、 DRA 或 REST）为属性创建自定义处理程序

  有关使用自定义处理程序的更多信息，请参见添加自定义处理程序。

创建新对象属性页

要创建新对象属性页：

1. 以 DRA 管理员身份登录到 Web 控制台。
2. 导航到**系统管理** > **自定义** > **属性页面**。
3. 单击+ **创建**。
4. 通过定义操作名称、图标、对象类型和操作配置来创建初始对象属性表单。

   用户从搜索列表中选择并编辑对象时，创建操作会添加到“创建”下拉菜单，而属性操作会显示在对象表单中。
5. 根据需要自定义新表单。请参见自定义对象属性页。

自定义请求表单

请求表单在创建或修改时将保存到 Web 服务器。 DRA 管理员可以从**系统管理** > **自定义** > **请求**中进行管理。助理管理员可以从**任务** > **请求**中进行管理。这些表单用于提交在工作流程自动化服务器中创建的自动化工作流程。表单创建者可以使用这些请求进一步自动化和改进对象管理任务。

您可以添加和修改现有表单属性和自定义处理程序。除可使用表单者的工作流程配置选项和控件以外，自定义对象属性时，在工作流程自动化表单中添加和自定义属性的界面行为通常相同。有关添加和修改属性、添加自定义处理程序以及了解工作流程自动化的更多信息，请参阅以下主题。

- 自定义属性页 （Web 客户端）
- 添加自定义处理程序
- 自动化工作流程

添加自定义处理程序

自定义处理程序在 DRA 中用于属性特性相互交互以完成工作流程任务，以及用于在工作流程、属性或创建表单中装载和提交自定义。

属性自定义处理程序

属性自定义处理程序的一些示例包含：

- 查询其他字段的值
- 更新字段值

- 切换字段的只读状态
- 根据配置的变量显示或隐藏字段

表单装载处理程序

表单装载处理程序通常会执行初始化控件。最初加载表单时，其仅执行一次。对于属性页，将在查询服务器以获取所选对象的属性前执行。

表单提交处理程序

表单提交处理程序允许用户进行一些类型的验证，如果出现问题，则可能会取消表单提交。

有关在 Web 控制台中使用自定义处理程序和自定义的更多详细示例，请参阅 DRA 文档页面上 *Product Customization* （产品自定义）中的 “Web Console Customization” （Web 控制台自定义）和 “Workflow Customization” （工作流程自定义）部分。

启用自定义 JavaScript

出于安全原因，默认情况下禁用自定义 JavaScript。启用自定义 JavaScript 使管理员能够编写 JavaScript 代码片段，而 Web 控制台将按原样执行。只有在您了解并接受风险时，才应启用此例外项。

要启用自定义以包含自定义 JavaScript 代码：

1. 导航到 C:\ProgramData\NetIQ\DRARESTProxy 位置。
2. 打开 restProxy.config 文件。
3. 将 allowCustomJavaScript="true" 添加到 <consoleConfiguration> 元素。

创建自定义处理程序的基本步骤：

以下步骤从预先选择的自定义处理程序页面开始。为此，您可以通过属性字段上的属性图标访问对象属性自定义处理程序。您可以通过所选工作流程表单、“ 创建对象 ” 页面或 “ 编辑属性 ” 页面上的**表单属性**按钮，访问**表单装载**和**表单提交**处理程序。

1. 根据要自定义的属性或页面选择适用的处理程序选项卡：
   - 自定义处理程序
   - 表单装载处理程序
   - 表单提交处理程序
2. 启用处理程序页面  ，然后执行任意下列操作：
   - **属性字段自定义处理程序：**
     1. 选择执行时间。*一般情况下，您会使用 “ 执行时间 ” 的第二个或第三个选项。*
     2. 单击 **+ Add** （+ 添加），然后从 **Add Custom Handler** （添加自定义处理程序）菜单中选择自定义处理程序。
   - **表单处理程序：**单击 **+ Add** （+ 添加），然后从 **Add Custom Handler** （添加自定义处理程序）菜单中选择自定义处理程序。

注释：通常您可能只需要一个自定义处理程序，但可以使用多个处理程序。多个处理程序会按列出的顺序执行。如果要更改处理程序的顺序或跳过不需要的处理程序，则可以在脚本中添加流控制宏。

3 您需要配置添加到页面的每个自定义处理程序。配置选项因处理程序类型而异。

您可以创建自己的处理程序类型。

- **LDAP 或 REST 查询处理程序：**
  1. 如果希望查询基于静态值，请定义**连接信息**和**查询参数**。

     如果希望查询是动态的，请在必填字段中输入占位符值。这是处理程序执行所必需的。脚本将覆盖占位符值。

     注释：您还可以为 REST 查询配置标题和 Cookie。
  2. 在预查询操作中，使用脚本编辑器编写将在提交查询前执行的自定义 JavaScript 代码。此脚本可以访问所有连接信息和查询参数，并且可以修改其中任何项以自定义查询。例如，根据用户在表单中输入的值设置查询参数。
  3. 在查询后操作中，包含脚本以处理查询结果。常见任务包含检查错误，根据返回的结果更新表单值，以及根据查询返回的对象数验证对象唯一性。
- **脚本：**插入自定义 JavaScript 代码以构建脚本。
- **DRA 查询：**在“查询参数”选项卡中，指定 JSON 有效负载。有效负载格式必须与将发送到 DRA 服务器的 VarSet 键或值对匹配。与 REST 和 LDAP 查询类似，您可以指定可用于在将有效负载提交给服务器前，修改有效负载的预查询操作，以及用于处理结果的查询后操作。
- **讯息框处理程序：**定义讯息框本身的属性后，您还可以为**显示前操作**和**关闭后操作**编写 JavaScript 段。

  这些均为可选操作。“显示前操作”用于在向用户显示任何讯息框属性前对其进行自定义，而“关闭后操作”用于处理用户的按钮选择并据此执行任何其他逻辑。

4 单击**确定**保存处理程序。

有关在 Web 控制台中使用自定义处理程序和自定义的更多详细示例，请参阅 DRA 文档页面上 *Product Customization*（产品自定义）中的“Web Console Customization”（Web 控制台自定义）和“Workflow Customization”（工作流程自定义）部分。

自定义用户界面品牌化

您可以使用自己的标题和徽标图像自定义 DRA Web 控制台的标题栏。展示位置直接位于 DRA 产品名称的右侧。由于此位置也用于顶级导航，因此登录后会由顶级 DRA 导航链接隐藏。但是，浏览器选项卡将继续显示自定义标题。

要自定义 DRA Web 控制台的品牌：

1 以 DRA 管理员身份登录到 Web 控制台。

2 导航到**系统管理** > **配置** > **品牌化**。

3 如果添加的是公司徽标图像，请将徽标图像保存在 Web 服务器上的 inetpub\wwwroot\DRAClient\assets 中。

4 更新刊头和登录磁贴的配置 （如果适用）。

5 完成所有更改后，单击保存。

IX 工具和实用程序

以下章节介绍 DRA 提供的 ActiveView Analyzer 实用程序、诊断实用程序、已删除对象实用程序、运行状况检查实用程序以及回收站实用程序。

25 ActiveView Analyzer 实用程序

每个 DRA ActiveView 都包含一个或多个规则，这些规则适用于 DRA 多主集合管理的 Active Directory (AD) 对象。ActiveView Analyzer 实用程序用于将每个 DRA ActiveView 规则应用于特定 DRA 操作中的 AD 对象时，监视其处理时间。在 DRA 操作期间， DRA 服务器会将该操作的目标对象与每个 ActiveView 中的每个规则进行比较。然后 DRA 会创建包含所有匹配规则的结果列表。 ActiveView Analyzer 会计算将每个规则应用到 DRA 操作时花费了多少时间进行处理。

使用此信息，您可以通过检查 ActiveView 处理时间的异常来诊断 ActiveView 问题，包括处理未使用的 ActiveView 所花费的时间。实用程序还简化了查找重复 ActiveView 的过程。

运行数据收集并查看报告后，您可能会发现需要修改一个或多个 ActiveView 的规则。

您可以从任何 DRA 管理服务器访问 ActiveView Analyzer 实用程序。但是，应在遇到问题的管理服务器上运行 ActiveView 实用程序。

要访问 ActiveView Analyzer 实用程序，请使用 DRA 管理角色特权登录到管理服务器，然后从“开始”菜单中导航到 **NetIQ Administration** （NetIQ 管理） > **ActiveView Analyzer Utility** （ActiveView Analyzer 实用程序）。您还可以从 DRA 安装路径 Program Files (x86)\NetIQ\DRA\X64 中起动 ActiveViewAnalyzer.exe。

使用此实用程序执行以下操作：

- 收集有关 ActiveView 的数据
- 生成 Analyzer 报告

示例

助理管理员 Paul 通知 DRA 管理员 Bob，创建用户所需要的时间似乎比平时更长。 Bob 决定对 Paul 的用户对象启动 ActiveView Analyzer，然后让 Paul 创建用户。收集后， Bob 生成了分析报告，并注意到名为 Share MBX 的规则需要 50 毫秒的时间来枚举。 Bob 识别了包含规则的 ActiveView，并在更改规则后观察到问题已解决。

启动 ActiveView 数据收集

使用 ActiveView Analyzer 实用程序，您可以从助理管理员对 ActiveView 执行的操作中收集有关 ActiveView 的数据。然后，可以在 Analyzer 报告中查看此数据。要收集数据，您需要指定助理管理员以收集数据，然后启动 ActiveView 收集。

注释：要收集数据的助理管理员必须连接到运行 Analyzer 的同一 DRA 服务器。

要启动 ActiveView 收集：

1 单击开始 > **NetIQ Administration** （NetIQ 管理） > **ActiveView Analyzer Utility** （ActiveView Analyzer 实用程序）。

2 在 ActiveView Analyzer 页中，指定以下内容：

2a 目标 DRA 服务器：收集有关助理 Admin 操作的性能数据的 DRA 服务器。

2b 目标助理管理员：单击浏览，然后选择要对其收集数据的助理管理员。

2c 监控持续时间：指定收集 Analyzer 数据所需的总小时数。超过指定时间后，将停止数据收集。

3 单击 **Start Collection** （开始收集）以收集 ActiveView 数据。

启动 ActiveView 数据收集后，实用程序将清除现有数据并显示最新状态。

4 （可选）在安排的持续时间结束之前，您可以手动停止数据收集，且仍会生成报告。单击 **Stop Collection** （停止收集）以停止记录 ActiveView 上的助理 Admin 操作。

5 （可选）要获取最新状态，请单击 **Collection Status** （收集状态）。

重要：如果停止收集并更改助理管理员或重启动同一助理管理员的数据收集，则 ActiveView Analyzer 将清除现有数据。一次只能为数据库中的一个助理管理员提供 Analyzer 数据。

生成 Analyzer 报告

生成 Analyzer 报告前，请确保您停止收集数据。

在 ActiveView Analyzer 页面中，将显示助理管理员执行的操作列表。要生成 Analyzer 报告：

1 单击 **Select Report** （选择报告），然后选择要查看的报告。

2 单击 **Generate Report** （生成报告）以生成包含 ActiveView 操作细节的分析报告，例如操作影响的 AD 对象、管理列出对象的 ActiveView、匹配、不匹配和处理每个 ActiveView 规则的持续时间。

使用该报告，您可以分析哪些规则需要更多时间来执行操作，然后决定是否应在其各自的 ActiveView 中修改或删除其中的任何规则。

3 （可选）将鼠标悬停在网格上，右键单击，然后使用复制菜单将报告复制到剪贴板。从剪贴板中，可以将列标题和数据粘贴到另一个应用程序，例如记事本或 Excel。

识别对象的性能

要识别由 ActiveView 或规则管理的所有对象的性能：

1 起动 Delegation and Configuration （委托和配置）控制台。

2 导航到 **Delegation Management** （委托管理），然后单击 **Manage ActiveViews** （管理 ActiveView）。

3 运行搜索以找到特定的 ActiveView。

在这里，您可以找到有问题的规则或对象并进行修改。

- 双击 ActiveView，然后选择 **Rules** （规则）以列出规则。您可以从右键单击菜单中修改特定规则。
- 右键单击 ActiveView，然后选择 **Show Managed Objects** （显示受管对象）以列出对象。您可以通过右键单击 > **Properties** （属性）修改对象。

4 对规则或受管对象进行更改，并校验这些更改是否可以解决问题。

26 诊断实用程序

诊断实用程序可从管理服务器收集信息，以帮助诊断 DRA 问题。使用此实用程序向技术支持代表提供日志文件。诊断实用程序提供了一个向导界面，可指导您设置日志级别和收集诊断信息。

您可以从任何管理服务器计算机访问诊断实用程序。但是，应在遇到问题的管理服务器上运行诊断实用程序。

要访问诊断实用程序，请使用具有本地管理员权限的管理员帐户登录到管理服务器计算机，然后从 Windows“ 开始 ” 菜单中的 NetIQ Administration （NetIQ 管理）程序组中打开实用程序。

有关使用此实用程序的更多信息，请联系技术支持。

27 已删除对象实用程序

此实用程序允许您在域访问帐户不是管理员时，为特定域启用增量帐户超速缓存刷新支持。如果域访问帐户对域中的 Deleted Objects （已删除对象）容器没有读取许可权限，则 DRA 无法执行增量帐户超速缓存刷新。

您可以使用此实用程序执行以下任务：

- 校验指定的用户帐户或组是否对指定域中的 Deleted Objects （已删除对象）容器具有读取许可权限
- 为指定用户帐户或组委托或去除读取许可权限
- 为用户帐户委托或去除同步目录服务数据用户权限
- 显示 Deleted Objects （已删除对象）容器的安全设置

您可以从管理服务器上的 Program Files (x86)\NetIQ\DRA 文件夹中运行 Deleted Objects Utility （已删除对象实用程序）文件 (DraDelObjsUtil.exe)。

Deleted Objects Utility （已删除对象实用程序）所需的许可权限

要使用此实用程序，您必须具有以下许可权限：

如果要 ...	则需要以下许可权限 ...
校验帐户许可权限	对 Deleted Objects （已删除对象）容器的读取许可权限
委托对 Deleted Objects （已删除对象）容器的读取许可权限	Deleted Objects （已删除对象）容器所在域中的管理员许可权限
委托同步目录服务数据用户权限	Deleted Objects （已删除对象）容器所在域中的管理员许可权限
去除之前委托的许可权限	Deleted Objects （已删除对象）容器所在域中的管理员许可权限
显示 Deleted Objects （已删除对象）容器的安全设置	对 Deleted Objects （已删除对象）容器的读取许可权限

Deleted Objects Utility （已删除对象实用程序）的语法

DRADELOBJSUTIL /DOMAIN:*DOMAINNAME*[/DC:*COMPUTERNAME*] {/DELEGATE:*ACCOUNTNAME*| /VERIFY:*ACCOUNTNAME*| /REMOVE:*ACCOUNTNAME*| /DISPLAY [/RIGHT]}

Deleted Objects Utility （已删除对象实用程序）的选项

可以指定以下选项：

/DOMAIN:*domain*	指定 Deleted Objects （已删除对象）容器所在域的 NETBIOS 或 DNS 名称。
/SERVER:*computername*	指定特定域的域控制器的名称或 IP 地址。
/DELEGATE:*accountname*	将许可权限委托给指定用户帐户或组。
/REMOVE:*accountname*	去除之前委托给指定用户帐户或组的许可权限
/VERIFY:*accountname*	校验指定用户帐户或组的许可权限。
/DISPLAY	显示指定域中 Deleted Objects （已删除对象）容器的安全设置
/RIGHT	确保指定的用户帐户或组具有同步目录服务数据用户权限。您可以使用此选项委托或校验此权限。同步目录服务数据用户权限允许帐户读取 Active Directory 中的所有对象和属性。

注释：

- 如果要指定的用户帐户或组的名称包含空格，请将帐户名称括在引号中。例如，如果要指定休斯顿 IT 组，请键入 "Houston IT"。
- 指定组时，请使用该组的 Windows 2000 之前的名称。

Deleted Objects Utility （已删除对象实用程序）的示例

以下示例演示了常见场景的示例命令。

示例 1

要校验 MYCOMPANY\JSmith 用户帐户是否对 hou.mycompany.com 域中的 Deleted Objects （已删除对象）容器具有读取许可权限，请输入：

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

示例 2

要将 MYCOMPANY 域中 Deleted Objects （已删除对象）容器的读取许可权限委托给 MYCOMPANY\DraAdmins 组，请输入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

示例 3

要将 MYCOMPANY 域中的 Deleted Objects （已删除对象）容器和同步目录服务数据用户权限的读取许可权限委托给 MYCOMPANY\JSmith 用户帐户，请输入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

示例 4

要使用 HQDC 域控制器显示 hou.mycompany.com 域中 Deleted Objects （已删除对象）容器的安全设置，请输入：

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

示例 5

要从 MYCOMPANY\DraAdmins 组中去除 MYCOMPANY 域中 Deleted Objects （已删除对象）容器的读取许可权限，请输入：

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 运行状况检查实用程序

DRA 运行状况检查实用程序是与 DRA 安装包一起打包的独立应用程序。您可以在安装后以及升级前后使用运行状况检查实用程序来校验、验证和通知 DRA 服务器、 DRA 网站和 DRA 客户端的组件和进程的状态。您还可以使用该实用程序来安装或更新产品许可证、在产品升级之前备份 AD LDS 实例、查看检查说明，以及修复问题或确定修复问题所需采取的操作，然后对其进行重新验证。

执行 NetIQAdminInstallationKit.msi 安装程序后，可以在 DRA 程序文件夹中访问运行状况检查实用程序。

通过执行 NetIQ.DRA.HealthCheckUI.exe 文件，可以随时运行运行状况检查实用程序。应用程序打开时，可以选择执行特定操作、对特定组件运行检查或对所有组件运行检查。有关使用运行状况检查实用程序执行的有用功能，请参见下文：

功能	用户操作
全选或取消全选	使用工具栏或“文件”菜单选项可选择或取消选择所有检查项目，或选择单个复选框以运行特定检查。
运行所选检查	使用此工具栏或“文件”菜单选项可运行选中的检查 （全部或特定）。
保存或写入结果	使用此工具栏或“文件”菜单选项可为运行的检查创建并保存详细报告。
运行此检查	选择项目标题以查看检查的说明，然后单击此工具栏图标以运行检查。例如，要运行以下操作之一： ◆ 许可证验证 （安装或更新产品许可证） ◆ AD LDS 实例备份 （备份 AD LDS 实例） ◆ 复制 （验证复制数据库）
修复此问题	选择项目标题，然后在检查失败时使用此工具栏选项。如果再次运行检查无法修复问题，则说明中应包含解决该问题的相关信息。

29 回收站实用程序

此实用程序允许您在管理域的子树时启用回收站支持。如果域访问帐户对指定域中隐藏的 NetIQRecycleBin 容器没有许可权限，则 DRA 无法将已删除的帐户移动到回收站。

注释：使用此实用程序启用回收站后，请执行完全帐户超速缓存刷新以确保管理服务器应用此更改。

您可以使用此实用程序执行以下任务：

- 校验指定的帐户是否对指定域中的 NetIQRecycleBin 容器具有读取许可权限
- 将读取许可权限委托给指定的帐户
- 显示 NetIQRecycleBin 容器的安全设置

回收站实用程序所需的许可权限

要使用此实用程序，您必须具有以下许可权限：

如果要 ...	则需要以下许可权限 ...
校验帐户许可权限	对 NetIQRecycleBin 容器的读取许可权限
委托对 NetIQRecycleBin 容器的读取许可权限	指定域中的管理员许可权限
显示 NetIQRecycleBin 容器的安全设置	对 NetIQRecycleBin 容器的读取许可权限

回收站实用程序的语法

DRARECYCLEBINUTIL /DOMAIN:*DOMAINNAME*[/DC:*COMPUTERNAME*] {/DELEGATE:*ACCOUNTNAME*| /VERIFY:*ACCOUNTNAME*| /DISPLAY}

回收站实用程序的选项

使用以下选项可以配置回收站实用程序：

/DOMAIN:domain	指定回收站所在域的 NETBIOS 或 DNS 名称。
/SERVER:*computername*	指定特定域的域控制器的名称或 IP 地址。
/DELEGATE:*accountname*	将许可权限委托给指定帐户。
/VERIFY:*accountname*	校验指定帐户的许可权限。

/DISPLAY	显示指定域中 NetIQRecycleBin 容器的安全设置。

回收站实用程序的示例

以下示例演示了常见场景的示例命令。

示例 1

要校验 MYCOMPANY\JSmith 用户帐户是否对 hou.mycompany.com 域中的 NetIQRecycleBin 容器具有读取许可权限，请输入：

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

示例 2

要将 MYCOMPANY 域中 NetIQRecycleBin 容器的读取许可权限委托给 MYCOMPANY\DraAdmins 组，请输入：

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

示例 3

要使用 HQDC 域控制器显示 hou.mycompany.com 域中 NetIQRecycleBin 容器的安全设置，请输入：

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```