法律声明

目录

关于本指南

本*用户指南*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。

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。

1 入门

在您开始使用 Directory and Resource Administrator™ (DRA) 管理 Active Directory 之前，您应了解 DRA 对企业的基本影响原则，以及产品结构中 DRA 组件的角色。

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

- **支持 Azure 和本地 Active Directory、 Exchange 及 Skype for Business：**提供对 Azure 和本地 Active Directory、本地 Exchange Server、本地 Skype for Business、 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。

1.2 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 PowerShell CLI DRA ADSI 提供程序	任何 DRA 服务器
Help Desk 临时管理员	Delegation and Configuration （委托和配置）控制台中的 Account and Resource Management （帐户和资源管理）节点 Web 控制台	任何 DRA 服务器

1.2.1 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。

1.2.2 Account and Resource Management （帐户和资源管理）

Account and Resource Management （帐户和资源管理）是 Delegation and Configuration （委托和配置）控制台中的一个节点，用于 DRA 助理管理员查看和管理所连接域和服务的委托对象。

1.2.3 Web 控制台

Web 控制台是一个基于 Web 的用户界面，可通过此界面快速轻松访问 DRA 助理管理员，从而查看和管理所连接域和服务的委托对象。

管理员可以自定义 Web 控制台的外观和使用，使其包含自定义企业品牌和自定义对象属性，也可以配置与 Change Guardian 服务器集成，从而能够对发生于 DRA 以外的更改进行审计。

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

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

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

1.2.4 报告组件

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

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

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

1.2.5 工作流程引擎

DRA 与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 文档网站中的工作流程自动化文档。

1.2.6 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

2 使用用户界面

DRA 用户界面可满足各种管理需求。这些界面包括：

Web 控制台

使您能够通过基于 Web 的界面执行常见的帐户和资源管理任务。您可以从运行 Internet Explorer、 Chrome 或 Firefox 的任何计算机访问 Web 控制台。

PowerShell

PowerShell 模块允许非 DRA 客户端使用 PowerShell cmdlet 请求 DRA 操作。

NetIQ Reporting Center 控制台

使您可以查看和部署管理报告，以便可以审计企业安全性及跟踪管理活动。管理报告包括活动报告、配置报告和摘要报告，其中许多报告都可以通过图形表示形式进行查看。

2.1 Web 控制台

Web 控制台是一个基于 Web 的用户界面，可通过此界面快速轻松访问许多用户帐户、组、计算机、资源和 Microsoft Exchange 邮箱任务。您可以自定义对象属性以提高例程任务的效率。您还可以管理自己的用户帐户的常规属性，例如街道地址或手机号码。

仅当您有权执行某项任务时， Web 控制台才会显示该任务。

2.1.1 启动 Web 控制台

您可以从运行 Internet Explorer 的任何计算机启动 Web 控制台。要启动 Web 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.entDomain.com/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面的较新版本。

2.1.2 配置 Web 控制台

借助相应的权限，您可以在 Web 控制台中配置所有必需的服务器连接和集成、自动注销行为和 Advanced Authentication。

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

您可以在 Web 控制台中配置三个选项之一，定义登录时的 DRA 服务器连接选项。

- 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）。您可以在 Web 控制台中配置三个选项之一，以定义登录时的 REST 服务连接选项。

- 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**。

Advanced Authentication

Advanced Authentication 可让您超越简单的用户名和口令，使用多因子鉴定以更安全的方式保护敏感信息。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。

DRA 管理员配置链和事件后，如果您具有所需的权限，则可以登录到 Web 控制台并启用 Advanced Authentication。启用鉴定后，每个用户都需要通过 Advanced Authentication 进行鉴定，然后才能访问 Web 控制台。

要启用 Advanced Authentication，请登录到 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。

有关 Advanced Authentication 的更多信息，请参见 *《DRA 管理员指南》* 中的 “ 鉴定 ”。

集成服务器

DRA 与工作流程自动化服务器和 Change Guardian 服务器集成，可分别提供对自动化工作流程表单和统一的更改历史记录 (UCH) 报告的访问权限。如果您具有所需的权限，则可以配置与工作流程自动化服务器和一个或多个 Change Guardian 服务器的连接。

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，必须在创建自动化工作流程的 Windows Server 上安装工作流程引擎。在 Web 控制台中配置 DRA 与工作流程自动化服务器的集成。

要配置工作流程自动化服务器，请登录到 Web 控制台并导航到**管理** > **集成** > **工作流程自动化**。

配置统一的更改历史记录服务器

要配置 UCH 服务器：

1. 起动 Web 控制台并使用助理 Admin 身份凭证登录。
2. 转到**管理 > 集成 > 统一的更改历史记录**，然后单击**添加**图标。
3. 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。
4. 测试服务器连接，然后单击**确定**以保存配置。
5. 根据需要添加其他服务器。

2.1.3 自定义 Web 控制台

在 Web 控制台中，您可以自定义对象属性和用户界面品牌化。正确实现后，属性自定义将有助于通过对象管理自动执行任务。

自定义属性页

您可以按对象类型自定义在 Active Directory 管理角色中使用的对象属性表单，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“属性页面”列表中明确定义，以便可以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。创建自定义处理程序后，它们便会在属性字段更改时或管理员响应运行查询的提示时自动执行，具体取决于自定义处理程序的配置方式。

“属性页面”中的对象列表可为每种对象类型提供两种操作类型：创建对象和编辑属性。这些操作是您在 Web 客户端中执行的主要操作，您的自定义可以改善在 DRA 中管理 Active Directory 对象时的效率和体验。

要在 Web 控制台中自定义对象属性页：

1. 导航到**自定义** > **属性页面**。
2. 在“属性页面”列表中选择一个对象和操作类型 （创建或编辑）。
3. 单击**编辑**按钮。
4. 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**
   - 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**添加字段**
     - 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。

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。属性自定义处理程序的一些示例包括查询其他字段的值、更新值、切换字段的只读状态，以及根据配置的变量显示或隐藏字段

DRA 还通过几个可选的 JavaScript (JS) 宏简化了创建自定义处理程序，您可以在自定义处理程序创建和验证过程中选择这些宏。

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编辑按钮 访问对象属性自定义处理程序。

1. 单击“自定义处理程序”选项卡并启用页面 。
2. 从下拉菜单中选择自定义处理程序，然后选择执行时间。一般情况下，您会使用“执行时间”的第二个或第三个选项。

   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，方法是在脚本中配置流程控制以将处理程序链接在一起。

   ---

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，但所有处理程序均从 JavaScript 执行。

   您可以创建自己的 Vanilla JavaScript 条目或使用内置宏。

   - **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文本。这是脚本执行所必需的。脚本将覆盖伪值。

注释：您还可以为 REST 查询配置标题和 Cookie。

2. 在“查询前操作”中，选择宏类型：**全局**、**查询**或**表单字段**。
3. 从下拉列表中选择一个宏，然后插入宏（**</> 插入宏**）。
4. 根据需要插入其他宏，然后提供所需的值以完成脚本。

   例如，在“查询前操作”中，我们将使用脚本来验证提交表单时，用户输入的组名称是否已存在于 Active Directory 中。

   我们需要使用用户输入的名称创建 LDAP 查询。我们使用 Field() 宏来访问“名称”字段的值，并构建查询字符串，然后使用 Filter() 宏将其设置为查询过滤器。

   ```
   Filter() = '(&(objectCategory=group)(objectClass=group)(name=' +
   Field(name) + '))';
   ```

5. 按照上面的示例，在“查询后操作”中，我们将检查查询返回的结果。结果作为与查询匹配的对象阵列返回，因此我们只需要检查阵列的长度是否大于 0。

   当找到匹配的组时，我们使用 Cancel() 宏来取消表单提交，向宏传递一条可选讯息以显示给用户。

   ```
   if (QueryResults().length > 0) { Cancel('A group with that name already exists, please enter a unique name.');}
   ```

- **脚本：**插入自定义 JavaScript 代码或使用宏来构建脚本。
- **DRA 查询：**对于查询参数，以 JSON 格式定义有效负载，然后以与上述 LDAP 和 REST 查询类似的方式使用宏。
- **讯息框处理程序：**在定义讯息框本身的属性后，以与上述 LDAP 和 REST 查询类似的方式使用宏，但不是使用“查询前”操作和“查询后”操作，而是撰写针对“显示前”操作和“关闭后”操作的宏脚本。

4 单击**测试处理程序**以在保存表单之前验证脚本。

此操作将生成一个测试结果摘要，您可以在其中查看执行结果。

注释：如果处理程序依赖于表单的当前状态（例如，某字段具有值时才处理），则它将无法成功执行，因为在编辑表单时不会装载任何数据。在这些情况下，需要在表单编辑器外部通过保存自定义、导航到相应表单以及填写所需数据来测试处理程序。

创建新对象属性页

要创建新对象属性页：

1 登录到 Web 控制台并导航到**自定义** > **属性页面**。

2 在“任务”下，单击**创建新行为**。

3 通过定义名称、图标、对象类型和操作配置来创建初始对象属性表单。

4 根据需要自定义新表单。请参见自定义对象属性页。

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。

要在 DRA 中自定义标题品牌化：

1. 登录到 Web 控制台并导航到**自定义** > **品牌化**。
2. 如果要添加公司徽标，请将徽标图像保存到 Web 服务器上的 components\lib\img 目录下。
3. 为品牌化自定义页面上的三个字段添加所需的信息 （如果适用），然后保存更改。

2.1.4 在 Web 控制台中管理对象

通过导航到 “ 管理 ” 标头，可以在 Web 控制台中管理对象。在此处，您可以按对象类型搜索域、容器和回收站中的对象。选择域、容器或 OU 后，您还可以创建新对象，添加成员、从组中去除成员以及移动对象。

如果在搜索结果列表中选择一个对象，则可以在网格上方的任务栏上找到可对该对象执行的所有适用操作。可用的选项取决于所选的对象类型、当前为 DRA 配置的组件以及分配的管理员特权。

要编辑对象的属性，将鼠标悬停在对象上，然后单击对象行上出现的**属性**图标 ✎。在此处，您可以访问左侧导航窗格中对象的所有 “ 属性 ” 页面。

重要：如果想要 **protect an object from accidental deletion** （保护对象以防意外删除），滚动至**常规**属性页的底部，选中复选框以启用此功能，然后**应用**更改。

有关可以对对象执行的操作的更多信息，请参见以下主题：

- 管理用户帐户、组和联系人
- 管理 Exchange 邮箱和公共文件夹
- 管理资源

2.1.5 使用统一的更改历史记录 (UCH)

有关配置 UCH 服务器的信息，请参见配置统一的更改历史记录服务器。

搜索和生成 UCH 报告

您可以使用搜索选项搜索所有统一的更改报告或缩小搜索范围。您只能从 Web 控制台查看 UCH 报告。如果不使用参数进行搜索，则会列出所有 UCH 报告。添加搜索参数将过滤搜索中返回的报告。

重要：要生成 UCH 报告，您需要具有 **Generate UI Reports** （生成 UI 报告）的权限。

要搜索和生成统一的更改历史记录报告：

1 起动 Web 控制台。

2 转到**管理 > 搜索**。

3 使用或不使用任何名称、位置或子容器准则执行搜索。

如果未使用任何准则，搜索结果将返回所有对象。要缩小结果范围，请包括搜索准则。

4 单击**搜索**图标以显示搜索结果。

5 选择要为其生成报告的对象。

6 单击**查看更改历史记录报告**图标。

在**更改历史记录报告准则**中，您可以使用报告类型、目标对象、开始日期、结束日期、最大行数或服务器 （DRA 或 Change Guardian 服务器）等准则编辑和生成报告。

7 单击**生成**以提取审计数据并生成 UCH 报告。

8 您可以将报告排序并导出为所需格式，例如 CSV 和 HTML。

查看统一的更改历史记录属性

要查看 UCH 配置服务器的属性，请导航到**管理** > **集成** > **统一的更改历史记录**，选择已配置的服务器，然后单击**选项**菜单以执行以下任何操作：

- **属性：**查看和更新 UCH 属性。
- **测试连接：**校验服务器连接。
- **删除：**删除配置的 UCH 服务器。

2.1.6 访问用户的更改历史记录

您可以使用 Web 控制台查看对用户所做更改或用户所做更改的历史记录。您可以查看以下类型的更改：

- 用户所作的更改
- 对用户所作的更改
- 用户创建的用户邮箱
- 用户删除的用户邮箱
- 用户建立的组和联系人电子邮件地址
- 用户删除的组和联系人电子邮件地址
- 用户创建或禁用的虚拟属性
- 用户移动的对象

要查看或生成“更改历史记录”报告：

1 启动 Web 控制台。

2 搜索要查看其历史记录的对象。

3 单击**查看更改历史记录报告**图标。

4 要更改报告生成准则，请单击**修改**。

您可以更改开始日期或结束日期、跟踪的对象、报告类型和其他准则。

5 要创建报告的 CSV 文件，请单击**生成**。

2.1.7 使用工作流程自动化

使用工作流程自动化，您可以通过起动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的工作流程表单，来自动化 IT 流程。

工作流程表单在创建或修改时将保存到 Web 服务器。当您登录此服务器的 Web 控制台时，您将可以根据委托的权限以及表单的配置方式访问表单。表单通常可供具有 Web 服务器身份凭证的所有用户使用。提交表单的能力需要相应的权限。

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 Web 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”配置的工作流程表单，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。

---

*《DRA 管理员指南》*中包含有关工作流程自动化的更多信息。

2.2 Account and Resource Management （帐户和资源管理）

通过 Delegation and Configuration （委托和配置）控制台中的 Account and Resource Management （帐户和资源管理）节点，可访问大多数 DRA 助理管理员任务，从而满足从基本管理到高级 Help Desk 问题的企业管理需求。通过 Account and Resource Management （帐户和资源管理），您可以执行帐户和资源管理任务以及管理 Microsoft Exchange 邮箱。

Account and Resource Management （帐户和资源管理）包含以下节点：

我的所有受管对象

使您可以管理您拥有特定权限的每个域中的对象，例如用户帐户、组、联系人、资源、动态组、动态分发组、资源邮箱和公共文件夹。

Temporary Group Assignments （临时组指派）

使您可以管理仅在特定时间段内需要组成员资格的用户的组成员资格。

Advanced Search Queries （高级搜索查询）

使您可以管理“管理”服务器上的高级查询。

回收站

使您可以管理已启用 Recycle Bin （回收站）的任何 Microsoft Windows 域的已删除用户帐户、组、联系人和资源。

要访问 Account and Resource Management （帐户和资源管理）节点，请在 NetIQ 管理员程序文件夹中单击 **Delegation and Configuration （委托和配置）**，然后在控制台中展开 Delegation and Configuration （委托和配置）节点。

启动 Delegation and Configuration （委托和配置）控制台时，最初将连接到本地域中最佳的可用管理服务器。最佳的可用管理服务器是最近的服务器，通常是网络站点中的服务器。通过寻找最佳的可用管理服务器， DRA 可提供更快的连接和更高的性能。

要了解有关在 Account and Resource Management （帐户和资源管理）中工作的更多信息，请参见以下主题：

2.2.1 连接到管理服务器或受管域

默认情况下， DRA 将连接到受管域或计算机的最佳可用管理服务器。最佳的可用管理服务器是最近的服务器，通常是网络站点中的服务器。如果站点不包含管理服务器，则 DRA 将连接到受管域或受管子树中的下一个可用服务器。您还可以指定要连接的管理服务器或域。

首次启动用户界面时， DRA 最初会连接到您的登录帐户的域。如果登录到未由管理服务器管理的域，或 DRA 无法连接到该域的管理服务器，则 DRA 可能会显示一条错误讯息。确保管理服务器可用，然后重试。

要连接到管理服务器：

1. 在 File （文件）菜单上，单击 **Connect to DRA server** （连接到服务器）。
2. 单击 **Connect to this DRA server** （连接到此 DRA 服务器）。

3 使用以下格式键入管理服务器的名称：*computername*。

4 单击 **OK** （确定）。

要连接到受管域或计算机：

1 在 File （文件）菜单上，单击 **Connect to DRA server** （连接到服务器）。

2 选择相应的选项，然后键入受管域或计算机的名称。

3 例如，要连接到 HOULAB 域，请单击 **Connect to a DRA server that manages this domain** （连接到管理此域的 DRA 服务器），然后键入 HOULAB。

4 要指定受管域或计算机的管理服务器，请单击 **Advanced** （高级），然后选择相应的选项。

5 单击 **OK** （确定）。

2.2.2 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 **OK** （确定）。

2.2.3 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 **OK** （确定）。

2.2.4 管理 Account and Resource Management （帐户和资源管理）中的对象

通过选择我的所有受管对象或目录树中的子节点，可以管理 Account and Resource Management（帐户和资源管理）中的对象。在此处，您可以按对象类型搜索域、容器和 OU 中的对象。

如果在搜索结果列表中选择一个对象，则可以在工具栏上的任务菜单或右键菜单中找到可对该对象执行的所有适用操作。可用的选项取决于所选的对象类型、当前为 DRA 配置的组件以及分配的管理员特权。

要编辑对象的属性，选择该对象，然后在任务菜单中单击属性。在此处，单击左侧导航窗格中的页面链接即可访问对象的所有“属性”页面。

重要：如果想要 **protect an object from accidental deletion** （保护对象以防意外删除），选择对象并打开属性，在导航窗格中选择常规，选中复选框以启用此功能，然后应用更改。

有关可以对对象执行的操作的更多信息，请参见以下主题：

- 管理用户帐户、组和联系人
- 管理 Exchange 邮箱和公共文件夹
- 管理资源

2.2.5 执行保存的高级查询

使用高级查询，您可以搜索用户、联系人、组、计算机、打印机、 OU 以及 DRA 支持的任何其他对象。如果您具有 Execute Saved Advanced Queries （执行保存的高级查询）权限，则可以执行 Account and Resource Management （帐户和资源管理）节点中任何容器的 **Saved Queries** （保存的查询）列表中的高级查询。有关指派的权限的更多信息，请参见查看指派的权限和角色。

要执行保存的高级查询：

1. 展开 **Account and Resource Management** （帐户和资源管理） > **All My Managed Objects** （我的所有受管对象）。
2. 选择相应容器。例如，如果您希望 DRA 搜索用户帐户信息，请选择 **Users** （用户）。
3. 要查看高级搜索窗格，请单击 **Advanced Search** （高级搜索）。
4. 在高级搜索窗格中，从 **Saved Queries** （保存的查询）列表中选择一个高级搜索查询。
5. 单击 **Load Query** （装载查询），然后单击 **Find Now** （立即查找）。

2.2.6 恢复控制台设置

DRA 允许您调整窗口大小，然后保持窗口大小。 DRA 还会保留许多其他设置，包括您连接的最后一个管理服务器、您在列表结果中添加或去除的列以及列宽。如果要将这些设置恢复到安装 DRA 的原始设置，则可以使用 Restore Default Settings （恢复默认设置）选项来执行此操作。

要恢复控制台默认设置：

1. 单击 **View** （查看） > **Options** （选项）。
2. 选择 **Saved Settings** （保存的设置）选项卡。
3. 查看窗口中提供的信息，然后单击 **Restore Default Settings** （恢复默认设置）。

2.2.7 使用特殊字符

命名用户帐户、组、联系人、 OU、计算机、 ActiveView、助理 Admin 组、角色、策略或自动化触发器时，不能使用以下特殊字符。这些命名限制适用于对象的名称以及定义对象的规则的名称。

命名用户帐户、组和计算机

指定 Windows 2000 之前的名称时，不能使用以下特殊字符：

反斜杠	\
冒号	:
逗号	,
双引号	"
等号	=
正斜杠	/
大于号	>
左中括号	[
小于号	<
加号	+
右中括号	]
分号	;
竖线	|

重要：关于公用文件夹管理，不支持反斜杠 \ 字符。

在 Microsoft Windows 域中命名用户帐户、组和计算机时，可以使用任何特殊字符。

命名联系人和 OU

在命名联系人和 OU 时，您可以使用任何特殊字符。

命名 ActiveView、助理 Admin 组和角色

命名 ActiveView、助理 Admin 组和角色时，不能使用反斜杠 (\)。

命名策略和自动化触发器

在命名策略和自动化触发器时，不能使用反斜杠 (\)。

Azure 中的无效字符

无效字符将导致 Azure Active Directory 与本地目录之间的同步失败。请参见 Microsoft Office 支持网站上的 Directory object and attribute preparation （目录对象和属性准备）子主题，以了解有关这些无效字符的更多信息。

要确保联机邮箱属性中未使用这些字符，请执行以下操作：

1. 单击 Delegation and Configuration （委托和配置）控制台中的 Configuration Management （配置管理）节点，然后选择 **Update Administration Server Options** （更新管理服务器选项）。
2. 单击选项卡菜单中的 **Azure Sync** （Azure 同步）。
3. 单击 **Enforce online mailbox policies for invalid characters and character length** （对无效字符和字符长度实施联机邮箱策略），然后单击**确定**。

2.2.8 使用通配符

DRA 支持 DRA 控制台许多字段和命令行界面命令中使用通配符。通配符使您可以定义将多个对象与特定条件或标准匹配的规则，例如命名约定。您可以使用通配符来缩小或扩大规则的范围，而不必使用正则表达式。通配符匹配不区分大小写。您还可以将问号 (?)、星号 (*) 或数字符号 (#) 通配符用作普通字符，方法是在特定通配符前加上反斜杠 (\)。例如，要搜索 abc*，请键入搜索文本 abc*。

DRA 支持以下通配符。名称中不能使用通配符。

匹配项目	字符	定义
任何字符	问号 ?	精确匹配一个字符
任意位数字	数字符号 #	匹配一位数字
任意字符， 0 个或更多匹配	星号 *	匹配 0 个或更多个字符

下表提供了通配符规范以及其匹配和不匹配内容的示例。

示例	匹配	不匹配
Den???	Denton 和 Dennis	Denison
El ????o	El Campo 和 El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA 不支持包含逻辑操作的通配符规范。

2.2.9 查看指派的权限和角色

角色和权限将定义管理对象的方式。角色是一组权限，可提供执行特定管理任务 （例如创建用户帐户或移动共享目录）所需的许可权限。

DRA 管理员可指派角色，将您添加到特定助理 Admin 组，并将您与 ActiveView （您可以管理的域对象集）相关联。您可以通过 Delegation and Configuration （委托和配置）控制台查看这些指派。您无需任何辅助权限即可查看指派给您的角色和权限。

要查看指派的权限和角色：

1. 在 File （文件）菜单上，单击 **DRA Properties** （DRA 属性）。
2. 单击 **Powers** （权限）。
3. 选择相应视图。例如，单击 **Flat View** （平面视图）以查看助理 Admin 组成员资格、指派的权限和角色以及关联的 ActiveView 的表。
4. 展开相应的项目。例如，在 **Has Power** （拥有权限）下，展开 **Roles and Powers** （角色和权限）以查看指派给您的各个角色或权限。
5. 单击 **OK** （确定）。

2.2.10 查看产品版本号和已安装的热修复

您可以从 DRA Properties （DRA 属性）窗口中查看产品版本号和已安装的热修复。此窗口提供管理服务器和 DRA 客户端计算机的版本号和已安装的热修复列表。

要查看产品版本号和已安装的热修复：

1. 在 File （文件）菜单上，单击 **DRA Properties** （DRA 属性）。
2. 单击 **General** （常规）。
3. 查看所需信息。
4. 单击 **OK** （确定）。

2.2.11 查看当前许可证

DRA 需要许可证密钥文件。您可以从任何管理服务器计算机查看您的产品许可证。您无需任何辅助权限即可查看产品许可证。

要查看许可证：

1. 在 File （文件）菜单上，单击 **DRA Properties** （DRA 属性）。
2. 单击 **License** （许可证）。
3. 查看许可证属性，然后单击 **OK** （确定）。

2.2.12 恢复 BitLocker 口令

Microsoft BitLocker 将其恢复口令储存在 Active Directory 中。如果您具有所需的权限，则可以使用 DRA BitLocker 恢复功能查找并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. 启动 Delegation and Configuration （委托和配置）控制台，然后导航到 **Account and Resource Management （帐户和资源管理）** > **我的所有受管对象**。
2. 选择域，然后执行搜索以列出该域中的所有计算机。
3. 在计算机列表中，右键单击所需的计算机，然后选择**属性** > **BitLocker 恢复口令**。
4. 右键单击并复制 BitLocker 恢复口令，然后将口令文本粘贴到文本文件中。

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. 启动 Delegation and Configuration （委托和配置）控制台，然后导航到 **Account and Resource Management （帐户和资源管理）** > **我的所有受管对象**。
2. 右键单击 **Managed Domain** （受管域），然后单击 **Find BitLocker Recovery Password** （查找 BitLocker 恢复口令）。

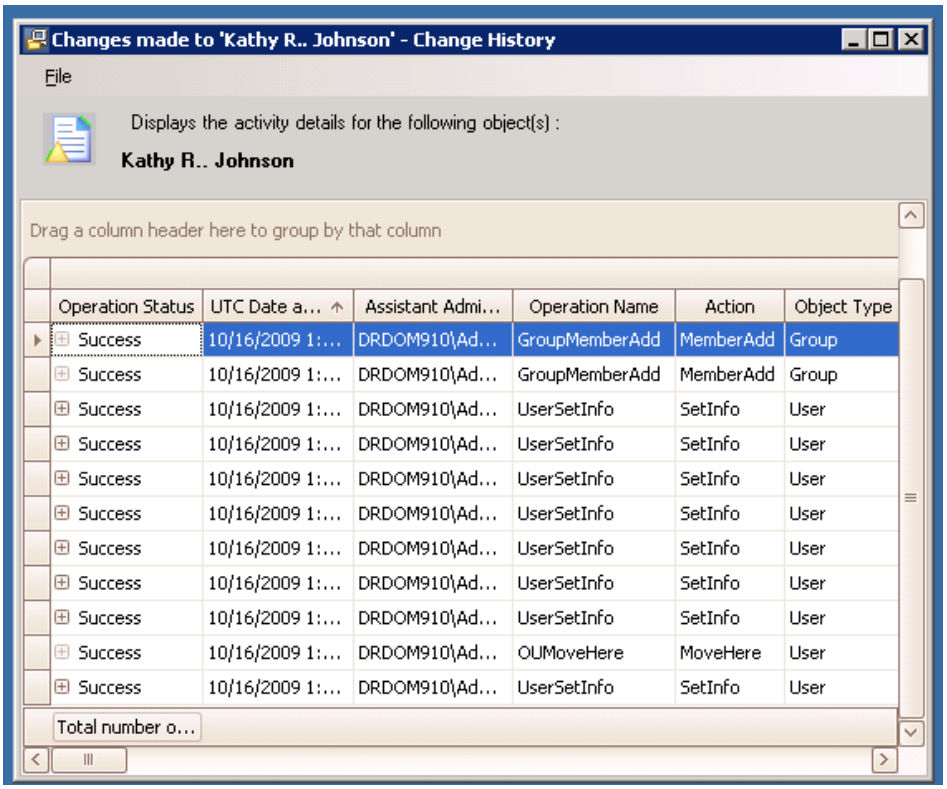
   要查找恢复口令的前八个字符，请参见查看和复制 BitLocker 恢复口令。
3. 在 **Find BitLocker Recovery Password** （查找 BitLocker 恢复口令）页面中，将复制的字符粘贴到搜索字段中，然后单击 **Search** （搜索）。

2.3 DRA Reporting

DRA Reporting 提供内置的即用型报告，可让您快速跟踪重复的帐户、上次帐户登录、Microsoft Exchange 邮箱细节等。报告还提供环境中所做更改的实时细节，包括属性更改前后的值。您可以导出、打印或查看报告，或将报告发布到 SQL Server Reporting Services。

DRA 提供了两种生成报告的方法，使您可以收集和查看域中的用户帐户、组和资源定义，报告有：**活动细节报告**和 **DRA 管理报告**。“活动细节报告”可通过 Delegation and Configuration（委托和配置）控制台进行查看，提供域中对象的实时更改信息。例如，您可以通过 Activity Detail reports （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。

下图显示了 Activity Detail report （活动细节报告）示例：



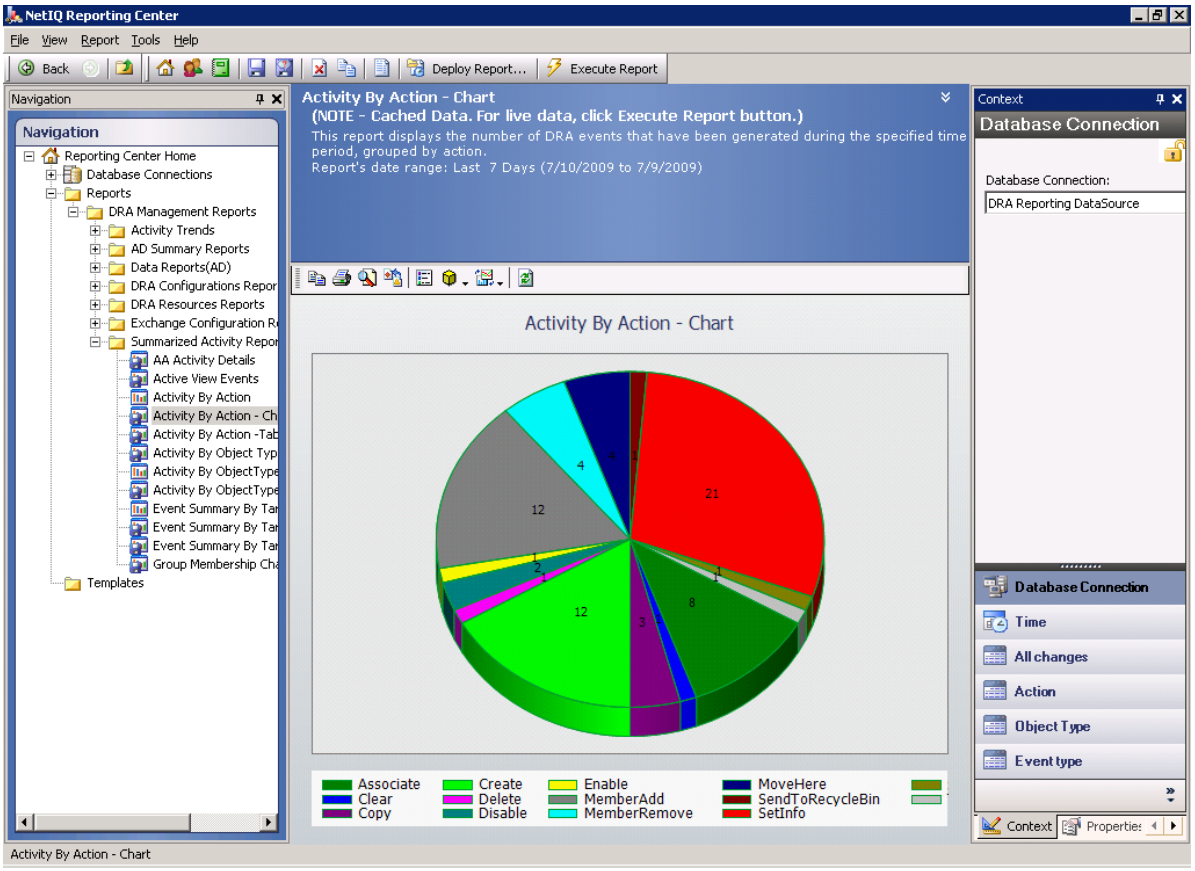
可通过 NetIQ Reporting Center (Reporting Center) 查看的可选 **DRA Management reports** （DRA 管理报告），提供有关受管域中事件的活动、配置和摘要信息。部分管理报告以数据的图形表示形式呈现。还可以自定义这些内置报告，以便为您准确提供所需的信息。

例如，您可以使用“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，您可以查看有关 DRA 安全模型的细节，例如 ActiveView 和助理 Admin 组定义。

您必须先安装并配置可选的管理报告，然后才能查看这些报告。有关安装报告组件的更多信息，请参见 *《安装指南》*。有关 DRA Reporting 的更多信息，请参见 DRA Reporting （第 29 页）。

在 NetIQ > Reporting Center 程序组中启动 Reporting Center 控制台。

下图显示了已选择 DRA Management reports （DRA 管理报告）的 Reporting Center 界面。



要了解有关在 DRA Reporting 的更多信息，请参见以下主题：

- 第 2.3.1 节 “ 了解 DRA Reporting”（第 30 页）
- 第 2.3.2 节 “DRA 如何使用日志存档 ”（第 31 页）
- 第 2.3.3 节 “ 了解日期和时间 ”（第 31 页）
- 第 2.3.4 节 “DRA Reporting 任务 ”（第 32 页）

2.3.1 了解 DRA Reporting

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 reports （活动细节报告）

这些报告可通过 Delegation and Configuration （委托和配置）控制台的 Account and Resource Management （帐户和资源管理）节点进行访问，提供域中对象的实时更改信息。

DRA Management reports （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 reports （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 Admin 组定义。

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。

DRA Management reports （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 *《管理员指南》*。

2.3.2 DRA 如何使用日志存档

为了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 reports （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。

有关 DRA 审计的更多信息，请参见 *《管理员指南》*。

2.3.3 了解日期和时间

DRA 使用“控制面板”的“区域设置”应用程序中指定的**短日期样式**和**时间样式**来显示报告。DRA 报告显示 UTC 日期和时间以及事件的本地日期和时间。 DRA 报告支持以下日期格式：

- m/d/yy
- m-d-yy
- m/d/yyyy

- m-d-yyyy
- mm/dd/yy
- mm-dd-yy
- mm/dd/yyyy
- mm-dd-yyyy
- dd/mm/yy
- dd-mm-yy
- dd/mm/yyyy
- dd-mm-yyyy

2.3.4 DRA Reporting 任务

要生成 DRA Management reports （DRA 管理报告），请安装 Reporting Center 并在 DRA 中启用数据收集。有关启用数据收集的更多信息，请参见 *《管理员指南》*。要生成 Activity Detail reports （活动细节报告），请右键单击任何对象，然后单击**报告**以查看针对该对象的报告的选择。以下部分将指导您完成各种报告任务。

查看 Activity Detail Reports （活动细节报告）

Activity Detail reports （活动细节报告）将显示有关环境中更改的信息。您可以查看或打印报告，也可以以 Excel、 CSV 或 TXT 格式保存报告。要查看或打印报告，您必须与 Reporting Administration （报告管理）角色相关联。

查看报告时，请输入准则以指定要显示其信息的时间段。您还可以选择查看仅显示在特定 DRA 服务器上所做更改的报告，并且可以限制要包含在报告中的行数。如果报告大小超过以下限制之一， DRA 将显示一条讯息，指出报告不完整：

- 大小超过 500 MB
- 查询所有 DRA 服务器所需的时间超过 5 分钟
- 要显示的行数超过 1000

您可以选择查看仅包含在达到其中一个限制之前检索到的信息的报告，或者您可以更改报告准则以查看满足这些限制的报告。

要查看报告：

1 在左窗格中，展开 **All My Managed Objects** （我的所有受管对象）。

2 要指定要查看其报告的对象，请完成以下步骤：

2a ***如果知道对象位置***，请选择包含此对象的域和 OU。

2b 在搜索窗格中，指定对象属性，然后单击 **Find Now** （立即查找）。

3 在列表窗格中，右键单击对象，然后单击 **Reporting** （报告）。

4 选择报告类型，例如 **Changes made to objectName** （对 objectName 所作的更改）或 **Changes made by objectName** （objectName 所作的更改）。可用报告因您选择的对象类型而异。

5 选择开始日期和结束日期以指定要查看的更改。

6 ***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。

---

7 ***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。

8 单击 **OK** （确定）。

注释：DRA 最多可能需要 5 秒钟即可在报告中显示最近更改。因此，在尝试查看包含更改的报告之前，请在进行更改后至少等待 5 秒钟。

导出 Activity Detail Reports （活动细节报告）

您可以使用以下格式导出 Activity Detail reports （活动细节报告）：XLS、 CSV 和 TXT。默认为 Microsoft Excel 格式。

要导出 Activity Detail reports （活动细节报告）：

1 在报告窗口的 File （文件）菜单上，单击 **Preview and Export** （预览和导出）。

2 在 Preview （预览）窗口的 File （文件）菜单上，单击 **Export Document** （导出文档） > **Excel File** （Excel 文件）。

3 选择导出选项，然后单击 **OK** （确定）。

4 在 Save as （另存为）窗口中，键入文件的名称，然后单击 **Save** （保存）。

打印 Activity Detail Reports （活动细节报告）

要打印报告，您必须与 Reporting Administration （报告管理）角色相关联。您可以查看或打印 Activity Detail reports （活动细节报告），以及以各种格式保存报告。

要打印 Activity Detail reports （活动细节报告）：

1 在报告窗口的 File （文件）菜单上，单击 **Preview and Export** （预览和导出）。

2 在 Preview （预览）窗口的 File （文件）菜单上，单击 **Print** （打印）。

查看管理报告

您必须安装 DRA Reporting 并配置 DRA 数据收集器，才能在 Reporting Center 中查看管理报告。有关安装 DRA Reporting 和配置 DRA Collector （DRA 收集器）的更多信息，请参见 *《管理员指南》*。

登录到 Reporting Center 时，Web Service 使用 IIS 根据您在安装期间配置 Web Service 的方式验证帐户身份凭证。

要查看管理报告：

1. 登录到运行 Reporting Center Console （Reporting Center 控制台）的计算机。
2. 在 NetIQ > Reporting Center 程序组中启动 **Reporting Center Console** （Reporting Center 控制台）。
3. 在 Logon （登录）对话框中提供所需信息，然后单击 **Logon** （登录）。
4. 在 Navigation （导航）窗格中，展开 **Reports （报告）** > **DRA Management Reports** （DRA 管理报告）。
5. 展开报告类别，直到找到要查看的报告。
6. 单击 Navigation （导航）窗格中的报告名称，报告将装载到中央 Results （结果）窗格，显示超速缓存的数据。
7. ***如果要查看包含最新数据的报告，***请单击 Results （结果）窗格中的 **Execute Report** （执行报告）。

您可以更改默认环境设置以显示不同的报告结果。有关 Reporting Center 中环境设置的更多信息，请参见 *《管理员指南》*。

自定义管理报告

DRA 附带了 60 多个管理报告。通过 Reporting Center，您可以灵活地以多种方式自定义和部署这些报告。有关在 Reporting Center 中自定义和部署管理报告的更多信息，请参见 *《管理员指南》*。

要自定义管理报告：

1. 查看与您要创建的报告类似的报告。有关更多信息，请参见查看管理报告。
2. 通过更改报告属性和环境设置来自定义报告，以显示所需的信息。
3. 单击 **Execute Report** （执行报告）。
4. 在 Report （报告）菜单上，单击 **Save Report As** （将报告另存为）并指定报告标题和位置以保存新报告。
5. 单击 **Save** （保存）。

有关在 Reporting Center 中使用管理报告的更多信息，请参见 *《管理员指南》*。

3 搜索对象

本章包含有关搜索和 LDAP 搜索功能的概念和过程信息。

3.1 搜索

DRA 允许您在本地 Active Directory 域、 Microsoft Exchange 和 Azure 租户中搜索对象。您可以在 Azure 租户中搜索用户和组，在 Active Directory 域中搜索用户、组、联系人、计算机、打印机和 OU 等对象，以及在 Exchange 中搜索会议室邮箱、设备邮箱、共享邮箱和动态分发组等对象。您可以使用搜索过滤器进行更有效的搜索。

注释：要在使用过滤器时准确返回搜索的对象，应在应用过滤器和执行搜索之前对分页进行任何更改。不支持在应用对象类型过滤器时更改 Web 控制台底部的**每页项目**设置。

要访问 Web 控制台中的搜索功能，请导航至**管理** > **搜索**。

3.1.1 使用通配符

DRA 支持问号 (?)、星号 (*) 或数字符号 (#) 等通配符，以最大化搜索结果。通配符匹配不区分大小写。

下表提供了通配符规范以及其匹配和不匹配内容的示例。

字符	匹配项目
问号 ?	任何一个字符或一个数字
数字符号 #	任何一个数字
星号 *	任意数量的字符或数字

3.1.2 多字段搜索

“ 多字段匹配 ” 选项允许您通过单个搜索来搜索多个属性的匹配项。使用 “ 多字段匹配 ” 进行搜索时，您的搜索字符串将与多个属性 （如名称、显示名称、名和姓）进行比较，如果搜索字符串与这些属性中的任何一个匹配，则在搜索结果中返回该对象。

“ 多字段匹配 ” 选项仅支持 “ **开头为** ” 搜索准则。

例如，如果您有两个用户，一个用户的*显示名称*为 “Martin Smith”，另一个用户的用户主体名称为 martha.jones@acme.com，并且如果您使用字符串 "Mart" 执行搜索，则会在搜索结果中返回这两个用户。

下表列出了为每个对象类型搜索的属性：

对象类型	搜索的属性
Azure 组	displayName, mail
Azure 用户	displayName, employeeId, givenName, mail, surname, userPrincipalName
计算机	displayName, name, sAMAccountName
联系人	displayName, employeeId, givenName, mail, mailNickname, name, surname
动态分发组	displayName, mail, mailNickname, name
组	displayName, mail, mailNickname, name, sAMAccountName
组织单元	name
回收站	name, sAMAccountName
用户	displayName, employeeId, givenName, mail, mailNickname, name, sAMAccountName, surname

注释：在为以下列出的 Exchange 对象添加委托或权限时， Delegation and Configuration （委托和配置）控制台中的“对象选择器”搜索不支持多重匹配功能：

- 用户邮箱
- 已启用邮件的用户
- 已启用邮件的组
- 已启用邮件的联系人
- 动态分发组
- 共享邮箱
- 资源邮箱

3.1.3 添加和排序列

单击属性的列标题时，可以按以下任意属性对搜索结果对象进行排序：

- 别名
- 显示名称
- 电子邮件
- 员工 ID
- 名字
- 姓
- 位置
- 名称

- Windows 2000 之前的名称
- 用户主体名称

要添加或去除属性列，请单击列图标。

3.2 高级搜索

通过 DRA，您可以从 “ 高级搜索 ” 页面在本地 Active Directory 域中执行 LDAP 和虚拟属性查询。您可以使用现有查询进行搜索、修改现有查询、创建新查询以及保存新查询和修改后的查询，以备将来用作公共查询或私用查询。使用搜索过滤器进行更有效的搜索。

要访问 Web 控制台中的高级搜索查询功能，请导航至**管理** > **高级搜索**。

3.2.1 高级搜索查询

DRA 支持虚拟属性和 LDAP 查询，以搜索 DRA 和 Active Directory 对象。虚拟属性可以与 Active Directory 对象类型相关联，例如用户、组、动态分发组、联系人、计算机和 OU。使用虚拟属性查询，您可以过滤从 LDAP 查询返回的结果，以便仅返回与虚拟属性查询匹配的结果。虚拟属性查询字符串必须以 (objectCategory=<object type>) 开头。要执行虚拟属性查询，必须同时为 LDAP 和虚拟属性查询指定字符串。

LDAP 查询示例：

- 要在 DRA 中搜索 “ 所有计算机对象 ”：

  LDAP 查询：(objectCategory=computer)
- 要在 DRA 中搜索说明为 "East\West Sales" 的用户对象：

  LDAP 查询：(&(objectCategory=user)(description=East\5CWest Sales))
- 要在 DRA 中搜索 “ 所有计算机对象 ”：

  LDAP 查询：(objectCategory=computer)

  重要：在 LDAP 过滤器中必须对反斜杠字符进行转义。替代 \5C。

- 要在 DRA 中 “ 列出所有禁用的用户对象 ”：

  LDAP 查询：

  (&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))

  字符串 1.2.840.113556.1.4.803 指定 LDAP_MATCHING_RULE_BIT_AND。这指定了标志属性 （一个整数）（例如 userAccountControl、 groupType 或 systemFlags）和位掩码 （例如 2、 32 或 65536）的按位 AND。如果属性值和位掩码的按位 AND 为非零，则该子句为 True，表示该位已设置。

虚拟属性查询示例：

- 要查找公司名称为 ABC 的所有用户：

  查询：(&(objectCategory=User)(CompanyName=ABC))

DRA 对象为 "User"，虚拟属性为 "CompanyName" （与用户关联）。

- 要在存储域中查找公司名称为 ABC 的所有用户：

  查询：(&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))

  DRA 对象为 "User"，虚拟属性为 "CompanyName" 和 "Domain" （与用户关联）。

- 要查找产品名称为 DRA 的所有组或公司名称为 ABC 的所有用户：

  查询：

  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC))
)

  DRA 对象为 "Group" 和 "User"，而虚拟属性为 CompanyName （与用户关联）和 ProductGroupName （与组关联）。

- 要在储存域中查找产品名称为 DRA 的所有组或公司名称为 ABC 的所有用户：

  查询：

  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC)(
  Domain=Storage)))

  DRA 对象为 "Group" 和 "User"，而虚拟属性为 CompanyName （与用户关联）、ProductGroupName （与组关联）和 Domain （与用户关联）。

3.2.2 管理高级查询

DRA 使用 LDAP 来支持高级搜索查询功能。使用高级查询，您可以搜索用户、联系人、组、计算机、 OU 以及 DRA 支持的任何其他对象。如果您具有 “ 执行保存的高级查询 ” 权限，则可以对所有容器执行**我的搜索**和**公共搜索**列表中可用的高级查询。

除了使用保存的高级查询执行搜索并查看其细节外，在具有相应的权限时，您还可以通过 “ 高级搜索 ” 页面中的高级查询执行以下操作：

创建新查询

通过为新高级查询提供查询字符串 （LDAP 和虚拟属性，如果适用），在主管理服务器或次管理服务器上创建高级查询。执行搜索后，展开**搜索**下拉菜单以将查询保存到 “ 我的搜索 ” 列表或 “ 公共搜索 ” 列表中。

修改查询

在 “ 我的搜索 ” 或 “ 公共搜索 ” 下选择现有高级查询，然后使用**修改**选项来更改任何搜索准则。使用更新的搜索准则执行搜索后，如果需要，可以展开**搜索**下拉菜单，然后选择**保存**以保存对该查询的更改。

复制查询

在 “ 我的搜索 ” 或 “ 公共搜索 ” 下选择现有高级查询，然后执行搜索。执行搜索后，可以展开**搜索**下拉菜单，然后选择**另存为**以使用其他名称保存查询。

自定义查询结果

DRA 可在搜索结果列表中为您提供一组默认列。要自定义已保存或未保存查询的搜索结果，请单击页面右侧的**添加 / 去除列**图标 以更改搜索结果的显示方式。

删除查询

可以删除**我的搜索**列表中的任何高级查询。拥有适用的权限时，还可以删除**公共搜索**列表中的高级查询。要删除已保存的高级查询，请在适用的列表中将其选中，然后在“搜索”下拉菜单中单击**删除**。

清除查询

在 Web 控制台中，可以清除已保存或未保存查询的表单字段，以从干净表单中进行更改。要清除查询中的字段，请在“搜索”下拉菜单中选择**清除**。

4 管理用户帐户、组和联系人

本章包含在 Delegation and Configuration （委托和配置）控制台的 Account and Resource Management （帐户和资源管理）节点以及 Web 控制台中管理用户帐户、组、动态组、动态分发组和联系人的概念和过程信息。用户帐户的信息更全面，提供了在两个客户端应用程序中如何管理对象的示例。

4.1 管理用户帐户

Microsoft Windows 依赖于用户帐户类型来确定关联用户帐户的访问许可权限。用户帐户可以是全局帐户或本地帐户。DRA 还支持 InetOrgPerson 对象，但会将 InetOrgPerson 对象识别为普通用户。

全局用户帐户

可以在信任创建用户帐户的域的任何域中使用的用户帐户。您可以向用户帐户授予特定许可权限。您还可以将用户帐户设为组的成员，然后为该组指派许可权限。对用户帐户进行分组有助于简化管理许多用户帐户的网络许可权限的过程。

本地用户帐户

本地用户帐户与用于登录 Windows 操作系统的任何帐户相同。允许您在自己的用户空间中访问系统资源。

要了解有关管理用户帐户的更多信息，请参见以下主题：

- 第 4.1.1 节 “ 受信任域中的用户帐户 ”（第 41 页）
- 第 4.1.2 节 “ 用户帐户管理任务 ”（第 42 页）
- 第 4.1.3 节 “ 转换用户帐户 ”（第 44 页）

4.1.1 受信任域中的用户帐户

Microsoft Windows 将用户帐户和组定义储存在受管域的目录中。因此，管理服务器无法修改受信任域中的目录信息，除非该域也由 DRA 管理。

例如，在 Account and Resource Management （帐户和资源管理）中，您可能会看到无法修改的用户帐户和组。这些用户帐户和组在任一个受管域信任的域中定义。但是，您可以将受信任域中的帐户和组添加到受管域中的其他组。

4.1.2 用户帐户管理任务

本节将指导您在 Delegation and Configuration （委托和配置）控制台的 Account and Resource Management （帐户和资源管理）节点以及 Web 控制台中管理用户帐户。通过相应的权限，您可以执行各种用户帐户管理任务，例如创建和删除帐户。如果选择多个用户帐户，则可以在一个操作中执行所选任务，例如删除、移动用户或向组添加用户。有关指派的权限的更多信息，请参见查看指派的权限和角色。

Account and Resource Management （帐户和资源管理）中的用户帐户任务

您可以从 **Tasks** （任务）菜单或右键单击菜单执行以下所有适用的任务。通常，您会选择 **All My Managed Objects** （我的所有受管对象）节点，然后执行 **Find Now** （立即查找）操作以查找并选择所需的用户对象。在创建新用户的情况下，您必须选择要在其中创建用户的域或 OU。 Tasks （任务）菜单指示在选择单个或多个用户帐户时可以执行的任务。

管理您自己的帐户

您可以通过修改常规属性 （例如电话号码）来管理自己的帐户。在管理帐户之前，请确保您拥有相应的权限。

将用户帐户复制到另一个 ActiveView

您可以将用户帐户复制到另一个 ActiveView。此操作称为转移用户帐户。要将用户帐户复制到另一个 ActiveView，您需要在源 ActiveView 和目标 ActiveView 中拥有 “ 将用户复制到另一个 ActiveView” 的权限。将用户帐户转移到另一个 ActiveView 不会从源 ActiveView 中去除该用户帐户。

注释：只能从 Delegation and Configuration （委托和配置）控制台通过 Account and Resource Management （帐户和资源管理）节点将用户帐户复制到另一个 ActiveView。

重命名用户帐户

您可以重命名受管域或受管子树中的用户帐户。更改用户登录名也会更改与用户帐户关联的邮箱的名称。

Web 控制台中的用户帐户任务

您可以从 Web 控制台的**管理** > **搜索**选项卡执行以下大多数任务。执行搜索操作以查找并选择所需的用户对象。在列表中选择一个或多个对象后，任务栏将变为活动状态，其中包含创建、帐户和交换等选项。单击这些选项以显示其功能。

创建用户帐户

您可以在受管域或受管子树中创建用户帐户。您还可以修改属性、创建邮箱、启用电子邮件以及为新帐户指定组成员资格。

注释：

- 您的公司可能具有通过策略强制执行的命名约定，该约定将确定您可以指派给新用户帐户的名称。
- 默认情况下， DRA 会将新用户帐户放在受管域的用户 OU 中。
- 您无法在 DRA 中创建 InetOrgPerson 对象。

克隆用户帐户

克隆用户帐户时，该用户所属的任何组都将自动添加到新用户帐户，从而节省您配置新帐户的时间。您可以添加或去除新帐户中的组、启用电子邮件以及进行任何其他属性配置，如同您使用任何新帐户一样。

注释：克隆 InetOrgPerson 对象时，您将创建一个用户帐户。

修改用户帐户属性

您可以管理受管域或受管子树中的用户帐户的属性。您拥有的权限决定了您可以为用户帐户修改的属性。如果已安装 Exchange 并已启用 Microsoft Exchange 支持，则可以在管理用户帐户时修改关联的邮箱属性。

注释：如果已启用用户主目录策略，则 DRA 会在您管理该帐户时自动修改用户帐户的用户主目录。例如，更改用户主目录位置时， 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。 DRA 还会将从先前目录中指派的 ACL 应用于新目录。

启用用户帐户

您可以启用受管域或受管子树中的用户帐户。如果您在管理 Microsoft Windows 帐户，则可以指定 DRA 应用此更改的域控制器。

将此更改应用于特定域控制器时， DRA 还会将此更改应用于此受管域的默认域控制器。要校验 DRA 正在使用的默认域控制器，请查看域属性。

禁用用户帐户

您可以禁用受管域中的用户帐户。如果您在管理 Microsoft Windows 帐户，则可以指定 DRA 应用此更改的域控制器。

将此更改应用于特定域控制器时， DRA 还会将此更改应用于此受管域的默认域控制器。要校验 DRA 正在使用的默认域控制器，请查看域属性。

解除锁定用户帐户

您可以解除锁定受管域或受管子树中的用户帐户。

由于 DRA 从帐户超速缓存中检索用户帐户状态，因此所选帐户实际锁定时，用户界面可能仍指示为已解除锁定。即使帐户状态指示当前已解除锁定， DRA 也允许您解除锁定用户帐户。您还可以在使用 DRA 控制台解除锁定用户帐户时指定域控制器，而无需重设置用户帐户口令。

重设置用户帐户口令

您可以重设置受管域或受管子树中帐户的口令。您拥有的权限决定了您可以为该用户帐户更改的字段。

重设置用户帐户的口令后， DRA 会自动解除锁定该帐户。您可以选择 DRA 是否为用户帐户生成新口令。您还可以修改该帐户的多个与口令相关的选项。如果您在管理 Microsoft Windows 帐户，则可以指定 DRA 应用这些更改的域控制器。

注释：将此更改应用于特定域控制器时， DRA 还会将此更改应用于此受管域的默认域控制器。要校验 DRA 正在使用的默认域控制器，请查看域属性。

将用户帐户移动到另一个容器

您可以将用户帐户移动到受管域或受管子树中的另一个容器，例如 OU。

删除用户帐户

您可以删除受管域或受管子树中的用户帐户。如果为该域禁用了回收站，则删除用户帐户将从 Active Directory 中永久去除该用户帐户。如果为该域启用了回收站，则删除用户帐户会将该用户帐户移动到回收站。

警告：创建用户帐户时， Microsoft Windows 会为该帐户指派安全标识符 (SID)。不会从帐户名称生成 SID。 Microsoft Windows 在访问控制列表 (ACL) 中使用 SID 记录每个资源的特权。如果删除用户帐户，则无法通过创建具有相同名称的新用户帐户来恢复该帐户的访问权限。

指定用户帐户的组成员资格

您可以在受管域或受管子树的特定组中添加或去除用户帐户。您还可以查看或修改此帐户所属的现有组的属性。

4.1.3 转换用户帐户

DRA 使您能够快速有效地转换用户帐户。当与用户帐户关联的个人转换为新的工作职责时，您可以使用 DRA 的转换功能。利用工作角色模板，您可以快速添加、去除或更新与帐户关联的组成员资格。无论是个人晋升、更换部门还是离开公司，转换用户帐户的功能都将为您省去时间和金钱成本。

了解转换过程

您可以使用转换用户帐户功能来满足以下任何需求：

- 从用户帐户中去除组成员资格
- 将组成员资格添加到用户帐户
- 更改用户属性
- 将其他组成员资格添加到用户帐户时，去除特定的组成员资格

尝试转换用户帐户之前，请考虑以下过程：

1. 确定是否需要添加、去除或同时添加和去除组成员资格。
2. 查看当前的减性和加性模板，以确保您拥有必要的模板用户帐户。
3. 如有必要，请创建任何所需的模板帐户。
4. 完成 Transform user （转换用户）向导。

当 DRA 转换用户时，减性模板指定的组成员资格将从用户帐户中去除，而加性模板指定的成员资格将指派给用户帐户。 DRA 不会对减性或加性模板之外的任何成员资格执行任何操作。例如，外部销售部门的某个人从美国销售部转移到欧洲销售部。在您的组织内，您拥有这些销售团队独有的分发组和安全组，以及所有销售团队共享的编号。美国销售团队拥有美国热点分发列表和美国销售管理分发列表分发组，而欧洲销售团队则拥有欧洲热点和欧洲销售管理分发组。两个团队都是“全球销售安全”安全组的成员，但也有单个特定于站点的安全组。

您的减性模板 （名为“美国销售模板”）将获指派以下组成员资格：

- 美国热点分发列表
- 美国销售管理分发列表
- 全球销售安全
- 美国安全

您的加性模板 （名为“欧洲销售模板”）将获指派以下组成员资格：

- 欧洲热点分发列表
- 欧洲销售管理分发列表
- 全球销售安全
- 欧洲安全

在转换过程中，转移销售人员的用户帐户首先从美国销售模板指定的所有组成员资格中去除，然后添加到欧洲销售模板指定的所有组成员资格。如果此人也是扑克玩家分发组的成员，则此组成员资格保持不变。

以下权限允许助理管理员在转换过程中进一步修改用户帐户：

- 在转换用户帐户时修改地址属性
- 在转换用户帐户时修改说明
- 在转换用户帐户时修改办公室
- 在转换用户帐户时修改电话属性

您还可以通过仅向助理管理员授予以下任意权限来限制添加或去除组成员资格的能力：

- 将用户添加到模板中的组
- 从模板中的组中去除用户

您可以使用上述任何一个基于权限的限制选项在组织内创建一个安全性层。通过为某些个人提供仅去除模板中的组的权限，您可以创建临时用户帐户。然后，可以在其他助理管理员使用加性模板帐户授予新的组成员资格之前，查看这些临时帐户。

创建用户转换模板

用户帐户的转换直接与组织的角色和工作阶梯相关。考虑为公司内的每个角色或工作创建一个模板。 DRA 并不区分用作减性和加性的用户帐户模板。为组织中的每个角色创建单个模板用户帐户。在转换过程中，您可以选择模板是加性还是减性。选择模板为减性不会阻止相同的模板在将来的转换中呈现加性。

要创建用户转换模板，您必须具有创建用户帐户，并将该用户帐户指派给相应组的权限。通过将您的帐户与相应 ActiveView 中的“创建和删除用户帐户”以及“组管理”角色相关联，或通过指派各个权限，可以获得这些权限。

转换用户帐户

通过转换用户帐户，您可以添加、去除或同时添加和去除用户帐户组成员资格。当个人在组织内从一项工作职责转移到另一项工作职责时，使用此工作流程可对您有所帮助。您必须具有“转换用户”角色或包含转换用户帐户的相应权限的角色。只能在 Delegation and Configuration （委托和配置）控制台中通过 Account and Resource Management （帐户和资源管理）节点执行此功能。

要转换用户帐户：

1. 在左窗格中，展开 **All My Managed Objects** （我的所有受管对象）。
2. 要指定要管理的用户帐户，请执行 **Find Now** （立即查找）操作以查找并选择用户对象。
3. 单击 **Tasks** （任务） > **Transform** （转换）。
4. 查看 Welcome （欢迎）窗口，然后单击 **Next** （下一步）。
5. 在 Select User Template （选择用户模板）窗口中，使用 **Browse** （浏览）选择相应的减性模板用户。
6. 如果要查看减性模板用户帐户的属性，请单击 **View** （查看）。
7. 使用 **Browse** （浏览）选择相应的加性模板用户。
8. 如果要查看加性模板用户帐户的属性，请单击 **View** （查看）。
9. 如果您具有相应权限，则可以选中 **Change other properties of the user** （更改用户的其他属性），然后选择要修改的属性。单击 **Next** （下一步）以浏览可用的属性。
10. 单击 **Next** （下一步）。
11. 查看 Summary （摘要）窗口，然后单击 **Finish** （完成）。

4.2 管理组

作为助理管理员，您可以使用 DRA 管理组和修改组属性。通过组，您可以为定义的一组用户帐户授予特定许可权限。组可让您控制用户帐户可以在任何域中访问的数据和资源。

您可以管理任何类型和范围的组。例如，您可以嵌套组，从而允许一个组可以继承另一个组的许可权限。您还可以通过将受信任域中的组添加到受管域中的其他组，以及管理 Temporary Group Assignments （临时组指派）来有效控制跨域的组成员资格。

要了解有关管理组的更多信息，请参见以下主题：

- 第 4.2.1 节“组管理任务”（第 47 页）
- 第 4.2.2 节“在 Delegation and Configuration （委托和配置）控制台中管理临时组指派”（第 49 页）
- 第 4.2.3 节“在 Web 控制台中管理临时组指派”（第 49 页）

4.2.1 组管理任务

本节将指导您在 Delegation and Configuration （委托和配置）控制台中通过 Account and Resource Management （帐户和资源管理）节点管理组。通过相应的权限，您可以执行各种组管理任务，例如修改组成员资格。如果选择多个组，则可以在一个操作中执行所选任务，例如删除、移动或向组添加成员。 Tasks （任务）菜单指示在选择单个或多个组时可以执行的任务。

将帐户添加到组

您可以将用户帐户、联系人和计算机添加到受管组。

注释：此任务会将多个帐户添加到所选组。您可以通过选择相应的帐户，然后单击 Tasks （任务）菜单上的 Add to groups （添加到组），将单个帐户添加到组中。

如果将帐户添加到其他组会提高您对该帐户的权限，则 DRA 不允许您添加该帐户。

将组添加到其他组

您可以通过将组添加到另一个受管组来嵌套组。当组嵌套在另一个组中时，子组可以从父组继承许可权限

注释：如果将组添加到其他组会提高您对源组的权限，则 DRA 不允许您添加该组。

修改组属性

您可以修改本地组和全局组的属性。您拥有的权限决定了您可以为受管域或受管子树中的组修改的属性。如果已安装 Exchange 并已启用 Microsoft Exchange 支持，则可以在管理组时修改通讯组列表属性。

创建组

您可以在受管域或受管子树中创建组。您还可以修改新组的属性，例如组成员。

注释：

- 您的公司可能具有通过策略强制执行的命名约定，该约定将确定您可以指派给新组的名称。
- 默认情况下， DRA 会将新组放在受管域的用户 OU 中。

指定组成员

您可以在受管组中添加或去除用户帐户、联系人、计算机或其他组。 DRA 允许您仅去除外部安全主体。您还可以查看或修改现有组成员的属性，但外部安全主体除外。

从组中去除成员时， DRA 不会删除对象。向组中添加成员时，您必须具有能够修改要添加的对象的权限。

注释：除非您是 Windows 管理员或该特定特殊组的成员，否则无法将用户帐户或组添加到任何 Windows 特殊组 （管理员、帐户操作员、备份操作员或服务器操作员）。

指定组的组成员资格

您可以在受管域或受管子树的其他组中添加或去除组。您还可以查看或修改此组所属的现有组的属性。

配置组成员资格安全许可权限

您可以为组成员资格设置 Active Directory 安全许可权限。这些许可权限指定可以使用 Microsoft Outlook 查看 （读取）和修改 （写入）组成员资格的用户。通过这些设置，您可以更有效地保护环境中的分发列表和安全组。您无法修改继承的安全许可权限。

注释：管理组成员资格安全性时，禁用的许可权限可能表示继承的许可权限。

配置组所有权

您可以设置任何 Microsoft Windows 分发或安全组的所有权。您可以将组所有权许可权限授予用户帐户、组或联系人。授予组所有权允许指定的用户帐户、组或联系人修改此组的成员资格。

注释：当从 Microsoft Exchange 服务器隐藏组成员资格时， DRA 会禁用 **Manager can update membership list** （管理员可以更新成员资格列表）复选框。要启用此复选框，请单击 Group Properties （组属性）窗口的 "Exchange" 选项卡上的 **Expose Group Membership** （公开组成员资格）。

克隆组

您可以克隆受管域中的本地组和全局组。克隆组会创建类型和属性与原始组相同的新组。 DRA 还会尝试将原始组中的所有成员添加到新组。

通过克隆组，您可以基于具有类似属性的其他组快速创建组。克隆组时， DRA 会使用所选组中的值填充 Clone Group Wizard （克隆组向导）。您还可以修改新组的属性。

注释：

- 您的公司可能具有通过策略强制执行的命名约定，该约定将确定您可以指派给新组的名称。
- 默认情况下， DRA 会将新组放在受管域的用户 OU 中。

删除组

您可以删除受管域或受管子树中的本地组和全局组。如果为该域禁用了回收站，则删除组将从 Active Directory 中永久去除该组。如果为该域启用了回收站，则删除组会将该组移动到回收站并禁用组属性。

有关回收站的更多信息，请参见管理回收站。

警告：创建组时， Microsoft Windows 会为该组指派安全标识符 (SID)。不会从组名称生成 SID。 Microsoft Windows 在访问控制列表 (ACL) 中使用 SID 记录每个资源的特权。如果删除组，则无法通过创建具有相同名称的新组来恢复该组的访问权限。

将组移动到另一个容器

您可以将组移动到受管域或受管子树中的另一个容器，例如 OU。

在分发列表中公开组成员资格

您可以在受管域或受管子树的组分发列表中公开组成员资格。

在分发列表中隐藏组成员资格

您可以在受管域或受管子树的组分发列表中隐藏组成员资格。

4.2.2 在 Delegation and Configuration （委托和配置）控制台中管理临时组指派

通过“临时组指派”，您可以管理仅在特定时间段内需要组成员资格的用户的组成员资格。本节将指导您在 Delegation and Configuration （委托和配置）控制台的 **Account and Resource Management** （帐户和资源管理）下管理临时组指派。通过相应的权限，您可以执行各种任务，例如创建临时组指派或去除失效的临时组指派。

助理管理员只能查看助理管理员有权添加或去除成员的组的临时组指派。

在临时组指派处于“活动”状态时，无法更改关联的组或修改用户列表。如果要修改这些项目，则必须取消临时组指派。

管理临时组指派属性

您可以管理临时组指派或已保存的失效临时组指派的属性。

如果要重安排临时组指派，请在指派的**属性**中更改日程表，然后保存更改。

创建临时组指派

您可以在主管理服务器和次管理服务器上创建临时组指派。

默认情况下，当临时组指派失效时，除非已选择**保留此临时组指派以供将来使用**选项，否则它将在 7 天后删除。要更改此保留期限，请右键单击“我的所有受管对象”下的**临时组指派**节点，选择**属性**，然后修改要保留临时组指派的天数。

管理临时组指派中的用户帐户

您可以在主管理服务器和次管理服务器上的临时组指派中添加或去除用户帐户。

注释：您只能管理尚未处于活动状态的临时组指派的用户帐户。

删除临时组指派

您可以删除主管理服务器和次管理服务器上的任何临时组指派。

4.2.3 在 Web 控制台中管理临时组指派

通过“临时组指派”，您可以管理在特定时间段内需要组成员资格的用户的组成员资格。在 Web 控制台中，可以从 DRA 主服务器和次服务器创建和管理指派。但是，可以对现有指派执行的操作因指派所处的状态而异。

助理管理员只能查看其有权通过其 ActiveView 指派进行修改的组的临时组指派，例如添加或去除该组的成员。

要在 Web 控制台中管理临时组指派，请导航至**任务** > **临时组指派**。

可以执行以下操作：

搜索现有指派

当您搜索现有的临时组指派 (TGA) 时，它们会根据指派的状态在结果中列出，其中可能包括以下状态：

- **待发：**TGA 已安排在未来启动。您可以执行取消、删除和重安排操作。
- **活动：**TGA 已启动并向组中添加了适用的成员。您可以执行取消和删除操作。
- **已激活，出错：**TGA 已启动，但未能将所有适用的成员添加到组中。您可以执行取消和删除操作。
- **已完成：**TGA 已失效，并从组中去除了所有适用的成员。您可以执行删除和重安排操作。
- **已完成，出错：**TGA 已失效，但未能从组中去除所有适用的成员。您可以执行删除和重安排操作。
- **已取消：**TGA 已由用户取消，并从组中去除了所有适用的成员。您可以执行删除和重安排操作。
- **已取消，出错：**TGA 已由用户取消，但未能从组中去除所有适用的成员。您可以执行删除和重安排操作。
- **错误：**TGA 未能添加或去除所有成员。您可以执行删除和重安排操作。

可以根据这些状态和其他准则 （包括指派名称、目标组、持续时间和创建指派的管理员）过滤结果。

创建临时组指派

您可以使用有权修改并指定域控制器的组来创建临时组指派。当临时组指派失效时，DRA 会在 7 天后自动将其删除，除非选择了保留临时组指派以供将来使用的选项。

查看或修改临时组指派属性

您可以查看或修改在创建临时组指派时定义的任何临时组指派。搜索临时组指派后，选择要查看或修改其属性的指派。

如果要重安排临时组指派，请在指派的**属性**中更改日程表，然后保存更改。如果指派处于“ 活动 ”状态，则只能更改结束日期。

重要：在临时组指派处于“ 活动 ”状态时，无法更改关联的组或修改用户列表。如果要修改这些项目，则必须先取消该指派。

取消临时组指派

仅当临时组指派处于以下状态之一时，才可以取消它：

- 活动
- 已激活，出错
- 待发

删除临时组指派

可以选择多个临时组指派并将其删除。如果所选的临时组指派处于“ 活动 ”、“ 已激活，出错 ”或“ 待发 ”状态，则还将启用**取消**选项。

4.3 管理动态分发组

动态分发组是启用邮件的 Active Directory 组对象，您可以创建该对象以加快大量发送电子邮件讯息和其他信息。

每次将讯息发送到组时，都会根据您定义的过滤器和条件计算动态分发组的成员资格列表。这与常规分发组不同，常规分发组包含一组定义的成员。将电子邮件讯息发送到动态分发组时，会将其递送给组织中与该组定义的准则匹配的所有收件人。

DRA 支持以下功能：

- 审计和用户界面报告
- 动态分发组的枚举支持
- 动态分发组的 NetIQ Reporting Center (NRC) 报告
- 动态分发组的触发器操作支持
- Exchange 动态通讯组的用户界面扩展支持

动态分发组任务：

创建动态分发组

您可以在受管域或受管子树中创建动态分发组。您还可以修改新动态分发组的属性，例如组成员。

注释：

- 您的公司可能具有通过策略强制执行的命名约定，该约定将确定您可以指派给新动态分发组的名称。
- 默认情况下， DRA 会将新动态分发组放在受管域的用户 OU 中。

克隆动态分发组

您可以克隆受管域中的本地动态分发组和全局动态分发组。克隆动态分发组会创建类型和属性与原始动态分发组相同的新动态分发组。

通过克隆动态分发组，您可以基于具有类似属性的其他动态分发组快速创建动态分发组。克隆动态分发组时， DRA 会使用所选动态分发组中的值填充 “ 克隆动态分发组向导 ”。您还可以修改新动态分发组的属性。

将动态分发组移动到另一个容器

您可以将动态分发组移动到受管域或受管子树中的另一个容器，例如 OU。

删除动态分发组

您可以删除受管域或受管子树中的本地动态分发组和全局动态分发组。如果为该域禁用了回收站，则删除动态分发组将从 Active Directory 中永久去除该动态分发组。如果为该域启用了回收站，则删除动态分发组会将其移动到回收站并禁用该动态分发组的属性。

有关回收站的更多信息，请参见管理回收站。

警告：创建动态分发组时， Microsoft Windows 会为该动态分发组指派安全标识符 (SID)。不会从动态分发组名称生成 SID。 Microsoft Windows 在访问控制列表 (ACL) 中使用 SID 记录每个资源的特权。如果删除动态分发组，则无法通过创建具有相同名称的新动态分发组来恢复该动态分发组的访问权限。

修改动态分发组属性

您可以修改本地动态分发组和全局动态分发组的属性。您拥有的权限决定了您可以为受管域或受管子树中的组修改的属性。

指定过滤器

动态分发列表的成员资格由其过滤器确定，而您可以定义该过滤器。

指定条件

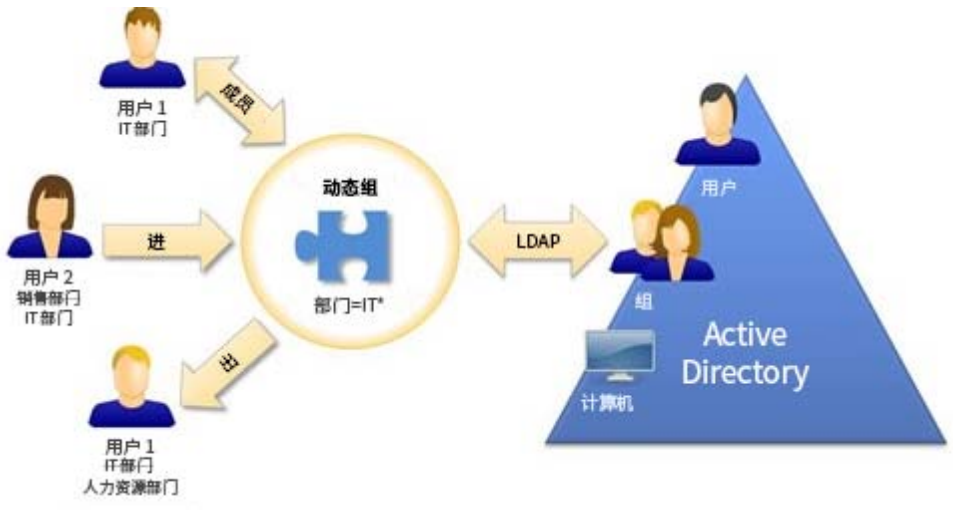
条件将定义对象要成为动态分发组的成员所必须满足的准则。

4.4 管理动态组

动态组的成员资格会根据一组定义的准则进行更改。在 DRA 中，可以在没有 Exchange 环境的情况下创建动态组。用于管理 Active Directory 中动态组的成员资格过滤器是 DRA 独有的。

下图描述了 Active Directory 动态组的典型用法。图中有三个动态组。每个组都有一组准则，用于确定可以添加到组中和不能添加到组中的用户。每个组控制对一组特定文件、文件夹和应用程序的访问权限。

提示：您可以创建包含动态组永久成员的*静态成员列表*；您还可以创建一个*排除的成员列表*，用于拒绝动态组中的用户成员资格。



User2 最近加入了 IT 部门。更新 IT 部门的动态组时，她将被添加到组中。更新销售部门的动态组时， User2 将从其成员列表中去除。

提示：通过右键单击动态组的成员列表并选择 **Update Members** （更新成员）即可进行刷新。

User3 已离开 IT 部门转到 HR 部门，将从 IT 部门动态组中去除，并添加到 HR 部门动态组。

创建动态组

您可以在受管域或受管子树中创建动态组。您还可以修改新动态组的属性，例如组成员。

注释：

- 您的公司可能具有通过策略强制执行的命名约定，该约定将确定您可以指派给新动态组的名称。
- 默认情况下， DRA 会将新动态组放在受管域的用户 OU 中。

创建过滤器

在每次刷新组时，动态组使用过滤器在其成员资格列表中添加或去除用户。

管理静态成员列表

放置在动态组的静态成员列表中的用户将成为该组的永久成员，直到您手动去除这些用户。

从动态组中去除成员时， DRA 不会删除对象。向动态组中添加成员时，您必须具有能够修改要添加的对象的权限。

管理排除的成员列表

放置在动态组的排除成员列表中的用户在您从此列表中手动去除之前，将不允许加入该组。

刷新成员列表

您可以通过更新成员操作刷新动态组中的成员。

克隆动态组

您可以克隆受管域中的本地动态组和全局动态组。克隆动态组会创建类型和属性与原始动态组相同的新动态组。

通过克隆动态组，您可以基于具有类似属性的其他动态组快速创建动态组。克隆动态组时， DRA 会使用所选动态组中的值填充 “ 克隆动态组向导 ”。您还可以修改新动态组的属性。

将动态组移动到另一个容器

您可以将动态组移动到受管域或受管子树中的另一个容器，例如 OU。

删除动态组

您可以删除受管域或受管子树中的本地动态组和全局动态组。如果为该域禁用了回收站，则删除动态组将从 Active Directory 中永久去除该动态组。如果为该域启用了回收站，则删除动态组会将其移动到回收站并禁用该动态组的属性。

有关回收站的更多信息，请参见管理回收站。

警告：创建动态组时， Microsoft Windows 会为该动态组指派安全标识符 (SID)。不会从动态组名称生成 SID。 Microsoft Windows 在访问控制列表 (ACL) 中使用 SID 记录每个资源的特权。如果删除动态组，则无法通过创建具有相同名称的新动态组来恢复该动态组的访问权限。

修改动态组属性

您可以修改本地动态组和全局动态组的属性。您拥有的权限决定了您可以为受管域或受管子树中的组修改的属性。

将动态组添加到其他动态组

您可以通过将动态组添加到另一个受管动态组来嵌套动态组。当动态组嵌套在另一个动态组中时，子动态组可以从父动态组继承许可权限。

注释：如果将动态组添加到其他动态组会提高您对源动态组的权限，则 DRA 不允许您添加该动态组。

配置组成员资格安全许可权限

您可以为动态组成员资格设置 Active Directory 安全许可权限。这些许可权限指定可以使用 Microsoft Outlook 查看 （读取）和修改 （写入）动态组成员资格的用户。通过这些设置，您可以更有效地保护环境中的分发列表和安全动态组。您无法修改继承的安全许可权限。

注释：管理动态组成员资格安全性时，禁用的许可权限可能表示继承的许可权限。

配置动态组所有权

您可以将动态组所有权许可权限授予用户帐户、组或联系人。授予动态组所有权允许指定的用户帐户、组或联系人修改此动态组的成员资格。

在分发列表中公开动态组成员资格

您可以在受管域或受管子树的组分发列表中公开动态组成员资格。

在分发列表中隐藏动态组成员资格

您可以在受管域或受管子树的组分发列表中隐藏动态组成员资格。

注释：Microsoft Exchange 2007 通讯组列表禁用隐藏组成员资格选项。

4.5 管理联系人

DRA 可让您管理许多网络对象，包括联系人和关联的电子邮件地址。联系人仅在混合模式或本机 Microsoft Windows 域中可用。联系人没有安全标识符 (SID)，用户帐户和组也没有。使用联系人将成员添加到分发列表或组，而不授予他们访问网络服务的权限。

您可以将联系人添加到混合和本机模式域中的安全组或分发组。由于安全组可用作 Microsoft Windows 中的分发列表，因此您可能希望向这些组添加联系人。迁移到 Microsoft Windows 本机模式域时，在全局安全组中拥有联系人并不会阻止该组转换为通用安全组。

修改联系人属性

您可以修改联系人属性。您拥有的权限决定了您可以为受管域中的联系人修改的属性。如果已安装 Exchange 并已启用 Exchange 支持，则可以在管理联系人时修改电子邮件地址属性。

创建联系人

您可以在受管域或受管子树中创建联系人。您还可以修改属性、启用电子邮件和指定电子邮件地址，以及为新联系人指定组成员资格。

克隆联系人

通过克隆联系人，您可以基于具有类似属性的其他联系人快速创建联系人。克隆联系人时， DRA 会使用所选联系人中的值填充 “ 克隆联系人向导 ”。您还可以修改属性、启用电子邮件和指定电子邮件地址，以及为新联系人指定组成员资格。

管理联系人的组成员资格

您可以在受管域或受管子树的特定组中添加或去除联系人。您还可以查看或修改此联系人所属的现有组的属性。

将联系人移动到另一个 OU

您可以将联系人移动到受管域或受管子树中的另一个容器，例如 OU。

删除联系人

您可以删除受管域或受管子树中的联系人。如果为该域禁用了回收站，则删除联系人将从 Active Directory 中永久去除该联系人。如果为该域启用了回收站，则删除联系人会将该联系人移动到回收站。

有关回收站的更多信息，请参见管理回收站。

5 管理 Azure 用户帐户和组

本章包含在 Web 控制台中管理 Azure 用户帐户和 Azure 组的概念和过程信息。通过相应的权限，您可以执行各种 Azure 用户和 Azure 组管理任务，例如创建和删除 Azure 用户帐户对象。

您可以在 Web 控制台的**管理** > **搜索**选项卡中搜索以下节点之一中的对象，从而执行针对 Azure 用户和 Azure 组对象的大多数任务：

- 我的所有受管对象
- 我的所有受管租户
- “ 我的所有受管租户 ” 的子节点

5.1 管理 Azure 用户帐户

作为助理管理员，当 DRA 管理员配置 Azure Active Directory 时，您可以使用 DRA 来管理 Azure 用户帐户和修改 Azure 用户帐户属性。

执行搜索操作以查找并选择所需的 Azure 用户对象。在列表中选择一个或多个对象后，任务栏将变为活动状态，其中包含删除、允许、阻止、口令重设置、 Office 365 邮箱属性和修改属性等选项。单击这些选项以显示其功能。

创建 Azure 用户帐户

您可以在 Azure Active Directory 中创建 Azure 用户帐户。

修改 Azure 用户帐户属性

您可以在 Azure Active Directory 中管理 Azure 用户帐户的属性。您拥有的权限决定了您可以为 Azure 用户帐户修改的属性

允许登录 Azure 用户帐户

您可以启用 Azure 用户帐户以登录到 Azure Active Directory。

阻止登录 Azure 用户帐户

您可以阻止 Azure 用户帐户登录到 Azure Active Directory。

重设置 Azure 用户帐户口令

您可以在 Azure Active Directory 中重设置 Azure 用户帐户的口令，并选择 DRA 是否为该帐户生成新口令。

删除 Azure 用户帐户

您可以从 Azure Active Directory 中删除 Azure 用户帐户，但不能从 DRA 恢复它。

指定 Azure 用户帐户的 Azure 组成员资格

您可以在 Azure Active Directory 的特定 Azure 组中添加或去除 Azure 用户帐户。

5.2 管理 Azure 组

作为助理管理员，当 DRA 管理员配置 Azure Active Directory 时，您可以使用 DRA 来管理 Azure 组。通过 Azure 组，您可以为定义的一组用户帐户授予特定许可权限。 Azure 组可让您控制用户帐户可以在任何租户中访问的数据和资源。

本节将指导您在 Web 控制台中管理 Azure 组。通过相应的权限，您可以执行各种 Azure 组任务。

注释：支持的成员； Azure 组成员可以是 Azure 用户、 Azure 组、已同步用户和已同步组。

向 Azure 组添加用户帐户

您可以将用户帐户 （本地和 Azure）添加到 Azure 受管组。

此任务会将多个帐户添加到所选组。通过选择适当的帐户，可以将单个帐户添加到组中。如果将帐户添加到其他组会增加您对该帐户的权限，则 DRA 不允许您添加该帐户。

在 Azure 中嵌套组

您可以通过将其他组 （本地和 Azure）添加到受管 Azure 组来嵌套组。当组嵌套在 Azure 组中时，子组将从父组继承许可权限。

如果将域或 Azure 组添加到其他 Azure 组会增加您对源组的权限，则 DRA 不允许您添加该组。

创建 Azure 组

您可以在 Azure Active Directory 中创建 Azure 组。您还可以修改属性，例如将 Azure 组成员添加到新组中。

如果没有指定拥有者，则默认情况下， DRA 会提供 Azure 租户访问帐户作为拥有者。

修改 Azure 组属性

您拥有的权限决定了您可以为 Azure Active Directory 中的组修改的属性。

配置 Azure 组所有权

您可以设置任何组的所有权。您可以将组所有权许可权限授予用户帐户或组。授予组所有权允许指定的用户帐户或组管理包括成员资格在内的组。

删除 Azure 组

您可以从 Azure Active Directory 中删除 Azure 组，但不能从 DRA 恢复它。

6 管理 Exchange 邮箱和公共文件夹

使用 DRA，您可以将 Microsoft Exchange 邮箱作为用户帐户属性的扩展进行管理。通过此集成，您可以简化管理工作流程，以便有效地管理 Exchange 属性。您还可以链接来自用户帐户和 Exchange 帐户林的邮箱，并管理资源邮箱、共享邮箱和公共文件夹。

在 Delegation and Configuration （委托和配置）控制台中管理邮箱任务

使用 Account and Resource Management （帐户和资源管理）节点时，可以从对象属性中的 **Exchange Tasks** （Exchange 任务）选项卡执行适用的邮箱任务，也可以从**任务**或所选对象的右键单击菜单访问该选项卡。通常，您会选择 **All My Managed Objects** （我的所有受管对象）节点，然后执行 **Find Now** （立即查找）操作以查找并选择所需的对象。

在 Web 控制台中管理邮箱任务

使用 Web 控制台时，可以从**管理** > **搜索**选项卡执行以下适用的邮箱任务。通常，您会执行搜索操作以查找并选择所需的邮箱对象。在列表中选择一个或多个对象后，任务栏将变为活动状态。单击这些选项以显示其功能。

6.1 用户邮箱的管理任务

您可以管理受管域或受管子树中的用户帐户的 Microsoft Exchange 邮箱。管理 Microsoft Exchange 邮箱的每个方面都需要不同的权限。您拥有的权限将控制您可以修改的邮箱属性，或您是否可以创建、克隆、查看或删除 Microsoft Exchange 邮箱。您还可以管理与用户帐户关联的邮箱许可权限，从而可以控制 Microsoft Exchange 环境的安全性。如果您没有修改所选邮箱的选项卡或字段所需的权限，则 DRA 将禁用您无法修改的选项卡和字段。

除了下面定义的任务外， DRA 管理员还可以在对象属性中启用用户帐户选项，以便配置 Skype 和 Skype Online 的设置。可以从 Delegation and Configuration （委托和配置）控制台及 Web 控制台中的用户帐户配置 Skype。 Skype Online 只能通过 Web 控制台进行配置。

创建邮箱

您可以为现有用户帐户创建 Microsoft Exchange 邮箱。您还可以修改新邮箱的属性。

注释：创建邮箱时， Exchange 会根据 Exchange 策略设置生成必要的代理字符串。Microsoft Exchange 还会生成默认代理字符串。因此，当您查看新创建的邮箱的属性时，您会看到两种类型的代理字符串。

克隆用户帐户

克隆用户帐户时，该用户所属的任何组都将自动添加到新用户帐户，从而节省您配置新帐户的时间。您可以添加或去除新帐户中的组、启用电子邮件以及进行任何其他属性配置，如同您使用任何新帐户一样。

注释：克隆 InetOrgPerson 对象时，您将创建一个用户帐户。

移动邮箱

您可以将用户帐户的 Microsoft Exchange 邮箱移动到另一个邮箱储存或 Microsoft Exchange 服务器。

修改邮箱属性

您可以在管理关联的用户帐户时修改 Microsoft Exchange 邮箱的属性。您拥有的权限决定了您可以修改的邮箱属性。

注释：您无法修改成员服务器上管理的用户帐户的邮箱属性。

配置邮箱安全许可权限

您可以指定要授予或拒绝使用特定 Microsoft Exchange 邮箱发送和接收电子邮件能力的用户帐户、组或计算机。通过这些设置，您可以更有效地保护 Exchange 环境。您无法修改继承的安全许可权限。

注释：管理邮箱安全性时，禁用的许可权限可能表示继承的许可权限。

去除邮箱安全许可权限

您可以从与 Microsoft Exchange 邮箱关联的用户帐户、组或计算机中去除邮箱安全许可权限。去除邮箱安全许可权限可防止用户帐户、组或计算机帐户通过指定的邮箱发送和接收电子邮件。您无法去除继承的安全许可权限。

配置邮箱权限

您可以授予或拒绝其他用户帐户、组或计算机对特定 Microsoft Exchange 邮箱的权限。通过这些设置，您可以更有效地保护 Exchange 环境。您无法修改继承的邮箱权限。

注释：管理邮箱权限时，禁用的许可权限可能表示继承的许可权限。

去除邮箱权限

您可以从与特定 Microsoft Exchange 邮箱关联的用户帐户、组或计算机中去除邮箱权限。去除邮箱权限可防止用户帐户、组或计算机帐户使用指定的邮箱。您无法去除继承的邮箱权限。

删除邮箱

您可以删除与受管域或受管子树中的用户帐户关联的邮箱。删除邮箱也会删除邮箱中的所有讯息。

添加或修改电子邮件地址

您可以为与受管域或受管子树中的用户帐户关联的邮箱指定电子邮件地址。您还可以将电子邮件地址指派给尚未拥有邮箱的用户帐户。管理 Microsoft Exchange 邮箱时，只能添加代理生成策略定义的电子邮件地址类型。

指定答复地址

您可以为与受管域或受管子树中的用户帐户关联的邮箱设置答复地址。您可以为邮箱设置多个答复地址。但是，您不能将多个电子邮件地址类型设置为答复地址。例如，您不能将多个因特网地址指定为答复地址。

删除电子邮件地址

您可以通过从邮箱中去除地址来删除电子邮件地址。

指定递送选项

您可以指定用户可用于发送讯息的邮箱、设置转发选项以及指定收件人限制。

指定递送限制

通过设置递送限制，您可以限制进来的和出去的讯息大小以及是否接受特定邮箱进来的讯息。

指定储存限制

您可以指定储存限制，例如基于邮箱大小的警告。您还可以指定已删除项目的保留时间。

检查邮箱移动状态

您可以检查邮箱移动的状态并对其执行操作，例如清除状态、取消移动以及继续已中断的移动。

6.2 Office 365 邮箱的管理任务

本节包含有关在 Delegation and Configuration （委托和配置）控制台中通过 Account and Resource Management（帐户和资源管理）节点以及在 Web 控制台中管理 Microsoft Office 365 邮箱的信息。通过相应的权限，您可以执行各种用户帐户管理任务，例如提起诉讼保留和设置电子邮件转发。

重要：DRA 可管理 Office 365 用户邮箱以及迁移的共享邮箱、会议室邮箱和设备邮箱。若要 DRA 管理这些邮箱，它们必须与 DRA 管理的本地用户相关联。邮箱属性将通过属性页面提供给那些关联用户。

设置诉讼保留

当存在合理的诉讼预期时，可能需要进行诉讼保留。组织必须保留与案件相关的电子储存信息，包括电子邮件。

在邮箱上设置诉讼保留以保留所有邮箱内容，包括已删除的项目和已修改项目的原始版本。将用户的邮箱置于诉讼保留状态也会保留用户存档邮箱中的内容 （如果存在）。内容保留期为指定的一段时间，或直到您从邮箱中去除诉讼保留。

您必须拥有 Exchange Online Enterprise E3 许可证才能设置诉讼保留。您可以通过用户对象属性中的**诉讼保留**选项卡配置该功能。

委托邮箱许可权限

您可以通过用户对象属性中的“ 邮箱委托 ”选项卡委托 Office 365 邮箱许可权限。有三种类型的许可权限可以委托、代理发送、代表发送和完全访问。可以委托的许可权限类型取决于接收对象类型。

设置电子邮件转发

您可以通过用户对象属性中的“邮件流”选项为用户帐户启用邮件转发。

6.3 资源邮箱的管理任务

Microsoft Exchange 的资源邮箱功能可让您创建代表资源（如会议室）的邮箱，以便您可以通过向其发送会议邀请来进行预留，如同您向个人发送一样。 DRA 包含一组角色、权限和策略，可让您有效地管理资源邮箱。

DRA 可提供对资源邮箱的用户界面扩展支持以及对生成审计或用户界面报告的支持。 DRA 中还集成了对 ADSI 脚本的支持。

创建资源邮箱

您可以在受管域或受管子树中创建资源邮箱。

将资源邮箱移动到另一个容器

您可以将资源邮箱移动到受管域或受管子树中的另一个容器，例如 OU。

将资源邮箱移动到另一个邮箱储存或 Exchange 服务器

您可以将资源邮箱移动到另一个邮箱储存或 Microsoft Exchange 服务器。

克隆资源邮箱

通过克隆资源邮箱，您可以快速创建具有类似属性的其他资源邮箱。克隆资源邮箱时，DRA 会使用所选资源中的值填充“克隆资源邮箱向导”。

重命名资源邮箱

您可以重命名受管域或受管子树中的资源邮箱。更改用户登录名也会更改与用户帐户关联的邮箱的名称。

将资源邮箱添加到组

您可以将资源邮箱添加到受管域或受管子树中的特定组。

删除资源邮箱

您可以删除受管域或受管子树中的资源邮箱。删除资源邮箱还将删除邮箱中的所有讯息以及与资源邮箱关联的所有已禁用的用户对象。如果需要，可以在删除邮箱时覆盖已禁用用户对象的删除。如果删除与资源邮箱关联的用户对象，则也会删除该资源邮箱。

恢复已删除的资源邮箱

如果启用了该域中的“回收站”，则可以恢复已删除的资源邮箱。

修改资源邮箱属性

您可以管理受管域或受管子树中的资源邮箱的属性。您拥有的权限决定了您可以修改的属性。

6.4 共享邮箱的管理任务

共享邮箱对于咨询台管理员和技术支持人员非常有用，因为可以将所有响应配置为进入多个用户可以访问的单个邮箱。邮箱必须位于启用了 Exchange 策略的 DRA 受管域中，并且必须已委托给您管理共享邮箱的权限。

创建共享邮箱时，可以将两种类型的许可权限委托给用户：“ 代理发送 ” 和 “ 完全访问权限 ”。“ 代理发送 ” 提供读取和发送电子邮件的许可权限。您可以将许可权限委托给用户和组对象。您还可以在对象的属性中指定递送限制、递送选项、储存限制、文件夹许可权限和其他多个选项。

注释：只能通过 Web 控制台执行共享邮箱的管理任务。

创建共享邮箱

您可以在受管域或受管子树中创建共享邮箱。

将共享邮箱移动到另一个容器

您可以将共享邮箱移动到受管域或受管子树中的另一个容器，例如 OU。

将共享邮箱移动到另一个邮箱储存

您可以将共享邮箱移动到另一个邮箱储存。

克隆共享邮箱

通过克隆共享邮箱，您可以快速创建具有类似属性的其他共享邮箱。

重命名共享邮箱

您可以重命名受管域或受管子树中的共享邮箱。更改用户登录名也会更改与用户帐户关联的邮箱的名称。

删除共享邮箱

您可以删除受管域或受管子树中的共享邮箱。如果为该域禁用了回收站，则删除共享邮箱会从 Active Directory 中将其永久去除。如果为该域启用了回收站，则删除共享邮箱会将其移动到回收站。

删除共享邮箱还将删除邮箱中的所有讯息以及与共享邮箱关联的所有已禁用的用户对象。如果删除与共享邮箱关联的用户对象，则也会删除该共享邮箱。

恢复已删除的共享邮箱

如果启用了该域中的 “ 回收站 ”，则可以恢复已删除的共享邮箱。

创建存档共享邮箱

您可以在受管域或受管子树中创建存档共享邮箱。

删除存档共享邮箱

您可以删除受管域或受管子树中的存档共享邮箱。

修改共享邮箱属性

您可以修改受管域或受管子树中的共享邮箱属性。您拥有的权限决定了您可以修改的属性。

6.5 链接邮箱的管理任务

在邮箱迁移很常见时，链接邮箱对于在合并、收购和公司拆分期间发生的大型组织更改非常有用。此功能可以链接来自不同 Exchange 林的邮箱，以消除用户电子邮件的中断。邮箱必须位于启用了 Exchange 策略的 DRA 受管域中，并且必须已委托给您管理链接邮箱的权限。创建链接邮箱时，**链接邮箱**选项卡将添加到用户对象的属性中。

仅 Web 控制台中支持链接邮箱管理。您可以从所选用户帐户的工具栏创建链接邮箱。仅当所选用户的域与 DRA 中的其他受管域具有外部林信任时，才会启用此选项。在其他 DRA 受管域中搜索要链接的帐户时，将仅列出已禁用的用户帐户。

创建链接邮箱

您可以从在不同受管 Exchange 林中选择的两个用户帐户创建链接邮箱。

删除链接邮箱

您可以从具有链接邮箱的所选用户的工具栏中删除链接邮箱。

修改链接邮箱属性

您可以从所选用户属性中的**链接邮箱**选项卡修改链接邮箱的属性。

创建链接存档邮箱

您可以从具有链接邮箱的所选用户创建链接存档邮箱。

删除链接存档邮箱

您可以从具有链接存档邮箱的所选用户的工具栏中删除链接存档邮箱。

恢复已删除的链接邮箱

如果启用了该域中的“回收站”，则可以恢复已删除的链接邮箱。

6.6 公共文件夹的管理任务

如果 DRA 管理员在 DRA 受管企业中创建了公共文件夹林，并授予您管理 DRA 中公共文件夹的权限，则您可以创建公共文件夹、修改其属性并生成更改历史记录报告。只能在 Web 控制台中创建和修改公共文件夹。可以使用搜索选项搜索公用文件夹。有关信息，请参见*第 3.1 节“搜索”（第 35 页）*。

您可以从**管理** > **公共文件夹**选项卡执行公共文件夹任务。

创建公共文件夹

您可以通过 Web 控制台在指定的公共文件夹域、子树和邮箱中创建新的公共文件夹。您可以使用所选域的默认邮箱或选择一个邮箱。

为公共文件夹启用电子邮件

您可以使用列表工具栏上的**启用邮件**选项为公共文件夹启用电子邮件。此操作使您可以将电子邮件地址与公共文件夹关联，并修改公共文件夹的属性。

为公共文件夹禁用电子邮件

您可以使用列表工具栏上的**禁用邮件**选项为公共文件夹禁用电子邮件。

修改公共文件夹属性

启用现有公共文件夹邮件后，您可以查看该文件夹的统计信息，并修改该公共文件夹的属性。在这些属性中，您可以指定用户递送和限制选项、大小限制和配额警告、邮件属性、储存期限、包含主持人以批准邮件以及自定义属性。

注释：当选择多个公共文件夹时，您还可以更新多个公共文件夹的某些属性，例如储存配额。

删除公共文件夹

如果公共文件夹没有任何子文件夹且已禁用电子邮件选项，则可以将其删除。

7 管理资源

DRA 可让您管理资源，包括计算机、打印机和其他设备，以及与这些资源关联的进程。例如，如果需要在受管计算机上启动特定服务，则可以在 DRA 中搜索该计算机对象，通过对象属性访问其服务，然后从 DRA 重启动该计算机上的特定服务，而无需远程访问该计算机。

7.1 管理组织单元 (OU)

本节将指导您在 Delegation and Configuration （委托和配置）控制台中通过 Account and Resource Management （帐户和资源管理）节点管理 OU。您可以通过相应权限执行各种 OU 管理任务，如将 OU 移动到其他容器。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理 OU。

修改 OU 属性

您可以修改 OU 的属性。您拥有的权限决定了您可以修改受管域或受管子树中 OU 的哪些属性。

创建 OU

您可以在受管域或受管子树中创建 OU。您还可以修改一般属性，如 OU 说明。

复制 OU

您可以通过克隆受管域或受管子树中的现有 OU 来创建一个新 OU。您还可以修改新 OU 的一般属性，如 OU 说明。克隆 OU 不会克隆 OU 中包含的对象。

将 Active Directory 树打开到 OU 位置

您可以快速轻松地将 Active Directory 树打开到受管域或受管子树中特定 OU 的位置。

将 OU 移动到其他容器

您可以将 OU 移动到受管域中的其他容器。管理域的子树时，您可以在该子树的层次结构中移动 OU。

注释：

- 如果将 OU 移动到其他容器会增加您对所移动 OU 的权限，则 DRA 不允许您移动该 OU。
- 您还可以通过将 OU 拖到新的位置来移动 OU。

删除 OU

您可以删除受管域或受管子树中的 OU。您只能删除空白 OU。如果 OU 中包含对象，那么您无法删除 OU。如要删除包含对象的 OU，请先删除所有对象，然后再删除 OU。

7.2 管理计算机

DRA 可让您管理受管域或受管子树中的计算机。例如，您可以在受管域中添加或去除计算机帐户，以及管理每台计算机上的资源。将计算机添加到域时， DRA 会在该域中为该计算机创建一个计算机帐户。然后，您可以连接该域中的计算机，并将计算机配置为使用该计算机帐户。您还可以查看和修改计算机帐户的属性。 DRA 还允许您关闭计算机并同步受管域中的域控制器。

注释：

- 您只能通过 Delegation and Configuration （委托和配置）控制台来管理计算机。
- 您无法管理隐藏的域控制器。域超速缓存不包括隐藏的域控制器。因此， DRA 不会在列表或属性窗口中显示隐藏的域计算机

指定计算机的组成员资格

您可以在受管域或受管子树的特定组中添加或去除计算机。您还可以查看或修改此计算机所属的现有组的属性。

管理计算机帐户属性

您可以管理计算机帐户属性。您拥有的权限决定了您可以为受管域或受管子树中的计算机修改的属性。

将计算机添加到域

您可以通过创建新的计算机帐户将计算机添加到受管域或受管子树中。

从域中去除计算机

您可以通过删除计算机帐户，从受管域或受管子树中去除计算机。

移动计算机

您可以将计算机移动到受管域或受管子树中的另一个容器，例如 OU。

关闭或重启动计算机

您可以立即或在设置的日期和时间关闭和重启动计算机。

重设置管理员帐户口令

要重设置计算机的管理员帐户口令，您必须具有本地管理员的重设置口令权限或与包含此权限的角色关联。您可以重设置受管域或受管子树中成员服务器的管理员口令。您无法重设置域控制器的管理员口令。

重设置计算机帐户

您可以重设置受管域或受管子树中成员服务器的计算机帐户。您无法重设置域控制器的计算机帐户。

删除计算机帐户

您可以删除受管域或受管子树中的计算机帐户。如果您在管理 Microsoft Windows 域，则可以删除包含其他对象 （例如共享资源）的计算机帐户。启用**强行删除**选项可从 Active Directory 删除计算机对象。这还将删除子对象，包括打印机和共享文件夹。删除的计算机及其相关对象将移至 DRA 回收站。如果删除时禁用了回收站，则对象将被永久删除。

注释：您无法删除受管域或受管子树中成员服务器的计算机帐户。

禁用计算机帐户

您可以禁用受管域或受管子树中的计算机帐户。禁用计算机帐户会阻止该计算机上的用户登录到任何域。

启用计算机帐户

您可以启用受管域或受管子树中的计算机帐户。启用计算机帐户将允许该计算机上的用户登录到任何域。

管理计算机资源

对于受管域或受管子树中的每个计算机帐户，您可以管理关联的资源，例如服务、共享、设备、打印机和打印作业。

7.3 管理服务

服务是一种可从 Windows 操作系统获得特殊处理的应用程序类型。即使当前没有用户登录到计算机，服务也可以运行。 DRA 允许具有适当权限的助理管理员通过 Delegation and Configuration （委托和配置）控制台的 Account and Resource Management （帐户和资源管理）节点管理服务。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理服务。

管理服务属性

您可以管理在受管域或受管子树中的计算机上运行的服务的属性。您可以在管理该计算机的其他资源时管理服务。

启动服务

您可以在受管域或受管子树中任何计算机上启动服务。

使用参数启动服务

启动接受参数的服务时，可以在启动时指定这些参数。您可以在受管域或受管子树中的计算机上启动服务。

指定服务启动类型

您可以更改服务的启动类型，例如需要手动启动。

指定服务登录帐户

您可以将服务登录帐户更改为当前系统帐户以外的帐户。您可以为在受管域或受管子树中的计算机上运行的服务指定登录帐户。您可以指定本地系统帐户或特定用户帐户。

重启动服务

您可以重启动在受管域或受管子树中的计算机上运行的服务。

要重启动服务，您必须同时拥有 Stop a Service （停止服务）和 Start a Service （启动服务）权限，或与包含这些权限的角色关联，例如 Start and Stop Service （启动和停止服务）角色。

停止服务

您可以停止在受管域或受管子树中的计算机上运行的服务。

暂停服务

您可以暂停在受管域或受管子树中的计算机上运行的服务。服务是否可以暂停取决于服务类型。例如，您可能无法暂停具有依赖服务的服务。

继续暂停的服务

您可以继续在受管域或受管子树中的计算机上暂停的服务。

7.4 管理打印机和打印作业

要管理打印机，您需要管理为这些打印机提供服务的打印队列。 DRA 可让您暂停或继续、启动、修改、停止和查看资源打印机及已发布的打印机。 DRA 还允许您修改打印作业的属性和优先级。要添加或删除打印机，请使用本机 Windows 工具。

打印服务器是已安装一个或多个逻辑打印机的计算机。可在具有打印机设备驱动程序的计算机上定义逻辑打印机。逻辑打印机包括打印机的打印驱动程序、打印队列和端口。打印服务器可将逻辑打印机与打印机设备相关联。

可在选择要打印文档的计算机上定义连接的打印机。连接的打印机是连接到网络上的打印共享。因此，您可以通过关联的计算机管理打印机和打印作业。

已发布的打印机是在 Active Directory 中发布的打印机。已发布的打印机可以是未直接连接到服务器的网络打印机，也可以是由群集服务器托管的打印机。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台来管理打印机和打印作业。

要了解有关管理打印机和打印任务的更多信息，请参见以下主题：

- 第 7.4.1 节“ 打印机管理任务 ”（第 70 页）
- 第 7.4.2 节“ 打印作业管理任务 ”（第 71 页）
- 第 7.4.3 节“ 已发布的打印机管理任务 ”（第 71 页）
- 第 7.4.4 节“ 已发布打印机的打印作业管理任务 ”（第 72 页）

7.4.1 打印机管理任务

您可以管理与受管域或受管子树中的计算机关联的打印机。 DRA 允许您在管理该计算机的其他资源时管理打印机。

本节将指导您在 Delegation and Configuration （委托和配置）控制台中通过 Account and Resource Management （帐户和资源管理）节点管理打印机。借助相应的权限，您可以执行各种打印机管理任务，例如停止打印机。

管理打印机属性

您可以管理受管域或受管子树中的打印机属性。 DRA 允许您在管理该计算机的其他资源时管理打印机。

暂停打印机

您可以暂停与受管域或受管子树中的计算机关联的打印机。 DRA 允许您在管理该计算机的其他资源时管理打印机。

恢复打印机

您可以恢复与受管域或受管子树中的计算机关联的打印机。 DRA 允许您在管理该计算机的其他资源时管理打印机。

7.4.2 打印作业管理任务

您可以管理与受管域或受管子树中的打印机关联的打印作业。由于打印作业与打印机相关联，因此您可以在管理打印机的同时管理打印作业。

本节将指导您在 Delegation and Configuration （委托和配置）控制台的 Account and Resource Management （帐户和资源管理）节点中管理打印作业。借助相应的权限，您可以执行各种打印作业管理任务，例如取消打印作业。

管理打印作业属性

您可以在打印机管理工作流程中修改打印作业属性。由于打印作业与打印机关联，因此您可以在管理相应的打印机时修改打印作业。您可以修改的打印作业属性取决于您拥有的权限类型。要修改打印作业属性，您必须能够访问相应的打印机和计算机。

暂停打印作业

您可以暂停受管域或受管子树中的打印机上的打印作业。要暂停打印作业，您必须能够访问相应的打印机和计算机。暂停打印作业不会从打印队列中删除打印作业。

继续打印作业

您可以继续暂停的打印作业。要继续打印作业，您必须能够访问相应的打印机和计算机。

重启动打印作业

您可以重启动已停止的打印作业。要重启动打印作业，您必须能够访问相应的打印机和计算机。

取消打印作业

您可以取消打印机队列中的打印作业。取消打印作业时， DRA 会从打印机队列中永久删除该打印作业。要取消打印作业，您必须能够访问相应的打印机和计算机。

7.4.3 已发布的打印机管理任务

您可以管理受管域或受管子树中的已发布打印机。您可以添加或搜索在 Active Directory 中发布的任何打印机或由群集服务器托管的打印机。

本节将指导您在 Account and Resource Management （帐户和资源管理）节点中管理已发布的打印机。借助相应的权限，您可以执行各种打印机管理任务，例如停止打印机。

管理已发布的打印机属性

您可以管理受管域或受管子树中已发布打印机的属性。 DRA 允许您在管理其他资源时管理已发布的打印机。

刷新已发布的打印机信息

您可以刷新受管域或受管子树中已发布的打印机信息。 DRA 允许您在管理其他资源时管理已发布的打印机。

暂停已发布的打印机

您可以暂停受管域或受管子树中已发布的打印机。 DRA 允许您在管理其他资源时管理已发布的打印机。

恢复已发布的打印机

您可以恢复受管域或受管子树中暂停的已发布打印机。 DRA 允许您在管理其他资源时管理已发布的打印机。

移动已发布的打印机

您可以将受管域中一个容器中的已发布打印机移动到同一域中的另一个容器。 DRA 允许您在管理其他资源时管理已发布的打印机。

重命名已发布的打印机

您可以在 Active Directory 中重命名共享的已发布打印机。 DRA 允许您在管理其他资源时管理已发布的打印机。

注释：在 Active Directory 中重命名已发布的打印机不会更改资源打印机共享名称或将名称更改传播到要管理的资源打印机。例如，如果资源打印机名称为 Emerald，并且您在 Active Directory 中将打印机重命名为 Ruby，则其他用户将看到打印机名称为 Ruby，但资源打印机名称将继续为 Emerald。

7.4.4 已发布打印机的打印作业管理任务

您可以管理与受管域或受管子树中已发布打印机关联的打印机作业。由于打印作业与打印机相关联，因此您可以在管理已发布打印机时管理打印作业。

本节将指导您在 Account and Resource Management （帐户和资源管理）节点中管理已发布的打印机。借助相应的权限，您可以执行各种打印作业管理任务，例如取消打印作业。

管理打印作业属性

您可以在已发布的打印机管理工作流程中修改打印作业属性。由于打印作业与打印机关联，因此您可以在管理相应的已发布打印机时修改打印作业。您可以修改的打印作业属性取决于您拥有的权限类型。要修改打印作业属性，您必须能够访问相应的已发布打印机。

暂停打印作业

您可以暂停受管域或受管子树中已发布打印机上的打印作业。要暂停打印作业，您必须能够访问相应的已发布打印机。暂停打印作业不会从打印队列中删除打印作业。

继续打印作业

您可以继续受管域或受管子树中暂停的打印作业。要继续打印作业，您必须能够访问相应的已发布打印机。

重启动打印作业

您可以重启动受管域或受管子树中停止的打印作业。要重启动打印作业，您必须能够访问相应的已发布打印机。

取消打印作业

您可以取消受管域或受管子树中打印机队列中的打印作业。取消打印作业时， DRA 会从打印机队列中永久删除该打印作业。要取消打印作业，您必须能够访问相应的已发布打印机。

7.5 管理共享

共享是使网络上的其他用户可以使用文件或打印机等资源的一种方式。每个共享都有一个共享名称，该名称指服务器上的共享文件夹。 DRA 仅管理受管域中计算机上的共享。要成功管理共享，访问帐户必须具备对要管理资源的所有计算机的管理员许可权限，例如是本地管理员组的成员。要指派这些许可权限，请将访问帐户添加到计算机域中的本机域 Admin 组。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理共享。

管理共享属性

您可以管理受管域或受管子树中共享的属性。 DRA 允许您在管理该计算机的其他资源时管理共享。

创建共享

您可以为受管域或受管子树中的计算机创建共享。您还可以修改此共享的属性。

克隆共享

您可以为受管域或受管子树中的计算机克隆共享。通过克隆共享，您可以基于具有类似属性的其他共享快速创建共享。这种灵活性允许您对在给定域中创建的所有共享实施一致性设置。

克隆共享时， DRA 会使用所选共享中的值填充“ 克隆共享向导 ”。您还可以修改新共享的属性。

删除共享

您可以从受管域或受管子树中的计算机中删除共享。

7.6 管理已连接的用户

只要用户连接到远程计算机上的特定资源，便会建立会话。已连接的用户是连接到网络上的共享资源的用户。

DRA 仅管理受管域中计算机上的已连接用户。访问帐户必须具备对要管理已连接用户的所有计算机的管理员许可权限，例如是本地管理员组的成员。要指派这些许可权限，请将访问帐户添加到计算机域中的本机域 Admin 组。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理已连接的用户。

断开用户

您可以从受管域或受管子树中的计算机断开已连接用户。您必须能够访问该计算机和此打开的会话。断开已连接用户将结束打开的会话。

刷新已连接用户的列表

要确保您正在查看有关计算机上打开会话的最新信息，请手动刷新已连接用户的列表。您必须能够访问该计算机和此打开的会话。

7.7 管理设备

设备是连接到网络的任何设备，例如计算机、打印机、调制解调器或任何其他外围设备。

虽然您的计算机上可能安装了某个设备，但在安装和配置相应的驱动程序之前， Windows 无法识别该设备。设备驱动程序使特定硬件能够与操作系统通信。

DRA 仅允许您配置和管理受管域中的计算机中的设备。访问帐户必须具备对要管理设备的所有计算机的管理员许可权限，例如是本地管理员组的成员。要指派这些许可权限，请将访问帐户添加到计算机域中的本机域 Admin 组。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理设备。

管理设备属性

您可以修改特定计算机上设备的属性。修改设备的设备属性允许您修改设备的启动类型。

启动设备

您可以启动受管域或受管子树中特定计算机上的设备。

停止设备

您可以停止受管域或受管子树中特定计算机上的设备。

7.8 管理事件日志

事件是重要的系统事件或应用程序事件。 Windows 操作系统会在事件日志文件中记录有关事件的信息。每台计算机上可能储存多个事件日志。使用本机 Windows 事件查看器查看事件日志。 DRA 仅管理受管域中计算机上的事件日志。

DRA 将在日志存档 （一个安全储存库）中记录用户启动的操作。除了在 DRA 日志存档中记录信息之外，您还可以让 DRA 在 Windows 事件日志中记录用户启动的操作。有关更多信息，请参见了解日期和时间。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理事件日志。

7.8.1 事件日志类型

运行 Microsoft Windows 的计算机将在各种日志中记录其他信息。日志简要描述如下：

日志类型	说明
ADAM	记录 ADAM 储存库记录的事件。
应用程序	记录计算机上的应用程序记录的事件，例如服务启动或故障。例如，DRA 将事件储存在应用程序日志中。
目录服务	记录与维护安全数据库的域控制器相关的事件。
文件复制服务	记录与操作系统提供的文件复制服务相关的事件。
安全性	记录包括登录尝试、文件和目录访问以及基于审计策略选项的安全策略更改的事件。
系统	记录 Windows 系统组件记录的事件，例如驱动程序故障或服务启动和停止。

7.8.2 事件日志管理任务

您可以指定事件日志文件的最大大小，以及当达到事件日志上限时如何处理。属性窗口还会显示日志的名称、日志文件路径和文件名、创建日志的时间、上次修改日志的时间以及上次访问日志的时间。如果选择备份日志文件，则 DRA 会在所选计算机的标准位置使用唯一的文件名保存事件日志。

DRA 允许您在管理该计算机的其他资源时管理事件日志。通过相应的权限，您可以执行各种共享管理任务，例如更改事件日志属性。

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）。

管理事件日志属性

您可以修改特定计算机的事件日志属性。

查看事件日志条目

您可以查看受管域或受管子树中计算机的特定事件日志中的条目。查看事件日志时，DRA 会起动本机 Windows 事件查看器。

清除事件日志

您可以清除受管域或受管子树中计算机的特定事件日志中的条目。您还可以在清除日志之前保存事件日志条目。

7.9 管理打开的文件

打开的文件是与共享资源 （如文件或管道）的连接。管道是一种进程间通信机制，使一个进程能够与另一个本地或远程进程通信。

DRA 仅管理受管域和受管子树中计算机上 的打开的文件。由于打开的文件与计算机关联，因此您可以在管理该计算机的其他资源时管理打开的文件。例如，您可能希望在关闭系统或安装新设备或服务时关闭打开的文件。您还可以监视用户最常访问的文件，从而帮助您更好地评估文件安全性。

注释：您只能通过 Delegation and Configuration （委托和配置）控制台管理打开的文件。

关闭文件

您可以从网络上的资源关闭打开的文件。当您打算关闭打开的文件时，最好通知用户。他们可能需要时间来保存其数据。要关闭打开的文件，您必须能够访问相应的计算机。

刷新打开的文件列表

要确保您正在查看有关计算机上打开会话的最新信息，请手动刷新已连接用户的列表。要刷新打开的文件列表，您必须能够访问相应的计算机。

8 管理回收站

回收站提供了一个安全网，允许您临时删除用户帐户、组、联系人和计算机帐户。然后，您可以将这些对象恢复到其原始状态，并且所有数据 （如 SID、 ACL 和组成员资格）都保持不变，或永久删除这些对象。这种灵活性提供了一种更安全的方式来管理用户帐户、组、联系人和计算机帐户。可以使用搜索选项搜索所需的对象。有关信息，请参见*搜索对象*。

从回收站恢复对象

您可以将已删除的对象恢复到对象删除前所在的容器。 DRA 可以将这些对象恢复到其原始状态，并且所有数据 （例如 SID、 ACL 和组成员资格）都保持不变。对象可以是用户帐户、组、联系人、动态组、资源邮箱、动态分发组或计算机帐户。

恢复所有对象

您可以从受管域的回收站恢复所有对象。您可以从特定域或所有受管域的回收站恢复对象。要从特定域的回收站恢复对象，必须为该域启用回收站。

从回收站中删除对象

您可以从受管域的回收站中永久删除对象。从回收站中删除对象后，便无法恢复该对象。对象可以是用户帐户、组、联系人、动态组、资源邮箱、动态分发组或计算机帐户。

清空回收站

您可以清空受管域的回收站。清空回收站会永久删除当前在回收站中的所有对象。您可以清空特定域或所有受管域的回收站。要清空特定域的回收站，必须为该域启用回收站。清空回收站后，便无法恢复已删除的对象。