IBM Security Directory Integrator
V 7.2.0.1

联合目录服务器管理指南

S151-2130-01

IBM Security Directory Integrator
V 7.2.0.1

联合目录服务器管理指南

S151-2130-01

注意

使用本资料及其支持的产品之前，请阅读第 87 页的『声明』中的常规信息。

修订版通知

注: 此修订版适用于 *IBM Security Directory Integrator* 许可程序 **(5724-K74)** 的 **V7.2.0.1** 及所有后续发行版和修订版，直到在新版本中另有声明为止。

目录

图

关于此出版物

IBM® Security Directory Integrator 是一种集成开发环境和运行时服务，适用于通用的、多格式的、多方向的并且实时的数据移动、同步和变换。

*IBM Security Directory Integrator V7.2.0.1 Federated Directory Integrator 管理指南*包含有关使用联合目录服务器控制台来设计、实现和管理数据集成解决方案的信息。

它还包含有关使用跨域身份管理系统 (SCIM) 协议和接口进行身份管理的信息。

对出版物和术语的访问

请阅读有关可以在线访问的 IBM Security Directory Integrator V7.2.0.1 资料库和相关出版物的描述。

本部分提供以下内容:

- 『IBM Security Directory Integrator 资料库』 中出版物的列表。
- 指向 第 viii 页的『联机出版物』 的链接。
- 指向第 viii 页的『IBM 术语 Web 站点』的链接。

IBM Security Directory Integrator 资料库

以下文档在 IBM Security Directory Integrator 资料库中可用:

- 《*IBM Security Directory Integrator V7.2.0.1 联合目录服务器管理指南*》

  包含有关使用联合目录服务器控制台来设计、实现和管理数据集成解决方案的信息。还包含有关使用跨域身份管理系统 (SCIM) 协议和界面进行身份管理的信息。
- *IBM Security Directory Integrator V7.2.0.1 入门指南*

  包含 IBM Security Directory Integrator 的简要教程和介绍。包含用于创建 IBM Security Directory Integrator 的交互与实际操作学习的示例。
- 《*IBM Security Directory Integrator V7.2.0.1 用户指南*》

  包含关于使用 IBM Security Directory Integrator 的信息。包含关于使用 Security Directory Integrator 设计器工具（配置编辑器）来设计解决方案或从命令行运行现成的解决方案的指示信息。还提供了关于界面、概念和 AssemblyLine 创建的信息。
- *IBM Security Directory Integrator V7.2.0.1 Installation and Administrator Guide*

  包含了关于安装、从前版本迁移、配置记录功能和 IBM Security Directory Integrator 远程服务器 API 底层安全模型的完整信息。包含关于如何部署和管理解决方案的信息。
- 《*IBM Security Directory Integrator V7.2.0.1 参考指南*》

  包含关于 IBM Security Directory Integrator 的独立组件（连接器、功能组件、解析器和对象等 – AssemblyLine 的构建模块）的详细信息。
- *IBM Security Directory Integrator V7.2.0.1 Problem Determination Guide*

提供关于 IBM Security Directory Integrator 工具、资源和技术的信息，这些信息可以协助确定和解决问题。

- *IBM Security Directory Integrator V7.2.0.1 Message Guide*

  提供与 IBM Security Directory Integrator 关联的所有参考、警告和错误消息的列表。

- 《*IBM Security Directory Integrator V7.2.0.1 Password Synchronization Plug-ins 指南*》

  包括安装和配置所有五个 IBM Password Synchronization Plug-ins（Windows Password Synchronizer、Sun Directory Server Password Synchronizer、IBM Security Directory Server Password Synchronizer、Domino® Password Synchronizer 以及 Password for UNIX and Linux）的完整信息。还提供了针对 LDAP 密码存储和 JMS 密码存储的配置指示信息。

- 《*IBM Security Directory Integrator V7.2.0.1 发行Notes®*》

  描述文档中未包含的关于 IBM Security Directory Integrator 的新功能和最新信息。

联机出版物

IBM 在发布产品和在以下位置更新出版物时发布产品出版物:

IBM Security Directory Integrator 资料库

产品文档站点 (http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome) 显示此资料库的欢迎页面和导航。

IBM Security Systems Documentation Central

IBM Security Systems Documentation Central 为每个产品的特定版本提供所有 IBM Security Systems 产品资料库和联机文档链接的按字母顺序排序的列表。

IBM 出版物中心

IBM 出版物中心站点（ http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) 提供定制的搜索功能，帮助您所需要的所有 IBM 出版物。

相关信息

与 IBM Security Directory Integrator 相关的信息在以下位置可用:

- IBM Security Directory Integrator 使用 Oracle 的 JNDI 客户机。有关 JNDI 客户机的信息，请参阅 http://download.oracle.com/javase/7/docs/technotes/guides/jndi/index.html 处的"*Java Naming and Directory Interface™ Specification*"。
- 可帮助回答与 IBM Security Directory Integrator 相关的问题的信息可以在 https://www-947.ibm.com/support/entry/myportal/over-accesspubsview/software/security_systems/tivoli_directory_integrator处找到。

IBM 术语 Web 站点

IBM 术语 Web 站点在一个位置整合了产品资料库术语。可在以下位置访问术语 Web 站点: http://www.ibm.com/software/globalization/terminology。

辅助功能选项

辅助功能选项帮助有身体残疾（例如行动不便或视力受限）的用户成功使用软件产品。通过此产品，可以使用辅助技术来听取和浏览界面。您还可以使用键盘代替鼠标来操作图形用户界面的所有功能。

有关更多信息，请参阅*配置 Directory Integrator*中的“辅助功能选项附录”。

技术培训

有关技术培训信息，请参阅 http://www.ibm.com/software/tivoli/education 处的以下 IBM 培训 Web 站点。

支持信息

IBM 支持机构可辅助代码相关问题以及例程、短持续时间安装或使用问题。可以直接访问 IBM 软件支持站点（http://www.ibm.com/software/support/probsub.html ）。

故障诊断 提供有关以下各项的详细信息:

- 联系 IBM 支持机构之前要收集哪些信息。
- 联系 IBM 支持机构的各种方法。
- 如何使用 IBM 支持助手。
- 用于隔离并自行解决问题的指示信息和问题确定资源。

良好安全性实践的语句

IT 系统安全性包括通过对从企业内外错误访问进行预防、检测和响应来保护系统和信息。错误访问可能导致信息变更、损坏、滥用或误用，也可能导致系统损坏或误用，其中包括用于对其他系统的攻击。没有任何 IT 系统或产品应视为完全安全，并且没有一个产品、服务或安全措施会完全有效地阻止错误的使用或访问。IBM 系统、产品和服务被设计为综合安全方法的一部分，它一定包含其他可操作性步骤，也可能需要其他系统、产品或服务做到最有效。IBM 不保证任何系统、产品或服务不受任何单位/个人的恶意或不合法行为的影响。

第 1 章 联合目录服务器

联合目录服务器 使一系列目录和其他数据源能够合并且视为单一分层目录。联合目录服务器控制台 是一种用于实现此目录集成的随时可用应用程序。

概述

IBM Security Directory Integrator 提供了用于开发复杂数据集成解决方案的大量功能。联合目录服务器控制台 基于这些功能进行构建，并提供了用于与各种源连接和同步数据的简单快捷的解决方案。

IBM Security Directory Server 是 联合目录服务器 的缺省核心集中式存储库。联合目录服务器控制台 提供了从一个或多个源系统（例如 Active Directory 或 Sun Directory）到目标目录的同步服务。

联合目录服务器控制台 有下列优势:

- 由于它是随时可用的高质量应用程序，因此需要的实现时间和工作量比定制构建的解决方案少。
- 不需要深入了解 IBM Security Directory Integrator; 因此，该产品部署和使用起来很轻松。
- 支持各种数据源（例如，目录、数据库、旧数据和平面文件）之间的集成，且不影响现有系统。
- 通过单点访问加快身份和访问管理应用程序的部署速度。
- 速度更快、性能更强且安全性级别更高。

功能

联合目录服务器 提供了多项功能，可以帮助您轻松快捷地实现目录集成解决方案。

- 可以进行目录集成，不需要对现有的旧数据进行更改。
- 它将数据自动拉至 IBM Security Directory Server。
- 所有关系都可包含高级映射和数据转换。
- 用户和组均可集成。
- 可维持目录层次结构，也可将其序列化。
- 可在跨多个源实施的 联合目录服务器 中创建组（包括动态组）。
- 可从多个源的链接数据和扩充数据创建人员的补充数据。
- 可以配置联合目录服务器，从而用户认证会直接进入现有的后端本地系统。不需要进行密码复制（被视为主要开销）。
- 可对现有目录和数据基础结构中的所有内容进行搜索。
- 用户可使用唯一属性（例如电子邮件或员工标识）来登录企业目录。
- 可通过易于使用的界面来管理旧数据以及属性的定制映射。
- 可以启用回写来更新原始源。

业务场景

联合目录服务器 是一种混合方法，用于满足各种业务场景中目录服务的安全性和协作需求。

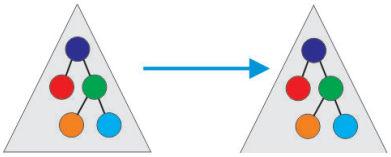
以下示例是 联合目录服务器 的功能可满足的一些业务需求:

- 您希望启用中央认证服务。但是，您可能希望将密码原样保留在原始源目录中。
- 您需要管理多个目录内的组以支持诸如企业消息传递和访问控制等服务。
- 您希望扩充您的身份信息，从而使中央 LDAP 目录能够支持应用程序和服务的特定需求。

缺省情况下，IBM Security Directory Server 为集中式核心后端目录服务器。管理员可以选择所需的服务级别，例如传递认证或回写。并且，有需要时，可以使用另一个系统作为中央身份存储库。

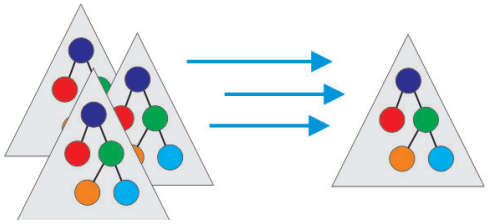
客户的特定需求可分为图中所示的下列场景。

迁移目录或共存



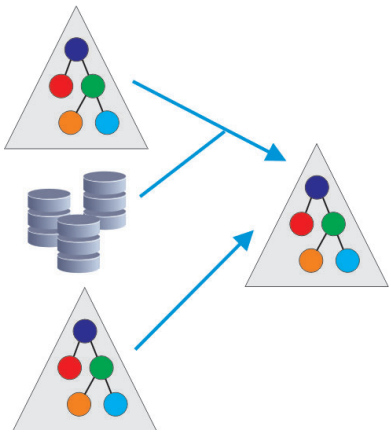
可定义必须迁移的模式和信息量。例如，可通过迁移到联合目录服务器 来使数据源更具伸缩性和灵活性，而不必扩展原始数据源中的模式。

合并多个数据源或目录



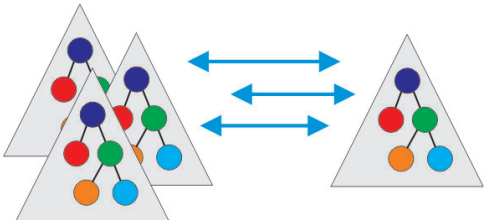
迁移或合并来自不同数据源的数据时，关系中可能包含高级映射和数据转换。例如，您可以集成用户和组，保持目录结构或将其序列化，还可以在 联合目录服务器 中创建跨多个数据源的动态组。

使用其他源中的数据进行增加或扩充



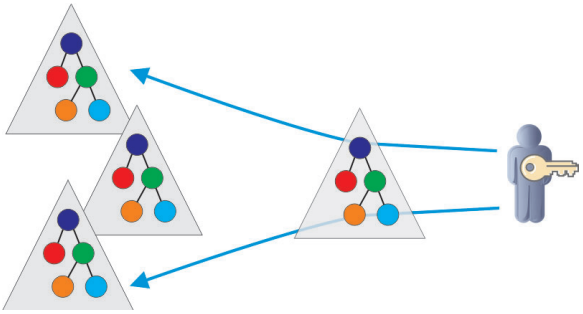
可以通过设置与端点的连接有选择地从另一个数据源添加更多具有特定条件的数据。

选择性地将更改写回原始源



如果已在目标目录服务器中修改信息，那么可将其回写到端点中。但是，回写具有选择性，这是因为某些客户可能想要一个屏障将原始数据保留在端点中。

将认证联合回原始源



联合目录服务器可以将认证请求传回存储了凭证的端点中，从而在端点中发生认证过程。不需要将凭证存储在 联合目录服务器 中，除非您选择这样做。

例如，可合并 联合目录服务器 的各种功能以创建特定于您的需求的定制解决方案。假设您具有一个 Active Directory，您希望将其用于单点登录。您希望它更具可伸缩性以使其用途更广泛（例如用于社交网络），但不希望扩展模式。您可以选择性地迁移数据，例如，仅迁移用户的电子邮件地址。联合目录服务器 还会从源目录中拉取专有名称 (DN)。然后，您可使用 联合目录服务器 的传递认证功能并在源目录本身中保留密码凭证，而不将其拉取至目标目录中。用户可使用唯一属性（在此例中为电子邮件地址）

登录 IBM Security Directory Server。IBM Security Directory Server 将使用 DN 与用户所来自于的 Active Directory 绑定。如果返回了成功响应，那么表示该用户已经过认证。

功能概述

了解联合目录服务器 的关键概念、组件和体系结构。

下图说明 联合目录服务器 的各种组件。

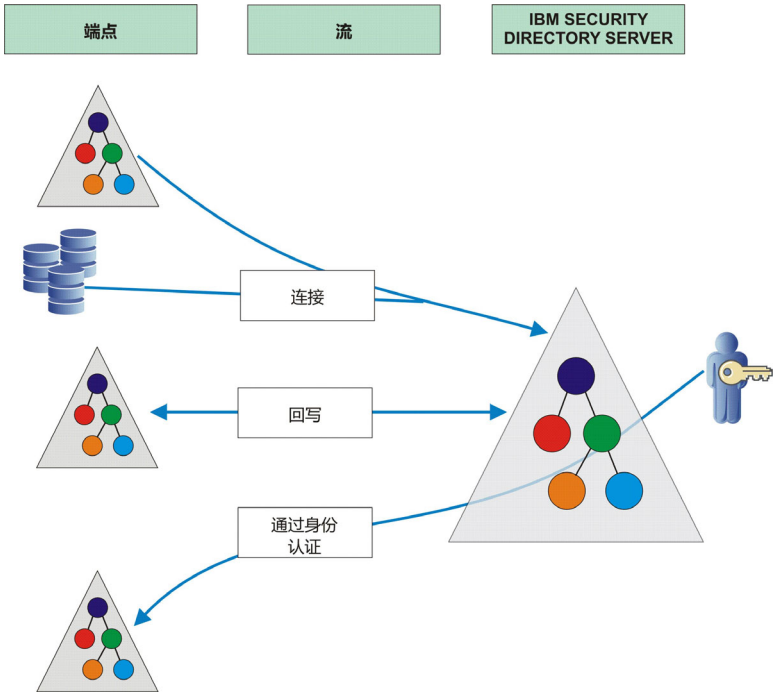


图 1. 联合目录服务器 组件

目录服务器

IBM Security Directory Server，项目中所有流的目标。

端点 已配置的可提供流中数据的源系统。当前可用的端点类型为 Active Directory、定制组装流水线、文件、JDBC、LDAP、IBM Security Directory Server 和 Sun Directory。

流量 定义端点和目标 IBM Security Directory Server 之间的关系的配置。只有在配置目标目录服务器连接设置并添加一个或多个端点之后，才必须创建流。

属性映射

一种映射，用于将源模式中的属性转换为目标模式中相应的属性。在联合目录服务器 中，您可以将其中一个随时可用属性映射或定制属性映射应用于流操作。

连接 已配置的源系统，提供可扩充并增加端点中的数据的数据。如果将流配置为指定与端点的连接，那么会使用以下方法处理条目：

1. 从端点读取一个条目。
2. 流在连接数据源中查询条目。
3. 条目与来自端点的数据进行合并。

4. 合并数据已添加至目标目录服务器。

传递认证

IBM Security Directory Server 的功能部件，可在其中通过对不同 LDAP 服务器指定认证来对用户进行认证。当为流启用传递认证时，它会将 IBM Security Directory Server 配置为将存储在端点中的凭证用于认证源自该流的用户。

入门路线图

使用路线图可以了解设置“联合目录服务器”配置的关键任务和运行同步操作。

表 1. “联合目录服务器”入门路线图

关键步骤	可选或高级任务
黎阿姐关键概念、组件和体系结构。	
访问“联合目录服务器”控制台。	配置访问控制台的安全设置。
连接到目标目录服务器。	定义源端点和目标目录服务器之间的定制属性映射。 为目录服务器指定日志设置。
添加端点并为它们配置以下一个或多个数据源: • LDAP • Active Directory • IBM Security Directory Server • Sun Directory • JDBC • 文件和文件解析器 • 慈宁宫只组装流水线 (AL)	配置传递认证以便将认证委派回端点。
创建用于定义端点和目标目录之间的关系的流。	
定义流设置。	扩展指定流的定制属性映射。 配置用于有选择地从数据源增加数据的连接。 启用回写以便将对目标目录服务器作出的更改传播回端点。
通过运行模拟同步操作验证流配置。	
运行初始同步将数据迁移到目标目录。	
调度定期增量同步。	手动运行同步操作。
对流启用和配置监视	
使用日志和报告对流配置和同步操作进行故障诊断。	检查已知问题和限制来解决指定的问题。

访问 联合目录服务器控制台

可以在浏览器中访问基于 Web 的 联合目录服务器控制台 应用程序。

开始之前

安装 IBM Security Directory Integrator V7.2 并应用最新修订包。

关于此任务

- 安装 IBM Security Directory Integrator 时，会将联合目录服务器工件和配置文件安装到 *tdi_install_dir*/LDAPSync 目录中。
- 首次启动 联合目录服务器控制台 时:
  1. 将填充 *sdi_solution_dir*/LDAPSync 目录。
  2. 缺省配置文件 LDAPSync.xml 将复制到 *sdi_solution_dir*/configs 文件夹中。
- 对于未来的更新，必须将 LDAPSync.xml 配置文件从 *sdi_solution_dir*/LDAPSync 手动复制到 *sdi_solution_dir*/configs。

过程

1. 从系统的启动界面，或者从命令行使用 **ibmditk** 或 **ibmdisrv** 命令启动 IBM Security Directory Integrator。

   注:

   - IBM Security Directory Integrator 服务器 (ibmdisrv) 必须处于活动状态，这样您才能继续操作。如果您已将配置编辑器的缺省属性修改为不启动 IBM Security Directory Integrator 服务器，那么下一个步骤将失败。
2. 打开联合目录服务器控制台。
   - 如果正在访问本地系统中的联合目录服务器，请单击**开始 > 程序 > IBM Security Directory Integrator 7.2 > 联合目录服务器控制台**。
   - 如果正在访问远程系统上的联合目录服务器，请在浏览器中打开以下链接:

     https://*hostname*:1098/fds

   注: 虽然 1098 是缺省端口号，但是您必须使用 IBM Security Directory Integrator 安装期间您为 **REST API 端口**字段输入的值。
3. 如果用于访问 联合目录服务器控制台 的安全设置指示必须进行认证，那么将显示登录屏幕。
   - 如果正在 localhost 上访问，请将用户名和密码分别指定为 admin 和 admin（缺省值），然后单击**登录**。
   - 缺省情况下，将拒绝远程访问。如果您希望允许从远程系统进行访问，那么必须根据管理员所指定的安全设置来指定相应的认证凭证。有关更多信息，请参阅第 7 页的『安全设置』。

下一步做什么

对于联合目录服务器，请完成下列步骤:

1. 连接到目标目录服务器。
2. 配置一个或多个端点。
3. 定义流设置。

注: 当在控制台中配置各种联合目录服务器功能时，缺省情况下将自动保存更改。要修改控制台的缺省自动保存和刷新设置，请完成下列步骤:

1. 在联合目录服务器控制台菜单栏上，单击**选项**。

2. 如果想要手动保存在控制台中作出的配置更改，请清除**启用自动保存**复选框。
3. 如果不想自动重新装入配置更改，请清除**当保存配置时自动更新 FDS** 复选框。
4. 要创建当前配置的快照，请指定**快照描述**，然后单击**创建快照**。
5. 可以稍后将更改回滚到创建快照时的级别。在**装入快照**中选择快照，然后单击**装入**。

安全设置

对 联合目录服务器控制台 的访问权由指定安全设置的一组属性控制。

必须在 IBM Security Directory Integrator 解决方案目录的 solution.properties 文件中指定安全设置。这些属性控制对所有 IBM Security Directory Integrator Web 应用程序（例如，仪表板、REST API 和联合目录服务器控制台）的访问权。

系统通过传入访问请求中的客户机 IP 地址来区分本地和远程用户:

- 如果 IP 地址属于正在运行 IBM Security Directory Integrator 的系统上的某一个网卡，那么会将其视为 localhost 用户。
- 会将所有其他 IP 地址都视为远程用户。

对 localhost 用户的访问许可权是内置的，并且凭证如下:

用户名: admin

密码: admin

要指定访问控制权和访问权，可以设置或修改以下认证属性:

dashboard.auth=true

指示是否要求用户进行认证。

有效值为 true（如果要求用户进行认证）或 false（如果无需任何认证）。

dashboard.auth.localhost

指示来自 localhost 的连接必须使用的认证类型。

有效值为:

- properties，指定必须使用基于属性的认证。
- none，指定不需要进行认证。
- deny，指定拒绝所有来自 localhost 的连接。
- ldap，指定通过登录 LDAP 服务器并选择性地验证组成员资格来进行认证。

dashboard.auth.remote

指示远程连接必须使用的认证类型。

有效值为:

- properties，指定必须使用基于属性的认证。
- none，指定不需要进行认证。
- deny，指定拒绝所有远程连接进行访问，即拒绝所有不是来自 localhost 的连接进行访问。
- ldap，指定通过登录 LDAP 服务器并选择性地验证组成员资格来进行认证。

{protect}-dashboard.auth.user.*username*=*password*

指定用于远程访问的用户凭证。

缺省用户名为 admin，密码为 admin:

```
{protect}-dashboard.auth.user.admin=admin
```

要指定多个联合目录服务器用户登录帐户，请参阅以下示例:

```
{protect}-dashboard.auth.user.admin=admin
{protect}-dashboard.auth.user.user1=user1passwd
{protect}-dashboard.auth.user.user2=user2passwd
```

dashboard.auth.ldap.url

指定用于对用户进行认证的 LDAP 服务器地址。仅当您指定了 ldap 作为认证机制时才会使用此属性。

按以下格式输入 LDAP 主机名、端口号以及可选的搜索基础:

ldap://*host*:*port* [/*search-base*]

例如:

```
ldap://localhost:10389/ou=system
```

如果用户在用户名输入字段中提供了电子邮件地址，那么 IBM Security Directory Integrator 首先会在从中抽取专有名称 (DN) 的 LDAP 服务器中搜索唯一条目。否则，LDAP 服务器应该能够接受所提供的值。IBM Security Directory Integrator 从用户那里获取用户名的 DN 和密码之后，将使用该 DN 和密码进行 LDAP 基本认证。

dashboard.auth.ldap.url.group

指定用于对经过认证的用户的组成员资格进行验证的 LDAP 服务器地址。仅当您指定了 ldap 作为认证机制时才会使用此属性。

按以下格式输入 LDAP 主机名、端口号以及可选的搜索基础:

ldap://*host*:*port* [/*search-base*]

例如:

```
ldap://localhost:389/cn=group1,ou=groups,ou=system
```

如果指定了此属性，那么根据 LDAP 存储库认证用户凭证之后，还将执行一个附加的认证步骤。该步骤先检查所认证的用户是否还是所指定组的成员，然后再允许进行访问。

还可以在 IBM Security Directory Integrator“仪表板”图形用户界面中配置这些属性。在“仪表板”窗口中，单击**操作 > 显示服务器详细信息 > 安全性和连接**。有关更多信息，请参阅 IBM Security Directory Integrator 文档并搜索*配置“仪表板”安全设置*。

用于进行远程访问的 Internet Explorer 设置

添加所需的配置设置，以便通过启用了 Internet Explorer 增强的安全配置 (IE ESC) 的 Internet Explorer 浏览器从远程系统访问联合目录服务器控制台。

缺省情况下，IE ESC 将阻止 Web 页面上运行的所有脚本。联合目录服务器将先装入多个脚本，然后才在控制台上显示内容。因此，您打开控制台时，启用了 IESC 的 Internet Explorer 浏览器将显示空白页面。要访问此页面，必须将托管联合目录服务器的站点添加到 Internet Explorer 的安全列表中。

1. 在 **Internet Explorer** 菜单中，单击**工具 > Internet 选项**。
2. 单击**安全**选项卡。

3. 单击**受信任的站点**。
4. 单击**站点**。
5. 在**将该网站添加到区域**字段中，输入联合目录服务器控制台的 URL。例如: `https://myfds.com/fds/*`。
6. 单击**添加**。
7. 单击**关闭**，然后单击**确定**以关闭页面并保存设置。
8. 重新启动 Internet Explorer 浏览器。
9. 在 Internet Explorer 浏览器中访问联合目录服务器控制台。

连接到 IBM Security Directory Server

IBM Security Directory Server 是 联合目录服务器 的缺省核心集中式存储库。要使用其从一个或多个源系统到目标目录服务器的同步服务，必须为联合目录服务器控制台中的目标 IBM Security Directory Server 定义连接参数。

过程

1. 在联合目录服务器控制台导航窗格中的**目录服务器**下方，单击**连接设置**。
2. 在**连接设置**页面的 **LDAP URL** 下方，输入目标 IBM Security Directory Server 的**主机名**和**端口**。
3. 对于安全连接，请选择 **SSL**。
4. 在**用户登录名**和**密码**字段中，输入用于向 IBM Security Directory Server 进行认证的专有名称和凭证。
5. 在**缺省目标容器**中，指定用于存储同步数据的目标 IBM Security Directory Server 中的容器。稍后，在创建流时，可以为每个方案指定另一个目标容器。
6. 在下一个字段中，还可以指定必须视为二进制的属性（比如 **jpegPhoto**）的列表。格式为每一行一个属性名称。
7. 请确保连接成功。单击**测试连接**。端点名称旁边显示的绿色勾选标记表明连接成功。
8. 要查看目标目录服务器中的条目，请单击**浏览数据**。您可以使用此功能来浏览目录条目以及添加、删除或修改这些条目。

下一步做什么

请参阅『浏览目录条目』。

相关信息:

安全套接字层 (SSL) 支持

浏览目录条目

使用目录浏览器可以查看目标 IBM Security Directory Server 中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

开始之前

确保您可以成功地从联合目录服务器连接到目标 IBM Security Directory Server。**连接设置**链接旁边显示的绿色勾选标记表明连接成功。如果连接不成功，那么**浏览目录**链接将处于禁用状态。

过程

1. 在联合目录服务器控制台上的**目录服务器**下方，单击**浏览目录**。另外，您还可以从目录服务器的“连接设置”页面中访问同一浏览器。
2. 单击**搜索**将在指定的**搜索起点**下搜索包含您输入的**搜索文本**的条目。
3. 单击**选择**并选择下列其中一个选项:
   - 要从目录服务器树的根开始进行浏览，请单击**从根浏览**。
   - 要从通过连接设置指定的缺省目标容器开始进行浏览，请单击**浏览端点搜索起点**。
4. 单击条目以查看其属性。 这将仅显示填充了值的属性。
5. 要显示所有适用于该条目的对象类的属性，而不考虑这些属性是否具有值，请选择**显示所有属性**。 这将在**必需属性**和**可选属性**这两个部分中显示这些属性。
6. 您可以添加、修改或删除条目。

   添加条目

   单击**操作 > 添加**。

   从显示的列表中选择实体类型。

   单击**确定**。

   修改属性的值

   在目录树导航窗格中单击条目。

   在显示的属性和值的表中，双击值并对其进行编辑。

   单击**保存**。在窗格标题中，将显示已修改条目消息。

   删除条目

   在目录树导航窗格中单击条目。

   单击**删除**。

   单击**确定**。
7. 可选: 测试对目录服务器的访问。
   a. 单击**登录测试**。
   b. 输入密码以验证凭证。

启用或禁用全局回写

使用全局回写选项可以指定是否必须将目标目录服务器中进行的更改传播回到源端点。

关于此任务

全局回写选项是一项安全功能，您可以将其禁用以便对所有的流关闭回写。但是，如果要选择性地对特定的流启用回写，必须使此全局回写选项保持启用状态。然后，使

用每个流配置中的回写选项来指定对于特定的流是启用还是禁用回写。请参阅第 31 页的『启用对流的回写』。

过程

1. 要启用全局回写功能，请在“目录服务器”下方单击**回写**，然后选择**启用回写**。**回写**旁边会显示一个绿色的刻度标记。
2. 选中**忽略 FDS 进行的更改**，以指示您不希望回写操作处理由 IBM Security Directory Server 连接设置中指定的用户修改的条目。

   示例:

   连接设置中指定的用户为 `cn=root`。

   如果未选中**忽略 FDS 进行的更改**，那么用户 `cn=root` 进行的所有更改都将回写到源端点。这将排除由联合目录服务器流操作进行的更改。

结果

完成回写操作后，将显示有关回写到端点的内容的摘要。摘要包括详细信息，例如流名称、已修改的属性以及目录服务器 DN 和端点 DN。可以使用**过滤器**字段来搜索回写摘要。

配置传递认证

使用传递认证功能可以在认证凭证不存在于目标 IBM Security Directory Server 中时，将认证委派回给端点进行。

开始之前

- 对 IBM Security Directory Server 进行传递认证配置。请参阅 IBM Security Directory Server 文档。
- 验证从联合目录服务器到目标 IBM Security Directory Server 的连接。在**目录服务器**下方，**连接设置**链接旁边的绿色勾选标记表明连接成功。如果连接不成功，那么**传递认证**链接将处于禁用状态。

关于此任务

传递认证是 IBM Security Directory Server 的一项可选功能，此功能将用户认证工作委派给其他 LDAP 服务器执行。使用此功能仅将认证凭证保留在端点中，而不会保留在目标 IBM Security Directory Server 中。如果配置了传递认证，那么 IBM Security Directory Server 将尝试代表客户机验证来自外部 LDAP 目录服务器的凭证。

过程

1. 在导航窗格中的**目录服务器**下，单击**传递认证**。
2. 单击**添加**，并指定**名称**以标识此配置。
3. 在**目标子树**字段中，指定 IBM Security Directory Server 目标子树。将仅对该目标子树的容器中的用户启用传递认证。
   - 单击**选择**以查看该子树并指定容器。
   - 单击**浏览数据**，以便在目标目录服务器中添加条目以及查看、删除或修改其中的条目。

4. 从**选择要从中复制连接详细信息的端点**列表中选择端点。这些详细信息根据您创建该端点时指定的连接参数进行自动填充。
5. 可选: 必要时，请编辑**主机名**、**端口**、**搜索起点**、**用户名**和**密码**字段。
6. 单击**测试连接**，以验证用于传递认证的连接设置。
7. 执行下列其中一项操作:
   - 单击**保存**，以便对此配置所影响的流启用传递认证机制。受影响的流是目标搜索起点匹配或者位于传递认证配置中指定的搜索起点的容器层次结构之下的一个或多个流。
   - 如果您不希望对受影响的流启用传递认证，请单击**删除**。
8. 手动重新启动 IBM Security Directory Server，以使更改生效并对受影响的流启用传递认证。

相关任务:

第 9 页的『浏览目录条目』

使用目录浏览器可以查看目标 IBM Security Directory Server 中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

指定日志设置

在配置了 IBM Security Directory Server 的连接设置之后，可以指定日志文件的路径和日志设置。

过程

1. 在导航窗格中的**公共设置**下方，单击**日志设置**。
2. 在**日志目录**字段中，请指定日志文件的路径。缺省路径为 `LDAPSync/logs`。

   注:
   - 您可以指定 IBM Security Directory Integrator 的解决方案目录或当前工作目录的相对路径。
   - 可以使用正斜杠，以便同时适用于 Windows 和 UNIX 系统。
3. 在**日志文件历史记录**字段中指定必须保留的先前日志文件的数目。缺省值为 `20`。

下一步做什么

将一个或多个数据资源配置为端点。请参阅以下有关配置不同端点类型的步骤的主题。

定制属性映射

从多个源联合数据时，在将属性与单个目标目录同步时，必须正确映射这些属性。可通过为属性定义定制映射来指定如何将属性从源端点模式转换为目标模式。

关于此任务

系统已内建了标准模式（例如，Active Directory 和 Sun Directory）的属性映射。此外，联合目录服务器 中还提供了一些现成可用的定制映射。但是，在某些情况下，您可能需

要修改或扩展这些属性映射或者创建新的定制映射。例如，如果将数据库或文件用作端点时，可能需要定制映射。

过程

1. 在导航窗格中的**公共设置**下方，单击**属性映射**。“属性映射”页面将显示人员对象、组对象和容器对象的各种属性映射。这些映射是现成可用的映射文件，它们位于 *sdi_solution_dir*/LDAPSync 目录中。
2. 从列表中选择要定制的属性映射的类型。 这将显示属性映射表。
3. 您可以执行下列任意操作:

   创建属性映射

   a. 单击**添加属性**。
   b. 从目标目录服务器的属性列表中选择属性。这将显示新的一行，并且选定的属性名显示在**目录服务器属性**中。

      注: 如果“添加属性”窗口未显示目标目录中的属性列表，请执行下列操作:

      1) 在导航窗格中的**目录服务器**下方，转到**连接设置**。
      2) 单击**测试连接**。确保端点名称旁边显示了绿色勾选标记，这表明连接成功。此操作还将填充用于浏览目标目录属性的字段。

   c. 在**端点属性/分配**下方，双击缺省值以更改该映射，并为该属性映射指定更多设置。
   d. 选中**已启用**以使用端点的此属性映射。
   e. 单击**简单分配**或**脚本化分配**指定映射的类型。

      注: 如果选中了**脚本化分配**，那么可以通过编写 JavaScript 代码或调用 *sdi_solution_dir*\LDAPSync\customScript.js 文件中的函数来定义分配。有关更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“IBM Security Directory Integrator 中的脚本编制”。

   f. 在**映射场合**下方，指定是要将此映射用于所有操作，还是只想在修改条目或创建条目时使用此映射。
   g. 在**选择属性**字段中，指定源端点中必须映射到目标属性的属性名。

   删除特定属性的映射

   a. 选中该属性旁的复选框。
   b. 单击**除去属性**。
   c. 单击**确定**。

   复制映射以便使用您自己的定制属性映射对其进行扩展。

   a. 单击**复制映射**。
   b. 为新映射文件输入名称。
   c. 单击**确定**。

   此时将创建具有源映射的所有属性映射条目的新属性映射。

   删除属性映射及其所有条目

   a. 单击**删除映射**。
   b. 单击**确定**。

4. 单击**保存**。除非保存每个已编辑的映射，否则更改将会丢失。

结果

所有属性映射都存储在 *sdi_solution_dir*/LDAPSync 目录中。

下一步做什么

在定义流规范时，您可以为流操作选择此定制属性映射。

配置端点

必须指定端点用于与目标 IBM Security Directory Server 同步。可以将多个 LDAP 目录、数据库、文件或者甚至是子树配置为联合目录服务器控制台中的端点。

开始之前

请确保为目标 IBM Security Directory Server 指定连接设置。请参阅第 9 页的『连接到 IBM Security Directory Server』。

过程

1. 要指定新的端点，请在导航窗格的“端点”部分单击**添加**。 将显示**添加端点**窗口。
2. 在**名称**字段中，输入一个用于识别端点的名称。
3. 在**选择端点类型**列表中，选择相应的端点类型。 提供了以下类型的端点:
   - Active Directory
   - 定制组装流水线
   - 文件
   - JDBC
   - LDAP
   - Sun Directory
   - Security Directory Server

   注: 在为指定的端点类型创建了配置页面之后就无法更改了。必须先删除，然后为想要配置的端点类型再次创建端点。

结果

将显示包含端点参数的配置页面，每个端点类型的参数都不同。

在导航窗格中，将在每个端点的旁边显示状态图标。可以单击**刷新**以查看最新的状态。

- 在创建了端点之后将马上显示一个绿点，并且直到在端点中单击**测试连接**后才消失。
- 经测试连接成功之后，绿色的刻度标记将替换这个绿点。
- 如果连接失败了，将显示红色的十字标记。

下一步做什么

为端点配置参数。请参阅以下有关不同端点类型的主题。

如果想要删除已创建并配置好的端点，请执行以下步骤:

1. 在导航窗格的**端点**部分，右键单击想要删除的端点名称，然后单击**删除**。
2. 当显示确认消息时，单击**确定**。

注: 基于端点的流会在删除端点时自动被删除。

配置 Active Directory 端点

要将 Active Directory 配置为端点，必须指定 LDAP URL、具有凭证的登录名、搜索基础和根后缀。

开始之前

确保创建了一个端点，并且将类型指定为 **Active Directory**。请参阅第 14 页的『配置端点』。

过程

1. 在 Active Directory 端点配置页面的 **LDAP URL** 下方，输入要访问的 Active Directory 的**主机名**和**端口**。缺省 LDAP 端口号为 389。如果您使用的是 SSL，那么缺省 LDAP 端口号为 636。 有关为 Active Directory 连接设置 SSL 的信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“Microsoft Active Directory SSL 配置”。
2. 对于受保护连接，请选择 **SSL**。
3. 在**用户登录名**和**密码**字段中，输入用于向服务进行认证的专有名称和凭证。

   例如: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 在**包括以下容器的条目**字段中，输入为了同步而读取的条目所属的源目录的搜索基础。或者，也可以单击**上下文**并从 **LDAP 搜索基础**列表中进行选择，然后单击**确定**。

   例如: `dc=your_domain,dc=com`

   注: 对于 Active Directory，此值必须设置为域控制器的根后缀；否则，不会检测“删除修改”。
5. 要验证 Active Directory 连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。
6. 配置端点后，要轻松访问目录中的数据，请单击**浏览数据**。您可以使用 LDAP 浏览器来查看目录层次结构以及用户、组和容器的类型。另外，还可以在此目录中添加、修改或删除条目。有关 LDAP 浏览器的更多信息，请参阅第 22 页的『浏览 LDAP 目录中的条目』。
7. 可选: 还可以配置以下高级参数。展开**高级**部分可查看这些参数。

   页面大小

   指定请求在每一页必须返回的条目数。缺省值为 500。

超时之前等待的秒数

指定等待下一个更改的 Active Directory 对象的最大秒数。缺省值为 0。

两次轮询之间的秒数

指定连续两次轮询之间相隔的休眠秒数。缺省值为 60。

更改状态键

指定用于存储更改检测迭代器状态的键或参数的名称。状态键用于在两次运行之间记住已处理的最后一次更改。如果同步由于任何原因而停止了，那么可以从停止的位置开始。

此关键字的值必须对于每个端点来说是唯一的。如果您未设置此参数，那么会自动计算一个值以确保唯一性。

二进制属性

指定必须解释为二进制值而非字符串的属性的列表。当您在此字段中输入属性名称时，请在每一行输入一个属性，并且不要使用任何分隔符。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

配置定制组装流水线端点

可以将之前在配置编辑器中创建的组装流水线指定为联合目录服务器中的端点。

开始之前

- 使用配置编辑器来创建组装流水线。请确保将组装流水线项目的配置 XML 文件复制到 *sdi_solution_dir*/configs 中。有关更多信息，请参阅 IBM Security Directory Integrator 文档并搜索*配置编辑器*。
- 在联合目录服务器控制台中，确保创建了一个端点并且将类型指定为**定制组装流水线**。请参阅第 14 页的『配置端点』。

过程

1. 在“定制组装流水线”端点配置页面上的 **SDI 项目配置名称**字段中，输入为包含组装流水线的项目定义的解决方案实例的名称。缺省情况下，解决方案实例名称与项目本身的名称相同。
2. 在下列字段中，指定必须用于处理每种条目的组装流水线:
   - **用于读取人员条目的 AL**
   - **用于读取组条目的 AL**
   - **用于读取容器条目的 AL**

   必须输入在配置编辑器中创建的组装流水线项目的以下详细信息:
   - 包含了组装流水线的 IBM Security Directory Integrator 项目的名称
   - 组装流水线的名称

   请使用以下格式:

   Project Name:/AssemblyLines/*AssemblyLine Name*

   例如，如果项目名为 OS400 并且包含了一个名为 ReadUsers 的组装流水线，那么可输入:

OS400:/AssemblyLines/ReadUsers

3. 要验证定制组装流水线端点连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

配置文件端点

要将文件配置为端点，必须指定文件路径、条目类型和文件解析器。

开始之前

确保创建了一个端点，并且将类型指定为**文件**。请参阅第 14 页的『配置端点』。

过程

1. 在文件端点配置页面的**文件路径**字段中，输入想要访问的文件路径。
2. 从**条目类型**列表中选择人员、组或容器。
3. 要验证文件连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。
4. 可选: 还可以配置以下高级参数。展开**高级**部分可查看这些参数。

   超时（以秒计）

   指定一个正数以指定两次操作之间等待的秒数，超过该时间将发生超时。

   指定 0（零）表示永久等待。

   如果您选择**锁定文件**选项，那么**超时**值将改为指定用于等待获取锁定的时间长度。

   锁定文件

   选择此选项以指定获取互斥锁定用于对文件进行写入。此锁定可防止其他 联合目录服务器 实例或任何其他程序打开该文件进行写入，直到锁定释放为止。

5. 从**解析器**列表中，选择访问文件时所需的解析器的名称。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

相关概念:

第 39 页的『文件解析器』

可以从联合目录服务器控制台的文件端点配置页面所提供的列表中选择并配置相应的文件解析器。

配置 JDBC 端点

要将 JDBC 连接配置为端点，必须指定 JDBC URL、用户名和密码、模式、表名和条目类型。

开始之前

确保创建了一个端点，并且将类型指定为 **JDBC**。请参阅第 14 页的『配置端点』。

过程

1. 在 JDBC 端点配置页面的 **JDBC URL** 下方，从**类型**列表中选择数据库类型。选项如下所示:
   - 选择常用数据库。
     a. 从列表中选择下列其中一种数据库: DB2、Derby、嵌入式 Derby、solidDB、Microsoft SQL 或 Oracle。
     b. 有需要时，请指定**数据库**的**主机名**、**端口**和名称。
   - 选择通用数据库。
     a. 选择 JDBC 详细信息。
     b. 在 **JDBC URL** 字段中，输入要访问的数据库的 JDBC 连接 URL。以下示例是各种 JDBC 提供程序的一些典型 URL:

        Informix®

        ```
        jdbc:informix-sqli://hostname:port/
        dbname:informixserver=Informix Server Name
        ```

        Sybase

        ```
        jdbc:sybase:Tds:hostname:port/
        ```

     c. 在 **JDBC 驱动程序**字段中，输入 JDBC 驱动程序实现类名。以下示例是各种 JDBC 提供程序的一些典型驱动程序实现类名:

        Informix

        ```
        com.informix.jdbc.IfxDriver
        ```

        Sybase

        ```
        com.sybase.jdbc3.jdbc.SybDriver
        ```

        有关 JDBC 驱动程序的更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索*"了解 JDBC 驱动程序"*。
2. 在**用户名**和**密码**字段中，输入用于访问所指定数据库的登录名和密码。
3. 从**表名**列表中，选择要操作的表或视图。此列表显示了所指定数据库中的表。
4. 从**条目类型**列表中选择人员、组或容器。
5. 要验证 JDBC 连接设置，请单击**测试连接**。

   端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。您可以使用此窗格来浏览记录以及按属性名进行**过滤**。
6. 可选: 还可以指定定制 SELECT 语句来指定操作的条目。
   a. 展开**高级**部分。
   b. 在**定制 Select** 字段中输入语句。
7. 可选: 在**其他提供程序参数**字段中，输入 JDBC 提供程序所支持的其他必需参数。
   a. 请使用 name:value 格式并且每行输入一个参数。
   b. 检查驱动程序文档以了解受支持的参数。
   c. 例如，下列附加参数特定于 DB2:

```
securityMechanism:KERBEROS_SECURITY
loginTimeout:20
readOnly:true
```

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

配置 LDAP 端点

要将 LDAP 目录配置为端点，必须指定 LDAP URL、具有凭证的登录名、搜索基础和根后缀。

开始之前

确保创建了一个端点，并且将类型指定为 **LDAP**。请参阅第 14 页的『配置端点』。

过程

1. 在 LDAP 端点配置页面的 **LDAP URL** 下方，输入要访问的 LDAP 目录的**主机名**和**端口**。缺省 LDAP 端口号为 389。如果您使用的是 SSL，那么缺省 LDAP 端口号为 636。
2. 对于受保护连接，请选择 **SSL**。
3. 在**用户登录名**和**密码**字段中，输入用于向服务进行认证的专有名称和凭证。

   例如: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 在**包括以下容器的条目**字段中，输入为了更改而轮询的 LDAP 目录中的搜索基础。或者，也可以单击**上下文**并从 **LDAP 搜索基础**列表中进行选择，然后单击**确定**。

   例如: `dc=your_domain,dc=com`
5. 要验证 LDAP 目录连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。
6. 配置端点后，要轻松访问目录中的数据，请单击**浏览数据**。您可以使用 LDAP 浏览器来查看目录层次结构以及用户、组和容器的类型。另外，还可以在此目录中添加、修改或删除条目。
7. 可选: 还可以配置以下高级参数。展开**高级**部分可查看这些参数。

   二进制属性

   指定必须解释为二进制值而非字符串的属性的列表。当您在此字段中输入属性名称时，请在每一行输入一个属性，并且不要使用任何分隔符。

   页面大小

   指定请求在每一页必须返回的条目数。缺省值为 500。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

相关信息:

第 22 页的『浏览 LDAP 目录中的条目』
使用目录浏览器可以查看端点中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

配置 Sun Directory 端点

要将 Sun Directory 配置为端点，必须指定 LDAP URL、具有凭证的登录名、搜索基础和根后缀。

开始之前

确保创建了一个端点，并且将类型指定为 **Sun Directory**。请参阅第 14 页的『配置端点』。

过程

1. 在 Sun Directory 端点配置页面的 **LDAP URL** 下方，输入要访问的 Sun Directory 服务的**主机名**和**端口**。缺省 LDAP 端口号为 389。如果您使用的是 SSL，那么缺省 LDAP 端口号为 636。
2. 对于受保护连接，请选择 **SSL**。
3. 在**用户登录名**和**密码**字段中，输入用于向服务进行认证的专有名称和凭证。

   例如: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 在**包括以下容器的条目**字段，输入为了更改而轮询的 Sun Directory 中的搜索基础。或者，也可以单击**上下文**并从 **LDAP 搜索基础**列表中进行选择，然后单击**确定**。

   例如: `dc=your_domain,dc=com`
5. 要验证 Sun Directory 连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。
6. 配置端点后，要轻松访问目录中的数据，请单击**浏览数据**。您可以使用 LDAP 浏览器来查看目录层次结构以及用户、组和容器的类型。另外，还可以在此目录中添加、修改或删除条目。
7. 可选: 还可以配置以下高级参数。展开**高级**部分可查看这些参数。

   超时之前等待的秒数

   指定等待下一个更改的 Sun Directory 对象的最大秒数。缺省值为 0。

   两次轮询之间的秒数

   指定连续两次轮询之间相隔的连接器休眠秒数。缺省值为 60。

   更改状态键

   指定用于存储更改检测迭代器状态的键或参数的名称。状态键用于在两次运行之间记住已处理的最后一次更改。如果同步由于任何原因而停止了，那么可以从停止的位置开始。

   此关键字的值必须对于每个端点来说是唯一的。如果您未设置此参数，那么会自动计算一个值以确保唯一性。

   二进制属性

   指定必须解释为二进制值而非字符串的属性的列表。当您在此字段中输入属性名称时，请在每一行输入一个属性，并且不要使用任何分隔符。

   页面大小

   指定请求在每一页必须返回的条目数。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

相关信息:

第 22 页的『浏览 LDAP 目录中的条目』
使用目录浏览器可以查看端点中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

配置 IBM Security Directory Server 源端点

要将 IBM Security Directory Server 配置为端点，必须指定 LDAP URL、具有凭证的登录名、搜索基础和根后缀。

开始之前

确保创建了一个端点，并且将类型指定为 **IBM Security Directory Server**。请参阅第 14 页的『配置端点』。

过程

1. 在 IBM Security Directory Server 源端点配置页面的 **LDAP URL** 下方，输入要访问的 IBM Security Directory Server 的**主机名**和**端口**。缺省 LDAP 端口号为 389。如果您使用的是 SSL，那么缺省 LDAP 端口号为 636。
2. 对于受保护连接，请选择 **SSL**。
3. 在**用户登录名**和**密码**字段中，输入用于向服务器进行认证的专有名称和凭证。

   例如: `cn=root`
4. 在**包括以下容器的条目**字段中，输入为了更改而轮询的目录服务器搜索基础。或者，也可以单击**上下文**并从 **LDAP 搜索基础**列表中进行选择，然后单击**确定**。

   例如: `o=sample`
5. 要验证 IBM Security Directory Server 连接设置，请单击**测试连接**。 端点名称旁边显示的绿色勾选标记表明连接成功。如果连接成功，那么将在单独的窗格中显示端点中的属性。可以使用**过滤器**字段搜索属性。
6. 配置端点后，要轻松访问目录中的数据，请单击**浏览数据**。您可以使用 LDAP 浏览器来查看目录层次结构以及用户、组和容器的类型。另外，还可以在此目录中添加、修改或删除条目。
7. 可选: 还可以配置以下高级参数。展开**高级**部分可查看这些参数。

   超时之前等待的秒数

   指定等待下一个更改的目录服务器对象的最大秒数。缺省值为 0。

   两次轮询之间的秒数

   指定连续两次轮询之间相隔的休眠秒数。缺省值为 60。

   更改状态键

   指定用于存储更改检测迭代器状态的键或参数的名称。状态键用于在两次运行之间记住已处理的最后一次更改。如果同步由于任何原因而停止了，那么可以从停止的位置开始。

   此关键字的值必须对于每个端点来说是唯一的。如果您未设置此参数，那么会自动计算一个值以确保唯一性。

二进制属性

指定必须解释为二进制值而非字符串的属性的列表。当您在此字段中输入属性名称时，请在每一行输入一个属性，并且不要使用任何分隔符。

页面大小

指定请求在每一页必须返回的条目数。

下一步做什么

在配置了端点之后，可以创建流来定义端点和目标目录服务器之间的关系。

相关信息:

『浏览 LDAP 目录中的条目』

使用目录浏览器可以查看端点中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

浏览 LDAP 目录中的条目

使用目录浏览器可以查看端点中的目录层次结构以及用户、组和容器的类型。另外，还可以验证是否正确地传输了数据以及添加、修改或删除条目。

开始之前

确保您可以成功地从联合目录服务器连接到端点目录。**端点**下方端点名称旁边显示的绿色勾选标记表明连接成功。如果连接不成功，那么您尝试浏览数据时，将显示错误。

关于此任务

此功能仅适用于 LDAP 目录。可以在联合目录服务器中配置的 LDAP 端点包括 Active Directory、LDAP、Sun Directory 和 IBM Security Directory Server。

过程

1. 在端点配置屏幕上，单击**浏览数据**。
2. 单击**搜索**将在指定的**搜索起点**下搜索包含您输入的**搜索文本**的条目。
3. 单击**选择**并选择下列其中一个选项:
   - 要从目录树的根开始进行浏览，请单击**从根浏览**。
   - 要从端点配置中指定的搜索起点开始进行浏览，请单击**浏览端点搜索起点**。
4. 单击条目以查看其属性。 这将仅显示填充了值的属性。
5. 要显示所有适用于该条目的对象类的属性，而不考虑这些属性是否具有值，请选择**显示所有属性**。 这将在**必需属性**和**可选属性**这两个部分中显示这些属性。
6. 您可以添加、修改或删除条目。

   添加条目

   单击**操作 > 添加**。

   从显示的列表中选择实体类型。

   单击**确定**。

   修改属性的值

   在目录树导航窗格中单击条目。

在显示的属性和值的表中，双击值并对其进行编辑。

单击**保存**。在窗格标题中，将显示已修改条目消息。

删除条目

在目录树导航窗格中单击条目。

单击**删除**。

单击**确定**。

7. 可选: 测试对目录服务器的访问。
   a. 单击**登录测试**。
   b. 输入密码以验证凭证。

创建流

创建定义端点和目标 IBM Security Directory Server 之间的关系的流。

开始之前

- 连接到目标目录服务器。
- 配置一个或多个端点。

过程

1. 单击**流**选项卡以查看“流”页面。
2. 在“流”页面中，单击**添加**。
3. 在“添加流”窗口中，指定流的**“名称”**。
4. 在**选择端点**列表中，选择某个已配置的端点为流提供数据。
5. 单击**确定**以创建流。

下一步做什么

编辑流以定义流设置。

定义流设置

在创建了一个流之后，可以编辑该流来定义设置或使用为大多数设置提供的缺省值。

开始之前

创建流。

过程

1. 要指定或修改流设置，请在**流**页面上单击流名称，然后单击**编辑**。 将打开选定流的配置页面。可以在**源**选项卡上查看并编辑流设置。
2. 要更改端点，请在**源**列表中选择某个已配置的端点为流提供数据。
3. 可以指定分组到以下类别中流设置:

   常规设置

   要处理的条目类别

   选择必须考虑为流操作使用的条目类型。

缺省情况下，将同时选中**处理个人条目**和**处理组条目**的选项。

在 Directory Server 中创建源层次结构的镜像

指定在同步期间必须如何处理层次结构。

选择中此复选框可保留容器并将目录信息树结构从端点复制到目标目录服务器。

清除此复选框可通过将所有条目从端点的多个容器中拉至目标目录的某个指定容器将层次结构序列化。

Directory Server 中的目标容器

指定目标目录服务器中的搜索基础。

仅当选中了对源层次结构进行镜像的选项时，才会显示此字段。

该值在创建源层次结构镜像时被用作根。

用户的目标容器

指定必须写入 Person 条目的容器。

仅当未选中对源层次结构进行镜像的选项时，才会显示此字段。

仅在将源层次结构序列化时才可使用此值。

组的目标容器

指定必须写入"组"条目的容器。

仅当未选中对源层次结构进行镜像的选项时，才会显示此字段。

仅在将源层次结构序列化时才可使用此值。

调试日志输出

选中此复选框可生成含有附加信息的详细日志消息，包括有关未经处理或同步的条目的错误。

过滤详细信息

指定过滤条件，用于在同步期间包括或排除条目。在下列字段中，请在每一行输入一个条件。条目可以是完整 DN 或部分文本。

包含以下内容

指定想要同步的端点中的节点列表。

用于在已返回的条目 DN 中搜索子字符串的值。

排除以下内容

指定在同步时想要排除的端点中的节点列表。

“用户/人员”设置

根据为流选择的端点类型，为以下设置提供的典型缺省值。

源人员条目对象类

指定端点中的 Person 条目对象类。

目标人员条目对象类

指定用于在目标目录中创建 Person 条目的条目。

“源用户 RDN®”属性

指定用作 Person 条目 DN 中的相对 DN 的属性。

“目标用户 RDN”属性

用作写入 SDS 的条目的 RDN 的属性。

组设置 根据为流选择的端点类型，为以下设置提供的典型缺省值。

源组条目对象类
指定端点中的"组"条目对象类。

目标组条目对象类
指定必须用于在目标目录中创建"组"条目的条目。

“目标组成员资格”属性
指定用于保留目标目录中组成员资格的属性。

流挂钩 您可以选择性地指定必须在执行各种类型的流操作之前或之后调用的组装流水线。

请参阅『使用流挂钩对流进行定制』。

高级设置
可以选择性地指定用于覆盖“联合目录服务器”控制台中指定设置的定制属性。

请参阅第 27 页的『配置定制属性』。

下一步做什么

如果想要删除一个不必要的流，请关闭该流的配置页面。在**流**页面上，单击流名称，然后单击**删除流**。当出现确认消息时，单击**确定**。

1. 您可以为流配置下列增强功能:
   - 定制属性映射
   - 定义连接
   - 启用回写
2. 在完成对所有流设置的定义之后，运行初始同步操作。
3. 然后，手动运行增量同步或者调度定期同步。

使用流挂钩对流进行定制

使用流挂钩，通过指定必须在执行各类流操作之前或之后调用的组装流水线，对流进行定制。您还可以指定用于覆盖联合目录服务器控制台中的设置的定制属性。

开始之前

1. 使用配置编辑器来创建组装流水线。
2. 将组装流水线项目的配置 XML 文件复制到 *sdi_solution_dir*/configs 文件夹中。

请参阅 IBM Security Directory Integrator 文档中的“配置编辑器”部分。

关于此任务

流挂钩是流的操作中的位置，在这些位置，可以调用定制组装流水线以执行各种任务。例如，您可以调用组装流水线以进行条目和属性过滤、审计以及发出警报和事件。另外，还可以调用组装流水线以进行流前处理和流后处理，例如移动文件或者将文件重命名。

下列示例是典型的情况，在这些情况下，您可能希望使用流挂钩:

- 在执行每项写操作前，要对条目或特定属性运行隐私控制。

- 要在完成写操作后供应其他系统，例如 IBM Security Access Manager。写入目标目录服务器的条目还将传递到 `afterwrite` 挂钩组装流水线。用户可以将此信息与其他系统同步，并且还可以发送审计事件。

过程

1. 在**流**页面上，单击流名称，然后单击**编辑**。
2. 在**源**选项卡上，单击**流挂钩**。
3. 选中**启用挂钩**以启用流挂钩。取消选中此复选框将禁用所有流挂钩。此选项将覆盖各项用于在每项操作之下启用各个流挂钩的设置。
4. 单击要激活的挂钩旁边的**已启用**复选框。仅当对所有流挂钩选中全局**启用挂钩**选项之后，此选项才有效。
5. 要指定组装流水线，请展开已启用的挂钩并单击**浏览**。 这将显示 *sdi_solution_dir*/`configs` 文件夹中的组装流水线。
6. 请选择要为该流挂钩调用的组装流水线。

   可以在联合目录服务器控制台中配置下列挂钩:

   流初始化
   在流操作开头调用指定的组装流水线。此挂钩在验证并处理属性之后但在建立任何与端点或目标目录服务器的连接之前发生。

   使用此挂钩可以运行用于为连接和处理作准备的命令。

   例如，此挂钩可用于扫描和移动文件，或者运行命令以便为文件端点源转储信息。

   属性名为 `hook.prolog`。

   写入之前
   在从源端点读取当前条目之后以及执行可选的连接操作后立即调用指定的组装流水线。此组装流水线在数据写入目标目录服务器之前进行调用。

   使用此挂钩可以对条目和属性或者它们的值进行进一步过滤。

   属性名为 `hook.beforewrite`。

   用户添加/修改/删除
   执行在目标目录服务器中添加、修改或删除人员条目的写操作之后，调用指定的组装流水线。

   另外，还可以使用此流挂钩来调用用于供应 IBM Security Access Manager 的组装流水线。

   组添加/修改/删除
   执行在目标目录服务器中添加、修改或删除组条目的写操作之后，调用指定的组装流水线。

   另外，还可以使用此流挂钩来调用用于供应 IBM Security Access Manager 的组装流水线。

   使用用于用户对象的组装流水线
   选中此复选框表示您对**用户添加/修改/删除**挂钩指定的属性还用于**组添加/修改/删除**挂钩。要对**组添加/修改/删除**挂钩指定其他属性，请取消选中此复选框。

   流错误 每当流操作中发生错误时，调用指定的组装流水线。

流完成 在流完成对来自源端点的输入条目进行循环处理之后，即，在流操作完成后关闭时，调用指定的组装流水线。

相关概念:

第 55 页的第 2 章，『Federated Directory Server Plug-in for IBM Security Access Manager』

配置此插件，以便将一个或多个目录用作 IBM Security Access Manager 的认证源。例如，您可以使用 Active Directory 和 Sun Directory Server 作为认证源，从而将用户管理和密码留在各自的身份存储库中。

配置定制属性

您可以指定用于覆盖联合目录服务器控制台中指定的设置的定制属性。

关于此任务

您可以使用定制属性针对端点、目标目录服务器连接或流覆盖联合目录服务器控制台中指定的设置。另外，您还可以使用定制属性来配置控制台中未提供的设置。

过程

1. 要指定定制属性，请在**流**页面上单击流名称，然后单击**编辑**。
2. 在**源**选项卡上，单击**高级设置**。
3. 在**定制属性**字段中，输入每个要配置的定制属性（每行一个）。

   您可以在 IBM Security Directory Integrator 配置编辑器中找到每项设置的定制属性名:

   a. 在连接器配置页面上，单击**连接**选项卡。
   b. 单击某个字段旁边的编辑图标文本以打开“表达式编辑器”。
   c. 所显示的**内部名称**是定制属性名。

   您可以将下列在控制台中未提供的流挂钩配置为定制属性:

   hook.onsuccess
   流成功完成时，将调用此挂钩。

   hook.onfailure
   流由于出错而停止时，将调用此挂钩。

   hook.onshutdownrequest
   向流发送关闭请求时，将调用此挂钩。

   hook.afterwrite
   通过控制台可以配置的 `afterwrite` 挂钩仅用于修改了条目的成功写操作。但是，在定制属性中，可以配置未限定的 `afterwrite` 挂钩，该挂钩将在写状态为成功、失败或者被跳过时进行调用。另外，还可以在操作产生了未经更改的条目时调用该挂钩。

示例

下列示例说明如何使用定制属性。

指定定制属性以覆盖控制台设置

在**常规设置**页面上，可以启用**调试日志输出**来生成详细的日志。要覆盖此设置，请输入以下定制属性设置: `global.debug=true`。此设置将传递到 IBM Security Directory Integrator 解决方案中。

指定控制台中未提供的定制属性

在联合目录服务器控制台中，未提供 `onfailure` 流挂钩。您可以使用这个流挂钩在流由于出错而停止时调用组装流水线。可以使用下列定制属性来启用这个流挂钩:

```
hook.onfailure.AL=hookProject:/AssemblyLines/FlowFailure
hook.onfailure.enabled=true
```

扩展流的属性映射

所有流关系都可包含高级映射和数据转换。设置流时，可指定必须在流操作期间应用的定制属性映射。可以从先前为用户和组定义的属性映射中选择，也可以扩展指定流的映射。

开始之前

定制属性映射。

关于此任务

定制属性映射用于将源端点模式中的属性转换为目标模式中相应的属性。

过程

1. 在**流**选项卡上，单击流名称，然后单击**编辑**以打开流配置页面（如果未打开）。
2. 在流配置页面上，单击**属性映射**选项卡，然后单击**人员对象**或**组对象**以查看用户或组的定制映射。
3. 从**为人员对象选择映射**或**为组对象选择映射**列表中，指定要应用于流操作的映射。

   缺省值为 `person.map`（对于人员对象）和 `group.map`（对于组对象）。

   可以从列表中选择另一个映射。列表同时包含了随联合目录服务器提供的随时可用的定制属性映射和先前定制的映射。
4. 要扩展属性映射，请执行下列任意操作:

   创建属性映射

   a. 单击**添加属性**。
   b. 从目标目录服务器的属性列表中选择属性。这将显示新的一行，并且选定的属性名显示在**目录服务器属性**中。

      注: 如果“添加属性”窗口未显示目标目录中的属性列表，请执行下列操作:

      1) 在导航窗格中的**目录服务器**下方，转到**连接设置**。
      2) 单击**测试连接**。确保端点名称旁边显示了绿色勾选标记，这表明连接成功。此操作还将填充用于浏览目标目录属性的字段。

   c. 在**端点属性/分配**下方，双击缺省值以更改该映射，并为该属性映射指定更多设置。

d. 选中**已启用**以使用端点的此属性映射。

e. 单击**简单分配**或**脚本化分配**指定映射的类型。

注: 如果选中了**脚本化分配**，那么可以通过编写 JavaScript 代码或调用 *sdi_solution_dir*\LDAPSync\customScript.js 文件中的函数来定义分配。有关更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“IBM Security Directory Integrator 中的脚本编制”。

f. 在**映射场合**下方，指定是要将此映射用于所有操作，还是只想在修改条目或创建条目时使用此映射。

g. 在**选择属性**字段中，指定源端点中必须映射到目标属性的属性名。

删除特定属性的映射

a. 选中该属性行的相应复选框。

b. 单击**除去属性**。

c. 单击**确定**。

5. 单击**保存**。除非保存每个已编辑的映射，否则更改将会丢失。

结果

作为预防措施，当扩展定制属性映射时，将对原始属性映射文件的副本作出更改。新的文件时特定于此流的。它使用前缀 Flow_*flow_name* 进行命名。例如：Flow_ADFlow_person.map。

所有属性映射都存储在 *sdi_solution_dir*\LDAPSync 目录中。

配置连接

要扩充并增加端点中的数据，可将流配置为从另一个数据源有选择地指定连接。

关于此任务

流可以将一个端点中的数据与另一个端点中的数据连接起来。例如，某个数据库可能包含有关人员的信息，但是它在 LDAP 目录中不可用。通过将 LDAP 目录与该数据库进行连接，联合目录服务器可以显示有关人员的更丰富的信息。

无论什么时候接收到了来自端点的条目，那么流将在连接数据源上查找该条目，将它与端点中的数据合并起来，然后添加到目标 IBM Security Directory Server。

注: 只有支持查找的端点才能用于连接。例如，类似端点的 LDAP 使用特定的条件支持查找，因此它们可以用于连接。基于文件的端点不支持查找，因此无法用于连接。

过程

1. 在**流**选项卡上，单击流名称，然后单击**编辑**以打开流配置页面（如果未打开）。
2. 单击**连接**选项卡以查看并编辑目录或数据源的属性用于连接。
3. 选择**启用**以将连接应用于此流。
4. 在**选择端点**列表中，选择想要用于连接的端点。**选择端点**列表显示已在联合目录服务器中配置的所有端点。如果您取消选中**启用**复选框，那么将禁用**选择端点**字段并且会保留您先前输入的设置，但不会在流操作期间应用。

5. 指定流操作期间连接中的条目发生错误或故障时必须执行的操作。从**连接失败时**列表中，选择以下一个选项:
   - **忽略错误并继续**，如果您选择此选项，那么会忽略错误，添加、修改或删除条目，然后会对下一个条目继续执行流操作。
   - **跳过当前条目并继续**，如果您选择此选项，那么会跳过导致错误的条目并继续执行流操作。
   - **中止并终止流**，如果您选择此选项，那么会在此条目处终止流操作。

   如果在**源**选项卡的**常规设置**中启用了**调试日志输出**，可以查看有关引起错误的条目的详细信息。
6. 可以选择使用语句来指定简单条件或高级条件的脚本。
   - 要指定简单条件在连接中查找匹配的条目，请清除**脚本标准**复选框，然后指定条件语句:
     - 在**属性**字段中输入连接端点中的属性。
     - 从**运算符**列表中，为语句选择适当的运算符。
     - 在**值**字段中，输入主端点中相应的属性。
   - 要使用脚本来指定高级条件，请选中**脚本化条件**。将提供一个字段，您可在其中编写条件脚本。有关更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“IBM Security Directory Integrator 中的脚本编制”。
7. 在**属性映射**中，可以添加、除去或修改连接的属性映射。
   a. 单击**添加属性**，然后从目标目录服务器的属性列表中选择属性。 将显示新的一行，在**目录服务器属性**列中显示选定的属性名。
   b. 在**端点属性/分配**中，指定在必须与目标属性映射的端点中指定属性名。
   c. 双击端点属性名以指定属性映射的多个设置。
      - 选中**已启用**以使用端点的此属性映射。
      - 单击**简单分配**或**脚本化分配**指定映射的类型。如果选中了**脚本化分配**，那么可以通过编写 JavaScript 代码或调用 *sdi_solution_dir*\LDAPSync\customScript.js 文件中的函数来定义分配。有关更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“IBM Security Directory Integrator 中的脚本编制”。
      - 指定是想将此映射用于所有操作，还是只想在修改条目或创建条目时使用此映射。
   d. 要删除指定属性的映射，请单击该行上的复选框。然后单击**除去属性**，当出现确认消息时单击**确定**。
8. 也可以提供自己的组装流水线而不是仅仅是端点来定义连接操作。展开**定制查找/连接组装流水线**部分，然后指定**人员对象**、**组对象**和**容器对象**。

   必须先使用“配置编辑器”创建组装流水线，然后才能使用这些字段。请确保将组装流水线项目的配置 XML 文件复制到 *sdi_solution_dir*/configs 文件夹中。有关更多信息，请参阅 IBM Security Directory Integrator 文档并搜索*配置编辑器*。

   在**定制的查找/连接组装流水线**字段中，输入在配置编辑器中创建的以下组装流水线项目详细信息:
   - 包含了组装流水线的 IBM Security Directory Integrator 项目的名称
   - 组装流水线的名称

使用以下格式在这些字段中输入名称:

Project Name:/AssemblyLines/*AssemblyLine Name*

例如，如果项目名为 OS400 并且包含了一个名为 ReadUsers 的组装流水线，那么可输入:

```
OS400:/AssemblyLines/ReadUsers
```

启用对流的回写

可以通过对选定属性启用在流中的回写，可以将在目标目录服务器中作出的更改传播回端点。

开始之前

将提供全局回写选项作为安全功能，可以用它来关闭所有流的回写。但是，当全局关闭回写功能时，将阻止所有流的回写，包括想要启用回写的指定流。因此，必须先确保在全局级别对所有的流启用回写功能。请参阅第 10 页的『启用或禁用全局回写』。

在启用全局回写功能之后，必须按完成以下步骤为指定的流启用回写。

关于此任务

只有对此流的目标人员条目作出的更改才能被回写。

回写操作仅处理下列步骤中描述的选定属性。

过程

1. 要为指定的流启用回写，请在**流**选项卡上单击流名称，然后单击**编辑**。 将打开流的配置页面。
2. 单击**回写**选项卡。
3. 选择**启用**为此流启用回写选项。
4. 在必须触发回写操作的目录服务器中指定属性，并且将它与端点中的属性进行映射。
   a. 单击**添加属性**，然后从端点的属性列表中选择属性。 将显示新的一行，在**端点属性**列中显示选定的属性名。
   b. 在 **Directory Server 属性/分配**中，在必须与端点属性映射的目录服务器中指定属性名。
   c. 双击目录服务器属性名为属性映射指定更多设置。
      - 选择**已启用**对回写操作使用此属性映射。
      - 单击**简单分配**或**脚本化分配**指定映射的类型。如果选中了**脚本化分配**，那么可以通过编写 JavaScript 代码或调用 *sdi_solution_dir*\LDAPSync\customScript.js 文件中的函数来定义分配。有关更多信息，请参阅 IBM Security Directory Integrator 文档，然后搜索“IBM Security Directory Integrator 中的脚本编制”。
   d. 要删除指定属性的映射，请单击该行上的复选框。然后单击**除去属性**，当出现确认消息时单击**确定**。

结果

当发生回写操作时，将显示回写到端点的内容摘要。摘要包含了详细信息，比如流名称、已修改的属性，并且将显示目录服务器和端点的 DN。可以使用**过滤器**字段来搜索回写摘要。

验证流配置

在配置了流并为流操作指定了条件之后，可以运行模拟同步已验证流。

开始之前

请确保创建并定义流。

关于此任务

模拟同步运行如初始同步一样的操作，但是不会在目录服务器中写入任何内容。此功能有助于在初始规划阶段验证流是否可以在端点中选择正确的数据子集。

过程

1. 在**流**页面上，单击流名称，然后单击**运行同步**。
2. 在“运行同步”窗口上，选择**模拟**。

结果

将根据为流指定的条件模拟源系统的完整同步。

进度条将显示在**最新活动**列下。状态和日志将显示在流的下方。

下一步做什么

如果想要停止正在进行中的模拟操作，请单击流名称，然后单击**终止**。当出现确认消息时，单击**确定**。

操作完成之后，将在新的选项卡上显示模拟的详细信息，比如日期、操作和已修改的属性。可以使用**过滤器**字段来搜索表格。

也可以查看状态和日志来验证模拟同步是否成功或者调试错误。

通过运行模拟同步验证流之后，可以运行初始同步将数据迁移到目录服务器。

同步目标目录上的数据

在定义流设置之后，可以将端点的数据与目标 IBM Security Directory Server 的同步。可以手动进行同步，或者设置调度定期自动同步。

运行初始同步

在定义了流设置之后，可以运行初始同步将数据从端点迁移到目标 IBM Security Directory Server。

开始之前

请确保创建并定义流。

关于此任务

初始同步是对流的一次性操作。它会选中与流条件匹配的端点中的所有条目并更新目录服务器。

过程

1. 在**流**页面上，单击流名称，然后单击**运行同步**。
2. 在“运行同步”窗口上，选择**初始同步**。

结果

对源系统的完整同步将根据为流指定的条件启动。任何当前同步状态数据都将复位。

进度条将显示在**最新活动**列下。状态和日志将显示在流的下方。

下一步做什么

如果想要停止正在进行中的同步操作，请单击流名称，然后单击**终止**。当显示确认消息时，单击**确定**。终止流的操作将使它保持部分同步状态，所以必须谨慎使用。

操作完成之后，可以查看状态和日志来验证同步是否成功或者调试错误。

在确保初始同步成功完成之后，可以按指定的时间间隔设置同步调度。

运行增量同步

在运行初始同步之后，可以根据对端点作出的更改增量同步目标 IBM Security Directory Server 上的数据。可以手动进行同步，或者可以设置调度定期自动同步。

开始之前

- 创建并定义流。
- 为流运行初始同步。

过程

1. 在**流**页面上，单击流名称，然后单击**运行同步**。
2. 在“运行同步”窗口上，选择**增量同步**。

结果

同步操作将启动，并且进度条将显示在**最新活动**列下。

下一步做什么

如果想要停止正在进行中的同步操作，请单击流名称，然后单击**终止**。当显示确认消息时，单击**确定**。终止流的操作将使它保持部分同步状态，所以必须谨慎使用。

操作完成之后，可以查看状态和日志来验证同步是否成功或者调试错误。

要定时自动运行同步，可以按指定的时间间隔设置同步调度。

安排同步

可以指定一个调度按定时的时间间隔在流中自动运行增量同步操作。

开始之前

- 创建并定义流。
- 为流运行初始同步。

过程

1. 首次为流操作创建调度时，请在**流**页面的流名称下单击**无调度**。要编辑已创建的调度，请单击显示在流下的下一个调度操作的日期和时间。
2. 在“调度”窗口中，单击**已启用**以激活调度程序。
3. 选择调度类型。
   - 如果选择**计时器**，那么将按在调度中指定的时间间隔运行同步。
   - 如果选择**保持活动**，那么即使在端点中指定了超时值，同步也会保持运行状态。
4. 为流操作选择频率**每个月**或**选定月份**。如果您选择**选定月份**，那么会显示月名称并且您必须选择一个或多个月份。
5. 从以下选项中选择想要运行流操作的天数：**每天**、**工作日**（指定星期数）或**选定日期**（指定每月日期）。
6. 在**小时数/分钟数/秒数**部分下，输入希望流操作启动的时间。也可以输入通配符 *（星号）、逗号分隔列表或一系列数字来指定小时、分钟和秒。

   例如:
   - 要在每个小时开始时运行同步，请在**小时数**字段中输入 *，然后在**分钟数**和**秒数**字段中输入 0。
   - 要在每个小时中每隔 15 分钟运行同步，请在**小时数**字段中输入 *，在**分钟数**字段中输入 0,15,30,45，然后在**秒数**字段中输入 0。
7. 选择**已启用**。
8. 如果您预期流操作可能无法在安排下一个操作启动之前完成，请选择**不要在已在运行的情况下启动**。此选项对于持续时间较长的操作来说很有用，因为它会阻止同一操作的两个实例同时运行。
9. 如果您想要在流操作遇到故障时停止，请选择**在组装流水线失败时终止调度**。 例如，可以在自动重复尝试失败的同步之前启用此选项来修正日志文件中的错误。
10. 单击**关闭**以保存调度。

结果

下一个已调度流操作的日期和时间将显示在流下。

下一步做什么

如果将来不想要使用调度程序，那么可以清除“调度”窗口中的**已启用**复选框。

查看日志和报告

完成同步活动之后，可以查看日志来验证它是否成功。

关于此任务

在**流**页面上，将在流的下方显示流操作的摘要，包含以下信息:

- 已添加、修改和删除的用户数。
- 已添加、修改和删除的组数。
- 在此流中运行的最新活动。
- 所处理的用户和组的总数

为流定义常规设置时，如果选中了**调试日志输出**选项，那么将生成包含详细信息的日志用于调试。

过程

1. 要查看详细日志，请从**显示以下项的日志**列表中选择操作。缺省情况下，将显示最新的操作。可以从列出的任何先前的日志中进行选择。

   注: 要更改必须存储的历史日志文件数，请参阅第 12 页的『指定日志设置』。
2. 单击日志中下列其中一个部分以查看详细报告:

   摘要 显示以下摘要:
   - 已处理的“人员”、“组”和“容器”条目的数量
   - 错误和警告数
   - 已跳过并且未成功写入目标目录的条目数

   错误日志
   显示所有错误和警告。可以使用详细信息对同步中的任何故障进行故障诊断。

   迁移日志或同步日志
   如果正在查看初始同步的日志，那么将显示迁移日志，否则将显示同步操作的日志。此日志包含整个流操作的详细信息。

监视

联合目录服务器控制台提供了用于监视流的行为和运行状况的选项。

提供了以下选项来执行监视:

- 可以通过 Syslog 将安全性事件发送到 QRadar。每当添加、修改或删除来自目标目录服务器的条目时，都将定义安全性事件。
- 每当发生并记录了错误时，可以发出错误事件作为 SNMP 陷阱。
- 如果启用了定制监视，那么此监视将正好在任何其他挂钩激活之前启动，对于标准挂钩和监视挂钩（QRadar 和 SNMP）均如此。

要配置监视设置，请在“联合目录服务器”导航窗格上的**公共设置**下方单击**监视**。

配置 QRadar 监视

配置 QRadar 监视以跟踪安全性事件，这是目标 IBM Security Directory Server 中添加、修改或删除条目时发出的事件。

过程

1. 在导航窗格中的**公共设置**下方，单击**监视**。
2. 在“监视”页面上，单击 **QRadar** 选项卡。
3. 在“QRadar”页面上，选中**启用**以指示您要监视安全事件。
4. 在**主机名**字段中，输入必须接收安全事件的 QRadar 服务器的主机名或 IP 地址。
5. 在**端口**字段中，输入必须接收 Syslog 事件的 QRadar 服务器所使用的端口号。
6. 从**严重性**列表中，选择用于 Syslog 事件的严重性值。
7. 从**设施**字段中，选择用于 Syslog 事件的设施值。
8. 在**映射文件**字段中，指定映射文件的路径和文件名，此文件用来设置事件的各种 QRadar LEEF 属性。
9. 单击**选择...**以浏览映射文件。缺省值指向 `LDAPSync/QRadar.map` 文件。
10. 可选: 在**日期格式掩码**字段中，请指定在映射的 LEEF 属性中写入的日期值的标准 Java `SimpleDateFormat` 掩码。

    此值控制 **devTimeFormat** 属性的值以及事件中日期值的格式。缺省值为 ISO 8601 标准掩码 `MMM dd yy HH:mm:ss`，它将创建如 `Oct 16 12 15:15:57` 的字符串。

配置 SNMP 监视

配置 SNMP 监视以跟踪错误事件，这是流操作期间记录了错误时发出的事件。

过程

1. 在导航窗格中的**公共设置**下方，单击**监视**。
2. 在“监视”页面上，单击 **SNMP** 选项卡。
3. 在“SNMP”页面上，选中**启用**以指示您要监视错误事件。
4. 在**主机名**字段中，输入必须接收错误事件的 SNMP 监视器的主机名或 IP 地址。
5. 在**陷阱端口**字段中，输入 SNMP 用于侦听陷阱的端口号。
6. 在**共用体字符串**字段中，指定用于发出的 SNMP 陷阱的共用体字符串。

   SNMP 共用名用作认证的格式，因为不了解正确共用名的设备将从 SNMP 操作中消除。与此共用体字符串不匹配的所有消息将被废弃。

   如果保留其为空白，那么将接受所有共用体字符串。缺省值为 `public`。
7. 在**映射文件**字段中，指定映射文件的路径和文件名，此文件用来设置要在发出的 SNMP 陷阱中传递的各种对象标识 (OID)。缺省值为 `LDAPSync/SNMP.map`

结果

如果启用，那么 SNMP 监视函数传送错误消息和错误级别，如 `ERROR`、`WARN` 或 `FATAL`。

下一步做什么

您可以将 `IBM-FDS-MIB.txt` 从 *sdi_solution_dir*`/LDAPSync` 复制到 SNMP 服务器的 MIB 存储库中，以使 SNMP 服务器能够正确理解联合目录服务器所发送的 SNMP 消息。请与 SNMP 服务器管理员联系，以获取有关将 SNMP 设备配置为使用联合目录服务器 MIB 文件的帮助。

配置定制监视

使用定制监视选项可以在流操作期间的每个活动挂钩点执行任意数目的操作。

关于此任务

如果配置了定制监视，那么将在流操作中的所有标准挂钩点调用指定的组装流水线。此组装流水线将在实际流挂钩的组装流水线启动前进行调用，即使处于禁用状态也是如此。

过程

1. 在导航窗格中的**公共设置**下方，单击**监视**。
2. 在“监视”页面上，单击**定制**选项卡。
3. 在“定制”页面上，选择**已启用**以指示您希望通过调用定制组装流水线来监视流事件。
4. 在**定制组装流水线**字段中，指定要用于进行定制监视的组装流水线。

结果

定制监视将正好在任何其他流挂钩激活之前启动。

定制目标配置

缺省情况下，联合目录服务器目标是 IBM Security Directory Server 实例，您可以通过控制台上的**连接设置**来配置该实例。要配置除 IBM Security Directory Server 以外的目标，您必须定义定制连接器和定制组装流水线，以处理连接设置以及与目标进行的同步。

要获取配置指示信息和示例，请参阅技术文档联合目录服务器定制目标配置。

已知问题、局限性和变通方法

使用问题描述及其所提供的解决方案来解决在使用联合目录服务器 时可能遇到的问题。

在初始同步期间，嵌套组成员资格可能丢失。

问题 在最初的同步期间，如果处理了某个组，而其中包含尚未同步的成员组，那么会将此成员视为缺失。

解决方案

要确保处理所有的嵌套成员资格，请在初始同步完成后，对所有缺少成员的组重新运行此流。并且，将所有的“缺少成员”错误消息推迟到最后一轮组处理完成后发出。

检索到页面大小值之后，初始同步失败了

问题 在 Windows Server 2008 R2 系统上，检索到页面大小设置的值之后，初始同步失败了。

此问题特定于涉及 Active Directory 的操作。

描述 以下场景下发生此问题:

- Windows Server 2008 R2 系统上的 Active Directory 具有很多用户和组，例如 10,000 个用户和 10,000 个组。
- Active Directory 端点的页面大小设置为 500（缺省值）。
- 已将流定义为将这些条目迁移到 IBM Security Directory Server。

在运行初始同步操作时，将迁移 500 个用户，然后会发生错误。然后，迁移 500 个组后发生错误。操作将终止，并发生类似于以下错误的 OperationNotSupportedException 异常:

```
2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
     - [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]
Stacktrace (for support):
javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
 at com.sun.jndi.ldap.LdapCtx.mapErrorCode(LdapCtx.java:3159)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:3045)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2852)
 at com.sun.jndi.ldap.LdapCtx.searchAux(LdapCtx.java:1861)
 at com.sun.jndi.ldap.LdapCtx.c_search(LdapCtx.java:1784)
 at com.sun.jndi.toolkit.ctx.ComponentDirContext.p_search(ComponentDirContext.java:398)
 at com.sun.jndi.toolkit.ctx.PartialCompositeDirContext.search(PartialCompositeDirContext.java:368)
 at javax.naming.directory.InitialDirContext.search(InitialDirContext.java:287)
 at com.ibm.di.connector.LDAPConnector.getNextEntry(LDAPConnector.java:750)
 at com.ibm.di.server.AssemblyLineComponent.executeOperation(AssemblyLineComponent.java:3355)
 at com.ibm.di.server.AssemblyLineComponent.getnext(AssemblyLineComponent.java:932)
 at com.ibm.di.server.AssemblyLine.msGetNextIteratorEntry(AssemblyLine.java:3666)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3375)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3151)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3091)
 at com.ibm.di.fc.AssemblyLineFC.executeCycle(AssemblyLineFC.java:451)
 at com.ibm.di.fc.AssemblyLineFC.perform(AssemblyLineFC.java:272)
 at sun.reflect.GeneratedMethodAccessor77.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:55)
 at java.lang.reflect.Method.invoke(Method.java:613)
 at com.ibm.jscript.types.JavaAccessObject.call(JavaAccessObject.java:321)
 at com.ibm.jscript.types.FBSObject.call(FBSObject.java:161)
 at com.ibm.jscript.ASTTree.ASTCall.interpret(ASTCall.java:175)
 at com.ibm.jscript.ASTTree.ASTAssign.interpret(ASTAssign.java:91)
 at com.ibm.jscript.ASTTree.ASTProgram.interpret(ASTProgram.java:119)
 at com.ibm.jscript.ASTTree.ASTProgram.interpretEx(ASTProgram.java:139)
 at com.ibm.jscript.JSExpression._interpretExpression(JSExpression.java:435)
 at com.ibm.jscript.JSExpression.interpretExpression(JSExpression.java:421)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:251)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:238)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:241)
 at com.ibm.jscript.JSInterpreter.interpret(JSInterpreter.java:57)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:940)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:925)
 at com.ibm.di.server.ScriptComponent.add1(ScriptComponent.java:244)
 at com.ibm.di.server.ScriptComponent.add(ScriptComponent.java:210)
 at com.ibm.di.server.AssemblyLine.msExecuteNextConnector(AssemblyLine.java:3759)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3379)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2988)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2971)
 at com.ibm.di.server.AssemblyLine.executeAL(AssemblyLine.java:2940)
 at com.ibm.di.server.AssemblyLine.run(AssemblyLine.java:1319)

2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - Make sure that the search base is visible in the source system,
     for example from an LDAP browser.
Also ensure that the credentials defined for the Source connection are
     authorized to see entries in this container.
***** Start dumping: ERROR *****
                    class: 'javax.naming.OperationNotSupportedException'
            connectorname: 'Read Groups'
                exception: 'javax.naming.OperationNotSupportedException:
     [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal''
                 message: '[LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]'
               operation: 'get'
                  status: 'fail'
***** End dumping: ERROR *****
***** Connector parameters: Read Groups *****
    ldapUrl: ldap://9.120.98.148:389
    ldapUsername: Administrator@adsync.tditest.internal
    ldapSearchBase: ou=set1,dc=adsync,dc=tditest,dc=internal
    ldapSearchFilter: objectClass=groupofuniquenames
    ldapSearchScope: subtree
    ldapSizeLimit: 0
    ldapPageSize: 500
    jndiExtraProviderParams: null
```

解决方案

完成以下步骤来解决此问题:

1. 在 Windows Server 2008 R2 Active Directory 上，请应用 Microsoft Knowledge Base Web 站点 (http://support.microsoft.com/kb/977180) 上的解决方案。
2. 备份 Windows 注册表。
3. 在以下注册表设置 `HKLM\System\CurrentControlSet\Services\NTDS\Parameters` 中，添加字符串值 `DSA Heuristics`。
4. 将值设置为 `000000000001`。
5. 重新启动系统。

参考

使用参考信息来了解有关联合目录服务器控制台 的功能和组件的更多详细信息。

文件解析器

可以从联合目录服务器控制台的文件端点配置页面所提供的列表中选择并配置相应的文件解析器。

文件端点的 CBE 解析器

使用 CBE 解析器可读取输入流中的 XML 并将此 XML 转换为公共基本事件 (CBE) 对象。当 CBE 解析器读取 XML 时，它将返回所有标准 CBE 属性以及作为输入映射属性的 CBE 对象。

要访问 CBE 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **CBE 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有附加信息的详细日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码

指定要用于读或写的字符编码。缺省值为 `UTF-8`。当解析器读取 XML 时，仅当尚未为输入源定义编码时才会使用此参数。

CBE 解析器将扩展 XML 解析器；因此，会应用相同的字符编码规则。有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索 *XML 解析器中的字符编码*。

验证 XML

选中此复选框可指示解析器必须使用从规范中请求而来的 XSD 模式来验证 XML。

省略 XML 声明

选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

有关 CBE 解析器及其输入和输出映射属性的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *CBE 解析器*。

文件端点的 CSV 解析器

使用 CSV 解析器可读写逗号分隔值 (CSV) 格式的数据。

要访问 CSV 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **CSV 解析器**。
3. 展开**解析器**部分以查看参数。

参数

字段分隔符
指定用于分隔每一列的字符，通常为逗号或分号。缺省值为分号 (**;**)。

字段排序
选中此复选框可按字母（升序）顺序写入头字段。缺省值为 `false`。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有附加信息的详细日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字段名称
指定解析器必须读写的每一列的名称。可在字段名称之间使用**字段分隔符**，也可以在单独一行上指定每一个名称。

指定列名的顺序控制将列写入输出文件的顺序。

启用引号
选中此复选框可在写操作期间带引号输出。缺省情况下已选中此选项。

如果您取消选中此复选框，那么字段将按原样输出，这可能会导致问题。如果选中**启用引号**复选框，那么在读操作期间，将忽略字段两侧的引号。解析器能够读取包含列分隔符的加引号属性。如果取消选中**启用引号**复选框，那么当输入中包含以引号定界的字段时，解析器会返回意外值。

对所有字段加引号
选中此复选框可带引号单独输出所有字段（如果这些字段包含引号、分隔符或换行符）。

写入头 选中此复选框可在第一行上输出所有字段名称，名称之间以列分隔符分隔。缺省情况下已选中此选项。

写入 BOM
选中此复选框可将字节顺序标记 (BOM) 写入文件。还必须选择**写入头**才能使此选项生效。

记录长行
指定一行的最大字节数。将记录长度大于此最大字节数的行的行号。

将剩余部分合并到最后一个字段中

选中此复选框可将超过已定义字段数的行中的所有其他字段合并到一个新的 **Remainder** 字段中。字段以及字段数由**字段名称**定义，如果没有字段名称，则由文件的第一行定义。

字符编码

指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

有关 CSV 解析器及其模式的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *CSV 解析器*。

文件端点的 DSMLv1 解析器

使用 DSMLv1 解析器可读写 XML 文档。目录服务标记语言 V1.0 (DSMLv1) 能够将目录结构信息表示为 XML 文档。该解析器会静默地忽略模式条目。

要访问 DSMLv1 解析器配置参数:

1. 添加文件端点。
2. 在"文件"端点配置页面上，单击**解析器**，然后从列表中选择 **DSMLv1 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

DN 属性

指定用于专有名称 DSML 属性的属性。缺省值为 `$dn`。

DSML 前缀

指定用于 XML 元素的前缀以指示这些元素属于 DSML 名称空间。缺省值为 `dsml`。

DSML 名称空间 URI

指定用于指示此名称空间的 URI。缺省值为 `http://www.dsml.org/DSML`。

省略 XML 声明

选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

文档验证

选中此复选框可请求根据所指定的 DTD 或模式进行文件验证。

可识别名称空间

选中此复选框可指示解析器必须请求可识别名称空间的解析器。

字符编码

指定要用于读或写的字符编码。缺省值为 `UTF-8`。

DSMLv1 解析器扩展了简单 XML 解析器；因此，相同的字符编码规则适用。有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*简单 XML 解析器中的字符编码*。

有关 DSMLv1 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *DSMLv1 解析器*。

文件端点的 DSMLv2 解析器

使用 DSMLv2 解析器可解析和创建 DSMLv2 请求和响应消息。目录服务标记语言 V2.0 (DSMLv2) 提供了一种将目录查询和更新以及这些操作的结果表达为 XML 文档的方法。

要访问 DSMLv2 解析器配置参数:

1. 添加文件端点。
2. 在"文件"端点配置页面，单击**解析器r**，然后从列表中选择 **DSMLv2 解析器**。
3. 展开**解析器**部分以查看参数。

参数

方式 指定解析器是以服务器方式还是客户机方式运行。在服务器方式下，将读取请求和写入响应。在客户机方式下，将写入请求和读取响应。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有附加信息的详细日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

DSMLv2 解析器将扩展简单 XML 解析器；因此，相同的字符编码规则适用。有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*简单 XML 解析器中的字符编码*。

二进制属性
指定逗号分隔的属性列表，解析器必须将这些属性视为二进制属性。缺省情况下提供了一组可修改的属性。

出错时 指定服务器在处理批处理请求元素时如何对故障进行响应。有效值为 exit 和 resume。缺省值为 exit。

处理 为批处理请求指定 **processing** DSML 属性的值。有效值为 sequential 和 parallel。缺省值为 sequential。

响应顺序
指定服务器如何对批处理响应内的各个响应进行排序。有效值为 sequential 和 unordered。缺省值为 sequential。如果您选择 sequential，那么服务器返回的批处理响应中各个响应的顺序必须与各个请求的顺序一致。

省略 XML 声明
选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

缩进输出
选中此复选框可根据语句行的深度对输出进行缩进。结果只是为了美观，与输出文件的语义内容无关。

SOAP 绑定

选中此复选框可创建 SOAP DSML 消息。否则，不会将 DSML 消息包括在 SOAP 中。

有关 DSMLv2 解析器、其操作、属性以及示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *DSMLv2 解析器*。

文件端点的固定记录解析器

使用固定记录解析器可读写固定长度的文本记录。

要访问“固定记录解析器”配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择**固定记录解析器**。
3. 展开**解析器**部分以查看参数。

参数

列描述 按照字段名称、偏移量和长度（以逗号分隔）来指定每个列描述。此字段是一个多行字段，您必须每行指定一个列描述。

例如:

```
field1, 1, 12
field2, 13, 4
field3, 17, 3
```

模式发现期间会显示字段名称。偏移量起始值为 1；无效值（例如 0）可能导致异常。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有附加信息的详细日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

修整值 选中此复选框可在读操作期间从字段中除去起始和结尾处的空格。

字符编码

指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

文件端点的 HTTP 解析器

使用 HTTP 解析器以根据 HTTP 规范解释字节流。

要访问 HTTP 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器r**，然后从列表中选择 **HTTP 解析器**。
3. 展开**解析器**部分以查看参数。

参数

客户机方式
选中此复选框可指示解析器必须以客户机 HTTP 响应方式运行。如果取消选中**客户机方式**复选框，那么解析器将以服务器方式运行。仅当解析器写入输出流时，此选项才有用。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有附加信息的详细日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

头作为属性
选中此复选框可检索头值并将其设置为属性。如果取消选中此复选框，那么会将头值读取为属性并返回为特性。

字符编码
指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符集/编码*。

有关 HTTP 解析器、其模式以及头字段的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *HTTP 解析器*。

文件端点的 IdML 解析器

使用 IdML 解析器可解析 IdML（身份标记语言）文件的内容。它只能用于读取 IdML 文档。它依靠 XML 解析器来处理 IdML 文件和片段。

要访问 IdML 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **IdML 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码
指定要用于读或写的字符编码。

有关 IdML 解析器及其模式的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *IdML 解析器*。

文件端点的 JSON 解析器

使用 JSON 解析器对 JavaScript 对象表示法 (JSON) 格式的条目进行读写操作。JSON 是一种轻量级的数据交换格式，它也是 JavaScript 编程语言的一个子集。JSON 使用下列两种结构构建: 有序的值列表（数组）和“名称/值”对的集合（对象）。

要访问 JSON 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **JSON 解析器**。
3. 展开**解析器**部分以查看参数。

参数

精简输出
选中此复选框可采用精简方式显示数据。精简方式会在单个无格式的行上写入 JSON 数据，该方式为缺省方式。

字符编码
指定要用于对数据进行读或写的字符编码。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

有关 JSON 解析器、其对象和属性及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *JSON 解析器*。

文件端点的 LDIF 解析器

使用 LDIF 解析器可读写 LDAP 数据交换格式 (LDIF) 的数据。LDIF 格式用于指定一组目录条目或要应用于目录条目的一组更改（但不能同时指定这两者）。LDIF 文件由使用行分隔符分隔的一系列记录组成。

要访问 LDIF 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **LDIF 解析器**。
3. 展开**解析器**部分以查看参数。

参数

DN 属性名称
指定要用于 dn 行的属性名称。缺省值为 $dn。

版本号 选中此复选框可在输出开始处显示版本属性（RFC2849 需要）。缺省情况下已选中此复选框。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

二进制属性
指定逗号分隔的属性列表，解析器必须将这些属性视为二进制属性。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

注: 符合规范的 LDIF 文件的**字符编码**必须始终设置为 UTF-8。**字符编码**还用于对 BASE64 编码字符串进行编码或解码。如果您不知道如何对 BASE64 编码进行解码，那么它看起来像乱码文本。

仅描述性记录

选中此复选框可仅写入描述性记录。LDIF 文件可包含更改记录或描述性记录。更改记录用于描述条目所需的更改。可通过 changetype 行进行标识，该行是紧跟在 dn 行之后的第二行。描述性记录用于描述条目。正确的 LDIF 文件仅包含更改记录或描述性记录。

缺省情况下未选中此复选框。

支持语言标记

如果您希望解析器支持语言标记，请选中此框。信息以多种语言表示时，服务器会将语言标记与属性值关联。

有关 LDIF 解析器的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *LDIF 解析器*。

文件端点的行读取器解析器

使用行读程序解析器可读取文件中的单行数据。将在单个属性中返回所读取的行。名为 linenumber 的属性包含从 1 开始的行号。

请将行读程序解析器仅用于读取文本文件，而不要用于读取二进制文件。如果您要复制二进制文件，可使用可脚本化的 FTP 对象。有关 FTP 对象的更多信息和示例，请转至 IBM Security Directory Integrator 文档 并搜索 *FTP 对象*。

要访问行读程序解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择**行读取器解析器**。
3. 展开**解析器**部分以查看参数。

参数

属性名称

指定包含已读取或者要写入的文本行的属性的名称。缺省值为 line。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码

指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

文件端点的脚本解析器

使用脚本解析器通过 JavaScript 编写自己的解析器。

要访问脚本解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择**脚本解析器**。
3. 展开**解析器**部分以查看参数。

参数

脚本 使用此字段可编写要运行的用户定义脚本。缺省情况下已提供了一个样本脚本。有关可在脚本中使用的对象和函数的更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*脚本解析器*。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

外部文件
如果要在运行时包含外部脚本文件，请在此处指定这些文件，每行指定一个文件。将在运行脚本之前运行这些文件。

包括全局脚本
选中此项可包括脚本库中的脚本。

字符编码
指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

有关脚本解析器、其对象、方法和模式的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索*脚本解析器*。

文件端点的简单解析器

使用简单解析器可读写由属性的“名称和值”对组成的条目。

这些条目采用以下格式:

- 每一行都有一个属性名称**:**值对。
- 多值属性将使用多个行。
- 带有句点的行用于标记条目的结尾。
- 值中的 **\r** 和 **\n** 是 CR 和 LF 换行符的编码。

要访问简单解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择**简单解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码

指定要用于读或写的字符编码。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

文件端点的简单 XML 解析器

使用简单 XML 解析器可读写 XML 文档。它可处理深度不超过两层的 XML 数据。

简单 XML 解析器使用 Apache Xerces 库和 Xalan 库。该解析器通过名为 `xmldom` 的脚本对象使您能够访问 XML 文档。`xmldom` 对象是 `org.w3c.dom.Document` 接口的实例。

注: 第 50 页的『文件端点的 XML 解析器』是经过改进和增强的 XML 解析器。

要访问简单 XML 解析器配置参数:

1. 添加文件端点。
2. 在"文件"端点配置页面上，单击**解析器**，然后从列表中选择**简单 XML 解析器**。
3. 展开**解析器**部分以查看参数。

参数

根标记 指定用于将条目括起来的根标记。缺省值为 `DocRoot`。

条目标记

指定传递给解析器的条目的元素名称。缺省值为 `Entry`。

值标记 指定传递给解析器的属性值的元素名称。缺省值为 `ValueTag`。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

省略 XML 声明

选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

文档验证

选中此复选框可请求根据所指定的 DTD 或模式进行文件验证。

可识别名称空间

选中此复选框可指示解析器必须请求可识别名称空间的解析器。

字符编码

指定要用于读或写的字符编码。缺省值为 `UTF-8`。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*简单 XML 解析器中的字符编码*。

缩进输出

选中此复选框可根据语句行的深度对输出进行缩进。结果只是为了美观，与输出文件的语义内容无关。

有关简单 XML 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索*简单 XML 解析器*。

相关信息:

W3C 文档 (http://www.w3schools.com)

Oracle Java API 文档 (http://docs.oracle.com)

文件端点的 SOAP 解析器

使用 SOAP 解析器可读写 SOAP XML 文档。

SOAP 解析器使用以下方式对 SOAP XML 文档和条目对象进行相互转换:

- 当该解析器对 XML 文档进行写入时，它将使用条目中的属性来构建文档。**SOAP_CALL** 属性应该包含用于 SOAP 调用的值。
- 当该解析器对 XML 文档进行读取时，**SOAP_CALL** 属性设置为反映跟在 SOAP-ENV:Body 标记后面的第一个标记。对于条目中的每个属性，都会创建一个具有该名称和值的标记。SOAP_CALL 标记下的每个标记都将转换为条目对象中的一个属性。

要访问 SOAP 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **SOAP 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

省略 XML 声明
选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

文档验证
选中此复选框可请求根据所指定的 DTD 或模式进行文件验证。

可识别名称空间
选中此复选框可指示解析器必须请求可识别名称空间的解析器。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*字符编码转换*。

有关 SOAP 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *SOAP 解析器*。

文件端点的 SPMLv2 解析器

使用 SPMLv2 解析器可解析或编写 SPML V2 (SPMLv2) 消息作为单独的 SPMLv2 请求和响应。

SPMLv2 定义了一个核心协议，不同的数据模型通过该协议可用于定义实际供应数据。数据模型与 SPML 核心规范的组合称为概要文件。使用 SPML 需要使用特定的概要文件。联合目录服务器控制台 随附的此 SPMLv2 解析器支持 SPMLv2 DSMLv2 概要文件。

要访问 SPMLv2 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **SPMLv2 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

二进制属性
指定逗号分隔的属性列表，解析器必须将这些属性视为二进制属性。缺省情况下提供了一组可修改的属性。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

SPMLv2 解析器扩展了 XML 解析器；因此，相同的字符编码规则适用。有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索 *XML 解析器中的字符编码*。

有关 SPMLv2 解析器、其操作和属性及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *SPMLv2 解析器*。

文件端点的 XML 解析器

使用 XML 解析器可读写 XML 文档。XML 解析器使用 StAX (JSR-173) 规范的 XLXP 实施。StAX 是基于游标的 XML 解析器，可对 XML 进行读写。

此 XML 解析器的速度比传统的基于 DOM 的简单 XML 解析器快得多，因为它不需要像 DOM 那样在内存中装入整个 XML 结构。

要访问 XML 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **XML 解析器**。
3. 展开**解析器**部分以查看参数。

参数

简单 XPath
指定用于发现元素的值（类似于 XPath 的表达式）以将这些元素解释为条目。此参数还用于显示要写入的 XML 文档的结构。

条目标记
指定元素的名称，该元素用于保存传递给 XML 解析器的每个条目。

值标记 指定元素的名称，该元素用于保存传递给 XML 解析器的每个属性值。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志

选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

名称空间映射的前缀

请使用以下格式指定前缀与名称空间之间映射的列表: *prefix=namespace*。

使用竖线 (|) 来分隔各个映射。

如果前缀以 $ 开头，那么会将其视为缺省名称空间声明。

缺省值为 prefix=namespace。

XSD 模式位置

指定模式位置，这仅用于显示目的。

字符编码

指定要用于读或写的字符编码。缺省值为 UTF-8。

有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索 *XML 解析器中的字符编码*。

静态属性声明

指定属性和前缀的声明。将使用**简单 XPath** 字段中所指定的静态元素来编写声明。

缺省情况下，此字段中提供了以下文本:

```
<!-- this is an example for statically declared XML attributes/namespaces -->
<!-- DocRoot xmlns="defaultNS" attr1="val2">
<Entry xmlns:p1="p1NS" p1:attr2="val2" />
</DocRoot-->
```

读取时忽略重复的 XML 声明

选中此复选框可始终识别第一个 XML 声明并忽略后续声明。

结合 选中此复选框可结合相邻的字符数据部分。

写入时省略 XML 声明

选中此复选框可禁止将 XML 声明写入输出。此选项对于附加到现有 XML 文件很有用。

多根文档

选中此复选框可将每个条目输出为独立元素，这将创建多根文档。

缩进输出

选中此复选框可根据语句行的深度对输出进行缩进。结果只是为了美观，与输出文件的语义内容无关。

允许在写入时使用无效 XML 字符

选中此复选框可将无效 XML 字符包含在 XML 标记中。如果未选中此复选框，那么对 XML 文档进行写操作期间会发生异常。

有关 XML 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *XML 解析器*。

文件端点的 XML SAX 解析器

使用 XML SAX 解析器可读取大型 XML 文档，基于 DOM 的 XML 解析器由于内存约束无法处理此类文档。XML SAX 解析器基于 Apache Xerces 库。

XML SAX 解析器将抽取引在您在配置中所指定的**组标记**内的数据。它将使用数据中存在的属性来创建条目。

要访问 XML SAX 解析器配置参数:

1. 添加文件端点。
2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择 **XML SAX 解析器**。
3. 展开**解析器**部分以查看参数。

参数

组标记 指定将条目括起的一个或多个 XML 组标记的名称。可指定多个标记，各个标记名称之间以逗号分隔。如果您不指定值，那么将使用根标记，并且会以单个条目的形式返回整个 XML 文档。

注释 使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

除去前缀
指定要从属性名称中除去的前缀。

忽略属性
选中此复选框可忽略组标记的属性及其子属性。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

文档验证
选中此复选框可请求根据所指定的 DTD 或模式进行文件验证。

使用 XSD 验证
选中此复选框可使用 XSD 而不是 DTD 来验证 XML 文件。

可识别名称空间
选中此复选框可指示解析器必须请求可识别名称空间的解析器。

读超时 指定解析器在未接收到任何数据时等待多少秒之后停止。

有关 XML SAX 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索 *XML SAX 解析器*。

文件端点的基于 XSL 的 XML 解析器

使用基于 XSL 的 XML 解析器可使用您指定的 XSL 来解析任何格式的 XML 文档。XML 文档将解析为属性/值对并存储在条目对象中。

要访问基于 XSL 的 XML 解析器配置参数:

1. 添加文件端点。

2. 在“文件”端点配置页面上，单击**解析器**，然后从列表中选择**基于 XSL 的 XML 解析器**。
3. 展开**解析器**部分以查看参数。

参数

注释　使用此字段可添加注释。解析数据时不会考虑注释。

详细日志
选中此复选框可生成带有详细调试信息的日志消息。

还可以配置以下高级参数。在**解析器**部分下，展开**高级**可查看这些参数。

字符编码
指定要用于读或写的字符编码。缺省值为 UTF-8。

基于 XSL 的 XML 解析器扩展了简单 XML 解析器；因此，相同的字符编码规则适用。有关更多信息，请转至 IBM Security Directory Integrator 文档 并搜索*简单 XML 解析器中的字符编码*。

缩进输出
选中此复选框可根据语句行的深度对输出进行缩进。结果只是为了美观，与输出文件的语义内容无关。

省略 XML 声明
选中此复选框可指示解析器必须在输出流中省略 XML 声明头。

文档验证
选中此复选框可请求根据所指定的 DTD 或模式进行文件验证。

可识别名称空间
选中此复选框可指示解析器必须请求可识别名称空间的解析器。

要配置输入参数，请在**解析器**部分下展开**输入**。

使用输入 XSL 文件
选中此复选框可使用输入 XSL 文件。如果您选中此复选框，那么会忽略**输入 XSL** 字段的内容。

输入 XSL 文件名
指定输入 XSL 文件的路径和文件名，该文件包含用于将用户 XML 转换为 IBM Security Directory Integrator 内部格式的匹配规则。

输入 XSL
使用此可编辑区域可输入或粘贴整个输入 XSL。

要配置输出参数，请在**解析器**部分下展开**输出**。

使用输出 XSL 文件
选中此复选框可使用输出 XSL 文件。如果您选中此复选框，那么会忽略**输出 XSL** 字段的内容。

输出 XSL 文件名
指定输出 XSL 文件的路径和文件名，该文件包含用于将 IBM Security Directory Integrator 内部格式转换回用户 XML 的匹配规则。

输出 XSL
使用此可编辑区域可输入或粘贴整个输出 XSL。

有关基于 XSL 的 XML 解析器及其使用示例的详细信息，请转至 IBM Security Directory Integrator 文档 并搜索*基于 XSL 的 XML 解析器*。

第 2 章 Federated Directory Server Plug-in for IBM Security Access Manager

配置此插件，以便将一个或多个目录用作 IBM Security Access Manager 的认证源。例如，您可以使用 Active Directory 和 Sun Directory Server 作为认证源，从而将用户管理和密码留在各自的身份存储库中。

此插件基于由联合目录服务器提供的同步服务以及 IBM Security Directory Server 的传递认证功能。联合目录服务器提供了现成可用的浏览器界面，用于配置将多个身份存储库与中央 IBM Security Directory Server 实例进行同步。并且，您还可以使用联合目录服务器浏览器控制台在 IBM Security Directory Server 中配置传递认证。

联合目录服务器通过流来处理以特定目录作为源的同步。您可以配置一个流，以便在处理每个条目并将其写入 IBM Security Directory Server 之后执行调出。在此项操作后功能中，Federated Directory Server Plug-in for IBM Security Access Manager 连接到所需的流。每当在目标目录中添加、修改或删除人员条目或组条目时，都将调用此插件。

调用此插件时，将向其传递联合目录服务器控制台中设置的配置参数。然后，此插件将身份信息更改作为流操作的组成部分传播到 IBM Security Access Manager。

IBM Security Directory Integrator 系统向联合目录服务器的服务器端功能提供强大支持。尽管不要求您具备 IBM Security Directory Integrator 的使用经验，但是了解此工具可以更轻松地部署和管理联合目录服务器解决方案。此工具帮助您使用联合目录服务器中的挂钩将自己的业务逻辑与运行中的各种后台联合进程相连接。

注: 仅对于 LDAP 端点，才支持 Federated Directory Server Plug-in for IBM Security Access Manager。不支持非 LDAP 端点。

相关信息:

IBM Security Directory Integrator 入门

IBM Security Access Manager V2 连接器

插件设置路线图

要设置此插件，必须在 IBM Security Access Manager API、IBM Security Directory Server 和联合目录服务器中配置所需的设置。

联合目录服务器通过使一个或多个身份存储库与中央 IBM Security Directory Server 实例保持同步，提供了身份联合服务。

IBM Security Directory Server 提供了传递认证功能，您可以通过联合目录服务器来配置此功能。

Federated Directory Server Plug-in for IBM Security Access Manager 通过将用户帐户和组与 IBM Security Access Manager 同步，对此解决方案进行了扩展。

以下路线图指定了用于设置此插件的端到端方案中的步骤。

表 2. Federated Directory Server plug-in for IBM Security Access Manager 设置路线图

关键步骤	更多信息
安装插件软件包。	『安装插件』
生成 IBM Security Access Manager API 属性文件并指定各个属性的值。	第 57 页的『插件 API 属性文件』
登录联合目录服务器控制台。	第 5 页的『访问 联合目录服务器控制台』
从联合目录服务器连接到 IBM Security Directory Server。	第 9 页的『连接到 IBM Security Directory Server』
配置源端点，以便与 IBM Security Directory Server 进行同步。 **注**: 仅对于 LDAP 端点，才支持 Federated Directory Server Plug-in for IBM Security Access Manager。不支持非 LDAP 端点。	第 14 页的『配置端点』
在 IBM Security Directory Server 中启用传递认证。	传递认证
在联合目录服务器中配置传递认证。	第 11 页的『配置传递认证』
在联合目录服务器中创建流并定义流设置。	第 23 页的『创建流』 第 23 页的『定义流设置』
将此插件连接到联合目录服务器中的流，并配置插件属性。	第 58 页的『配置插件属性』
将源端点属性映射到 IBM Security Access Manager 用户条目和组条目。	第 60 页的『映射属性』
运行模拟同步以测试该流。	第 32 页的『验证流配置』
运行初始同步，以便将数据从该端点迁移到目标 IBM Security Directory Server。	第 32 页的『运行初始同步』
测试 IBM Security Access Manager 认证是否正常工作。	第 61 页的『验证插件设置』
创建一个调度，以便按时间间隔自动运行递增同步。	第 33 页的『安排同步』

安装插件

您必须使 IBM Security Access Manager API 可供 IBM Security Directory Integrator 使用。

开始之前

安装下列产品:

- IBM Security Directory Integrator V7.2（并应用最新的修订包）。此插件从 V7.2.0.1 开始提供。
- IBM Security Access Manager V6.1.1 或更高版本。

并且，请确保联合目录服务器目标目录与 IBM Security Access Manager 使用的目录是同一个 IBM Security Directory Server 实例。否则，需要对 IBM Security Directory Server

进行手动配置。如果已对 IBM Security Directory Server 中的 IBM Security Access Manager 模式添加了扩展属性，那么必须将赋值添加到 FDS_ISAM_Plugin.map 映射文件中。

关于此任务

sdi_solution_dir 是指安装期间选择的 IBM Security Directory Integrator 解决方案目录，此目录在 *tdi_install_dir*/bin/defaultSolDir 脚本中。

tdi_install_dir 是 IBM Security Directory 安装目录。

将安装此插件的下列文件:

FDS_ISAM_Plugin.xml

此文件是提供了组装流水线的 IBM Security Directory Integrator 配置 XML 文件，该组装流水线用于处理与 IBM Security Access Manager 进行的同步。

您首次访问联合目录服务器控制台时，此文件将复制到 *sdi_solution_dir*/configs 目录中。

对于未来的更新，必须将此文件从 *sdi_solution_dir*/LDAPSync 手动复制到 *sdi_solution_dir*/configs。

FDS_ISAM_Plugin.map

控制将源端点属性映射到 IBM Security Access Manager 用户条目的方式。

此文件位于 *sdi_solution_dir*/LDAPSync 目录中。

过程

通过下列任意一种方法使 IBM Security Access Manager API 可供 IBM Security Directory Integrator 使用:

- 从 *ISAM_install_dir*/java/export/rgy 目录中，将 com.tivoli.pd.rgy.jar 文件复制到 *tdi_install_dir*/jars 目录。
- 在 *sdi_solution_dir*/solution.properties 文件中的 **com.ibm.di.userjars** 属性中添加 *ISAM_install_dir*/java/export/rgy。

下一步做什么

必须生成包含 IBM Security Access Manager API 连接详细信息的配置文件。请参阅『插件 API 属性文件』。

插件 API 属性文件

通过使用 IBM Java 运行时环境运行 **com.tivoli.pd.rgy.until.RgyConfig** 工具，以便为插件创建并设置 API 属性文件。

注: 在 *tdi_install_dir*/jvm/jre/bin 文件夹中，提供了 IBM Java 运行时环境。

语法

```
java com.tivoli.pd.rgy.util.RgyConfig properties_file_destination
  create Default Default "ldaphostname:389:readwrite:5" "DN" DN_password
```

参数

properties_file_destination
指定运行此命令时创建的文件的完整路径。

缺省值是以下相对路径: LDAPSync/ISAM_API.properties。

ldaphostname:*port*:*settings*
指定下列详细信息:

- 配置了 IBM Security Access Manager 的 LDAP 服务器的主机名。LDAP 服务器主机名在 Security Access Manager 运行时配置文件中指定。
- LDAP 服务器的端口号。缺省值为 389。您可以更改此值。
- 设置为 :readwrite:5。

请将整个值 (*ldaphostname*:*port*:*settings*) 括在双引号内。

DN 指定用于向 IBM Security Access Manager 进行认证的 LDAP 专有名称 (DN)。请将此值括在双引号内。

DN_password
指定 DN 的相应密码。

示例

```
java com.tivoli.pd.rgy.util.RgyConfig
     sdi_solution_dir/LDAPSync/ISAM_API.properties
     create Default Default "9.118.51.177:389:readwrite:5"  "cn=root" cnrootpassword
```

命令语句中的 Default 对应于要与其集成的 IBM Security Access Manager 域以及 IBM Security Access Manager 插件组装流水线参数中设置的值。

结果与以下属性文件类似，其中属性设置反映了运行 **RgyConfig** 工具时指定的值。

```
#IBM Tivoli Access Manager
#Mon Dec 03 10:40:06 MHT 2013
ldap.ssl-enable=false
ldap.bind-pwd={obf2}dwTRqM+riTiJyfwSscdYIsiAAb2aAXkqmJrtiJm2Hp4\=
ldap.bind-dn=cn\=root
ldap.mgmt-version=6.1.1
ldap.svrs=9.118.51.177 \1:389\:readwrite\:5;
local_domain=Default
ldap.mgmt=true
mgmt_domain=Default
delFromRegistry=true
```

完成下列步骤，以使配置生效:

1. 将新创建的 ISAM_API.properties 文件复制到 *sdi_solution_dir*/LDAPSync 目录中。
2. 重新启动 IBM Security Directory Integrator

配置插件属性

将插件连接到联合目录服务器中的流，并对插件配置属性指定值。

开始之前

完成第 55 页的『插件设置路线图』中的步骤 1 - 8。

过程

1. 在联合目录服务器控制台的**流**页面上单击流名称，然后单击**编辑**。
2. 在**源**选项卡上，单击**流挂钩**。
3. 选择**已启用**，以启用将组装流水线连接到流的功能。
4. 展开**用户添加/修改/删除**并选择**已启用**，以指示添加、修改或删除每个用户后，此特定流挂钩必须调用该组装流水线。
5. 单击**组装流水线**旁边的**浏览**。
6. 在浏览菜单中，展开 FDS_ISAM_Plugin，选择 ProvisionISAM，并单击**确定**。
7. 指定下列属性以配置此插件:

   isam.api.properties.filepath
   指定 IBM Security Access Manager API 属性文件的路径。

   缺省值为 LDAPSync/ISAM_API.properties。

   isam.domain
   指定要集成的 IBM Security Access Manager 域。

   此域名必须与用于创建 IBM Security Access Manager API 属性文件的域名相同。

   缺省值为 Default。

   isam.map.principalName
   指定所要同步的当前 Person 的相应 IBM Security Access Manager 条目的 principalName 映射指示信息。

   您可以使用下列其中一个特殊值:

   - targetRDN 指定目标 Person RDN。
   - sourceRDN 指定源 Person RDN。

   否则，此属性的值必须是从源端点读取的条目中某个属性的名称。

   缺省值为 targetRDN。

   注: 此解决方案的设置要求联合目录服务器与 IBM Security Access Manager 共享同一个 IBM Security Directory Server 实例。在这种情况下，必须指定 targetRDN 作为值。

   isam.map.secDN
   指定所要同步的当前 Person 的相应 IBM Security Access Manager 条目的 secDN 映射指示信息。

   您可以使用下列其中一个特殊值:

   - targetDN 指定目标 Person DN。
   - sourceDN 指定源 Person DN。
   - mapFile 指定映射文件处理 secDN。

   否则，此属性的值必须是从源端点读取的条目中某个属性的名称。

   缺省值为 targetRDN。

注: 此解决方案的设置要求联合目录服务器与 IBM Security Access Manager 共享同一个 IBM Security Directory Server 实例。在这种情况下，必须指定 targetRDN 作为值。

isam.mapFile
这是一个可选属性，用于指定要使用的映射文件的路径和文件名。

由于解决方案目录始终是 IBM Security Directory Integrator 的当前工作目录，因此您可以使用相对路径，例如 LDAPSync/FDS_ISAM_Plugin.map。

缺省值为 LDAPSync/FDS_ISAM_Plugin.map。

映射属性

将源端点属性映射到 IBM Security Access Manager 用户条目和组条目。

关于此任务

在联合目录服务器控制台中，流配置提供了用于映射属性的选项。但是，如果您尝试在流配置的**属性映射**选项卡上修改 FDS_ISAM_Plugin.map，那么结果可能并非您所需。您所作的更改不会保存在 FDS_ISAM_Plugin.map 文件中。这些更改将保存在具有另一文件名的 FDS_ISAM_Plugin.map 副本中，该文件名与流名称相对应。这可能与“流挂钩”页面中 **isam.mapFile** 属性值的配置有冲突，该属性值通常为 FDS_ISAM_Plugin.map。

过程

1. 在联合目录服务器控制台中的**公共设置**下方，单击**属性映射**。 这将列出 *sdi_solution_dir*/LDAPSync 目录中的属性映射。
2. 请选择 **FDS_ISAM_Plugin.map**。这将显示插件的属性映射表，其中列出了缺省映射。
3. 为 FDS_ISAM_Plugin.map 配置属性映射。请按第 12 页的『定制属性映射』中的指示信息执行操作。所需的最低限度映射是用于相应 IBM Security Access Manager 用户的 principalName 的源 Person 属性。缺省情况下，此值设置为源条目中的 UID 值。如果在源条目中找不到 UID，那么此插件将使用 sAMAccountName，后跟 employeeCode。

   在缺省的 FDS_ISAM_Plugin.map 中，存在下列属性:

   cn 用户或组的公共名称。

   description
   用户或组的描述。

   secAcctValid
   用户条目标志，用于启用或禁用 IBM Security Access Manager 用户帐户。

   - true 表示将帐户禁用。缺省值为 true。此值必须设置为 true，这样传递认证才会对供应的 IBM Security Access Manager 用户帐户生效。
   - false 表示不禁用帐户。

   secPwdValid
   用户条目标志，用于指示 IBM Security Access Manager 用户的 **userPassword** 属性是否有效。

- `true` 表示将帐户禁用。缺省值为 `true`。此值必须设置为 `true`，这样传递认证才会对供应的 IBM Security Access Manager 用户帐户生效。
- `false` 表示不禁用帐户。

sn 用户的姓氏。

并非所有属性都可能存在于缺省的 `FDS_ISAM_Plugin.map` 文件中。例如，由于不对密码进行同步，因此不需要 **userPassword**。IBM Security Directory Server 的传递认证功能会将来自 IBM Security Access Manager 的认证请求传递到源端点。以下列表对一些属性作了描述:

secDN
IBM Security Access Manager 目录中的用户条目和组条目的条目 DN。**isam.map.secDN** 属性描述如何映射此属性。仅当此属性的值设置为 `mapFile` 时，才会使用映射文件条目。

member
uniqueMember
为用户条目提供的属性，用于指定 IBM Security Access Manager 用户主体名称或其 `secDN` 值的可选列表。如果这些用户作为用户条目而存在，那么将添加到 IBM Security Access Manager 安全组中。

如果确定某个值是 `secDN` 值，那么将假定 DN 的 RDN 是用户主体名称。如果设置了变化量操作标志，那么将从组成员资格中除去所有标记为 `delete` 的值。

memberOf
为组条目提供的属性，用于指定用户条目所属 IBM Security Access Manager 安全组的可选名称列表。

此功能是为了您方便而提供。但是，通常通过映射用户条目的 `member` 属性来处理组成员资格。

userPassword
IBM Security Access Manager 用户的可选密码。

结果

属性映射将保存到 *sdi_solution_dir*/LDAPSync 目录中的 `FDS_ISAM_Plugin.map` 文件中。

验证插件设置

要测试此插件是否正常工作，您必须验证目标 IBM Security Directory Server 中的同步条目。

关于此任务

在联合目录服务器控制台中，您可以使用 LDAP 浏览器来验证目标 IBM Security Directory Server 中的条目。有关更多信息，请参阅第 9 页的『浏览目录条目』。

过程

1. 验证此插件是否已添加 IBM Security Access Manager 用户。这些用户条目必须出现在 IBM Security Directory Server 的 `SECAUTHORITY=instance name,cn=Users` 容器之下。

2. 如果您使用了 Default 作为 IBM Security Access Manager 实例，请在搜索起点 cn=Users,SECAUTHORITY=DEFAULT 下进行检查，并使用 principalname=* 作为过滤器进行搜索。验证是否每个与 IBM Security Directory Server 同步的 LDAP 人员条目也表示为 IBM Security Access Manager 用户。该用户的 secDN 必须指向相应的 LDAP 条目。
3. 使用已经与 IBM Security Directory Server 同步但其原始密码在源目录中的用户的凭证。如果登录成功，那么表明传递认证也正常工作。

故障诊断

了解常见错误的限制、日志文件和说明可以帮助您对 Federated Directory Server Plug-in for IBM Security Access Manager 进行故障诊断。

已知局限性

此解决方案使用了 IBM Security Access Manager Registry Direct API。不支持添加、修改或删除全局登录 (GSO) 用户。

日志文件

IBM Security Access Manager 同步过程将创建以下日志文件: *sdi_solution_dir*/LDAPSync/logs/*flow*-ProvisionISAM.log，其中 *flow* 是同步流的名称，这个同步流调用此插件以供应 IBM Security Access Manager。并且，还维护 50 个旧日志的历史记录。此日志通常包含有关问题的更多详细信息，包括所要同步的条目的 principalName 和 secDN。

IBM Security Access Manager 供应过程所报告的错误显示在联合目录服务器中。这些日志在记录的消息中通常包含文本 *afterwrite* 或 *post-write*。记录的消息通常由两部分组成，即，首先输出联合目录服务器错误，接着输出另一条消息以指示该错误的根本原因。

例如，执行写操作后，可能会发生以下错误:

```
CTGDII761E Error invoking afterwrite Hook
```

有时，初始消息还包含“配置和组装流水线”名称，缺省情况下，此名称为 FDS_ISAM_Plugin:/AssemblyLines/ProvisionISAM。

每个错误报告的最后一部分提供深入的信息，用于帮助您解决问题。

Mandatory attribute is missing from output map
此错误消息还包含 IBM Security Access Manager 所需的属性的名称。您必须更新映射文件，以确保返回此值。

CTGDIS047W Entry is not found
此错误仅在递增同步期间要从 IBM Security Access Manager 中删除用户时发生。此错误表示在 IBM Security Access Manager 注册表中找不到该用户。

CTGDKD262E Could not start Config Instance
在 *sdi_solution_dir*/configs 文件夹中找不到包含 IBM Security Access Manager 供应组装流水线的配置 XML 文件时，将发生此错误。缺省情况下，此文件为 FDS_ISAM_Plugin.xml。请确保将配置文件复制到此文件夹并重试。

HPDAA0321E The Distinguished Name does not map to an existing entry in the registry.

HPDAA0320E The Distinguished Name that is provided has incorrect syntax. 这些错误表示 secDN 属性值无效。

如果您将 **isam.map.secDN** 属性设置为 compute，请检查 **isam.user.container** 属性的值。此属性包含 IBM Security Access Manager 目录中的一个现有容器的 DN，用户条目将写入该容器。并且，请确保 **isam.map.secDN.type** 属性设置为 CN 或 UID。

如果 **isam.map.secDN** 属性设置为 mapFile，请确保映射文件包含 secDN 属性。映射分配必须生成语法正确的 DN 值。并且，DN 的后缀必须引用 IBM Security Access Manager 目录中的现有容器。

第 3 章 跨域身份管理系统

跨域身份管理系统 (SCIM) 是一种为身份管理定义模式和协议的标准。可使用 IBM Security Directory Integrator 和 IBM Security Directory Server 中提供的 SCIM 服务作为后端目录。还可以使用 SCIM 连接器来使 IBM Security Directory Integrator 解决方案能够读写支持 SCIM 协议的服务器。

概述

SCIM 是一种用户和组管理的新兴标准，通常用于替代传统 LDAP 协议。SCIM 提供了 HTTP REST、跨企业和云应用程序部署所需的灵活性。由于许多云服务不会提供 LDAP 接口，因此您可以使用与底层协议不同的 SCIM。

SCIM 协议是一种用于定制和管理 Web 上身份数据的应用程序级别的 REST 协议。该协议支持核心身份资源（这些资源为用户和组）以及定制资源扩展的创建、修改、检索和发现。

功能

SCIM 规范旨在轻松、快捷而又廉价地管理云应用程序和服务中的用户身份。

SCIM 提供以下功能:

- 基于现有模式和部署体验。
- 重点简化开发和集成。
- 应用现有认证、授权和隐私模型。

目的在于通过提供常见用户模式和扩展模型来降低用户管理操作的成本和复杂性。还会绑定文档以提供用于通过使用标准协议交换此模式的模式。

有关更多信息，请参阅 http://www.simplecloud.info/ 处的 SCIM Web 站点。

业务场景

非 LDAP 系统上的用户和组管理通常采用 SCIM 协议。企业内和云相关方案中的新应用程序均可使用 HTTP REST 来过滤掉基础技术。

SCIM 可成功用于下列方案:

- 使用 SCIM 作为供未来长期使用的配置协议来内部部署新身份服务。
- 不可接受 LDAP 作为协议的内部或外部云。
- 对将 SCIM 作为用户管理界面的 SaaS 应用程序进行配置。

有关更多信息，请参阅 http://www.simplecloud.info/ 处的 SCIM Web 站点并搜索 *SCIM 方案*。

IBM Security Directory Integrator 中的 SCIM 服务

IBM Security Directory Integrator 中的 SCIM 服务为 IBM Security Directory Server 提供 SCIM 接口并为使用 SCIM 协议的服务器提供 SCIM 连接器。

SCIM 服务可通过使用 IBM Security Directory Integrator 本身构建。该服务实际上是充当服务器的 IBM Security Directory Integrator 组装流水线。SCIM 服务器后端必须是包含身份数据的 IBM Security Directory Server。SCIM 服务器接收到 SCIM 请求并在内部连接到 IBM Security Directory Server 以访问用于服务这些请求的数据。

SCIM 连接器通过使用 JavaScript 和 HTTP 客户机连接器来实施 SCIM 协议。

受支持的软件

从 IBM Security Directory Integrator V7.2 开始随附且支持 IBM Security Directory Server V6.3.1 的 SCIM 服务。

在 IBM Security Directory Integrator 中实现的 SCIM 服务遵循 SCIM 1.1 规范。有关更多信息，请参阅 http://www.simplecloud.info/ 处的 SCIM Web 站点并搜索*规范*。

受支持的功能部件

IBM Security Directory Integrator 中的 SCIM 服务支持 SCIM V1.1 的大多数操作，并适当关注 V2.0 中的更改。

以下功能在当前版本的 SCIM 服务中受支持:

- 使用 IBM Security Directory Server 作为后端目录来管理用户和组
- 模式: 企业用户模式扩展
- JSON 数据类型
- GET/PUT/POST/DELETE 请求
- 补丁: 通过补丁 (HTTP) 请求进行修改以帮助使用者仅发送需要修改的属性
- 分页
- 认证方案: HTTP 基本认证
- 过滤功能让使用者能够使用 **filter** 查询参数来请求一部分资源。
- 部分资源让使用者能够使用 **attributes** 查询参数来指定必须在资源表示中返回的属性
- 排序功能让使用者能够指定返回资源的顺序。

当前版本的 SCIM 服务器不支持:

- OAuth 认证
- 批量更新
- 自动限制返回的资源数。

注: 要根据需要获取要工作的 SCIM 参数 **active**，必须在 IBM Security Directory Server 中开启密码策略。要打开密码策略，请根据 `cn=pwdpolicy,cn=ibmpolicies` 将 **ibm-pwdPolicy** 设置为 `true`。此设置允许 SCIM 从 IBM Security Directory Server 中读取 **ibm-pwdAccountLocked** 设置。有关设置密码策略的更多信息，请参阅 IBM Security Directory Server 文档并搜索“设置密码策略”。

配置文件

在部署 SCIM 服务之前，必须修改配置文件才能指定连接设置、用户和组映射以及模式。

在安装 IBM Security Directory Integrator 之后，可在 *tdi_install_dir* 中查找名为 SCIM 的文件夹。手动或者在启动服务器的情况下创建解决方案目录时，SCIM 文件夹将自动复制到解决方案目录。或者，也可以手动将 SCIM 文件夹复制到您的解决方案目录。

SCIM 文件夹包含以下文件集，其中包括您可修改以配置设置的配置文件。在大多数情况下，可能需要您仅更新 SCIM.properties 文件。其他文件可能不需要进行任何修改。

SCIM.properties

SCIM.properties 文件包含以下服务器系统特定属性，其中包括后端 IBM Security Directory Server 的详细信息。

位置
: 可从外部访问的 SCIM 服务的 URL。它仅影响 SCIM 答复中的位置头。

httpPort
: SCIM 服务用于侦听的端口。SCIM 服务始终使用 SSL。

LDAP.LookupLimit
: SCIM 服务可以找到的资源最大数。为了防止内存溢出，缺省值仅为 20000。

LDAPServer
: 用于存储用户数据的 IBM Security Directory Server 的 URL。

userSearchBase
: IBM Security Directory Server 中用户的搜索基础。

groupSearchBase
: IBM Security Directory Server 中组的搜索基础。

userObjectClass
: 在 IBM Security Directory Server 中创建用户时所使用的对象类的列表。

groupObjectClass
: 在 IBM Security Directory Server 中创建组时所使用的对象类的列表。

userSearchFilter
: 用于查找 userSearchBase 中的所有用户。

groupSearchFilter
: 用于查找 groupSearchBase 中的所有组。

dummyGroupMember
: 创建新组时，如果 **dummyGroupMember** 具有一个值并且组中没有任何成员，那么会添加此值以避免对象违例错误。

audit.log
: 将此参数设置为 true 以创建审计日志。

audit.logFile
: 审计日志文件的名称。

audit.logFileDatePattern
日期模式用于指定日志文件回滚到备份文件的频率。它也指定如何将日期附加到存储了先前日志的备份文件的文件名后。

audit.syslog
表明是否启用了 QRadar® 的系统日志记录。将值设置为 `true` 可启用它。

audit.QRadarHost
QRadar 所属的主机。

audit.QRadarPort
QRadar 的端口号。

audit.facility
审计消息的工具。

audit.eventID
审计日志中使用的事件标识。

audit.devTimeFormat
审计日志中使用的日期格式。

mapTenantNames
将此属性设置为 `true` 可以更改完成 SCIM 认证的方式。要获取更多信息以及此属性设置为 `true` 时可以使用的属性的列表，请参阅第 83 页的『对 SCIM 请求进行的认证』。

AuthenticationRealm
要求认证时提供给用户的域。

authenticationEndpoint
如果此属性设置为 `true`，那么将启用认证端点。缺省值为 `false`。

UserMapping.json and GroupMapping.json

`UserMapping.json` 和 `GroupMapping.json` 文件用于指定 SCIM 属性与 IBM Security Directory Server 用户或组属性之间的映射。这些文件中的每个条目包含 SCIM 属性名称和 LDAP 属性名称。条目中可能还包含以下附加属性。

ReadOnly
指定仅从 LDAP 映射到 SCIM 的值（而不采用其他方式）。

WriteOnly
指定仅从 SCIM 映射到 LDAP 的值（而不采用其他方式）。必须将此条目用于密码。

CreateDN
指定还用于在 IBM Security Directory Server 中创建专有名称 (DN) 的值，方法是将 userSearchBase 附加到该值。为能够创建新资源，必须存在一个具有 **CreateDN** 属性的条目，该属性使用始终提供的 SCIM 属性名称。

类型
提供多值属性的规范类型。

转换
指定属性值的转换。转换属性可具有下列其中一个值:

- **DateTime**，将值从 LDAP 日期格式转换为 SCIM 日期格式。

- **Group**，将值从 LDAP 组转换为 SCIM 组。
- **NewLines**，将 SCIM 值中的新行转换为 LDAP 值中的 $，反之亦然。

注:

- 每个 SCIM 名称必须只有一个映射条目，除非条目具有唯一的 **Type**。
- 每个 LDAP 名称必须只有一个条目，除非条目是 **ReadOnly** 的。

UserSchema.json and GroupSchema.json

UserSchema.json 和 GroupSchema.json 文件根据 SCIM 规范提供用户或组的模式定义。指定的属性必须与 UserMapping.json 和 GroupMapping.json 文件中定义的属性匹配。

ServiceProviderConfig.json
定义规范合规性、受支持的数据模型和认证方案等等。

SCIM.xml
用于实施 SCIM 服务的配置文件。

QRadarLogging.map

QRadarLogging.map 文件指定了当启用 QRadar 系统日志记录时发送到 QRadar 系统的属性值。

有关更多信息，请参阅 IBM Security Directory Integrator 安装的 *sdi_solution_dir* 内 SCIM 文件夹中的 Readme.txt 文件。

启动 SCIM 服务

使用 **ibmdisrv** 命令来启动 SCIM 服务。

开始之前

- 根据需要修改 SCIM 配置文件。

过程

运行以下命令:

```
ibmdisrv -c SCIM/SCIM.xml -r SCIM_Service -w
```

结果

启动 SCIM 服务时，它将尝试向 IBM Security Directory Server 进行匿名绑定。如果此操作失败，那么 SCIM 服务将停止并在 ibmdi.log 文件中显示一条消息: CTGDIS1930E 无法连接到 LDAP 服务器。

SCIM 连接器

可在 IBM Security Directory Integrator 中使用 SCIM 连接器来读写支持 SCIM 协议的服务器。

SCIM 连接器像其他 IBM Security Directory Integrator 连接器一样工作，但在后台会传递 REST 调用并使用 SCIM 操作。

有关如何配置和使用 SCIM 连接器的信息，请参阅 IBM Security Directory Integrator 文档 并搜索 *SCIM 连接器*。

日志记录和跟踪

SCIM 的日志记录和跟踪功能可帮助您找出问题的原因并解决这些问题。

可在 SCIM.properties 文件中将 **debug** 参数设置为 true，以增加日志文件中记录的数据量。

要配置审计日志记录，可在 SCIM.properties 文件中设置以下属性。

audit.log
指示是否开启日志记录功能。将值设置为 true 以开启日志记录功能。

auditLogFile
指定要在其中完成每日日志记录的文件名。

audit.logFileDatePattern
指定日志文件必须回滚到备份文件的频率。缺省值为 daily。仅当新的一天记录第一条消息时，才会发生回滚。可通过使用 log4j DailyRollingFileAppender 完成日志记录。

日志记录将以 JSON 格式完成，其中每一行都是一个 JSON 对象，如以下示例中所示:

```
{"url":"\/Users", "date":"2013-08-03 14:19:25,234","host":"127.0.0.1",
     "method":"POST","user":"cn=root",
     "resourceID":"cn=John Doe,ou=People,DC=EXAMPLE,DC=COM",
     "date":"2013-08-03 14:19:25,296","user":"cn=root","status":"201 Created"}
```

JSON 对象具有以下属性:

user
用于授权请求的用户名。

date
接收到请求的日期和时间。

remoteHost
从其接收请求的主机的 IP 地址。

remotePort
请求所来自的端口。

localHost
本地 IP 地址。

localPort
本地端口。

method
请求中的方法。

url
请求中的 URL。

userAgent
请求所来自的浏览器的名称（如果可用）。

resourceID
请求所创建或者所返回的资源标识。

status
所返回的 HTTP 状态。

SCIM 对象模型

SCIM 基于资源为常用分母且所有 SCIM 对象都从其派生的对象模型构建。

SCIM 当前具有三个直接从资源对象继承的对象。ServiceProviderConfiguration 和 Schema 用于发现且不包含任何用户信息。CoreResource 对象包含其两个子资源“用户”和“组”内的用户和组数据。

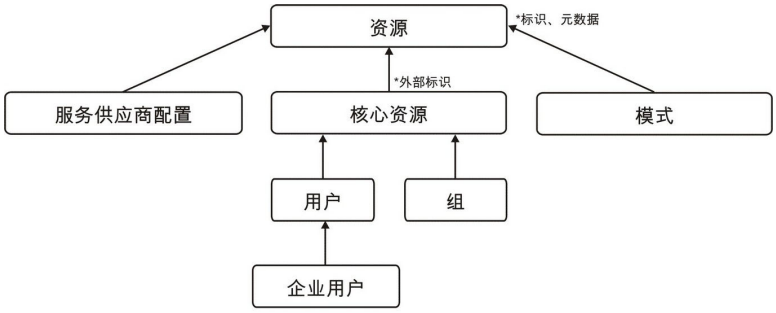


图 2. SCIM 对象模型

操作

SCIM 向 REST API 提供了一组您可用来管理资源的丰富而简单的操作。

SCIM 操作支持每一项内容，包括对特定用户修补特定属性到执行大批量更新。

创建 `POST https://example.com/{v}/{resource}`

读取 `GET https://example.com/{v}/{resource}/{id}`

替换 `PUT https://example.com/{v}/{resource}/{id}`

删除 `DELETE https://example.com/{v}/{resource}/{id}`

更新（Update）
`PATCH https://example.com/{v}/{resource}/{id}`

搜索

```
GET https://example.com/{v}/{resource}?filter={attribute}{op}{value}
    &sortBy={attributeName}&sortOrder={ascending|descending}
```

批量 `POST https://example.com/{v}/Bulk`

发现操作

为简化互操作性，SCIM 提供了两个端点来发现受支持的功能和特定属性详细信息。

GET /ServiceProviderConfigs
发现规范合规性、认证方案和数据模型。

GET /Schemas

- GET /Schemas/User
- GET /Schemas/Group

反思资源和属性扩展。

SCIM 操作示例

可使用 SCIM 操作来搜索、创建、修改或删除各种场景中的用户和组。

示例 1

要获取所有用户的列表，请发送以下请求:

```
GET /users
```

示例 2

以下示例说明如何获取所有用户的列表但仅包括 **displayName** 和 **id** 属性。它还将结果限制为从编号 11 到 20 的用户。

请求:

```
GET /users?attributes=displayName,id&count=10&startIndex=11
```

结果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"7b401115-35f2-4a74-8384-a684cb4f31a1",
      "displayName":"Alexander Shelton"
    }
,
        {
      "id":"44216fbe-36a1-4215-b6f7-032775bc5e07",
      "displayName":"Andy Walker"
    }
,
        {
      "id":"c5292b7e-ffeb-4855-a086-7289d3445bd6",
      "displayName":"Alan White"
    }
,
        {
      "id":"5ad2d53c-9844-48ca-8460-c0d80fec5972",
      "displayName":"Alan Worrell"
    }
,
        {
      "id":"2b62e6a0-a698-4ffb-a107-1078b2d56437",
      "displayName":"Barbara Francis"
    }
,
        {
      "id":"3904d440-3f54-46cf-b63a-aacab03ac767",
      "displayName":"Bjorn Free"
    }
,
```

```
        {
      "id":"abb9526e-dfa8-452a-9d88-9eff3d79da90",
      "displayName":"Barbara Hall"
    }
,
        {
      "id":"d7df93df-d0bd-4c60-ad52-ec2bf8917fbc",
      "displayName":"Benjamin Hall"
    }
,
        {
      "id":"f98c9470-d7fe-490f-ab71-e84c9d3e9448",
      "displayName":"Barbara Jablonski"
    }
,
        {
      "id":"87fd1385-7d13-4423-851a-fb1d047bc2f0",
      "displayName":"Bjorn Jensen"
    }

  ]
,
  "totalResults":"163",
  "startIndex":"11",
  "itemsPerPage":"10"
}
```

示例 3

以下示例用于获取 **familyName** 以 k 开头的所有用户的列表。

请求:

```
GET /users?filter=name.familyName sw "k"
```

结果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"6f0fa17b-d988-4f95-98c0-095a545cc44e",
      "externalID":"aknutson",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=aknutson,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Ashley Knutson",
      "name":      {
        "givenName":"Ashley",
        "familyName":"Knutson"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 2169"
        }
,
                {
          "type":"fax",
```

```
          "value":"+1 408 555 4774"
        }

      ]
,
      "emails":      [
            {
          "type":"work",
          "value":"aknutson@example.com"
        }

      ]

    }
,
        {
      "id":"6f7a3e28-db6c-4846-ae78-2346f39f65ee",
      "externalID":"ekohler",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=ekohler,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Elba Kohler",
      "name":      {
        "givenName":"Elba",
        "familyName":"Kohler"
      }
,
      "phoneNumbers":      [
            {
          "type":"work",
          "value":"+1 408 555 1926"
        }
,
            {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
            {
          "type":"work",
          "value":"ekohler@example.com"
        }

      ]

    }
,
        {
      "id":"e5318e13-1534-4eb9-9237-e1367a2744e1",
      "externalID":"skellehe",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=skellehe,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Sue Kelleher",
      "name":      {
        "givenName":"Sue",
        "familyName":"Kelleher"
      }
```

```
,
      "phoneNumbers":      [
                {
           "type":"work",
           "value":"+1 408 555 3480"
         }
,
                {
           "type":"fax",
           "value":"+1 408 555 8721"
         }

      ]
,
      "emails":      [
                {
           "type":"work",
           "value":"skellehe@example.com"
         }

      ]

    }
,
        {
      "id":"3bac3d16-33ee-4a39-a6d1-063c5537530a",
      "externalID":"tkelly",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=tkelly,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Timothy Kelly",
      "name":      {
        "givenName":"Timothy",
        "familyName":"Kelly"
      }
,
      "phoneNumbers":      [
                {
           "type":"work",
           "value":"+1 408 555 4295"
         }
,
                {
           "type":"fax",
           "value":"+1 408 555 1992"
         }

      ]
,
      "emails":      [
                {
           "type":"work",
           "value":"tkelly@example.com"
         }

      ]

    }

  ]
,
  "totalResults":"4"
}
```

示例 4

以下示例说明如何搜索具有**标识**为 2064f364-260b-4c29-8c28-b12583486ca3 的用户。

请求:

```
GET /users/2064f364-260b-4c29-8c28-b12583486ca3
```

结果:

```
{
  "id":"2064f364-260b-4c29-8c28-b12583486ca3",
  "externalID":"abergin",
  "meta":  {
    "created":"2013-04-16T09:14:02Z",
    "modified":"2013-04-16T09:14:02Z"
  }
,
  "userName":"uid=abergin,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "groups":  [
        {
      "value":"57a96228-48a6-4f29-a8ad-345828fccd6a",
      "display":"QA Managers"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

示例 5

以下示例说明如何获取在所指定的日期之后创建的所有用户的列表。

请求:

```
GET /users?filter=meta.created gt "2013-05-17T00:00:00Z"
```

结果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"78a13de7-0ef9-42ae-ba7c-b9c64a2050aa",
      "externalID":"wlutz2",
      "meta":      {
        "created":"2013-05-21T11:39:48Z",
        "modified":"2013-05-21T11:53:30Z"
      }
,
      "userName":"uid=wlutz2,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Wendy Lutz",
      "name":      {
        "givenName":"Wendy",
        "familyName":"Lutz"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 3358"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"wlutz@example.com"
        }

      ]

    }
,
        {
      "id":"a4cc7512-1530-4adc-952b-cd752aa79828",
      "externalID":"wlutz4",
      "meta":      {
        "created":"2013-05-21T11:54:12Z",
        "modified":"2013-05-21T11:54:12Z"
      }
,
      "userName":"uid=wlutz4,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Wendy Lutz",
      "name":      {
        "givenName":"Wendy",
        "familyName":"Lutz"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 3358"
```

```
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"wlutz@example.com"
        }

      ]

    }
,
        {
      "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
      "externalID":"abergin2",
      "meta":      {
        "created":"2013-05-24T11:29:51Z",
        "modified":"2013-05-24T11:51:09Z"
      }
,
      "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Andy Bergin Jr",
      "name":      {
        "givenName":"Andy",
        "familyName":"Bergin"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 8585"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 7472"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"abergin@example.com"
        }

      ]

    }

  ]
,
  "totalResults":"3"
}
```


示例 6

要创建用户，请发送以下请求:

```
POST /users
```

正文必须包含有关 JSON 格式的新用户的信息，如以下示例中所示:

```
{
      "externalID":"abergin2",
      "displayName":"Andy Bergin",
      "name":      {
        "givenName":"Andy",
        "familyName":"Bergin"
      }
,
      "phoneNumbers":      [
                {
           "type":"work",
           "value":"+1 408 555 8585"
         }
,
                {
           "type":"fax",
           "value":"+1 408 555 7472"
         }

      ]
,
      "emails":      [
                {
           "type":"work",
           "value":"abergin@example.com"
         }

      ]
}
```

结果:

```
200 OK
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
```

```
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

示例 7

以下示例说明如何修改用户。它仅包含在上一示例中创建的标识为 b9be8c033-cf93-448e-a96b-d1290ff6d445 的用户的 **displayName**。

请求:

```
PATCH /users/b9be8c033-cf93-448e-a96b-d1290ff6d445
```

HTTP 正文必须包含以下信息:

```
{
 "displayName":"Andy Bergin Jr"
}
```

结果:

```
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin Jr",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "schemas":  [
```

```
    "urn:scim:schemas:core:1.0"
  ]

}
```

注: 要使用没有 **PATCH** 命令的浏览器来测试操作，您可将 HTTP 头 X-HTTP-Method-Override 的值设置为 PATCH。也可以使用此设置来解决阻止某些 HTTP 方法的防火墙。

示例 8

以下示例说明如何删除**标识** 为 2064f364-260b-4c29-8c28-b12583486ca3 的用户。

请求:

```
DELETE /users/2064f364-260b-4c29-8c28-b12583486ca3
```

结果:

```
200 OK
```

示例 9

要获取所有组的列表，请使用以下请求:

```
GET /groups
```

示例 10

以下示例说明如何按特定组的**标识**来对其进行搜索。

请求:

```
GET /groups/5653c887-1d5a-42cf-a470-6a2fe2608730
```

结果:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
    "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

示例 11

以下示例说明如何按组的**标识**来对其进行搜索。

请求:

```
GET /groups?filter=displayName eq "Accounting Managers"
```

结果:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
     "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

示例 12

以下示例说明如何创建组。

请求:

```
POST /groups
```

正文必须包含有关新组的信息:

```
{
       "externalID":"Test Group",
       "displayName":"Test Group",
      "members":      [
     "5156d423-3c74-415b-844f-606a2aabafcc",
     "900faa78-d7c6-421c-9181-313134d17dd0"
      ]
    }
```

结果:

```
201 Created
{
  "id":"7e15ce9e-2fe7-4624-b5d5-adedc242e07a",
  "externalID":"Test Group",
  "meta":  {
    "created":"2013-05-27T02:37:38Z",
    "modified":"2013-05-27T02:37:38Z"
```

```
  }
,
  "displayName":"Test Group",
  "members":  [
        {
      "value":"5156d423-3c74-415b-844f-606a2aabafcc",
      "display":"Kirsten Vaughan"
    }
,
        {
      "value":"900faa78-d7c6-421c-9181-313134d17dd0",
      "display":"Robert Daugherty"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

对 SCIM 请求进行的认证

SCIM 认证服务对 SCIM 标准进行了扩展，以启用认证调用以及用户和组管理。

除了对 Schema 或 ServiceProviderConfig 对象发出的请求以外，所有 SCIM 请求都必须经过认证。如果此类请求未经认证，那么将返回 401 Unauthorized 消息。

此认证将使用典型的 HTTP 基本授权头，后者包含用户名和密码的基本 64 位编码。此机制与大多数浏览器使用的过程相同。

认证凭证的情况分为两种:

- 在 SCIM.properties 文件中，未将 **mapTenantNames** 属性的值指定为 true。在这种情况下，用户名必须是作为 SCIM 服务组装流水线后端服务器的 LDAP 服务器所知的 LDAP 名称。用户名及其相应密码将发送到此 LDAP 服务器以进行验证。
- 在 SCIM.properties 文件中，将 **mapTenantNames** 属性的值指定为 true。在这种情况下，必须在 SCIM.properties 文件中指定更多属性以定义此用户名。例如，如果用户名为 domain，那么可以指定 domain.ldapName=cn=root。这表示来自 HTTP 用户名 domain 的请求将使用用户名 cn=root 与 LDAP 服务器绑定。对于密码，如果您指定了 domain.password=Secret 和 domain.ldapPassword=VerySecret，那么 HTTP 请求密码必须为 Secret，否则认证将失败。发送到 LDAP 服务器的密码为 VerySecret。如果未指定这两个属性，那么密码将直接发送到 LDAP 服务器。

如果对用户 domain 实施了访问权限制，那么对请求进行的授权也可能失败。如果未指定 **domain.access** 属性，或者此属性与使用的资源和方法不匹配，那么将不会对该请求进行授权。如果将 **mapTenantNames** 设置为 true，那么此设置还将允许使用所有用户的访问权属性。

访问权验证

如果将 **mapTenantNames** 属性设置为 true，那么所有请求还将验证用户的访问权。要对请求进行授权，您必须对 **domain.access** 属性指定与请求的资源和方法匹配的值。**domin.access** 属性值必须是以逗号分隔的关键字字符串。缺省情况是无访问权。可以使用下列关键字:

all 允许进行所有访问。

createUser
发布 (POST) 用户。

createGroup
发布 (POST) 组。

modifyUser
修补 (PATCH) 或保存 (PUT) 用户。

modifyGroup
修补 (PATCH) 或保存 (PUT) 组。

deleteUser
删除 (DELETE) 用户。

deleteGroup
删除 (DELETE) 组。

readUser
获取 (GET) 一个或多个用户。

readGroup
获取 (GET) 一个或多个组。

auth 通过非标准端点或认证来认证用户。

为了确保安全，访问控制还验证所请求资源的 LDAP DN 是否与 LDAP 搜索起点匹配。

认证端点

如果在 SCIM.properties 文件中设置了属性 authenticationEndpoint=true，那么将启用 SCIM 协议的本地扩展，并且可以认证用户名。

即使是对认证端点的使用也必须获得授权。与所有其他 SCIM 请求相同，Authorization 头必须包含用户名和密码。此用户名和密码的用法如上一节所述。授权凭证与所要认证的用户并非直接相关。请使用 userName sw "Je" 之类的过滤器来指定所要认证的用户，其中 sw 表示开始内容为。认证服务在授权凭证的帮助下查找此用户。必须正好有一个用户与过滤条件匹配。然后，此服务使用此用户的 DN 以及 Authentication-Password 头中指定的密码来尝试与 LDAP 服务器绑定。此尝试将产生下列其中一个结果:

- 如果绑定成功，那么将返回 204 No Content 应答。
- 如果由于该用户不存在或者密码不匹配而导致认证失败，那么将返回 403 Forbidden 应答。
- 如果不存在 Authentication-Password 头，那么将返回 403 No Password 应答。

使用端点名称 authentication 来访问认证端点，如以下示例请求所示:

```
GET /authentication?filter=userName eq "Some User"
Authorization: Basic  QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Authentication-Password: secret
```

HTTP 响应码

这里描述针对成功的操作和错误返回的 HTTP 响应码。

成功的操作

200 OK

操作成功完成。

201 Created

创建用户或组成功。

204 No Content

认证请求成功。

错误

400 Bad Request

在 URL 中缺少路径部分。

已尝试更改常量端点（例如模式）。

端点未知。

提供了不具有外部标识的 POST 请求（创建用户或组）。

在修改（PUT、PATCH 或 DELETE）请求中未提供标识。

在尝试解析请求时发生异常。

在修改（PUT 或 PATCH）请求中未包括 HTTP 主体。

在修改（PUT 或 PATCH）请求中未能将 HTTP 主体解析为 JSON。

未能将组成员属性中提供的标识转换为 LDAP DN。

未能成功地解析搜索过滤器。

401 Unauthorized

未提供凭证。

凭证（用户名或密码）不正确。

试图在用户名的作用域外部修改该用户。

此用户不具有访问权。

此用户无权执行所尝试的操作。

403 Forbidden

试图认证不存在的用户。

提供的用于认证用户的密码不正确。

403 No Password

已尝试认证用户，但 HTTP 头“Authentication-Password”中未提供密码。

404 Not Found

针对未知的模式发出了请求。

试图修改（PUT、PATCH 或 DELETE）找不到的用户或组。

试图查找（GET）找不到的用户或组。

409 Conflict

试图创建已存在的用户或组。

409 Duplicate

至少两个用户与 AUTHENTICATE 请求中的过滤器匹配。

500 Internal server error

创建用户或组后找不到该用户或组。

尝试处理请求时发生异常。

找不到模式文件。

找不到用户或组映射文件。

无法解析用户或组映射文件。

用户或组映射未包含创建 DN 的方式。

501 Not Implemented

试图发送或接收 XML 编码信息。

未识别 HTML 操作。

503 Service Unavailable

无法连接到后端 LDAP 服务器。

声明

本信息是为在美国提供的产品和服务编写的。IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档中描述的内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

下图不适用英国或任何这样的条款与当地法律不一致的国家或地区:

INTERNATIONAL BUSINESS MACHINES CORPORATION“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。

某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

这些信息包含日常业务操作中使用的数据和报告示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名称均是虚构的，如与实际的商业企业使用的名称和地址有任何相似之处，纯属巧合。

版权许可:

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。用户如果是为了按照 IBM 应用程序编程接口开发、使用、经销或分发应用程序，那么可以任何形式复制、修改和分发这些样本程序，而无须向 IBM 付费。

凡这些样本程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明:

© （公司名称）（年份）。此部分代码是根据 IBM Corp. 公司的样本程序衍生出来的。
© Copyright IBM Corp.（输入年份）。All rights reserved.

如果您正以软拷贝格式查看本信息，图片和彩色图例可能无法显示。

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. 当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上“版权和商标信息”部分获取。

Adobe、Acrobat、PostScript 以及所有基于 Adobe 的商标是 Adobe Systems Incorporated 在美国和／或其他国家或地区的注册商标或商标。

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的商标。

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open、LTO、LTO 徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 和 Quantum 在美国和其他国家的商标。

索引

J

L

Q

S

Printed in China

S151-2130-01