Red Hat Directory Server 12

安装 Red Hat Directory Server

管理目录服务器安装、更新和卸载的说明。开始使用实例所需的基本任务

Last Updated: 2024-07-09

Red Hat Directory Server 12 安装 Red Hat Directory Server

管理目录服务器安装、更新和卸载的说明。开始使用实例所需的基本任务

法律通告

摘要

使用命令行或 Web 控制台安装、更新和卸载目录服务器 12 和相关服务。了解如何以 FIPS 模式运行实例，创建测试条目、登录到 Web 控制台、启动和停止目录服务器实例，以及更改 LDAP 和 LDAPS 端口号。

目录

提供有关红帽目录服务器的反馈

我们感谢您对我们文档和产品的输入信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交有关红帽目录服务器文档的反馈（需要帐户）：
  1. 转至 红帽问题跟踪程序。
  2. 在 **Summary** 字段中输入描述性标题。
  3. 在 **Description** 字段中输入您对改进的建议。包括到文档相关部分的链接。
  4. 点对话框底部的 **Create**。
- 通过 JIRA 提交有关红帽目录服务器产品的反馈（需要帐户）：
  1. 转至 红帽问题跟踪程序。
  2. 在 **Create Issue** 页面上，单击 **Next**。
  3. 填写 **Summary** 字段。
  4. 在 **Component** 字段中选择组件。
  5. 填写 **Description** 字段，包括：
     a. 所选组件的版本号。
     b. 重现问题的步骤或您的建议以改进。
  6. 点 **Create**。

第 1 章 在命令行中使用 .INF 文件设置新实例

当您在命令行中使用 **.inf** 文件设置 Directory 服务器时，您可以自定义高级设置。例如，您可以在 **.inf** 文件中自定义以下设置：

- 在服务启动后，用户和组 **ns-slapd** Directory Server 进程使用。请注意，如果您使用不同的用户和组，则必须在开始安装前手动创建用户和组。
- 路径，如配置、备份和数据目录。
- 证书的有效性。

1.1. 前提条件

- 服务器满足最新红帽目录服务器版本要求，如 Red Hat Directory Server 12 发行注记 所述。

1.2. 安装 DIRECTORY 服务器软件包

使用以下步骤安装 Directory 服务器软件包。

前提条件

- 在 Red Hat Subscription Management 服务中注册了该系统。
- 您的红帽帐户中有有效的红帽目录服务器订阅。
- RHEL 默认软件仓库 **BaseOS** 和 **AppStream** 已被启用。

流程

1. 如果您的帐户禁用了简单内容访问(SCA)：
   a. 列出您的红帽帐户中的可用订阅，该订阅提供 Red Hat Directory Server 订阅，并记录池 ID：

```
# subscription-manager list --all --available --matches 'Red Hat Directory Server'
...
Subscription Name:   Example Subscription
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

   b. 使用其池 ID 将红帽目录服务器订阅附加到系统：

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Example Subscription
```

2. 启用 Directory Server 存储库。例如，要启用 Directory Server 12.4 存储库，请运行：

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. 安装 **redhat-ds:12** 模块：

```
# dnf module install redhat-ds:12
```

这个命令会自动安装所有必需的依赖项。

其他资源

- 使用 Red Hat Subscription Manager
- 简单内容访问
- 需要启用的红帽软件仓库的名称

1.3. 为 DIRECTORY SERVER 实例安装创建 .INF 文件

为 **dscreate** 实用程序创建一个 **.inf** 文件，并将 文件调整为您的环境。在后续步骤中，您将使用此文件创建新的 Directory 服务器实例。

前提条件

- 已安装 **redhat-ds:12** 模块。

流程

1. 使用 **dscreate create-template** 命令创建模板 **.inf** 文件。例如，要在 **/root/instance_name.inf** 文件中存储模板，请输入：

```
# dscreate create-template /root/instance_name.inf
```

创建的文件包含所有可用的参数，包括描述。

2. 编辑您在上一步中创建的文件：

   a. 取消注释您要设置为自定义安装的参数。
   所有参数都有默认值。但是，红帽建议您为生产环境自定义某些参数。例如，在 **[slapd]** 部分至少设置以下参数：

```
instance_name = instance_name
root_password = password
```

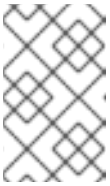
   b. 要在实例创建过程中自动创建后缀，请在 **[backend-userroot]** 部分中设置以下参数：

```
create_suffix_entry = True
suffix = dc=example,dc=com
```

重要

如果在实例创建过程中没有创建后缀，则必须稍后手动创建它，然后才能将数据存储到这个实例中。

c. 可选：卸载其他参数，并将其设置为适合您的环境值。例如，使用这些参数指定复制选项，如身份验证凭据和更改日志修剪，或为 LDAP 和 LDAPS 协议设置不同的端口。



注意

默认情况下，您创建的新实例包含自签名证书和启用 TLS。为提高安全性，红帽建议您不要禁用此功能。请注意，您可以稍后将自签名证书替换为认证机构 (CA)发布的证书。

其他资源

- 启用到目录服务器的 TLS 加密连接

1.4. 使用 .INF 文件设置新的 DIRECTORY SERVER 实例

这部分论述了如何使用 **.inf** 文件使用命令行设置新的 Directory Server 实例。

前提条件

- 您为 Directory Server 实例创建了一个 **.inf** 文件。

流程

1. 将 **.inf** 文件传递给 **dscreate from-file** 命令，以创建新实例：

```
# dscreate from-file /root/instance_name.inf
Starting installation ...
Validate installation settings ...
Create file system structures ...
Create self-signed certificate database ...
Perform SELinux labeling ...
Perform post-installation tasks ...
Completed installation for instance: slapd-instance_name
```

dscreate 工具会自动启动实例，并将 RHEL 配置为在系统引导时启动服务。

2. 在防火墙中打开所需端口：

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

3. 重新载入防火墙配置：

```
# firewall-cmd --reload
```

第 2 章 使用交互式安装程序在命令行中设置新实例

管理员可以通过回答有关新实例配置的问题，来使用 Directory Server 互动安装程序设置新实例。

如果要在安装过程中自定义附加设置，请使用 **.inf** 文件，而不是互动安装程序。详情请查看 第 1 章 *在命令行中使用 .inf 文件设置新实例*。

2.1. 前提条件

- 服务器满足最新红帽目录服务器版本要求，如 Red Hat Directory Server 12 发行注记 所述。

2.2. 安装 DIRECTORY 服务器软件包

使用以下步骤安装 Directory 服务器软件包。

前提条件

- 在 Red Hat Subscription Management 服务中注册了该系统。
- 您的红帽帐户中有有效的红帽目录服务器订阅。
- RHEL 默认软件仓库 **BaseOS** 和 **AppStream** 已被启用。

流程

1. 如果您的帐户禁用了简单内容访问(SCA)：
   a. 列出您的红帽帐户中的可用订阅，该订阅提供 Red Hat Directory Server 订阅，并记录池 ID：

```
# subscription-manager list --all --available --matches 'Red Hat Directory Server'
...
Subscription Name:   Example Subscription
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

   b. 使用其池 ID 将红帽目录服务器订阅附加到系统：

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Example Subscription
```

2. 启用 Directory Server 存储库。例如，要启用 Directory Server 12.4 存储库，请运行：

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. 安装 **redhat-ds:12** 模块：

```
# dnf module install redhat-ds:12
```

这个命令会自动安装所有必需的依赖项。

其他资源

- 使用 Red Hat Subscription Manager
- 简单内容访问
- 需要启用的红帽软件仓库的名称

2.3. 使用互动安装程序创建实例

本节介绍如何使用交互式安装程序创建新的 Directory Server 实例。

流程

1. 启动交互式安装程序：

```
# dscreate interactive
```

2. 回答交互式安装程序的问题。
要使用安装程序中大部分问题后面的方括号中显示的默认值，请按 **Enter** 键，而无需输入值。

```
Install Directory Server (interactive mode)
===========================================

Enter system's hostname [server.example.com]:

Enter the instance name [server]: instance_name

Enter port number [389]:

Create self-signed certificate database [yes]:

Enter secure port number [636]:

Enter Directory Manager DN [cn=Directory Manager]:

Enter the Directory Manager password: password
Confirm the Directory Manager Password: password

Enter the database suffix (or enter "none" to skip) [dc=server,dc=example,dc=com]:
dc=example,dc=com

Create sample entries in the suffix [no]:

Create just the top suffix entry [no]: yes

Do you want to start the instance after the installation? [yes]:

Are you ready to install? [no]: yes
```

注意

您可以设置由 **pwdhash** 生成的 **{*algorithm*}*hash*** 字符串来设置密码，而不是使用明文密码。

3. 在防火墙中打开所需端口：

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

4. 重新载入防火墙配置：

```
# firewall-cmd --reload
```

第 3 章 使用 WEB 控制台设置新实例

如果您希望基于浏览器的界面来设置 Directory 服务器，您可以使用 Directory Server Web 控制台。

3.1. 前提条件

- 服务器满足最新 Red Hat Directory Server 版本的要求，如 Red Hat Directory Server 12 发行注记所述。
- 已安装 Directory 服务器软件包，如 安装 Directory 服务器软件包所述

3.2. 使用 WEB 控制台设置新的 DIRECTORY SERVER 实例

本节论述了如何使用 Web 控制台设置新的 Directory Server 实例。

前提条件

- 已安装 **cockpit** Web 控制台软件包。
- **cockpit.socket** systemd 单元已启用并启动。
- 您在本地防火墙中打开了端口 **9090**，以允许访问 Web 控制台。

流程

1. 使用浏览器连接到在 Directory Server 主机上端口 9090 上运行的 Web 控制台：

   https://*server.example.com*:9090

2. 以 **root** 用户身份登录，或者以具有 sudo 权限的用户登录。
3. 选择 **Red Hat Directory Server** 条目。
4. 创建新实例：
   - 如果服务器上不存在任何实例，请单击 **Create New Instance** 按钮。
   - 如果服务器已在运行现有的实例，请选择 **Actions**，再单击 **Create New Instance**。
5. 完成 **Create New Server Instance** 表单的字段：
   - **实例名称** ：设置实例的名称。请注意，您不能在创建实例后更改实例的名称。
   - **端口**：设置 LDAP 协议的端口号。端口不能被其他实例或服务使用。默认端口为 389。
   - **安全端口** ：设置 LDAPS 协议的端口号。端口不能被其他实例或服务使用。默认端口为 636。
   - **创建自签署的 TLS 证书 DB：在实例中启用 TLS 加密，并创建一个自签名证书。**
     为提高安全性，红帽建议您创建一个启用了自签名证书和 TLS 的新实例。请注意，您可以稍后将自签名证书替换为认证机构(CA)发布的证书。
   - **目录管理器 DN** ：设置实例的管理用户的可分辨名称(DN)。默认值为 **cn=Directory Manager**。

- **目录管理器** 密码：设置实例的管理用户的密码。
- **确认密码**: Must 的值与 **Directory Manager Password** 字段中的值相同。
- **Create Database** ：选择此字段以在实例创建过程中自动创建后缀。

重要

如果在实例创建过程中没有创建后缀，则必须稍后手动创建它，然后才能将数据存储到这个实例中。

如果启用了这个选项，请填写添加字段：

- **Database Suffix** ：设置后端的后缀。
- **Database Name** ：设置后端数据库的名称。
- **数据库初始化** ：将此字段设置为 **Create Suffix Entry**。

6. 点 **Create Instance**。
新实例启动，并配置为在系统引导时自动启动。
7. 在防火墙中打开所需端口：

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

8. 重新载入防火墙配置：

```
# firewall-cmd --reload
```

其他资源

- 启用到目录服务器的 TLS 加密连接

第 4 章 以非 ROOT 用户身份设置新实例

如果您没有 **root** 权限，您可以以用户身份执行目录服务器安装。使用此方法测试目录服务器和开发 LDAP 应用程序。但请注意，**非 root** 用户运行的实例存在限制，例如：

- 它们不支持简单网络管理协议(SNMP)。
- 它们只能使用大于或等于 1024 的端口。

4.1. 准备环境以作为用户安装目录服务器

如果没有 **root** 权限，在创建和管理目录服务器实例前，您需要使用 **dscreate ds-root** 命令准备适当的环境。

前提条件

- 您以 **root** 用户身份安装了 Directory Server 软件包。

流程

1. 确保 PATH 变量中有 **$HOME/bin**。如果没有：
   a. 在 **~/.bash_profile** 文件中附加以下内容：

   ```
   PATH="$HOME/bin:$PATH"
   ```

   b. 重新读取 **~/bash_profile** 文件：

   ```
   $ source ~/.bash_profile
   ```

2. 配置实例创建的环境以使用自定义位置：

   ```
   $ dscreate ds-root $HOME/dsroot $HOME/bin
   ```

   此命令将标准安装路径替换为 **$HOME/dsroot/**，并在 **$HOME/bin/** 目录中创建标准目录服务器管理工具的副本。

3. 要使 shell 使用新路径：
   a. 清除缓存：

   ```
   $ hash -r dscreate
   ```

   b. 验证 shell 是否使用正确的命令路径：

   ```
   $ which dscreate
   ~/bin/dscreate
   ```

对于 **dscreate** 命令，shell 现在使用 **$HOME/bin/dscreate** 而不是 **/usr/bin/dscreate**。

4.2. 以非 ROOT 用户身份安装新实例

要在没有 **root** 权限的情况下安装目录服务器，您可以使用交互式安装程序。安装后，Directory 服务器会在自定义位置创建一个实例，用户可以像常一样运行 **dscreate**、**dsctl**、**dsconf** 实用程序。

前提条件

- 为非 root 安装准备了环境。
- 您有 **sudo** 权限来使用 **firewall-cmd** 工具，如果要从外部提供目录服务器实例。

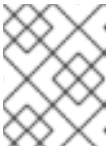
流程

1. 使用互动安装程序创建实例

   a. 启动交互式安装程序：

   ```
   $ dscreate interactive
   ```

   b. 回答交互式安装程序的问题。
   要使用安装程序中大部分问题后面的方括号中显示的默认值，请按 **Enter** 键，而无需输入值。

   注意

   在安装过程中，您必须选择实例端口和安全端口号 **大于 1024** （例如 1389 和 1636）。否则，用户没有绑定到特权端口(1-1023)的权限。

   ```
   Install Directory Server (interactive mode)
   ===========================================
   Non privileged user cannot use semanage, will not relabel ports or files.

   Selinux support will be disabled, continue? [yes]: yes

   Enter system's hostname [server.example.com]:

   Enter the instance name [server]: instance_name

   Enter port number [389]: 1389

   Create self-signed certificate database [yes]:

   Enter secure port number [636]: 1636

   Enter Directory Manager DN [cn=Directory Manager]:

   Enter the Directory Manager password: password
   Confirm the Directory Manager Password: password

   Enter the database suffix (or enter "none" to skip) [dc=server,dc=example,dc=com]:
   dc=example,dc=com

   Create sample entries in the suffix [no]:

   Create just the top suffix entry [no]: yes
   ```

```
Do you want to start the instance after the installation? [yes]:

Are you ready to install? [no]: yes
```

注意

您可以设置由 **pwdhash** 生成的 **{*algorithm*}*hash*** 字符串来设置密码，而不是使用明文密码。

2. 可选：如果要使目录服务器实例从外部可用：

   a. 在防火墙中打开端口：

   ```
   # sudo firewall-cmd --permanent --add-port={1389/tcp,1636/tcp}
   ```

   b. 重新载入防火墙配置：

   ```
   # sudo firewall-cmd --reload
   ```

验证

- 运行 **ldapsearch** 命令来测试用户可以连接到实例：

```
$ ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com:1389 -b
"dc=example,dc=com" -s sub -x "(objectclass=*)"
```

其他资源

- 为非 root 用户安装准备环境
- 如何使用非 root 权限绑定 1024 以下的端口

第 5 章 使用负载均衡器后面的 KERBEROS 身份验证安装 DIRECTORY 服务器

安装在负载均衡器后面工作的 Directory 服务器实例并支持 Kerberos 身份验证需要在安装过程中比较额外的步骤。

如果用户使用通用安全服务 API (GSSAPI)访问服务，则 Kerberos 主体包括服务的 DNS 名称。如果用户连接到负载均衡器，则主体包含负载均衡器的 DNS 名称，例如：**ldap/loadbalancer.example.com@EXAMPLE.COM**，而不是 Directory Server 实例的 DNS 名称。

为便于成功连接，接收请求的 Directory 服务器实例必须使用与负载均衡器相同的名称，即使负载均衡器 DNS 名称不同。

这部分论述了如何使用负载均衡器后面的 Kerberos 身份验证设置 Directory Server 实例。

5.1. 前提条件

- 服务器满足最新红帽目录服务器版本要求，如 Red Hat Directory Server 12 发行注记 所述。

5.2. 安装 DIRECTORY 服务器软件包

使用以下步骤安装 Directory 服务器软件包。

前提条件

- 在 Red Hat Subscription Management 服务中注册了该系统。
- 您的红帽帐户中有有效的红帽目录服务器订阅。
- RHEL 默认软件仓库 **BaseOS** 和 **AppStream** 已被启用。

流程

1. 如果您的帐户禁用了简单内容访问(SCA)：
   a. 列出您的红帽帐户中的可用订阅，该订阅提供 Red Hat Directory Server 订阅，并记录池 ID：

```
# subscription-manager list --all --available --matches 'Red Hat Directory Server'
...
Subscription Name:   Example Subscription
Provides:            ...
                     Red Hat Directory Server
                     ...
Pool ID:             5ab6a8df96b03fd30aba9a9c58da57a1
Available:           1
...
```

   b. 使用其池 ID 将红帽目录服务器订阅附加到系统：

```
# subscription-manager attach --pool=5ab6a8df96b03fd30aba9a9c58da57a1
Successfully attached a subscription for: Example Subscription
```

2. 启用 Directory Server 存储库。例如，要启用 Directory Server 12.4 存储库，请运行：

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. 安装 **redhat-ds:12** 模块：

```
# dnf module install redhat-ds:12
```

这个命令会自动安装所有必需的依赖项。

其他资源

- 使用 Red Hat Subscription Manager
- 简单内容访问
- 需要启用的红帽软件仓库的名称

5.3. 为 DIRECTORY SERVER 实例安装创建 .INF 文件

为 **dscreate** 实用程序创建一个 **.inf** 文件，并将 文件调整为您的环境。在后续步骤中，您将使用此文件创建新的 Directory 服务器实例。

前提条件

- 已安装 **redhat-ds:12** 模块。

流程

1. 使用 **dscreate create-template** 命令创建模板 **.inf** 文件。例如，要在 **/root/instance_name.inf** 文件中存储模板，请输入：

```
# dscreate create-template /root/instance_name.inf
```

创建的文件包含所有可用的参数，包括描述。

2. 编辑您在上一步中创建的文件：

   a. 取消注释您要设置为自定义安装的参数。
   所有参数都有默认值。但是，红帽建议您为生产环境自定义某些参数。例如，在 **[slapd]** 部分至少设置以下参数：

```
instance_name = instance_name
root_password = password
```

   b. 要在带有 GSSAPI 身份验证的负载均衡器后使用实例，将 **[general]** 部分中的 **full_machine_name** 参数设置为负载均衡器的完全限定域名(FQDN)，而不是 Directory Server 主机的 FQDN:

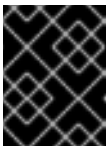
```
full_machine_name = loadbalancer.example.com
```

   c. 取消注释 **[general]** 部分中的 **strict_host_checking** 参数，并将它设为 **False** ：

```
strict_host_checking = False
```

d. 要在实例创建过程中自动创建后缀，请在 **[backend-userroot]** 部分中设置以下参数：

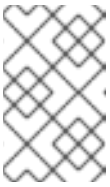
```
create_suffix_entry = True
suffix = dc=example,dc=com
```



重要

如果在实例创建过程中没有创建后缀，则必须稍后手动创建它，然后才能将数据存储到这个实例中。

e. 可选：卸载其他参数，并将其设置为适合您的环境值。例如，使用这些参数指定复制选项，如身份验证凭据和更改日志修剪，或为 LDAP 和 LDAPS 协议设置不同的端口。



注意

默认情况下，您创建的新实例包含自签名证书和启用 TLS。为提高安全性，红帽建议您不要禁用此功能。请注意，您可以稍后将自签名证书替换为认证机构(CA)发布的证书。

其他资源

- 启用到目录服务器的 TLS 加密连接

5.4. 使用 .INF 文件设置新的 DIRECTORY SERVER 实例

这部分论述了如何使用 **.inf** 文件使用命令行设置新的 Directory Server 实例。

前提条件

- 您为 Directory Server 实例创建了一个 **.inf** 文件。

流程

1. 将 **.inf** 文件传递给 **dscreate from-file** 命令，以创建新实例：

```
# dscreate from-file /root/instance_name.inf
Starting installation ...
Validate installation settings ...
Create file system structures ...
Create self-signed certificate database ...
Perform SELinux labeling ...
Perform post-installation tasks ...
Completed installation for instance: slapd-instance_name
```

dscreate 工具会自动启动实例，并将 RHEL 配置为在系统引导时启动服务。

2. 在防火墙中打开所需端口：

```
# firewall-cmd --permanent --add-port={389/tcp,636/tcp}
```

3. 重新载入防火墙配置：

```
# firewall-cmd --reload
```

5.5. 为负载均衡器创建 KEYTAB，并将 DIRECTORY 服务器配置为使用 KEYTAB

在用户使用 GSSAPI 在负载均衡器后对 Directory 服务器进行身份验证之前，您必须为负载均衡器创建 Kerberos 主体，并将 Directory 服务器配置为使用 Kerberos 主体。本节描述了这个步骤。

前提条件

- 包含以下 **.inf** 文件配置的实例：
  - **full_machine_name** 参数设为负载均衡器的 DNS 名称。
  - **strict_host_checking** 参数设置为 **False**。

流程

1. 为负载均衡器创建 Kerberos 主体，如 **ldap/*loadbalancer.example.com*@*EXAMPLE.COM***。创建服务主体的步骤取决于您的 Kerberos 安装。详情请查看您的 Kerberos 服务器文档。
2. 可选：您可以在 keytab 文件中添加更多主体。例如，要让用户通过使用 Kerberos 身份验证直接连接到负载均衡器后面的 Directory Server 实例，可以为 Directory Server 主机添加额外的主体。例如： **ldap/*server1.example.com*@*EXAMPLE.COM***.
3. 将服务 keytab 文件复制到 Directory 服务器主机上，并将其存储，例如在 **/etc/dirsrv/slapd-*instance_name*/ldap.keytab** 文件中。
4. 将服务 keytab 的路径添加到 **/etc/sysconfig/slapd-*instance_name*** 文件中：

```
KRB5_KTNAME=/etc/dirsrv/slapd-instance_name/ldap.keytab
```

5. 重启 Directory Server 实例：

```
# dsctl instance_name restart
```

验证

- 验证您可以使用 GSSAPI 协议连接到负载均衡器：

```
# ldapsearch -H ldap://loadbalancer.example.com -Y GSSAPI
```

如果您在 keytab 文件中添加了额外的 Kerberos 主体，如 Directory Server 主机本身，还要验证这些连接：

```
# ldapsearch -H ldap://server1.example.com -Y GSSAPI
```

第 6 章 以 FIPS 模式运行 DIRECTORY 服务器

目录服务器全面支持联邦信息处理标准 (FIPS) 140-2。当您以 FIPS 模式运行 Directory 服务器时，与安全相关的设置改变。例如，SSL 会自动禁用，且只使用 TLS 1.2 和 1.3 加密。

6.1. 启用 FIPS 模式

要在联邦信息处理标准(FIPS)模式中使用 Directory Server，请在 RHEL 和 Directory Server 中启用模式。

前提条件

- 在 RHEL 中启用了 FIPS 模式。

流程

1. 为网络安全服务(NSS)数据库启用 FIPS 模式：

```
# modutil -dbdir /etc/dirsrv/slapd-instance_name/ -fips true
```

2. 重启实例：

```
# dsctl instance_name restart
```

验证

- 验证为 NSS 数据库启用了 FIPS 模式：

```
# modutil -dbdir /etc/dirsrv/slapd-instance_name/ -chkfips true
FIPS mode enabled.
```

如果模块采用 **FIPS 模式，该命令会返回启用了** FIPS 模式。

6.2. 其他资源

- 联邦信息处理标准(FIPS)
- 将系统切换到 FIPS 模式

第 7 章 将 DIRECTORY SERVER 更新至新的次版本

红帽经常发布对 Red Hat Directory Server 12 的更新版本。这部分论述了如何更新 Directory 服务器软件包。

如果要将 Red Hat Directory Server 11 迁移到版本 12，请参阅 迁移目录服务器 11 到 Directory Server 12 。

7.1. 更新 DIRECTORY 服务器软件包

使用 **dnf** 工具更新模块，该模块也会自动更新相关软件包。以下流程将目录服务器从版本 12.3 更新至 12.4。

前提条件

- Red Hat Directory Server 12.3 已安装在服务器上。
- 您的红帽帐户中有有效的红帽目录服务器订阅。

流程

1. 禁用 Directory Server 12.3 存储库：

```
# subscription-manager repos --disable dirsrv-12.3-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.3-for-rhel-9-x86_64-rpms' is disabled for this system.
```

2. 启用 Directory Server 12.4 存储库：

```
# subscription-manager repos --enable=dirsrv-12.4-for-rhel-9-x86_64-rpms
Repository 'dirsrv-12.4-for-rhel-9-x86_64-rpms' is enabled for this system.
```

3. 更新 Directory 服务器软件包：

```
# dnf module update redhat-ds
```

dnf module update redhat-ds 命令将目录服务器软件包及其依赖项更新至版本 12.4。

更新过程会自动重启服务器上的所有实例的 **dirsrv** 服务。

其他资源

- 需要启用的红帽软件仓库的名称

第 8 章 将 DIRECTORY SERVER 11 迁移到 DIRECTORY SERVER 12

了解从红帽目录服务器 11 迁移到 12，包括迁移开始前必须执行的任务。

重要

红帽支持只在 Red Hat Directory Server 10 或 11 迁移到版本 12。要从早期版本中迁移目录服务器，您必须执行增量迁移到目录服务器 10 或 11。

红**帽不支持使用 leapp** 升级工具将 Directory Server 10 或 11 服务器的原位升级为 12 版本。

8.1. 前提条件

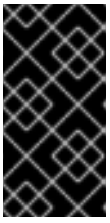
- 现有 Directory Server 安装在版本 11 上运行，并安装了所有可用的更新。

8.2. 使用复制方法迁移到 DIRECTORY SERVER 12

在复制拓扑中，使用复制方法迁移到 Directory Server 12。

流程

1. 安装目录服务器 12.
2. 在 Directory Server 12 主机上，启用复制，但不创建复制协议。有关启用复制的详情，请参阅 *配置和管理 红帽目录服务器 12 的复制* 文档。
3. 在 Directory Server 11 主机上，启用复制并创建指向 Directory Server 12 主机的复制协议。如需更多信息，请参阅 *Red Hat Directory Server 11 管理员指南中的 多供应商复制 部分*。



重要

如果您在 Directory Server 11 主机上使用了自定义配置，**请不要将** Directory Server 12 主机上的 **dse.ldif** 配置文件替换为 Directory Server 11 主机上的文件，因为版本间的 **dse.ldif** 布局变化。反之，使用 **dsconf** 工具或 Web 控制台为您需要的每个参数和插件添加自定义配置。

4. 可选：设置其他目录服务器 12 个主机，在 Directory Server 12 主机之间使用复制协议。
5. 将您的客户端配置为使用 Directory Server 12 主机。
6. 在 Directory Server 11 主机上，删除指向目录服务器 12 主机的复制协议。请参阅 *红帽目录服务器 11 管理指南中的从复制拓扑中删除* 目录服务器实例。
7. 卸载 Directory Server 11 主机。请参阅 *Red Hat Directory Server 11 安装指南中的 卸载* 目录服务器。

8.3. 使用导出和导入方法迁移到 DIRECTORY SERVER 12

使用导出和导入方法迁移小型目录服务器环境，如没有复制的实例。

流程

1. 在现有的 Directory Server 11 主机上执行以下步骤：

   a. 停止并禁用 **dirsrv** 服务：

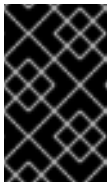
   ```
   # dsctl instance_name stop
   # systemctl disable dirsrv@instance_name
   ```

   b. 导出后端。例如，要导出 **userRoot** 后端，并将其存储在 **/var/lib/dirsrv/slapd-*instance_name*/userRoot.ldif** 文件中，请运行：

   ```
   # dsctl instance_name db2ldif userroot
   /var/lib/dirsrv/slapd-instance_name/userRoot.ldif
   ```

   c. 将以下文件复制到您要安装 Directory Server 12 的新主机：

   - 您在上一步中导出的 **/var/lib/dirsrv/slapd-*instance_name*/userRoot.ldif** 文件。
   - **/etc/dirsrv/slapd-*instance_name*/dse.ldif** 配置文件。

   重要

   不要将 Directory Server 12 主机上的 **dse.ldif** 配置文件替换为 Directory Server 11 主机上的文件，因为 **dse.ldif** 布局更改了不同的版本。存储 **dse.ldif** 文件以备参考。

   - 如果您使用自定义模式，**/etc/dirsrv/slapd-*instance_name*/schema/99user.ldif**
   - 如果要迁移启用了 TLS 的实例，并重复使用 Directory Server 12 安装的相同主机名，请将以下文件复制到新主机：
     - **/etc/dirsrv/slapd-*instance_name*/cert9.db**
     - **/etc/dirsrv/slapd-*instance_name*/key4.db**
     - **/etc/dirsrv/slapd-*instance_name*/pin.txt**

   d. 如果要在 Directory Server 12 主机上使用相同的主机名和 IP，请断开旧服务器与网络的连接。

2. 在新主机上执行以下步骤：

   a. 安装目录服务器 12.

   b. 可选：配置 TLS 加密：

   - 如果新安装使用与 Directory Server 11 实例不同的主机名，请参阅 *保护红帽目录服务器* 文档中的 启用 TLS 加密连接 部分。
   - 使用与之前的 Directory Server 11 安装相同的主机名：

     i. 停止实例：

     ```
     # dsctl instance_name stop
     ```

     ii. 删除网络安全服务(NSS)数据库和目录服务器的密码文件（如果存在）：

```
# rm /etc/dirsrv/slapd-instance_name/cert*.db
/etc/dirsrv/slapd-instance_name/key*.db
/etc/dirsrv/slapd-instance_name/pin.txt
```

iii. 将您从 Directory Server 11 主机复制的 **cert9.db**、**key4.db** 和 **pin.txt** 文件放在 **/etc/dirsrv/slapd-*instance_name*/** 目录中。

iv. 为 NSS 数据库和密码文件设置正确的权限：

```
# chown dirsrv:root /etc/dirsrv/slapd-instance_name/cert9.db
/etc/dirsrv/slapd-instance_name/key4.db
/etc/dirsrv/slapd-instance_name/pin.txt

# chmod 600 /etc/dirsrv/slapd-instance_name/cert9.db
/etc/dirsrv/slapd-instance_name/key4.db
/etc/dirsrv/slapd-instance_name/pin.txt
```

v. 启动实例：

```
# dsctl instance_name start
```

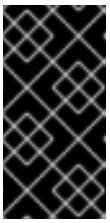
c. 如果您使用自定义模式，请将 **99user.ldif** 文件放在 **/etc/dirsrv/slapd-*instance_name*/schema/** 目录中，设置适当的权限，然后重启实例：

```
# cp /tmp/99user.ldif /etc/dirsrv/slapd-instance_name/schema/

# chmod 644 /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# chown root:root /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# dsctl instance_name restart
```

d. 导入 LDIF 文件。例如：将 ***/var/lib/dirsrv/slapd-*instance_name*/ldif/migration.ldif*** 文件导入到 **用户Root** 数据库中：

```
# dsconf -D 'cn=Directory Manager' ldap://server.example.com backend import
userRoot /var/lib/dirsrv/slapd-instance_name/ldif/migration.ldif
```

请注意，Directory 服务器需要您要导入到 **/var/lib/dirsrv/slapd-*instance_name*/** 目录的 LDIF 文件。



重要

如果您在 Directory Server 11 主机上使用了自定义配置，**请不要将** Directory Server 12 主机上的 **dse.ldif** 配置文件替换为 Directory Server 11 主机上的文件。反之，使用 **dsconf** 工具或 Web 控制台为每个所需的参数和插件手动添加自定义配置。

第 9 章 将目录服务器 10 迁移到目录服务器 12

了解从红帽目录服务器 10 迁移到 12 的信息，包括开始迁移前必须执行的任务。

重要

红帽支持只在 Red Hat Directory Server 10 或 11 迁移到版本 12。要从早期版本中迁移目录服务器，您必须执行增量迁移到目录服务器 10 或 11。

红**帽不支持使用 leapp** 升级工具将 Directory Server 10 或 11 服务器的原位升级为 12 版本。

9.1. 前提条件

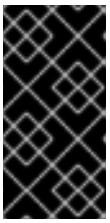
- 现有目录服务器安装在版本 10 上运行，并安装了所有可用的更新。

9.2. 使用复制方法将目录服务器 10 迁移到版本 12

在复制拓扑中，使用复制方法迁移到目录服务器 12。

流程

1. 在新主机上安装目录服务器 12。
2. 在 Directory Server 12 主机上，启用复制，但不创建复制协议。有关启用复制的详情，请参考 *Red Hat Directory Server 12* 文档中的 配置和管理复制。
3. 在 Directory Server 10 主机上，启用复制并创建指向目录服务器 12 主机的复制协议。有关启用复制的详情，请参考 Red Hat Directory Server 10 管理指南中的第 15 章"管理复制"。



重要

如果您在 Directory Server 10 主机上使用了自定义配置，**请不要将** Directory Server 12 主机上的 **dse.ldif** 配置文件替换为之前版本中的文件，因为 **dse.ldif** 布局在版本之间有所变化。反之，使用 **dsconf** 工具或 Web 控制台为您需要的每个参数和插件添加自定义配置。

4. 可选：设置 Directory Server 12 主机之间的复制协议的进一步目录服务器 12 主机。
5. 将客户端配置为使用 Directory Server 12 主机。
6. 在 Directory Server 10 主机上，删除指向目录服务器 12 主机的复制协议：

```
# ldapmodify -D "cn=Directory Manager" -W -x -p 389 -h server_ds_10.example.com
dn: cn=agreement-to-DS-12-server,cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping
tree,cn=config
changetype: delete
```

7. 卸载目录服务器 10 主机。请参阅 Red Hat Directory Server 10 安装指南中的第 4.8 章节"卸载目录服务器"。

9.3. 使用导出和导入方法将目录服务器 10 迁移到版本 12

使用导出和导入方法迁移大型目录服务器环境。

流程

1. 在现有目录服务器 10 主机上执行以下步骤：

   a. 停止并禁用 **dirsrv** 服务：

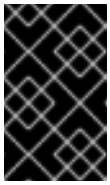
   ```
   # dsctl instance_name stop
   # systemctl disable dirsrv@instance_name
   ```

   b. 导出后端。例如，要导出 **userRoot** 后端并将其存储在 **/tmp/userRoot.ldif** 文件中：

   ```
   # db2ldif -Z instance_name -n userRoot -a /tmp/userRoot.ldif
   ```

   c. 将以下文件复制到您要安装 Directory Server 12 的新主机：

   - 您在上一步中导出的 LDIF 文件 **userRoot.ldif**。
   - 如果您使用自定义模式，**/etc/dirsrv/slapd-*instance_name*/schema/99user.ldif** 文件。
   - **/etc/dirsrv/slapd-*instance_name*/dse.ldif** 配置文件。

   重要

   不要将 Directory Server 12 主机上的 **dse.ldif** 配置文件替换为 Directory Server 10 主机上的文件，因为 **dse.ldif** 布局在版本之间有所变化。存储 **dse.ldif** 文件以备参考。

   - 如果要迁移启用了 TLS 并重复使用目录服务器 12 安装相同的主机名的实例，请复制：
     - **/etc/dirsrv/slapd-*instance_name*/cert8.db**
     - **/etc/dirsrv/slapd-*instance_name*/key3.db**
     - **/etc/dirsrv/slapd-*instance_name*/pin.txt**

   d. 如果要在 Directory Server 12 主机上使用相同的主机名和 IP，请断开旧服务器与网络的连接。

2. 在新目录服务器 12 主机上执行以下步骤：

   a. 安装目录服务器 12.

   b. 可选：配置 TLS 加密：

   - 如果全新安装使用了与 Directory Server 10 实例不同的主机名，请参阅 *保护 Red Hat Directory Server* 文档中的启用 TLS 加密连接到 Directory Server 部分。
   - 如果要使用与之前的目录服务器 10 安装相同的主机名：

     i. 停止实例：

     ```
     # dsctl instance_name stop
     ```

     ii. 删除网络安全服务(NSS)数据库和目录服务器的密码文件（如果存在）：

```
# rm /etc/dirsrv/slapd-instance_name/cert*.db
/etc/dirsrv/slapd-instance_name/key*.db
/etc/dirsrv/slapd-instance_name/pin.txt
```

iii. 将从 Directory Server 10 主机复制的 **cert8.db**、**key3.db** 和 **pin.txt** 文件移到 **/etc/dirsrv/slapd-*instance_name*/** 目录中。

iv. 为 NSS 数据库和密码文件设置正确的权限：

```
# chown dirsrv:root /etc/dirsrv/slapd-instance_name/cert8.db
/etc/dirsrv/slapd-instance_name/key3.db
/etc/dirsrv/slapd-instance_name/pin.txt

# chmod 600 /etc/dirsrv/slapd-instance_name/cert8.db
/etc/dirsrv/slapd-instance_name/key3.db
/etc/dirsrv/slapd-instance_name/pin.txt
```

v. 启动实例：

```
# dsctl instance_name start
```

c. 如果您使用了自定义模式，请将 **99user.ldif** 文件恢复到 **/etc/dirsrv/slapd-*instance_name*/schema/** 目录，并设置适当的权限并重启实例：

```
# cp /tmp/99user.ldif /etc/dirsrv/slapd-instance_name/schema/

# chmod 644 /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# chown root:root /etc/dirsrv/slapd-instance_name/schema/99user.ldif

# dsctl instance_name restart
```

d. 将您准备在 Directory Server 10 主机上的 **/tmp/userRoot.ldif** 文件放在 **/var/lib/dirsrv/slapd-*instance_name*/ldif/** 目录中。

e. 导入 **userRoot.ldif** 文件，以使用所有条目恢复 **userRoot** 后端：

```
# dsconf -D 'cn=Directory Manager' ldap://server.example.com backend import
userRoot /var/lib/dirsrv/slapd-instance_name/ldif/userRoot.ldif
```

请注意，Directory Server 12 只能从 **/var/lib/dirsrv/slapd-*instance_name*/** 目录中导入 LDIF 文件。

重要

如果您在 Directory Server 10 主机上使用了自定义配置，**请不要将** Directory Server 12 主机上的 **dse.ldif** 配置文件替换为之前版本中的文件。反之，使用 **dsconf** 工具或 Web 控制台为每个所需的参数和插件手动添加自定义配置。

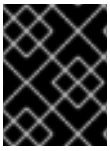
第 10 章 安装、更新和卸载密码同步服务

要在 Active Directory 和 Red Hat Directory Server 之间同步密码，您可以使用密码同步服务。您可以安装、更新和删除密码同步服务。

10.1. 密码同步服务

当您设置密码与 Active Directory 同步时，Directory 服务器会检索除密码以外的用户对象的所有属性。Active Directory 仅存储加密的密码，但目录服务器使用不同的加密。因此，Active Directory 用户密码必须由 Directory Server 加密。

要启用 Active Directory 和 Directory 服务器之间的密码同步，**Red Hat Directory Password Sync** 服务 hook 最多为 Windows 密码更改域控制器(DC)的例程。如果用户或管理员设置或更新密码，服务会在加密并存储在 Active Directory 之前以纯文本形式检索密码。这个过程可让 **Red Hat Directory Password Sync** 将纯文本密码发送到 Directory 服务器。为保护密码，该服务只支持到 Directory 服务器的 LDAPS 连接。当 Directory 服务器在用户的条目中存储密码时，密码会自动使用 Directory Server 中配置的密码存储方案加密。



重要

在 Active Directory 中，所有可写 DC 都可以处理密码操作。因此，您必须在 Active **Directory 域中的每个可写 DC 上安装 Red Hat Directory 密码同步**。

10.2. 下载密码同步服务安装程序

要安装 **Red Hat Directory 密码同步** 服务，请从客户门户网站下载安装程序。

前提条件

- 您有一个有效的红帽目录服务器订阅。
- 在红帽客户门户网站中有一个帐户 。

流程

1. 登录到红帽客户门户网站。
2. 点页面顶部的 **Downloads**。
3. 从产品列表中选择 **Red Hat Directory Server**。
4. 在 **Version** 字段中选择 **12**。
5. 下载 **PassSync 安装程序**。
6. 将安装程序复制到每个可写的 Active Directory 域控制器(DC)中。

10.3. 安装密码同步服务

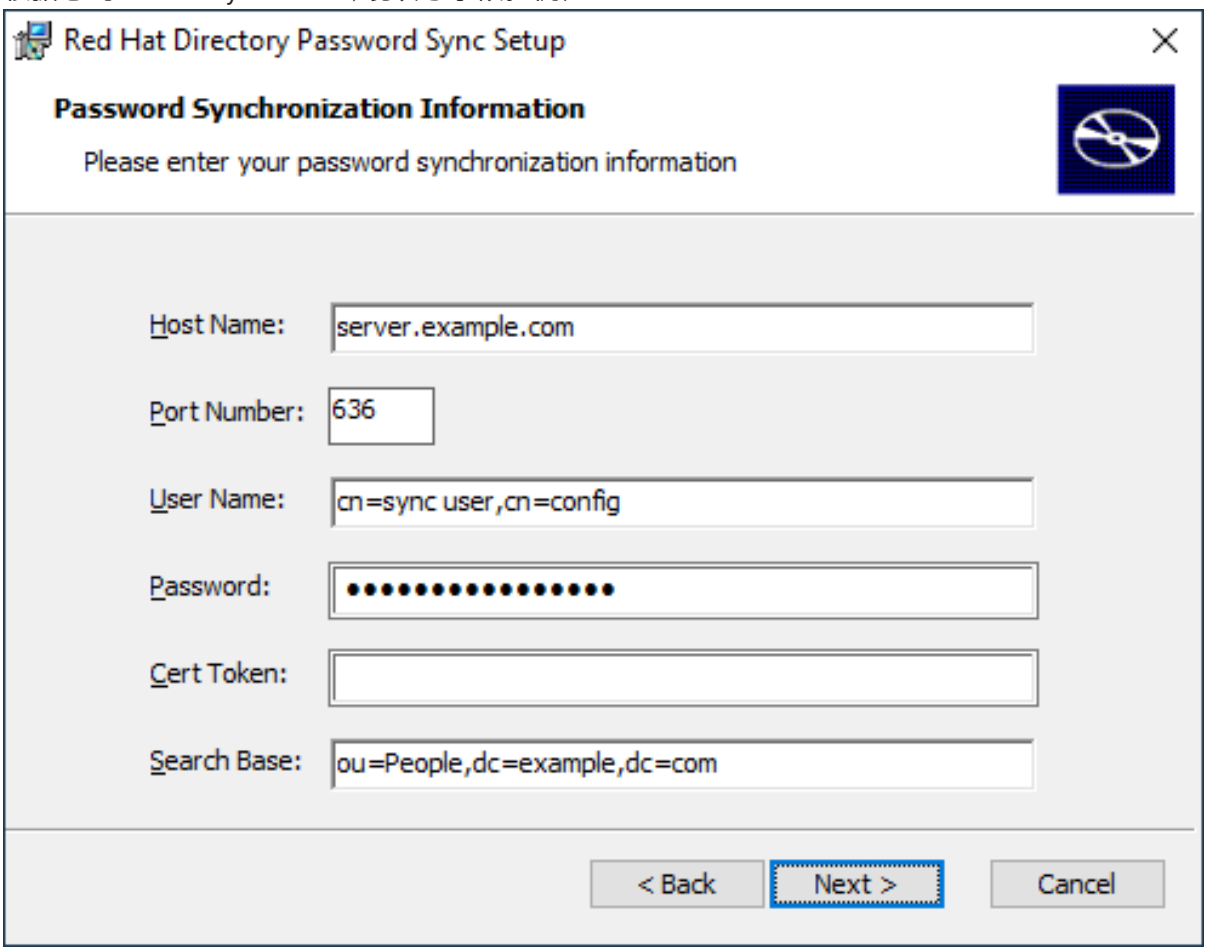
这部分论述了如何在 Windows 域控制器(DC)上安装 **Red Hat Directory Password Sync**。在每个可写 Windows DC 上执行这个步骤。

前提条件

- 将 **PassSync** 安装程序的最新版本下载到 Windows Active Directory 域控制器(DC)。
- 您在 Directory 服务器中启用了 TLS 加密。
- 您已准备 Active Directory 域。
- 您在 Directory Server 中创建了一个用于同步的帐户。

流程

1. 使用具有在 DC 上安装软件权限的用户登录到 Active Directory DC。
2. 双击 **RedHat-PassSync-ds12.*-x86_64.msi** 文件来安装它。
3. 此时会出现 **Red Hat Directory Password Sync Setup**。点击 **Next**。
4. 根据您的 Directory Server 环境填写字段。例如：



将 Directory Server 主机的以下信息填写到字段中：

- **主机名** ：设置目录服务器主机的名称。另外，您可以将该字段设置为 Directory Server 主机的 IPv4 或 IPv6 地址。
- **端口号** ：设置 LDAPS 端口号。
- **User Name** ：设置同步用户帐户的可分辨名称(DN)。
- **Password** ：设置同步用户的密码。
- **cert Token** ：设置从 Directory Server 主机复制的服务器证书的密码。

- **搜索 Base** ：设置包含同步用户帐户的 Directory Server 条目的 DN。

5. 点 **Next** 开始安装。
6. 点 **Finish**。
7. 重新引导 Windows DC。

重要

在不重新启动 DC 的情况下，**密码Hook.dll** 库不会被启用，密码同步会失败。

8. 在 Directory 服务器中启用复制并创建 WinSync 协议。

其他资源

- 启用到目录服务器的 TLS 加密连接

10.4. 更新密码同步服务

这部分论述了如何在 Windows 域控制器(DC)上更新现有 **Red Hat Directory Password Sync** 安装。

在每个可写 Windows DC 上执行这个步骤。

前提条件

- **Red Hat Directory 密码同步** 在您的 Windows DC 上运行。
- 将 **PassSync** 安装程序的最新版本下载到 Windows Active Directory DC。

流程

1. 使用具有在 DC 上安装软件权限的用户登录到 Active Directory 域控制器。
2. 双击 **RedHat-PassSync-ds12.*-x86_64.msi** 文件。
3. 点 **Next** 开始安装。
4. 点 **修改** 按钮。
5. 设置显示上一个安装过程中设置的配置。点 **Next** 以保留现有设置。
6. 点 **Next** 开始安装。
7. 点 **Finish**。
8. 重新引导 Windows DC。

重要

在不重新启动 DC 的情况下，**PasswordHook.dll** 库不会被启用，密码同步将失败。

10.5. 卸载密码同步服务

如果您不再需要 **Red Hat Directory Password Sync** 服务，将其从 Active Directory 域控制器(DC)中删除。

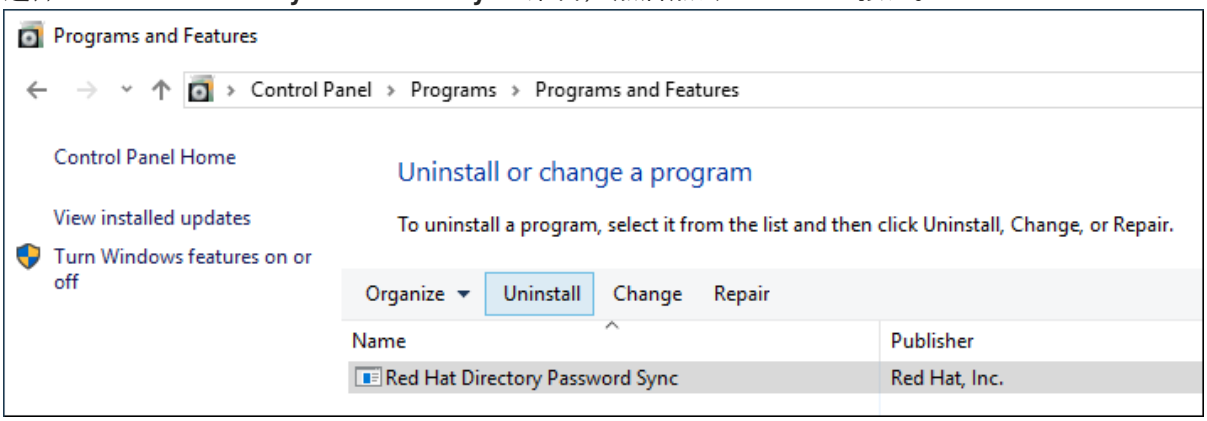
前提条件

- **Red Hat Directory 密码同步** 安装在 Windows DC 上。

流程

使用具有从 DC 中删除软件权限的用户登录到 Active Directory 域控制器。

1. 打开 **Control Panel**
2. 单击 **"程序"**，然后单击 **"程序"和功能**
3. 选择 **Red Hat Directory Password Sync** 条目，然后点击 **Uninstall** 按钮。



4. 单击 **Yes** 进行确认。

第 11 章 删除 DIRECTORY 服务器实例

如果不再需要 Directory Server 实例，您可以将其删除来重新获取磁盘空间。如果您在一个服务器上运行多个实例，删除特定实例不会影响其他实例。

11.1. 使用命令行删除实例

您可以使用命令行删除 Directory 服务器实例。

前提条件

- 该实例已从复制拓扑中删除，如果它属于其中一个。

流程

1. 可选：创建 Directory 服务器目录的备份：
   a. 停止实例：

```
# dsctl instance_name stop
```

   b. 复制 **/var/lib/dirsrv/slapd-*instance_name*/** 目录：

```
# cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/var-lib-
dirsrv-instance_name.bak/
```

   此目录包含数据库，以及备份和恢复目录。

   c. 复制 **/etc/dirsrv/slapd-*instance_name*/** 目录：

```
# cp -rp /etc/dirsrv/slapd-instance_name/ /root/etc-dirsrv-instance_name.bak/
```

2. 删除实例：

```
# dsctl instance_name remove --do-it
Removing instance ...
Completed instance removal
```

验证

- 验证 **/var/lib/dirsrv/slapd-*instance_name*/** 和 **/etc/dirsrv/slapd-*instance_name*/** 目录已被删除：

```
# ls /var/lib/dirsrv/slapd-instance_name /etc/dirsrv/slapd-instance_name/
ls: cannot access '/var/lib/dirsrv/slapd-instance_name': No such file or directory
ls: cannot access '/etc/dirsrv/slapd-instance_name': No such file or directory
```

其他资源

- 从复制拓扑中删除实例

11.2. 使用 WEB 控制台删除实例

您可以使用 Web 控制台删除 Directory Server 实例。但是，如果要创建包含的 Directory 服务器目录的备份，例如数据库和配置文件，则必须在命令行中复制这些目录。

前提条件

- 该实例已从复制拓扑中删除，如果它属于其中一个。
- 在 web 控制台中登录到实例。

流程

1. 可选：创建 Directory 服务器目录的备份。
   a. 点 **Actions** 按钮，然后选择 **Stop instance**。
   b. 复制 **/var/lib/dirsrv/slapd-*instance_name*/** 目录：

   ```
   # cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/var-lib-dirsrv-instance_name.bak/
   ```

   此目录包含数据库，以及备份和恢复目录。
   c. 复制 **/etc/dirsrv/slapd-*instance_name*/** 目录：

   ```
   # cp -rp /var/lib/dirsrv/slapd-instance_name/ /root/etc-dirsrv-instance_name.bak/
   ```

2. 单击 **Actions** 按钮，然后选择 **Remove this instance**。
3. 选择" **是"，我确定**，然后单击" **删除实例** "以确认。

验证

- 验证 **/var/lib/dirsrv/slapd-*instance_name*/** 和 **/etc/dirsrv/slapd-*instance_name*/** 目录已被删除：

```
# ls /var/lib/dirsrv/slapd-instance_name /etc/dirsrv/slapd-instance_name/
ls: cannot access '/var/lib/dirsrv/slapd-instance_name': No such file or directory
ls: cannot access '/etc/dirsrv/slapd-instance_name': No such file or directory
```

其他资源

- 从复制拓扑中删除实例

第 12 章 卸载 DIRECTORY 服务器

如果不再需要 Directory Server 实例，可以将其卸载以回收空间。

12.1. 卸载 DIRECTORY 服务器

如果您不再需要服务器上运行的 Directory 服务器，请卸载软件包，如本节所述。

流程

1. 从复制拓扑中删除所有实例。如果您的实例不是复制拓扑的成员，则跳过这一步。
2. 从服务器移除所有实例。对于每个实例，请输入：

```
# dsctl instance_name remove --do-it
```

3. 删除 Directory Server 软件包：

```
# dnf module remove redhat-ds
```

4. 可选：禁用 **dirsrv-12-for-rhel-8-x86_64-rpms** 存储库：

```
# subscription-manager repos --disable=dirsrv-12-for-rhel-8-x86_64-rpms
Repository 'dirsrv-12-for-rhel-8-x86_64-rpms' is disabled for this system.
```

5. 可选：从系统中删除 Red Hat Directory Server 订阅：

重要

如果您删除比目录服务器提供额外的产品的订阅，您将无法为这些产品安装或更新软件包。

- 列出附加到主机的订阅：

```
# subscription-manager list --consumed
Subscription Name:   Example Subscription
...
Pool-ID:             5ab6a8df96b03fd30aba9a9c58da57a1
...
```

- 使用上一步中的池 ID 删除订阅：

```
# subscription-manager remove --pool=5ab6a8df96b03fd30aba9a9c58da57a1
2 local certificates have been deleted.
The entitlement server successfully removed these pools:
  5ab6a8df96b03fd30aba9a9c58da57a1
The entitlement server successfully removed these serial numbers:
  1658239469356282126
```

其他资源

- 从复制拓扑中删除实例

第 13 章 使用 WEB 控制台登录到目录服务器

Web 控制台是一个基于浏览器的图形用户界面(GUI)，用于执行管理任务。Directory Server 软件包会自动为 Web 控制台安装 Directory Server 用户界面。

前提条件

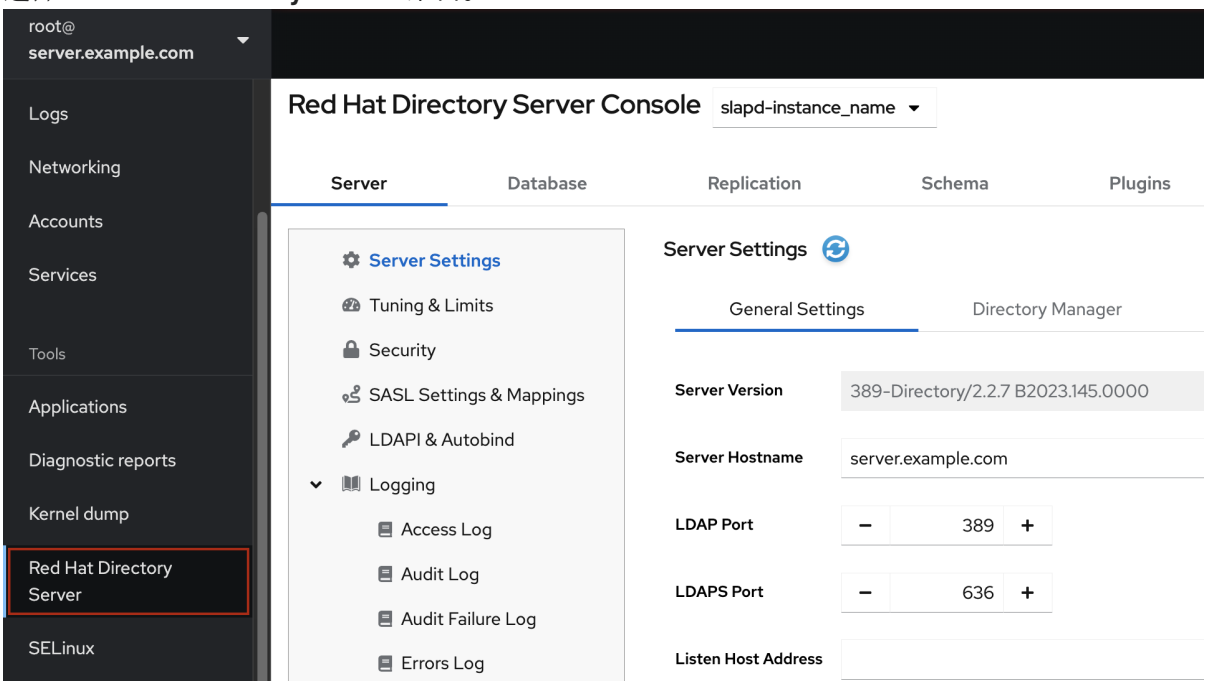
- 有访问 Web 控制台的权限。

流程

1. 使用您的浏览器中的以下 URL 访问 Web 控制台：

```
https://<directory_server_host>:9090
```

2. 以具有 **sudo** 权限的用户身份登录。
3. 选择 **Red Hat Directory Server** 条目。



其他资源

- 登录到 RHEL web 控制台。

第 14 章 启动和停止目录服务器实例

您可以使用命令行或 Web 控制台启动、停止和重新启动目录服务器实例。

14.1. 使用命令行启动和停止目录服务器实例

使用 **dsctl** 工具启动、停止或重启 Directory 服务器实例。

重要

dsctl 工具是停止目录服务器实例的唯一正确方法。不要使用 **kill** 命令来终止 **ns-slapd** 进程，以避免出现数据丢失和崩溃的问题。

流程

- 要启动实例，请运行：

```
# dsctl instance_name start
```

- 要停止实例，请运行：

```
# dsctl instance_name stop
```

- 要重启实例，请运行：

```
# dsctl instance_name restart
```

另外，您可以启用目录服务器实例在系统引导时自动启动：

- 对于单个实例，请运行：

```
# systemctl enable dirsrv@instance_name
```

- 对于服务器中的所有实例，请运行：

```
# systemctl enable dirsrv.target
```

验证

您可以使用 **dsctl** 或 **systemctl** 实用程序检查实例状态：

- 要使用 **dsctl** 工具查看实例状态，请运行：

```
# dsctl instance_name status
```

- 要使用 **systemctl** 实用程序查看实例状态，请运行：

```
# systemctl status dirsrv@instance_name
```

其他资源

- 使用 systemctl 管理系统服务

14.2. 使用 WEB 控制台启动和停止目录服务器实例

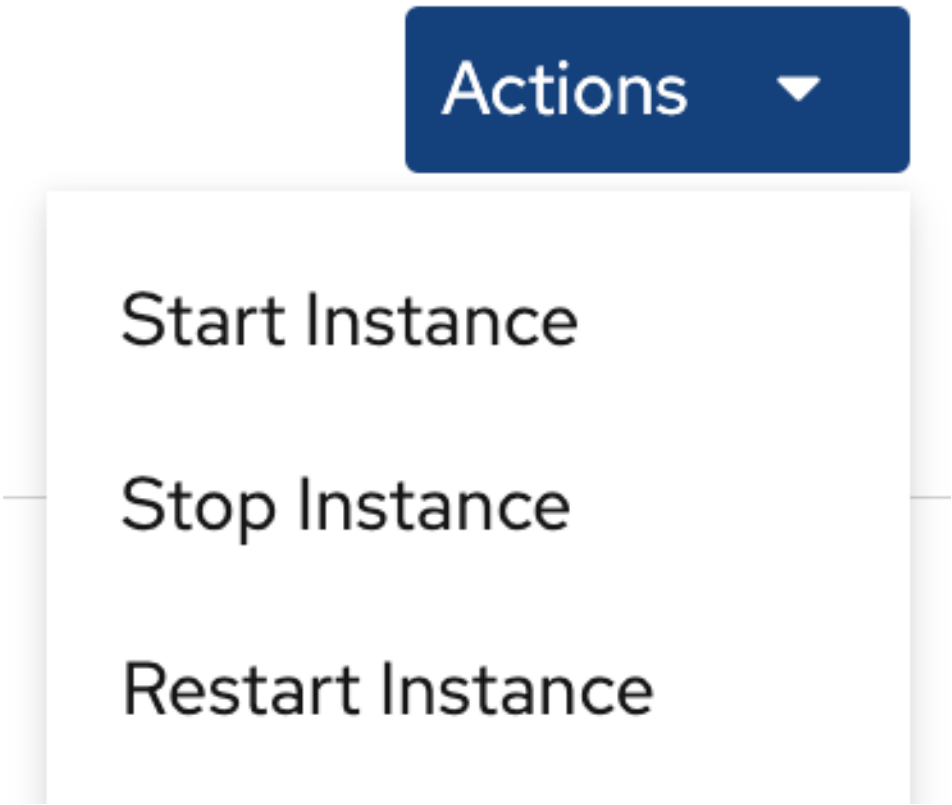
您可以使用 Web 控制台启动、停止或重启目录服务器实例。

前提条件

- 已登陆到 web 控制台。如需了解更多详细信息，请参阅
- 使用 Web 控制台登录到目录服务器

流程

1. 选择 Directory Server 实例。
2. 点击 **Actions** 按钮并选择要执行的操作：
   - **启动实例**
   - **停止实例**
   - **重启实例**



验证

- 确保 Directory 服务器实例正在运行。当实例没有运行时，Web 控制台会显示以下信息：

> This server instance is not running, either start it from the **Actions** dropdown menu, or choose a different instance.

第 15 章 更改 LDAP 和 LDAPS 端口号

默认情况下，Directory 服务器使用端口 **389** 作为 LDAP，如果您启用了 LDAPS 协议的端口 **636**。您可以更改端口号，例如，在一个主机上运行多个目录服务器实例。

重要

其他服务不得使用分配给实例的协议的新端口。

15.1. 使用命令行更改端口号

您可以使用命令行更改 LDAP 和 LDAPS 协议的端口号。LDAP 和 LDAP 端口更改需要更新 **nsslapd-port** 和 **nsslapd-securePort** 参数。

流程

1. 可选：显示实例的当前端口号：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-port nsslapd-securePort
```

2. 更改 LDAP 端口：
   a. 为 LDAP 协议设置新端口。例如，要将其设置为 **1389**，请运行：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-port=1389
```

   b. 为您在上一步中分配的 LDAP 端口设置 **ldap_port_t** 类型：

```
# semanage port -a -t ldap_port_t -p tcp 1389
```

3. 更改 LDAPS 端口：
   a. 为 LDAPS 协议设置新端口。例如，要将其设置为 **1636**，请运行：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-securePort=1636
```

   b. 为您在上一步中分配的 LDAPS 端口设置 **ldap_port_t** 类型：

```
# semanage port -a -t ldap_port_t -p tcp 1636
```

4. 重启实例：

```
# dsctl instance_name restart
```

验证

1. 使用以下命令验证 Directory 服务器现在使用新的 LDAP 端口：

```
# dsconf instance_name config get nsslapd-port
```

2. 使用以下命令验证 Directory 服务器现在使用新的 LDAPS 端口号：

```
# dsconf instance_name config get nsslapd-securePort
```

其他资源

- 有关 **nsslapd-securePort** 参数的详情，请参阅 nsslapd-securePort 参数的描述
- 有关 **nsslapd-port** 参数的详情，请参阅 nsslapd-port 参数的描述

15.2. 使用 WEB 控制台更改端口号

您可以使用 Web 控制台更改 LDAP 和 LDAPS 协议的端口号。

前提条件

- 在 web 控制台中登录到实例。

流程

1. 更改 LDAP 端口：
   a. 打开 **Server Setting** 菜单。
   b. 在 **Server Setting** 选项卡中，在 **LDAP Port** 字段中输入新端口号。
2. 点击 **Save**。
3. 更改 LDAPS 端口：
   a. 打开 **Server Setting** 菜单。
   b. 在 **General Settings** 选项卡中，在 **LDAPS Port** 字段中输入新端口号。
   c. 点击 **Save**。
4. 点 **Action** 并选择 **Restart Instance** 来重新启动实例。

验证

1. 在服务器设置中验证更改的端口是否反映。

其他资源

- 有关重启实例的详情，请参阅使用 Web 控制台启动和停止目录服务器实例
- 有关使用 Web 控制台登录到目录服务器的更多信息，请参阅使用 Web 控制台登录到目录服务器

第 16 章 使用 .DSRC 文件管理目录服务器命令行工具

~/**.dsrc** 文件简化了使用 Directory Server 命令行工具的命令。默认情况下，您可以将 **LDAP URL** 或绑定区分名称(DN)传递给这些命令的信息。您可以将设置存储在 ~/**dsrc** 文件中，以使用命令行工具，而无需在每次指定这些设置。

16.1. .DSRC 文件如何简化命令

您可以在 ~/**.dsrc** 文件中指定实例的 LDAP URL 和绑定 DN：

```
# server1
uri = ldap://server1.example.com
binddn = cn=Directory Manager
basedn = dc=example,dc=com
```

您可以在这些设置中使用较短的目录服务器命令。例如，要创建一个用户帐户：

```
# dsidm server1 user create
```

如果没有 ~/**.dsrc** 文件，则必须在命令中指定绑定 DN、LDAP URL 和基本 DN：

```
# dsidm -D cn=Directory Manager ldap://server1.example.com -b "dc=example,dc=com" user create
```

16.2. 使用 DSCTL 实用程序创建 .DSRC 文件

您可以使用 **dsctl** 实用程序创建 ~/**.dsrc** 文件，而不是手动创建它。

流程

- 运行：

```
# dsctl instance_name dsrc create ...
```

您可以在命令中添加这些选项：

- **--uri**

使用 **--uri** 选项时，以 **protocol://host_name_or_IP_address_or_socket**格式将 URL 设置为实例

例如：

a. **--uri ldap://server.example.com**

b. **--uri = ldaps://server.example.com**

c. **--uri = ldapi://%%2fvar%%2frun%%2fslapd-instance_name.socket**

当您设置目录服务器套接字的路径时，请在路径中使用 **%%02** 而不是斜杠 (**/**)。

重要

在使用 **ldapi** URL 时，服务器会标识运行 Directory Server 命令行工具的用户的用户 ID (UID)和组 ID (GID)。如果您以 **root** 用户身份运行该命令，UID 和 GID 为 **0,** Directory 服务器会在不输入对应的密码的情况下自动以 **cn=Directory Manager** 验证。

- **--starttls**

使用 **--starttls** 选项时，将实用程序配置为连接到 LDAP 端口，然后发送 **STARTTLS** 命令以切换到加密的连接。

- **--basedn**

使用 **--basedn** 选项时，设置基础可分辨名称(DN)。

例如： **--basedn dc=example,dc=com**

- **--binddn**

使用 **--basedn** 选项时，设置绑定 DN。

例如： **--binddn cn=Directory Manager**

- **--pwdfile**

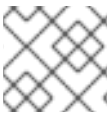
使用 **--pwdfile** 时，设置包含绑定 DN 密码的文件的路径。

例如： **--pwdfile /root/rhds.pwd**

- **--tls-cacertdir**

使用 **--tls-cacertdir** 选项时，设置此参数中的路径，该参数定义了使用 LDAPS 连接验证服务器证书所需的证书颁发机构(CA)证书的目录。

例如： **--tls-cacertdir /etc/pki/CA/certs/**



注意

只有在将 CA 证书复制到指定的目录时，才能使用 **c_rehash /etc/pki/CA/certs/** 命令。

- **--tls-cert**

使用 **--tls-certl** 选项时，设置服务器证书的绝对路径。

例如： **--tls-cert /etc/dirsrv/slapd-instance_name/Server-Cert.crt**

- **--tls-key**

使用 **--tls-key** 选项时，设置服务器私钥的绝对路径。

例如： **--tls-key /etc/dirsrv/slapd-instance_name/Server-Cert.key**

- **--tls-reqcert**

使用 **--tls-reqcert** 选项时，设置在 TLS 会话中的服务器证书上执行的检查客户端实用程序执行什么操作。

例如 ：**--tls-reqcert hard**

这些参数可用：

a. **Never** ：实用程序不请求或检查服务器证书。

b. **Allow** ：实用程序忽略证书错误，连接是建立的。

c. **hard** ：实用程序在证书错误时终止连接。

- **--saslmech**

使用 **--saslmech** 选项时，将 SASL 机制设置为使用 **PLAIN** 或 **EXTERNAL**。

例如 ：**--saslmech PLAIN**

16.3. 使用目录服务器工具时远程和本地连接解析

在保护目录服务器连接时，您可以在远程和本地调用 Directory Server 命令。当您使用指定 LDAP URL 运行 Directory Server 命令时，服务器会将它视为远程连接，并检查 **/etc/openldap/ldap.conf** 配置文件以及系统范围的设置，以继续执行该命令。

当您运行带有指定实例名称的 Directory Server 命令时，服务器会检查 **~/.dsrc** 文件是否存在，并应用以下逻辑进行：

1. 目录服务器将 **~/.dsrc** 文件视为远程连接，并检查 **/etc/openldap/ldap.conf** 配置文件和系统范围的设置是否包含实例名称和 LDAP URL。

2. 目录服务器将 **~/.dsrc** 文件视为本地连接，并使用本地 **dse.ldif** 文件中的 **nsslapd-certdir** 设置来保护连接，如果 **~/.dsrc** 文件只包含指定的实例名称，或者 **~/.dsrc** 文件不存在。如果 **nsslapd-certdir** 不存在，服务器使用默认路径 **/etc/dirsrv/slapd-instance_name/** 来存储实例的网络安全服务(NSS)数据库。

其他资源

- nsslapd-certdir parameter

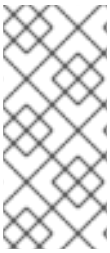
第 17 章 创建测试条目

dsctl ldifgen 命令创建了包含不同类型的 test 条目的 LDIF 文件。例如，您可以使用此 LDIF 文件填充测试实例或子树，以使用示例条目测试目录服务器的性能。

17.1. 您可以创建的测试条目概述

您可以将以下条目类型参数之一传递给 **dsctl ldifgen** ：

- **users** ：创建一个包含用户条目的 LDIF 文件。
- **Group** ：创建包含静态组和成员条目的 LDIF 文件。
- **COS-def** ：创建一个 LDIF 文件，其中包含经典指针或间接类服务(CoS)定义。
- **COS-template** ：创建一个包含 CoS 模板的 LDIF 文件。
- **角色** ：创建一个包含受管、过滤或间接角色条目的 LDIF 文件。
- **mod-load** ：创建包含修改操作的 LDIF 文件。使用 **ldapmodify** 实用程序将文件加载到 目录中。
- **nested** ：创建一个 LDIF 文件，该文件在级联或侵犯树中包含大量嵌套条目。



注意

dsctl ldifgen 命令仅创建 LDIF 文件。要将文件加载到 Directory Server 实例中，请使用：

- 使用 **mod-load** 选项创建 LDIF 文件后 **ldapmodify** 程序
- 所有其他选项的 **ldapadd** 工具

除了嵌套条目类型外，如果您不提供任何命令行选项，则 **dsctl ldifgen** 命令使用互动模式：

```
# dsctl instance_name ldifgen entry_type
```

17.2. 使用示例用户条目创建 LDIF 文件

使用 **dsctl ldifgen users** 命令创建带有示例用户条目的 LDIF 文件。

流程

1. 例如，要创建一个名为 **/tmp/users.ldif** 的 LDIF 文件，可将 100,000 个通用用户添加到 **dc=example,dc=com** 后缀，请输入：

```
# dsctl instance_name ldifgen users --suffix "dc=example,dc=com" --number 100000 --generic --ldif-file=/tmp/users.ldif
```

请注意，命令会创建以下机构单元(OU)，并随机将用户分配给这些 OU：

- **ou=accounting**
- **ou=product development**

- **ou=product testing**
- **ou=human resources**
- **ou=payroll**
- **ou=people**
- **ou=groups**
  如需更多详细信息和可用于创建 LDIF 文件的选项，请输入：

  ```
  # dsctl instance_name ldifgen users --help
  ```

2. 可选：在目录中添加测试条目：

   ```
   # ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
   /tmp/users.ldif
   ```

17.3. 使用示例组条目创建 LDIF 文件

使用 **dsctl ldifgen groups** 命令创建带有示例用户条目的 LDIF 文件。

流程

1. 例如，要创建一个名为 **/tmp/groups.ldif** 的 LDIF 文件，可将 500 组添加到 **ou=groups,dc=example,dc=com** 条目，每个组具有 100 个成员，请输入：

   ```
   # dsctl instance_name ldifgen groups --number 500 --suffix "dc=example,dc=com" --
   parent "ou=groups,dc=example,dc=com" --num-members 100 --create-members --
   member-parent "ou=People,dc=example,dc=com" --ldif-file /tmp/groups.ldif
   example_group__
   ```

   请注意，命令还会创建 LDIF 语句，以在 **ou=People,dc=example,dc=com** 中添加用户条目。

   如需更多详细信息和可用于创建 LDIF 文件的选项，请输入：

   ```
   # dsctl instance_name ldifgen groups --help
   ```

2. 可选：在目录中添加测试条目：

   ```
   # ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
   /tmp/groups.ldif
   ```

17.4. 使用示例 COS 定义创建 LDIF 文件

使用 **dsctl ldifgen cos-def** 命令创建带有类服务(CoS)定义的 LDIF 文件。

流程

1. 例如，要创建一个名为 **/tmp/cos-definition.ldif** 的 LDIF 文件，在 **ou=cos-definitions,dc=example,dc=com** 条目中添加经典的 CoS 定义，请输入：

```
# dsctl instance_name ldifgen cos-def Postal_Def --type classic --parent "ou=cos
definitions,dc=example,dc=com" --cos-specifier businessCatagory --cos-template
"cn=sales,cn=classicCoS,dc=example,dc=com" --cos-attr postalcode
telephonenumber --ldif-file /tmp/cos-definition.ldif
```

如需更多详细信息和可用于创建 LDIF 文件的选项，请输入：

```
# dsctl instance_name ldifgen cos-def --help
```

2. 可选：在目录中添加测试条目：

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/cos-definition.ldif
```

17.5. 使用示例修改语句创建 LDIF 文件

使用 **dsctl ldifgen mod-load** 命令创建一个包含更新操作的 LDIF 文件。

流程

1. 例如，要创建一个名为 **/tmp/modifications.ldif** 的 LDIF 文件：

```
# dsctl instance_name ldifgen mod-load --num-users 1000 --create-users --
parent="ou=People,dc=example,dc=com" --mod-attrs="sn" --add-users 10 --modrdn-
users 100 --del-users 100 --delete-users --ldif-file=/tmp/modifications.ldif
```

这个命令会创建一个名为 **/tmp/modifications.ldif** 文件并带有以下内容的声明：

- 创建一个具有 1000 **ADD** 操作的 LDIF 文件，以在 **ou=People,dc=example,dc=com** 中创建用户条目。
- 通过更改其 **sn** 属性来修改所有条目。
- 添加额外的 10 个用户条目。
- 执行 100 **MODRDN** 操作。
- 删除 100 个条目
- 删除末尾所有剩余条目
  如需更多详细信息和可用于创建 LDIF 文件的选项，请输入：

```
# dsctl instance_name ldifgen mod-load --help
```

2. 可选：在目录中添加测试条目：

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/modifications.ldif
```

17.6. 创建带有嵌套示例条目的 LDIF 文件

使用 **dsctl ldifgen 嵌套** 命令创建一个 LDIF 文件，其中包含大量的嵌套级结构。

流程

1. 例如，要创建一个名为 **/tmp/nested.ldif** 的 LDIF 文件，在 **dc=example,dc=com** 条目下将 600 个用户添加到不同机构单元(OU)下，每个 OU 均包含最大数量 100 个用户，请输入：

```
# dsctl instance_name ldifgen nested --num-users 600 --node-limit 100 --suffix
"dc=example,dc=com" --ldif-file /tmp/nested.ldif
```

   如需更多详细信息和可用于创建 LDIF 文件的选项，请输入：

```
# dsctl instance_name ldifgen nested --help
```

2. 可选：在目录中添加测试条目：

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com -x -c -f
/tmp/nested.ldif
```