



Red Hat Directory Server 12

导入和导出数据

有关如何填充和提取目录数据库的流程

有关如何填充和提取目录数据库的流程

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

当实例离线或在线时，您可以将数据导入到目录服务器实例中。您也可以从目录服务器数据库中提取数据。

目录

提供有关红帽目录服务器的反馈	3
第 1 章 将数据导入到目录服务器	4
1.1. 在服务器运行时使用命令行导入数据	4
1.2. 在服务器离线时使用命令行导入数据	5
1.3. 在服务器运行时使用 WEB 控制台导入数据	7
第 2 章 从 DIRECTORY 服务器导出数据	10
2.1. 在服务器运行时使用命令行导出数据	10
2.2. 在服务器离线时使用命令行导出数据	11
2.3. 在服务器运行时使用 WEB 控制台导出数据	12
2.4. 其他资源	13
第 3 章 启用组成员来导出数据，并将导出作为组成员之一执行	15
3.1. 启用组导出数据	15
3.2. 以普通用户身份执行导出	16

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 将数据导入到目录服务器

使用命令行或 Web 控制台将数据从 LDIF 文件导入到目录服务器数据库。



重要

要导入数据，您必须将要导入的 LDIF 文件存储在 `/var/lib/dirsrv/slapd-instance_name/ldif/` 目录中。

1.1. 在服务器运行时使用命令行导入数据

要在 Directory Server 实例运行时导入数据，请使用 `dsconf backend import` 命令。



警告

当您启动导入操作时，目录服务器首先从数据库中删除所有现有数据，然后从 LDIF 文件中导入数据。因此，如果导入失败，服务器不会返回条目或部分条目集合。

先决条件

- LDIF 文件权限允许 `dirsrv` 用户读取该文件。
- 要导入的 LDIF 文件包含 `root` 后缀条目。
- 要导入数据的后缀及其数据库存在于目录中。
- 目录服务器实例正在运行。
- 要导入的 LDIF 文件使用 UTF-8 字符集编码。

流程

1. 可选：默认情况下，Directory 服务器将所有导入的条目序列号(USN)设置为 0。要设置替代的 **initial USN** 值，请设置 `nsslapd-entryusn-import-initval` 参数。例如，要将所有导入的值的 **USN** 设置为 `12345`，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
nsslapd-entryusn-import-initval=12345
```

- 2.

如果要将要导入的文件复制到 `/var/lib/dirsrv/slapd-instance_name/ldif/`，请在该文件中重置 SELinux 上下文：

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
```


3. 使用 `dsconf backend import` 命令从 LDIF 文件中导入数据。

例如，要将 `/var/lib/dirsrv/slapd-instance_name/ldif/example.ldif` 文件导入到 `userRoot` 数据库中：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend import
userRoot /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
The import task has finished successfully
```

4. 搜索 `/var/log/dirsrv/slapd-instance_name/errors` 日志在导入过程中出现问题。

验证

- 搜索导入的后缀下的条目，如 `dc=example,dc=com`：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -b
"dc=example,dc=com" -s sub -x
```

其他资源

- [在单独的数据库中存储后缀](#)
- [nsslapd-entryusn-import-initval](#)

1.2. 在服务器离线时使用命令行导入数据

如果 Directory 服务器实例离线，请使用 `dsctl ldif2db` 命令导入数据。



警告

当您启动导入操作时，目录服务器首先从数据库中删除所有现有数据，然后从 LDIF 文件中导入数据。因此，如果导入失败，服务器不会返回条目或部分条目集合。

先决条件

- LDIF 文件权限允许 `dirsrv` 用户读取该文件。
- 要导入的 LDIF 文件包含 `root` 后缀条目。
- 要导入数据的后缀及其数据库存在于目录中。
- 目录服务器实例没有运行。
- 要导入的 LDIF 文件使用 UTF-8 字符集编码。

流程

1.

可选：默认情况下，Directory 服务器将所有导入的条目序列号(USN)设置为 0。要设置替代的 initial USN 值，请设置 `nsslapd-entryusn-import-initval` 参数。例如，要将所有导入的值的 USN 设置为 12345，请输入：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace
nsslapd-entryusn-import-initval=12345
```

2.

如果要将要导入的文件复制到 `/var/lib/dirsrv/slapd-instance_name/ldif/`，请在该文件中重置 SELinux 上下文：

```
# restorecon -Rv /var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
```

3.

使用 `dsctl ldif2db` 命令从 LDIF 文件中导入数据。例如，要将 `/var/lib/dirsrv/slapd-instance_name/ldif/example.ldif` 文件导入到 `userRoot` 数据库中：

```
# dsctl instance_name ldif2db userRoot /var/lib/dirsrv/slapd-
instance_name/ldif/example.ldif
OK group dirsrv exists
OK user dirsrv exists
[17/Jul/2021:13:42:42.015554231 +0200] - INFO -
ldbm_instance_config_cachememsize_set - force a minimal value 512000
...
[17/Jul/2021:13:42:44.302630629 +0200] - INFO - import_main_offline - import
userRoot: Import complete. Processed 160 entries in 2 seconds. (80.00 entries/sec)
ldif2db successful
```

4. 搜索 `/var/log/dirsrv/slaped-instance_name/errors` 日志在导入过程中出现问题。
5. 可选：启动实例：

```
# dsctl instance_name start
```

验证

- 搜索导入的后缀下的条目，如 `dc=example,dc=com`：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -b "dc=example,dc=com" -s sub -x
```

其他资源

- [在单独的数据库中存储后缀](#)
- [nsslapd-entryusn-import-initval](#)
- 要显示可用于导入数据的所有额外设置，请查看 `dsctl ldif2db --help` 命令的输出。

1.3. 在服务器运行时使用 WEB 控制台导入数据

目录服务器支持使用 Web 控制台导入数据。



警告

当您启动导入操作时，目录服务器首先从数据库中删除所有现有数据，然后从 LDIF 文件中导入数据。因此，如果导入失败，服务器不会返回条目或部分条目集合。

先决条件

- LDIF 文件权限允许 `dirsrv` 用户读取该文件。
- 要导入的 LDIF 文件包含 `root` 后缀条目。
- 要导入数据的后缀及其数据库存在于目录中。
- LDIF 文件存储在 `/var/lib/dirsrv/slapped-instance_name/ldif/` 目录中，并设置了 `dirsrv_var_lib_t` SELinux 上下文。
- 目录服务器实例正在运行。
- 在 web 控制台中登录到实例。
- 要导入的 LDIF 文件使用 UTF-8 字符集编码。

流程

1. 在 Web 控制台中，打开 **Database** 菜单。
2. 选择后缀条目。
3. 点 **后缀任务**，然后选择 **Initialize Suffix**。
4. 点您要导入的 LDIF 文件旁边的 **导入** 按钮。如果 LDIF 文件存储在与 `/var/lib/dirsrv/slapped-instance_name/ldif/` 不同的目录中，请输入文件的完整路径，然后点 **Import** 按钮。
5. 选择 **Yes, I am sure**，然后单击 **Initialize Database** 进行确认。
6. 要检查导入过程中的日志是否存在问题，请打开 **Monitoring** → **Logging** → **Errors Log** 菜单。

验证

1. 搜索导入的后缀下的条目，如 `dc=example,dc=com` ：

```
# ldapsearch -D "cn=Directory Manager" -W -H ldap://server.example.com -b  
"dc=example,dc=com" -s sub -x
```

其他资源

- [在单独的数据库中存储后缀](#)

第 2 章 从 DIRECTORY 服务器导出数据

使用命令行或 Web 控制台将数据从 Directory Server 数据库导出到 LDIF 文件。



注意

导出操作仅包含目录数据。导出不包含配置信息(`cn=config`)、模式信息(`cn=schema`)和监控信息(`cn=monitor`)。

使用导出功能：

- 将数据复制到另一个目录服务器。
- 将数据导出到另一个应用程序。
- 在更改目录拓扑后，`repopulate` 数据库。
- 分割数据库。

2.1. 在服务器运行时使用命令行导出数据

要在 Directory Server 实例运行时导出数据，请使用 `dsconf backend export` 命令。

先决条件

- `dirsrv` 用户在目标目录中具有写入权限。

请注意，目录服务器默认使用自己的私有目录。因此，除非您禁用了 `PrivateTmp systemd` 指令，否则在 `/var/tmp/`、`/tmp/` 和 `/root/` 目录下备份和导出会失败。

- 目录服务器实例正在运行。

流程

1. 使用 `dsconf backend export` 命令将数据导出到 LDIF 文件。

例如，要导出 `userRoot` 数据库：

```
# dsconf -D "cn=Directory Manager" ldap://server.example.com backend export
userRoot
The export task has finished successfully
```

默认情况下，`dsconf` 将导出存储在 `/var/lib/dirsrv/slapd - instance_name /ldif/` 目录中的名为 `instance_name_database_time_stamp.ldif` 的文件中。或者，在命令中添加 `-l file_name` 选项来指定不同的位置。

2. 在导出过程中搜索 `/var/log/dirsrv/slapd-instance_name/errors` 日志。

其他资源

- 要显示可用于导出数据的所有附加设置，请查看 `dsconf ldap://server.example.com backend export --help` 命令的输出。
- [在服务器运行时使用命令行导入数据](#)
- [备份目录服务器](#)

2.2. 在服务器离线时使用命令行导出数据

如果 Directory 服务器实例离线，请使用 `dsctl db2ldif` 命令导出数据。

先决条件

- `dirsrv` 用户在目标目录中具有写入权限。

请注意，目录服务器默认使用自己的私有目录。因此，除非您禁用了 `PrivateTmp systemd` 指令，否则在 `/var/tmp/`、`/tmp/` 和 `/root/` 目录下备份和导出会失败。

- 目录服务器实例没有运行。

流程

1. 使用 `dsctl db2ldif` 命令将数据导出到 LDIF 文件。例如，将 `userRoot` 数据库导出到 `/var/lib/dirsrv/slapd-instance_name/ldif/example.ldif` 文件中：

```
# dsctl instance_name db2ldif userRoot
/var/lib/dirsrv/slapd-instance_name/ldif/example.ldif
OK group dirsrv exists
OK user dirsrv exists
ldiffile: /var/lib/dirsrv/slapd-instance_name/example.ldif
[18/Jul/2021:10:46:03.353656777 +0200] - INFO -
ldbm_instance_config_cachememsize_set - force a minimal value 512000
[18/Jul/2021:10:46:03.383101305 +0200] - INFO - ldbm_back_ldbm2ldif - export
userRoot: Processed 160 entries (100%).
[18/Jul/2021:10:46:03.391553963 +0200] - INFO - dblayer_pre_close - All database
threads now stopped
db2ldif successful
```

2. 在导出过程中搜索 `/var/log/dirsrv/slapd-instance_name/errors` 日志。

3. 可选：启动实例：

```
# dsctl instance_name start
```

其他资源

- 要显示可用于导入数据的所有额外设置，请查看 `dsctl db2ldif --help` 命令的输出。
- [在服务器离线时使用命令行导入数据](#)
- [备份目录服务器](#)

2.3. 在服务器运行时使用 WEB 控制台导出数据

目录服务器支持使用 Web 控制台导出数据。

先决条件

- **dirsrv 用户在目标目录中具有写入权限。**

请注意，目录服务器默认使用自己的私有目录。因此，除非您禁用了 **PrivateTmp systemd** 指令，否则在 **/var/tmp/**、**/tmp/** 和 **/root/** 目录下备份和导出会失败。
- 目录服务器实例正在运行。
- 在 web 控制台中登录到实例。

流程

1. 打开 **Database** 菜单。
2. 选择后缀条目。
3. 点 **Suffix Tasks**，然后选择 **Export Suffix**。
4. 输入您要存储导出的 **LDIF** 文件的名称。目录服务器将使用指定的文件名将文件存储在 **/var/lib/dirsrv/slaped-*instance_name*/ldif/** 目录中。
5. 单击 **Export Database**。
6. 要在导出期间检查日志是否有问题，请打开 **Monitoring** → **Logging** → **Errors Log** 菜单。

其他资源

- [在服务器运行时使用 Web 控制台导入数据](#)
- [备份目录服务器](#)

2.4. 其他资源

- [LDIF 技术规范 - RFC 2849.](#)

第 3 章 启用组成员来导出数据, 并将导出作为组成员之一执行

您可以配置组成员具有导出数据的权限。这会提高安全性, 因为您不再需要在脚本中设置 `cn=Directory Manager` 的凭证。此外, 您可以通过修改组来轻松授予和撤销导出权限。

3.1. 启用组导出数据

使用这个流程添加 `cn=export_users,ou=groups,dc=example,dc=com` 组, 并启用此组的成员来创建导出任务。

流程

1.

创建 `cn=export_users,ou=groups,dc=example,dc=com` 组 :

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" group create --cn export_users
```

2.

添加一个访问控制指令(ACI), 允许 `cn=export_users,ou=groups,dc=example,dc=com` 组的成员来创建导出任务 :

```
# ldapadd -D "cn=Directory Manager" -W -H ldap://server.example.com

dn: cn=config
changetype: modify
add: aci
aci: (target = "ldap:///cn=export,cn=tasks,cn=config")
(targetattr="*") (version 3.0 ; acl "permission:
  Allow export_users group to export data" ;
  allow (add, read, search) groupdn
  = "ldap:///cn=export_users,ou=groups,dc=example,dc=com");
-
add: aci
aci: (target = "ldap:///cn=config")(targetattr =
  "objectclass || cn || nsslapd-suffix || nsslapd-ldifdir")
(version 3.0 ; acl "permission: Allow export_users
  group to access ldifdir attribute" ; allow
  (read,search) groupdn = "ldap:///cn=export_users,ou=groups,dc=example,dc=com");
```

3.

创建用户 :

a.

创建用户帐户 :

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" user create --uid="example" --cn="example" --
uidNumber="1000" --gidNumber="1000" --homeDirectory="/home/example/" --
displayName="Example User"
```

- b. 在用户帐户中设置密码：

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" account reset_password
"uid=example,ou=People,dc=example,dc=com" "password"
```

4. 将 uid=example,ou=People,dc=example,dc=com 用户添加到 cn=export_users,ou=groups,dc=example,dc=com 组：

```
# dsidm -D "cn=Directory manager" ldap://server.example.com -b
"dc=example,dc=com" group add_member export_users
uid=example,ou=People,dc=example,dc=com
```

验证

- 显示 cn=config 条目中设置的 ACI：

```
# ldapsearch -o ldif-wrap=no -LLLx -D "cn=directory manager" -W -H
ldap://server.example.com -b cn=config aci=* aci -s base
dn: cn=config
aci: (target = "ldap:///cn=export,cn=tasks,cn=config")(targetattr="*)(version 3.0 ; aci
"permission: Allow export_users group to export data" ; allow (add, read, search)
groupdn = "ldap:///cn=export_users,ou=groups,dc=example,dc=com");)
aci: (target = "ldap:///cn=config")(targetattr = "objectclass || cn || nsslapd-suffix ||
nsslapd-ldifdir")(version 3.0 ; aci "permission: Allow export_users group to access
ldifdir attribute" ; allow (read,search) groupdn =
"ldap:///cn=export_users,ou=groups,dc=example,dc=com");)
...
```

3.2. 以普通用户身份执行导出

您可以以普通用户而不是 cn=Directory Manager 执行导出。

前提条件

- 启用了 cn=export_users,ou=groups,dc=example,dc=com 组的成员来导出数据。

- 您用来执行导出的用户是 `cn=export_users,ou=groups,dc=example,dc=com` 组的成员。

流程

- 使用以下方法之一创建导出任务：
 - 使用 `dsconf backend export` 命令：

```
# dsconf -D "uid=example,ou=People,dc=example,dc=com"  
ldap://server.example.com backend export userRoot
```

- 通过手动创建任务：

```
# ldapadd -D "uid=example,ou=People,dc=example,dc=com" -W -H  
ldap://server.example.com  
  
dn: cn=userRoot-2021_07_23_12:55_00,cn=export,cn=tasks,cn=config  
changetype: add  
objectClass: extensibleObject  
nsFilename: /var/lib/dirsrv/slapd-instance_name/ldif/None-userroot-  
2021_07_23_12:55_00.ldif  
nsInstance: userRoot  
cn: export-2021_07_23_12:55_00
```

验证

- 验证备份是否已创建：

```
# ls -l /var/lib/dirsrv/slapd-instance_name/ldif/*.ldif  
total 0  
-rw-----. 1 dirsrv dirsrv 10306 Jul 23 12:55 None-userroot-2021_07_23_12_55_00.ldif  
...
```

其他资源

- [启用组导出数据](#)