# Red Hat Directory Server 12

## Red Hat Directory Server 12 发行注记

值得注意的功能和更新与 Red Hat Directory Server 12 (12.4)

Last Updated: 2024-07-03

# Red Hat Directory Server 12 Red Hat Directory Server 12 发行注记

值得注意的功能和更新与 Red Hat Directory Server 12 (12.4)

## 法律通告



## 摘要

了解在红帽目录服务器 12 中实施的改进和附加功能。这包括重要的程序错误修复、已知问题、技术预览、已弃用的功能和其他有关此发行版本的详情。

# 目录

# 对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 要通过 JIRA 提交反馈（需要帐户）：
  1. 登录到 Jira 网站。
  2. 在顶部导航栏中点 **Create**
  3. 在 **Summary** 字段中输入描述性标题。
  4. 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。
  5. 点对话框底部的 **Create**。
- 要通过 Bugzilla 提交反馈（需要帐户）：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

# 第 1 章 常规信息

精益地说，Red Hat Directory Server 12 独立于次版本的通用信息。

## 1.1. 目录服务器支持政策和生命周期

详情请查看 Red Hat Directory Server 勘误支持政策 文档。

## 1.2. 软件冲突

您不能在安装了 Red Hat Enterprise Linux Identity Management(IdM)服务器的系统中安装 Directory Server。同样，没有可以在带 Directory Server 实例的系统上安装 Red Hat Enterprise Linux IdM 服务器。

## 1.3. 迁移到 DIRECTORY SERVER 12

- 有关将目录服务器 11 迁移到目录服务器 12 的步骤，请参阅将 目录服务器 11 迁移到目录服务器 12 章节。
- 有关将目录服务器 10 迁移到目录服务器 12 的步骤，请参阅将 目录服务器 10 迁移到目录服务器 12 章节。

## 1.4. 有关迁移到目录服务器 12 的备注

### 目录服务器 12 默认密码存储模式是 PBKDF2-SHA512

目录服务器 12 使用 **PBKDF2-SHA512** 方案作为默认密码存储方案，其比 **SSHA**、**SSHA512** 和其他方案更安全。因此，如果某些应用程序（如 **freeradius** ）不支持 **PBKDF2-SHA512** 方案，且您必须设置弱的密码存储方案，请注意，目录服务器只有在应用程序添加或修改用户条目时更新用户密码，而且可以在成功绑定操作期间更新用户密码。但是，您可以通过将 **cn=config** 条目中的 **nsslapd-enable-upgrade-hash** 参数设置为 **off** 来禁用对绑定操作的更新。

### 启动目录服务器 11 的新命令行工具

自版本 11 起，目录服务器提供新的命令行实用程序来管理服务器实例和用户。这些工具替换了用于 Directory Server 10 及更早的版本中管理任务的 Perl 脚本。

有关目录服务器 12 中以前版本及其替换命令的列表，请参阅 Red Hat Directory Server *安装指南中的 Red Hat Directory Server 11 附录中的命令行实用程序*。

**重要**

在 Directory Server 10 和更早版本中用于管理任务的 Perl 脚本在 **389-ds-base-legacy-tools** 软件包中仍然可用。但是，红帽只支持新的 **dsconf**、**dsctl**、**dscreate** 和 **dsidm** 命令行工具。

# 第 2 章 硬件要求

硬件要求基于以下先决条件运行的测试：

- 服务器使用默认的索引。
- 每个 LDAP 条目的大小为 1.5 KB 和 30 个或更多属性。

## 磁盘空间

下表根据条目数为 Directory 服务器提供了推荐的磁盘空间指南。

**表 2.1. 所需的磁盘空间**

| 条目数 | 数据库大小 | 数据库缓存 | 服务器和日志 | 总磁盘空间 |
|---|---|---|---|---|
| 10,000 - 500,000 | 2 GB | 2 GB | 4 GB | **8 GB** |
| 500,000 - 1,000,000 | 5 GB | 2 GB | 4 GB | **11 GB** |
| 1,000,000 - 5,000,000 | 21 GB | 2 GB | 4 GB | **27 GB** |
| 5,000,000 - 10,000,000 | 42 GB | 2 GB | 4 GB | **48 GB** |

总磁盘空间不包括备份和复制元数据的空间。启用复制后，其元数据最多可能需要总磁盘空间 10%。

具有 100万更改的复制更改日志可以至少为总磁盘空间要求添加 315 MB。

挂载到 **/dev/shm/** 中的临时文件系统(tmpfs)应该至少有 4 GB 的可用空间来存储 RHDS 临时文件。

## 所需的 RAM

请确定您的系统有足够的可用 RAM 来在缓存中保留整个数据库。所需的 RAM 大小可能高于推荐的 RAM 大小，具体取决于服务器配置和使用模式。

**表 2.2. 所需的 RAM 大小**

| 条目数 | 条目缓存 | 使用复制的条目缓存 [a] | 数据库缓存 | DN 缓存 | NDN 缓存 | RAM 大小总量 [b] |
|---|---|---|---|---|---|---|
| 10,000 - 500,000 | 4 GB | 5 GB | 1.5 GB | 45 MB | 160 MB | **7 GB** |
| 500,000 - 1,000,000 | 8 GB | 10 GB | 1.5 GB | 90 MB | 320 MB | **12 GB** |
| 1,000,000 - 5,000,000 | 40 GB | 50 GB | 1.5 GB | 450 MB | 1.6 GB | **54 GB** |

| 条目数 | 条目缓存 | 使用复制的条目缓存 [a] | 数据库缓存 | DN 缓存 | NDN 缓存 | RAM 大小总量 [b] |
|---|---|---|---|---|---|---|
| 5,000,000 - 10,000,000 | 80 GB | 100 GB | 1.5 GB | 900 MB | 3.2 GB | **106 GB** |

[a] 使用复制的条目缓存包括条目的复制状态和元数据。

[b] RAM 大小总量假设您启用了复制。

# 第 3 章 软件要求

## Directory 服务器支持的平台

如果红帽目录服务器在以下平台上运行，红帽支持它：

- Red Hat Directory Server 12.4 在 Red Hat Enterprise Linux 9.4 上运行。
- Red Hat Directory Server 12.3 在 Red Hat Enterprise Linux 9.3 上运行。
- Red Hat Directory Server 12.2 在 Red Hat Enterprise Linux 9.2 上运行。
- Red Hat Directory Server 12.1 在 Red Hat Enterprise Linux 9.1 上运行。
- Red Hat Directory Server 12.0 在 Red Hat Enterprise Linux 9.0 上运行。
- Red Hat Enterprise Linux 为 **AMD64** 和 **Intel 64** 架构构建。
- Red Hat Enterprise Linux 虚拟客户机在认证的管理程序上运行。详情请查看 哪个 hypervisor 经过认证以运行 Red Hat Enterprise Linux？ 解决方案文档。

## 在 web 控制台中为 Directory Server 用户界面支持的平台

红帽在以下环境中，在 Web 控制台中支持基于浏览器的目录服务器用户界面：

| 操作系统 | 浏览器 |
| --- | --- |
| Red Hat Enterprise Linux 9.4 | • Mozilla Firefox 115 及更新的版本<br>• Chrome 88 及更新的版本 |
| Windows Server 2016 和 2019： | • Mozilla Firefox 115 及更新的版本<br>• Chrome 88 及更新的版本 |
| Windows 10 | • Mozilla Firefox 115 及更新的版本<br>• Microsoft Edge 88 及更新的版本<br>• Chrome 88 及更新的版本 |

## Windows 同步工具支持的平台

红帽支持为运行的 Active Directory 支持 Windows Synchronization 程序：

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

# 第 4 章 RED HAT DIRECTORY SERVER 12.4

了解目录服务器 12.4 中实施的重要更新和新功能、已知问题和程序错误修复。

## 4.1. 389-DS-BASE 软件包中的重要更新和新功能

Red Hat Directory Server 12.4 中包含的重要更新包括在 Red Hat Enterprise Linux 9.4 发行注记中：

- **389-ds-base rebase 到版本 2.4.5**
- **现在，对于 ns-slapd 进程，默认禁用透明巨页**
- **新的 lastLoginHistSize 配置属性现在可用于 Account Policy 插件**
- **访问日志中新的 notes=M 信息来标识 MFA 绑定**
- **新的 chainMatch 匹配规则现在可用**
- **现在 389-ds-base 软件包支持 HAProxy 协议**

### 4.2. 程序错误修复

**了解红帽目录服务器 12.4 中修复的、对用户有严重影响的错误。**

**目录服务器现在更频繁地清除条目缓存**

**在以前的版本中，即使不需要，Directory 服务器会清除其条目缓存。因此，在某些情况下，目录服务器没有响应，性能不正确。在这个版本中，Directory 服务器仅在需要时清除条目缓存。**

**(BZ#2234613)**

**当添加 attributeTypes 时，web 控制台不再将属性名称改为小写字符**

**在以前的版本中，当您使用 Web 控制台向对象类添加属性时，属性名称中的大写字符将变为小写字符。在这个版本中，属性 name case 不再更改。**

(BZ#2236181)

389-ds-base 软件包中包含的目录服务器 12.4 程序错误修复包括在 Red Hat Enterprise Linux 9.4 发行注记中：

- 在放弃页面结果搜索后，目录服务器不再失败
- 如果 nsslapd-numlisteners 属性值大于 2，目录服务器不再会失败
- autobind 操作现在不会影响对其他连接执行的操作

## 4.3. 已知问题

了解已知问题，以及 Directory Server 12.4 中的临时解决方案。

### 目录服务器 Web 控制台不会自动更新在 web 控制台外更改的设置

由于在 Red Hat Enterprise Linux 8 web 控制台中设计 Directory Server 模块，如果更改控制台窗口外的配置，Web 控制台不会自动显示最新的设置。例如，如果您在打开 Web 控制台时使用命令行更改配置，则在 web 控制台中不会自动更新新设置。如果您在不同的计算机上使用 Web 控制台更改配置，这也适用。

要临时解决这个问题，如果配置在控制台窗口外更改，请在浏览器中手动刷新 Web 控制台。

(BZ#1654281) (BZ#1751047)

### 目录服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/导入 LDIF 文件

从 RHEL 8.3 开始，红帽目录服务器(RHDS)使用自己的私有目录，并且 LDAP 服务默认启用 PrivateTmp systemd 指令。因此，RHDS 只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录导入 LDIF 文件。如果 LDIF 文件存储在不同的目录中，如 /var/tmp、/tmp 或 /root，则导入会失败，并显示类似如下的错误：

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

要临时解决这个问题，请完成以下步骤：

1. 将 LDIF 文件移到 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录中：

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
```

2. 设置允许 dirsrv 用户读取文件的权限：

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

3. 恢复 SELinux 上下文：

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

如需更多信息，请参阅 LDAP 服务无法访问主机 /tmp 和 /var/tmp 目录下的文件。

(BZ#2075525)

### 389-ds-base 软件包中的已知问题

Red Hat Directory Server 12.4 已知的影响 389-ds-base 软件包 的问题记录在 Red Hat Enterprise Linux 9.4 发行注记中：

- 在线备份和在线自动成员重建任务可能会获得两个锁定，从而导致死锁

# 第 5 章 RED HAT DIRECTORY SERVER 12.3

了解新的系统要求、重要的更新和新功能、已知问题以及目录服务器 12.3 中实施的功能。

## 5.1. 重要更新和新功能

了解红帽目录服务器 12.3 中的新功能和重要更新。

### 目录服务器现在备份配置文件、证书数据库和自定义架构文件

在以前的版本中，目录服务器只备份数据库。有了这个更新，当运行 dsconf backup create 或 dsctl db2bak 命令时，目录服务器还会备份配置文件、证书数据库和存储在 /etc/dirsrv/slapd-*instance_name*/ 目录中的自定义模式文件到备份默认目录 /var/lib/dirsrv/slapd-*instance_name*/bak/config_files/。

在使用 Web 控制台执行备份时，目录服务器还会备份这些文件。

(BZ#2147446)

### Alias Entries 插件现在包括在目录服务器中

启用 Alias Entries 插件时，搜索条目会返回您设置为别名条目的条目。例如，Example 公司的员工 Barbara Jensen 发生了发生了变化。她的旧条目 uid=bjensen,ou=people,dc=example,dc=com 包含对新条目 uid=bsmith,ou=people,dc=example,dc=com 的别名。启用插件后，搜索 uid=bjensen,ou=people,dc=example,dc=com 条目会返回 uid=bsmith,ou=people,dc=example,dc=com 条目信息。

使用 ldapsearch 命令的 -a find 参数检索别名的条目。

目前，Alias Entries 插件只支持 *基本* 级别搜索。

如需更多信息，请参阅 Alias Entries 插件 描述。

(BZ#2203173)

### checkAllStateAttrs 配置选项现在可用

在使用 checkAllStateAttrs 设置进行身份验证时，您可以同时应用帐户不活跃和密码过期。启用此参数时，它会检查 main state 属性，如果帐户信息正确，它会检查备用状态属性。

(BZ#2174161)

现在，您可以使用 Directory Server Web 控制台为复制报告保存凭证和别名

在以前的版本中，当使用 Web 控制台为复制监控报告设置凭证和别名时，在 web 控制台重新载入后，这些设置将不再存在。在这个版本中，当您为复制报告设置凭证和别名时，Directory 服务器会在 .dsrc 文件中保存新设置，web 控制台会在重新载入后上传保存的设置。

(BZ#2030884)

389-ds-base 软件包中的重要更新和新功能

389-ds-base 软件包中包含的目录服务器 12.3 功能记录在 Red Hat Enterprise Linux 9.3 发行注记中：

- RHEL 9.3 提供 389-ds-base 2.3.4
- 现在，如果 绑定 操作失败，目录服务器可以关闭客户端连接
- 自动成员规则插件改进。默认情况下，它不再清理组
- 新的 passwordAdminSkipInfoUpdate: on/off 配置选项现在可用
- 新的 slapi_memberof （） 插件功能现在可用于目录服务器插件和客户端应用程序
- 目录服务器现在将虚拟属性 nsRole 替换为受管和过滤的角色的索引属性
- 新的 nsslapd-numlisteners 配置选项现在可用

## 5.2. 程序错误修复

了解红帽目录服务器 12.3 中修复的、对用户有严重影响的错误。

**cockpit-389-ds 软件包升级现在更新 389-ds-base 和 python3-lib389 软件包**

在以前的版本中，cockpit-389-ds 软件包没有指定它所依赖的 389-ds-base 软件包的版本。因此，只只升级 cockpit-389-ds 软件包不会更新 389-ds-base 和 python3-lib389 软件包，这可能会导致软件包之间的错误对齐和兼容性问题。在这个版本中，cockpit-389-ds 软件包依赖于 389-ds-base 准确版本，cockpit-389-ds 软件包的更新也会升级 389-ds-base 和 python3-lib389 软件包。

(BZ#2240021)

**禁用消费者上的复制不再使服务器崩溃**

在以前的版本中，当您在消费者服务器上禁用复制时，Directory 服务器会尝试删除不存在的消费者上的 changelog。因此，服务器意外终止并显示以下错误：

```
Error: -1 - Can't contact LDAP server - []
```

在这个版本中，禁用对消费者的复制可以正常工作。

(BZ#2184599)

**非 root 实例在创建后不再无法启动**

在以前的版本中，在非 root 实例模板中错误地禁用了 Rust 插件，默认的密码方案被移到基于 Rust 的已完全。因此，无法创建非 root 实例。在这个版本中，非 root 实例支持 Rust 插件，您可以使用 PBKDF2-SHA512 默认密码方案创建实例。

(BZ#2151864)

**dsconf 工具现在在设置 hub 或消费者角色时只接受值 65535 作为 replica-id**

在以前的版本中，当您配置 hub 或消费者角色时，dsconf 工具也会接受名为 65535 以外的值的 replica-id 选项。在这个版本中，dsconf 工具只接受 65535 作为 hub 或消费者角色的 replica-id 值。如果您没有在 dsconf 命令中指定这个值，则目录服务器会自动分配 replica-id 值 65535。

(BZ#1987373)

**dscreate ds-root 命令现在规范化路径**

在以前的版本中，当您在非 root 用户下创建实例时，并提供包含尾部斜杠的 bin_dir 参数值，dscreate ds-root 无法在 $PATH 变量中找到 bin_dir 值。因此，非 root 用户下的实例不会被创建。在这个版本中，dscreate ds-root 命令规范化路径，实例会如预期创建。

(BZ#2151868)

**dsconf 工具现在具有为 entryUUID 插件创建修复任务的 fixup 选项**

在以前的版本中，dsconf 工具没有提供为 entryUUID 插件创建修复任务的选项。因此，管理员无法使用 dsconf 创建任务来自动将 entryUUID 属性添加到现有条目。在这个版本中，您可以使用 dsconf 实用程序和 fixup 选项为 entryUUID 插件创建修复任务。例如，要修复包含 uid 属性的 dn=example,dc=com 条目下的所有条目，请输入：

```
# dsconf instance_name plugin entryuuid fixup -f "(uid=*)" "dn=example,dc=com"
```

(BZ#2047175)

**在 FIPS 模式下目录服务器安装过程中，访问日志不再显示错误消息**

在以前的版本中，当您以 FIPS 模式安装 Directory 服务器时，访问日志文件会显示以下出错信息：

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won't work correctly (for
example, users with PBKDF2_SHA256 password scheme won't be able to log
in). It's highly advisable to enable TLS on this instance.
```

在这个版本中，这个问题已被解决，访问日志中不再显示错误消息。

(BZ#2153668)

**389-ds-base 软件包中包含的目录服务器 12.3 程序错误修复包括在 Red Hat Enterprise Linux 9.3 发行注记中：**

- 现在，常规用户的分页搜索不会影响性能

- LMDB 导入现在可以更快地工作
- 模式复制现在可以在目录服务器中正常工作
- 引用模式现在可以在目录服务器中正常工作
- dirsrv 服务现在在重启后正确启动
- 更改安全参数现在可以正常工作

## 5.3. 已知问题

了解已知问题，以及 Directory Server 12.3 中的临时解决方案。

### 目录服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/导入 LDIF 文件

从 RHEL 8.3 开始，红帽目录服务器(RHDS)使用自己的私有目录，并且默认为 LDAP 服务启用 PrivateTmp systemd 指令。因此，RHDS 只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录导入 LDIF 文件。如果 LDIF 文件存储在不同的目录中，如 /var/tmp、/tmp 或 /root，则导入会失败，并显示类似如下的错误：

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

要临时解决这个问题，请完成以下步骤：

1. 将 LDIF 文件移到 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录中：

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
```

2. 设置允许 dirsrv 用户读取文件的权限：

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

3. 恢复 SELinux 上下文：

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

如需更多信息，请参阅 LDAP 服务无法访问主机 /tmp 和 /var/tmp 目录下的文件。

(BZ#2075525)

389-ds-base 软件包中的已知问题

Red Hat Directory Server 12.3 已知的影响 389-ds-base 软件包 的问题记录在 Red Hat Enterprise Linux 9.3 发行注记中：

- 当 nsslapd-numlisteners 属性值超过 2 时，目录服务器会失败

## 5.4. 过时的功能

了解在 Red Hat Directory Server 12.3 中弃用的功能。

389-ds-base 软件包中已弃用的功能

在 389-ds-base 软件包中弃用的目录服务器 12.3 功能记录在 Red Hat Enterprise Linux 9.3 发行注记中：

- nsslapd-ldapimaprootdn 参数已弃用

## 5.5. 删除的功能

了解在红帽目录服务器 12.3 中删除的功能。

删除 389-ds-base 软件包中的功能

删除的 Red Hat Directory Server 中的功能包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.3 发行注记中：

- **nsslapd-conntablesize 配置参数已从 389-ds-base中删除**

# 第 6 章 RED HAT DIRECTORY SERVER 12.2

了解新的系统要求、重要的更新和新功能、已知问题以及目录服务器 12.2 中实施的功能。

## 6.1. 重要更新和新功能

了解红帽目录服务器 12.2 中的新功能和重要更新。

### 目录服务器 12.2 rebase 到上游版本 2.2.7

目录服务器 12.2 基于上游版本 2.2.7，它提供很多程序错误修复和增强。如需显著变化的完整列表，请在更新前阅读上游发行注记： https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-1.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-2.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-3.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-4.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-5.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-5.html https://directory.fedoraproject.org/docs/389ds/releases/release-2-2-5.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-6.htmlhttps://directory.fedoraproject.org/docs/389ds/releases/release-2-2-7.html

### dsconf 工具现在可以为任务设置超时

在以前的版本中，如果任务的时间超过四分钟，则 dsconf 会返回以下信息：

```
DEBUG: The backup create task has failed with the error code: (None)
...
```

在这个版本中，您可以使用 --timeout 选项为任务设置所需的超时时间。超时不会停止任务，但它会停止 dsconf 工具等待任务结果。

(BZ#1993124)

### 现在，您可以使用 Web 控制台导入和导出证书

在以前的版本中，您只能使用 Web 控制台从服务器文件系统上的文件导入证书。在这个版本中，您还可以通过复制 base64- 编码的证书来导入文件。另外，您可以导出证书颁发机构和服务器证书。

(BZ#1751264)

### 389-ds-base 软件包中的重要更新和新功能

389-ds-base 软件包中包含的目录服务器 12.2 功能记录在 Red Hat Enterprise Linux 9.2 发行注记中：

- 目录服务器现在支持 TLS 的 ECDSA 私钥
- 目录服务器现在支持搜索操作的扩展日志记录
- NUNC_STANS 错误日志记录级别被新的 1048576 日志记录级别替代
- 目录服务器引入了安全日志
- 目录服务器现在可以压缩归档的日志文件
- 默认行为更改：目录服务器现在返回一个与添加到数据库时拼写完全相同的 DN
- Directory 服务器审计日志的新 nsslapd-auditlog-display-attrs 配置参数
- 新的 pamModuleIsThreadSafe 配置选项现在可用
- 目录服务器现在可以导入证书包

## 6.2. 程序错误修复

了解红帽目录服务器 12.2 中修复的、对用户有严重影响的错误。

389-ds-base 软件包中包含的目录服务器 12.2 程序错误修复包括在 Red Hat Enterprise Linux 9.2 发行注记中：

- 目录服务器复制管理器帐户的密码更改现在可以正常工作

- 现在，当使用带有 db_dir 参数的自定义路径时，dscreate 工具现在可以正常工作

### 6.3. 已知问题

了解已知问题，以及 Directory Server 12.2 中的临时解决方案。

目录服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/导入 LDIF 文件

从 RHEL 8.3 开始，红帽目录服务器(RHDS)使用自己的私有目录，并且默认为 LDAP 服务启用 PrivateTmp systemd 指令。因此，RHDS 只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录导入 LDIF 文件。如果 LDIF 文件存储在不同的目录中，如 /var/tmp、/tmp 或 /root，则导入会失败，并显示类似如下的错误：

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

要临时解决这个问题，请完成以下步骤：

1. 将 LDIF 文件移到 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录中：

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name__/ldif/
```

2. 设置允许 dirsrv 用户读取文件的权限：

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

3. 恢复 SELinux 上下文：

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

如需更多信息，请参阅 LDAP 服务无法访问主机 /tmp 和 /var/tmp 目录下的文件。

(BZ#2075525)

访问日志在 Directory Server 安装过程中以 FIPS 模式显示错误消息

当您以 FIPS 模式安装目录服务器时，访问日志文件会显示以下错误消息：

```
[time_stamp]
- WARN - slapd_do_all_nss_ssl_init - ERROR: TLS is not enabled, and the
machine is in FIPS mode. Some functionality won't work correctly (for
example, users with PBKDF2_SHA256 password scheme won't be able to log
in). It's highly advisable to enable TLS on this instance.
```

发生此行为的原因是，目录服务器会发现 TLS 未初始化并记录错误消息。但是，当 dscreate 实用程序完成 TLS 初始化并启用安全性时，便不再存在错误消息。

(BZ#2153668)

389-ds-base 软件包中的已知问题

Red Hat Directory Server 12.2 已知的影响 389-ds-base 软件包的问题记录在 Red Hat Enterprise Linux 9.2 发行注记中：

- dsconf 工具没有选项来为 entryUUID 插件创建修复任务
- 在 Directory 服务器中为后缀配置引用失败
- 当以引用模式启动时，目录服务器会意外终止

## 6.4. 过时的功能

了解在 Red Hat Directory Server 12.2 中弃用的功能。

389-ds-base 软件包中已弃用的功能

在 389-ds-base 软件包中弃用的目录服务器 12.2 功能记录在 Red Hat Enterprise Linux 9.2 发行注记中：

- nsslapd-idlistscanlimit 参数已弃用，其默认值已更改

# 第 7 章 RED HAT DIRECTORY SERVER 12.1

了解新的系统要求，突出显示了 Directory Server 12.1 中实施的更新和新功能、已知问题和已弃用的功能。

## 7.1. 突出显示更新和新功能

本节记录了目录服务器 12.1 中的新功能和重要更新。

### 目录服务器 12.1 rebase 到上游版本 2.1.3

目录服务器 12.1 基于上游版本 2.1.3，它提供很多程序错误修复和增强。如需显著变化的完整列表，请在更新前阅读上游发行注记：

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-0.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-1.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-1-3.html

### LDAP 浏览器现已获得全面支持

借助此项功能增强，您可以从 Web 控制台中的 LDAP 浏览器 选项卡中管理 LDAP 条目。例如，您可以：

- 使用 Tree 或 Table 视图 浏览目录。
- 管理条目，如用户、组、角色、组织单元(OU)和自定义条目。
- 管理访问控制指令(ACI)。
- 管理服务定义类(CoS)。

- 搜索条目。

突出显示 389-ds-base 软件包中的更新和新功能

Red Hat Directory Server 中的功能包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.1 发行注记中：

- 目录服务器现在在使用 ldapdelete时支持递归删除操作
- 现在，您可以在 Directory 服务器安装过程中设置基本复制选项
- 目录服务器现在支持取消 Auto Membership 插件任务
- 目录服务器现在支持非 root 用户创建实例
- 现在，在 Directory 服务器中默认启用复制更改日志修剪

## 7.2. 已知问题

本节记录了已知问题，如果适用，目录服务器 12.1 中的临时解决方案。

目录服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/导入 LDIF 文件

dsconf backend import 命令要求您指定您要导入的 LDIF 文件的路径。但是，由于文件系统及 SELinux 权限，以及其他操作系统的限制，Directory 服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录导入 LDIF 文件。如果 LDIF 文件存储在另一个目录中，则导入会失败，并显示类似如下的错误：

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

要临时解决这个问题：

1. 将文件移动到 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录中：

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
```

2. 设置允许 dirsrv 用户读取文件的权限：

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

3. 恢复 SELinux 上下文：

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

(BZ#2081352)

**更改复制管理器帐户的密码后目录服务器复制会失败**

更改密码后，Directory 服务器无法正确更新复制协议的密码缓存。因此，当您更改复制管理器帐户的密码时，复制中断。要临时解决这个问题，重启 Directory Server 实例。因此，缓存会在启动时重建，复制连接会与新密码绑定，而不是旧连接。

(BZ#1956987)

**389-ds-base 软件包中的已知问题**

Red Hat Directory Server 中已知的问题包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.1 发行注记中：

- dsconf 实用程序没有为 entryUUID 插件创建修复任务的选项
- 在 Directory 服务器中为后缀配置引用失败
- 当以引用模式启动时，目录服务器会意外终止

**389-ds-base 软件包中已弃用的功能**

Red Hat Directory Server 弃用的功能已从 389-ds-base 软件包中删除，记录在 Red Hat Enterprise Linux 9.1 发行注记中：

- **-h 和 -p 选项在 OpenLDAP 客户端工具中已弃用**

# 第 8 章 RED HAT DIRECTORY SERVER 12.0

本节包含与安装 Directory 服务器 12.0 相关的信息，包括先决条件和平台要求。

## 8.1. 突出显示更新和新功能

本节记录了目录服务器 12.0 中的新功能和重要更新。

### 目录服务器 12.0 基于上游版本 2.0.14

目录服务器 12.0 基于上游版本 2.0.14，它提供很多程序错误修复和增强。如需显著变化的完整列表，请在更新前阅读上游发行注记：

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-14.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-13.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-12.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-11.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-10.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-9.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-8.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-7.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-6.html

- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-5.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-4.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-3.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-2.html
- https://directory.fedoraproject.org/docs/389ds/releases/release-2-0-1.html

突出显示 389-ds-base 软件包中的更新和新功能

Red Hat Directory Server 中的功能包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.0 发行注记中：

- 目录服务器不再使用全局更改日志
- 目录服务器现在在 tmpfs 文件系统中存储数据库的内存映射文件

## 8.2. 程序错误修复

这部分论述了 Directory Server 12.0 中修复的、对用户有严重影响的错误。

手动更改条目缓存配置现在可以在 web 控制台中正常工作。

默认情况下，Directory 服务器使用自动缓存调整。但是，之前您无法在 web 控制台中禁用自动缓存调整设置，并手动设置所需的条目缓存配置。在这个版本中解决了这个问题，您现在可以在 web 控制台中手动配置条目缓存。

修复了 web 控制台不同部分的拼写错误

在以前的版本中，web 控制台的不同部分包含文本字段中的错误。因此，用户会显示不正确的信息。在这个版本中解决了这个问题，Web 控制台现在显示正确的文本信息。

更改多个插件的配置现在可以在 web 控制台中正常工作

在以前的版本中，当您尝试使用 web 控制台更改插件配置时，会显示不正确的错误消息，或者加载循环不会消失。因此，您无法保存新配置，或者不知道配置是否已成功保存。以下插件会受到影响：

- POSIX Winsync 插件
- referential Integrity 插件
- RootDN Access Control 插件
- Retro Changelog 插件

在这个版本中解决了这个问题。现在，您可以使用 Web 控制台按预期配置这些插件。

现在，在 web 控制台中更改日志导出可以正常工作

在以前的版本中，在 web 控制台中，在导出 changelog 中用于调试目的，您可以选择两个选项：Decode Base64 更改，且只有 Export CSNs。但是，只有 Export CSNs 选项被考虑。在本发行版本中，可以只检查其中一个选项，changelog 会根据预期的所选值导出。

为复制拓扑报告配置凭证和命名别名现在可以在 web 控制台中正常工作

在以前的版本中，您无法使用 Web 控制台为复制拓扑报告设置凭证或命名别名，因为弹出窗口 添加 Report Credentials 和 Add Report Alias 字段（您可以在输入所需信息时）不可写入。在这个发行版本中，弹出窗口中的字段是可写的，您可以设置报告凭证，或者按预期配置命名别名。

Directory Server web 控制台现在验证日志记录配置值

在以前的版本中，Directory Server Web 控制台在 Logging 页面中接受不同类型的日志的无效值。因此，当用户试图保存设置时会出现一个错误。在这个版本中，为日志记录配置值添加了验证。因此，Web 控制台不接受无效的输入。

使用搜索功能后，架构 页中的属性不再可编辑

在以前的版本中，在 Directory Server web 控制台的 Schema 页面中搜索属性后，一个 Cascading Style Sheet(CSS)错误配置会导致属性编辑。在这个版本中，编辑功能已被禁用。

启用 DNA 插件不再失败

在以前的版本中，在 Directory Server web 控制台中启用 Distributed Numeric Assignment(DNA) 插件会失败，并导致浏览器错误。在这个版本中，启用 DNA 插件可以正常工作。

在帐户策略插件中添加配置条目不再失败

在以前的版本中，尝试在 Account Policy 插件中添加配置条目有时会失败。要解决这个问题，如果未指定 共享配置 DN 值，这个更新会禁用 Create Config 按钮。

从带有复制元数据的 LDIF 文件中导入现在可以正常工作

在以前的版本中，导入带有复制元数据的 LDIF 文件可能会导致复制在某些情况下失败：

在第一个情况下，在导入的 LDIF 文件的 suffix 条目前放置复制向量(RUV)条目会被忽略。因此，带有导入副本的复制会失败，因为生成 ID 不匹配。在这个版本中，Directory 服务器会在导入结束时写入跳过的 RUV 条目。

在第二个情况下，在 RUV 不匹配后，更改日志重新初始化不包含起始更改序列号(CSN)。因此，带有导入副本的复制会失败，因为 changelog 中缺少 CSN。在这个版本中，当重新初始化更改日志时，Directory 服务器会创建 RUV maxcsn 条目。

因此，在从包含复制元数据的 LDIF 文件导入后，管理员不必重新初始化复制。

389-ds-base 软件包中的程序错误修复

Red Hat Directory Server 中的程序错误修复包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.0 发行注记中：

- 现在，使用 PBKDF2 算法以 FIPS 模式验证目录服务器可以正常工作

## 8.3. 技术预览

本节包括了在 Directory Server 12.0 中不受支持的技术预览。

Directory Server Web 控制台提供 LDAP 浏览器作为技术预览

已将 LDAP 浏览器添加到 Directory Server Web 控制台。在 web 控制台中使用 LDAP Browser 选项卡，您可以：

- 浏览目录
- 管理条目，如用户、组、组织单元(OU)和自定义条目
- 管理 ACI

请注意，红帽将此功能作为不受支持的技术预览提供。

### 8.4. 已知问题

本节记录了已知问题的信息，并在 Directory Server 12.0 中解决一个临时解决方案。

**目录服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/导入 LDIF 文件**

dsconf backend import 命令要求您指定您要导入的 LDIF 文件的路径。但是，由于文件系统及 SELinux 权限，以及其他操作系统的限制，Directory 服务器只能从 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录导入 LDIF 文件。如果 LDIF 文件存储在另一个目录中，则导入会失败，并显示类似如下的错误：

```
Could not open LDIF file "/tmp/example.ldif", errno 2 (No such file or directory)
```

要临时解决这个问题：

1. 将文件移动到 /var/lib/dirsrv/slapd-*instance_name*/ldif/ 目录中：

```
# mv /tmp/example.ldif /var/lib/dirsrv/slapd-instance_name/ldif/
```

2. 设置允许 dirsrv 用户读取文件的权限：

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

3. 恢复 SELinux 上下文：

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

### 更改复制管理器帐户的密码后目录服务器复制会失败

更改密码后，Directory 服务器无法正确更新复制协议的密码缓存。因此，当您更改复制管理器帐户的密码时，复制中断。要临时解决这个问题，重启 Directory Server 实例。因此，缓存会在启动时重建，复制连接会与新密码绑定，而不是旧连接。

### 389-ds-base 软件包中的已知问题

Red Hat Directory Server 中已知的问题包括在 389-ds-base 软件包中，记录在 Red Hat Enterprise Linux 9.0 发行注记中：

- dsconf 实用程序没有为 entryUUID 插件创建修复任务的选项
- 在 Directory 服务器中为后缀配置引用失败
- 当以引用模式启动时，目录服务器会意外终止

## 8.5. 删除的功能

本节记录了已在目录服务器 12.0 中删除的功能。

### nsslapd-subtree-rename-switch 参数已被删除

在以前的版本中，管理员可以配置 Directory 服务器，以防止在数据库中的子树之间移动条目。由于稳定性问题，这个功能已被删除，因此 nsslapd-subtree-rename-switch 参数不再存在。因此，在子树间移动条目不再可以被取消激活。另外，如果您需要这个功能，请创建访问控制指令(ACI)。