

美国硅谷第二可用区开放

10余款云产品上线

全美双可用区尽享ECS88折, 10.10~11.9 仅此一月

[查看详情](#)[🏠](#) » [技术](#) » [学习](#) » [查看内容](#)

RHCSA 系列（七）：使用 ACL（访问控制列表）和挂载 Samba/NFS 共享

2015-9-22 09:07 评论: 2 收藏: 6

原文：<http://www.tecmint.com/rhcsa-exam-configure-acls-and-mount-nfs-samba-shares/>
译文：LCTT <https://linux.cn/article-6263-1.html>作者：Gabriel Cánepa
译者：FSSlc

在上一篇文章(**RHCSA 系列（六）** <<https://linux.cn/article-6257-1.html>>)中，我们解释了如何使用 parted 和 ssm 来设置和配置本地系统存储。

RHCSA 系列: 配置 ACL 及挂载 NFS/Samba 共享 - Part 7

我们也讨论了如何创建和在系统启动时使用一个密码来挂载加密的卷。另外，我们告诫过你要避免在挂载的文件系统上执行危险的存储管理操作。记住了这点后，现在，我们将回顾在 RHEL 7 中最常使用的文件系统格式，然后将涵盖有关手动或自动挂载、使用和卸载网络文件系统（CIFS 和 NFS）的话题以及在你的操作系统上实现 [访问控制列表](#) 的使用。

前提条件

在进一步深入之前，请确保你可使用 Samba 服务和 NFS 服务（注意在 RHEL 7 中 NFSv2 已不再被支持）。

在本次指导中，我们将使用一个 IP 地址为 192.168.0.10 且同时运行着 Samba 服务和 NFS 服务的机器来作为服务器，使用一个 IP 地址为 192.168.0.18 的 RHEL 7 机器来作为客户端。在这篇文章的后面部分，我们将告诉你在客户端上你需要安装哪些软件包。

RHEL 7 中的文件系统格式

从 RHEL 7 开始，由于 XFS 的高性能和可扩展性，它已经被作为所有的架构中的默认文件系统。根据 Red Hat 及其合作伙伴在主流硬件上执行的最新测试，当前 XFS 已支持最大为 500 TB 大小的文件系统。

另外，XFS 启用了 `user_xattr`（扩展用户属性）和 `acl`（POSIX 访问控制列表）来作为默认的挂载选项，而不像 ext3 或 ext4（对于 RHEL 7 来说，ext2 已过时），这意味着当挂载一个 XFS 文件系统时，你不必显式地在命令行或 `/etc/fstab` 中指定这些选项（假如你想在后一种情况下禁用这些选项，你必须显式地使用 `no_acl` 和 `no_user_xattr`）。

请记住扩展用户属性可以给文件和目录指定，用来存储任意的额外信息如 mime 类型，字符集或文件的编码，而用户属性中的访问权限由一般的文件权限位来定义。

访问控制列表

作为一名系统管理员，无论你是新手还是专家，你一定非常熟悉与文件和目录有关的常规访问权限，这些权限为所有者，所有组和“世界”（所有的其他人）指定了特定的权限（可读，可写及可执行）。但如若你需要稍微更新下你的记忆，请参考 **RHCSA 系列（三）**

<https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Storage_Administration_Guide/ch-acls.html> .

但是，由于标准的 `ugo/rwx` 集合并不允许为不同的用户配置不同的权限，所以 ACL 便被引入了进来，为的是为文件和目录定义更加详细的访问权限，而不仅仅是这些特别指定的特定权限。

事实上，ACL 定义的权限是由文件权限位所特别指定的权限的一个超集。下面就让我们看看这个转换是如何在真实世界中被应用的吧。

1. 存在两种类型的 ACL：访问 ACL，可被应用到一个特定的文件或目录上；以及默认 ACL，只可被应用到一个目录上。假如目录中的文件没有 ACL，则它们将继承它们的父目录的默认 ACL。
2. 从一开始，ACL 就可以为每个用户，每个组或不在文件所属组中的用户配置相应的权限。
3. ACL 可使用 `setfacl` 来设置（和移除），可相应地使用 `-m` 或 `-x` 选项。

例如，让我们创建一个名为 `tecmint` 的组，并将用户 `johndoe` 和 `davenull` 加入该组：

```
1. # groupadd tecmint
2. # useradd johndoe
3. # useradd davenull
4. # usermod -a -G tecmint johndoe
5. # usermod -a -G tecmint davenull
```

并且让我们检验这两个用户都已属于追加的组 `tecmint`：

```
1. # id johndoe
2. # id davenull
```

检验用户

现在，我们在 `/mnt` 下创建一个名为 `playground` 的目录，并在该目录下创建一个名为 `testfile.txt` 的文件。我们将设定该文件的属组为 `tecmint`，并更改它的默认 `ugo/rwx` 权限为 `770`（即赋予该文件的属主和属组可读、可写和可执行权限）：

```
1. # mkdir /mnt/playground
2. # touch /mnt/playground/testfile.txt
3. # chown :tecmint /mnt/playground/testfile.txt
4. # chmod 770 /mnt/playground/testfile.txt
```

接着，依次切换为 `johndoe` 和 `davenull` 用户，并在文件中写入一些信息：

```
1. # su johndoe
2. $ echo "My name is John Doe" > /mnt/playground/testfile.txt
3. $ su davenull
4. $ echo "My name is Dave Null" >> /mnt/playground/testfile.txt
```

到目前为止，一切正常。现在我们让用户 `gacanepa` 来向该文件执行写操作 - 则写操作将会失败，这是可以预料的。

```
1. $ su gacanepa
2. $ echo "My name is Gabriel Canepa" >> /mnt/playground/testfile.txt
```

管理用户的权限

但实际上我们需要用户 `gacanepa`（他不是组 `tecmint` 的成员）在文件 `/mnt/playground/testfile.txt` 上有写权限，那又该怎么办呢？首先映入你脑海里的可能是将该用户添加到组 `tecmint` 中。但那将使得他在所有该组具有写权限位的文件上均拥有写权限，但我们并不想这样，我们只想他能够在文件 `/mnt/playground/testfile.txt` 上有写权限。

现在，让我们给用户 `gacanepa` 在 `/mnt/playground/testfile.txt` 文件上有读和写权限。

以 root 的身份运行如下命令：

```
1. | # setfacl -R -m u:gacanepa:rwX /mnt/playground
```

则你将成功地添加一条 ACL，允许 gacanepa 对那个测试文件可写。然后切换为 gacanepa 用户，并再次尝试向该文件写入一些信息：

```
1. | $ echo "My name is Gabriel Canepa" >> /mnt/playground/testfile.txt
```

要观察一个特定的文件或目录的 ACL，可以使用 `getfacl` 命令：

```
1. | # getfacl /mnt/playground/testfile.txt
```

检查文件的 ACL

要为目录设定默认 ACL（它的内容将被该目录下的文件继承，除非另外被覆写），在规则前添加 `d:` 并特别指定一个目录名，而不是文件名：

```
1. | # setfacl -m d:o:r /mnt/playground
```

上面的 ACL 将允许不在属组中的用户对目录 /mnt/playground 中的内容有读权限。请注意观察这次更改前后 `getfacl /mnt/playground` 的输出结果的不同：

在 Linux 中设定默认 ACL

在官方的 [RHEL 7 存储管理指导手册的第 20 章](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Storage_Administration_Guide/ch-acls.html) <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Storage_Administration_Guide/ch-acls.html> 中提供了更多有关 ACL 的例子，我极力推荐你看一看它并将它放在身边作为参考。

挂载 NFS 网络共享

要显示你服务器上可用的 NFS 共享的列表，你可以使用带有 `-e` 选项的 `showmount` 命令，再跟上机器的名称或它的 IP 地址。这个工具包含在 `nfs-utils` 软件包中：

```
1. | # yum update && yum install nfs-utils
```

接着运行：

```
1. | # showmount -e 192.168.0.10
```

则你将得到一个在 192.168.0.10 上可用的 NFS 共享的列表：

检查可用的 NFS 共享

要按照需求在本地客户端上使用命令行来挂载 NFS 网络共享，可使用下面的语法：

```
1. | # mount -t nfs -o [options] remote_host:/remote/directory /local/directory
```

其中，在我们的例子中，对应为：

```
1. | # mount -t nfs 192.168.0.10:/NFS-SHARE /mnt/nfs
```

若你得到如下的错误信息：`Job for rpc-statd.service failed. See "systemctl status rpc-statd.service" and "journalctl -xn" for details.`，请确保 `rpcbind` 服务被启用且已在你的系统中启动了。

```
1. | # systemctl enable rpcbind.socket
2. | # systemctl restart rpcbind.service
```

接着重启。这就应该达到了上面的目的，且你将能够像先前解释的那样挂载你的 NFS 共享了。若你需要在系统启动时自动挂载 NFS 共享，可以向 `/etc/fstab` 文件添加一个有效的条目：

```
1. | remote_host:/remote/directory /local/directory nfs options 0 0
```

上面的变量 `remote_host`, `/remote/directory`, `/local/directory` 和 `options`(可选) 和在命令行中手动挂载一个 NFS 共享时使用的一样。按照我们前面的例子，对应为：

```
1. | 192.168.0.10:/NFS-SHARE /mnt/nfs nfs defaults 0 0
```

挂载 CIFS (Samba) 网络共享

Samba 代表一个特别的工具，使得在由 *nix 和 Windows 机器组成的网络中进行网络共享成为可能。要显示可用的 Samba 共享，可使用带有 `-L` 选项的 `smbclient` 命令，再跟上机器的名称或它的 IP 地址。这个工具包含在 `samba_client` 软件包中：

你将被提示在远程主机上输入 root 用户的密码：

```
1. | # smbclient -L 192.168.0.10
```

检查 Samba 共享

要在本地客户端上挂载 Samba 网络共享，你需要已安装好 `cifs-utils` 软件包：

```
1. | # yum update && yum install cifs-utils
```

然后在命令行中使用下面的语法：

```
1. | # mount -t cifs -o credentials=/path/to/credentials/file //remote_host/samba_share
    /local/directory
```

其中，在我们的例子中，对应为：

```
1. | # mount -t cifs -o credentials=~/.smbcredentials //192.168.0.10/gacanepa /mnt/samba
```

其中 `.smbcredentials` 的内容是：

```
1. | username=gacanepa
```

```
2. | password=XXXXXX
```

它是一个位于 root 用户的家目录(/root/) 中的隐藏文件，其权限被设置为 600，所以除了该文件的属主外，其他人对该文件既不可读也不可写。

请注意 samba_share 是 Samba 共享的名称，由上面展示的 `smbclient -L remote_host` 所返回。

现在，若你需要在系统启动时自动地使得 Samba 分享可用，可以向 /etc/fstab 文件添加一个像下面这样的有效条目：

```
1. | //remote_host:/samba_share /local/directory cifs options 0 0
```

上面的变量 remote_host, /remote/directory, /local/directory 和 options(可选) 和在命令行中手动挂载一个 Samba 共享时使用的一样。按照我们前面的例子中所给的定义，对应为：

```
1. | //192.168.0.10/gacanepa /mnt/samba cifs credentials=/root/smbcredentials,defaults 0 0
```

结论

在这篇文章中，我们已经解释了如何在 Linux 中设置 ACL，并讨论了如何在一个 RHEL 7 客户端上挂载 CIFS 和 NFS 网络共享。

我建议你练习这些概念，甚至混合使用它们（试着在一个挂载的网络共享上设置 ACL），直至你感觉掌握了。假如你有问题或评论，请随时随地使用下面的评论框来联系我们。另外，请随意通过你的社交网络分享这篇文章。

via: <http://www.tecmint.com/rhcsa-exam-configure-acls-and-mount-nfs-samba-shares/>

<<http://www.tecmint.com/rhcsa-exam-configure-acls-and-mount-nfs-samba-shares/>>

作者：Gabriel Cánepa <<http://www.tecmint.com/author/gacanepa/>> 译者：FSSlc <<https://github.com/FSSlc>> 校

对：wxy <<https://github.com/wxy>>

本文由 LCTT <<https://github.com/LCTT/TranslateProject>> 原创翻译，Linux 中国 <[file:///root/github/my-notes/Manual/Linux.cn/RHCSA/RHCSA%E7%B3%BB%E5%88%97%E4%BD%BF%E7%94%A8%20ACL%E7%BC%88%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6%E5%88%97%E8%A1%A8\)%20.html](file:///root/github/my-notes/Manual/Linux.cn/RHCSA/RHCSA%E7%B3%BB%E5%88%97%E4%BD%BF%E7%94%A8%20ACL%E7%BC%88%E8%AE%BF%E9%97%AE%E6%8E%A7%E5%88%B6%E5%88%97%E8%A1%A8)%20.html)> 荣誉推出

原文：<http://www.tecmint.com/rhcsa-exam-configure-acls-and-mount-nfs-samba-shares/> <<http://www.tecmint.com/rhcsa-exam-configure-acls-and-mount-nfs-samba-shares/>>

作者：Gabriel Cánepa

译文：LCTT <<http://lctt.github.io/>> <https://linux.cn/article-6263-1.html> <<https://linux.cn/article-6263-1.html>>

译者：FSSlc

发表评论

验证码 换一个



热点评论

来自上海的 Microsoft Edge 12.10536|Windows Phone 10.0 用户 2015-9-22 20:08

应该是7了不是6



- **RHEL 7 中的文件系统格式**
 - 访问控制列表
 - 挂载 NFS 网络共享
 - 挂载 CIFS (Samba) 网络共享
- **结论**



ACL



RHCSA

- RHCSA 系列（六）：使用 Parted 和 SSM 来配置和加密系统存储 2015-9-21
- RHCSA 系列（八）：加固 SSH，设定主机名及启用网络服务 2015-9-23
- RHCSA 系列（九）：安装、配置及加固一个 Web 和 FTP 服务器 2015-9-24
- RHCSA 系列（十）：Yum 包管理、Cron 自动任务计划和监控系统日志 2015-9-26
- RHCSA 系列（十一）：使用 firewalld 和 iptables 来控制网络流量 2015-9-29
- RHCSA 系列（十二）：使用 Kickstart 完成 RHEL 7 的自动化安装 2015-10-2