

RHCE 系列（七）：在 Linux 客户端配置基于 Kerberos 身份验证的 NFS 服务器

2015-11-17 13:38

参考原文：<http://www.tecmint.com/setting...>

作者：Gabriel Cánepa

编译文章：LCTT <https://linux.cn/article-6593-1.html>

译者：ictlyh

在本系列的前一篇文章，我们回顾了如何在可能包括多种类型操作系统的网络上配置 Samba 共享 <<https://linux.cn/article-6550-1.html>>。现在，如果你需要为一组类 Unix 客户端配置文件共享，很自然的你会想到网络文件系统，或简称 NFS。



RHCE 系列：第七部分 - 设置使用 Kerberos 进行身份验证的 NFS 服务器

在这篇文章中我们会介绍配置基于 Kerberos 身份验证的 NFS 共享的整个流程。假设你已经配置好了一个 NFS 服务器和一个客户端。如果还没有，可以参考 [安装和配置 NFS 服务器](http://www.tecmint.com/configure-nfs-server/) <<http://www.tecmint.com/configure-nfs-server/>> - 它列出了需要安装的依赖软件包并解释了在进行下一步之前如何在服务器上进行初始化配置。

另外，你可能还需要配置 SELinux <<http://www.tecmint.com/selinux-essentials-and-control-file-system-access/>> 和 firewalld <<http://www.tecmint.com/firewalld-rules-for-centos-7/>> 以允许通过 NFS 进行文件共享。

下面的例子假设你的 NFS 共享目录在 box2 的 /nfs：

```
# semanage fcontext -a -t public_content_rw_t "/nfs(/.*)"
# restorecon -R /nfs
# setsebool -P nfs_export_all_rw on
# setsebool -P nfs_export_all_ro on
```

(其中 -P 标记指示重启持久有效)。

最后，别忘了：

创建 NFS 组并配置 NFS 共享目录

1、新建一个名为 nfs 的组并给它添加用户 nfsnobody，然后更改 /nfs 目录的权限为 0770，组属主为 nfs。于是，nfsnobody (对应请求用户) 在共享目录有写的权限，你就不需要在 /etc/exports 文件中使用 `norootsquash` (LCTT 译注：设为 `root_squash` 意味着在访问 NFS 服务器上的文件时，客户机上的 root 用户不会被当作 root 用户来对待)。

```
# groupadd nfs
# usermod -a -G nfs nfsnobody
# chmod 0770 /nfs
# chgrp nfs /nfs
```

2、像下面那样更改 export 文件 (/etc/exports) 只允许从 box1 使用 Kerberos 安全验证的访问 (sec=krb5)。

注意：anongid 的值设置为之前新建的组 nfs 的 GID：

exports – 添加 NFS 共享

```
/nfs box1(rw,sec=krb5,anongid=1004)
```

3、再次 `export (-r)` 所有 `(-a)` NFS 共享。为输出添加详情 `(-v)` 是个好主意，因为它提供了发生错误时解决问题的有用信息：

```
# exportfs -arv
```

4、重启并启用 NFS 服务器以及相关服务。注意你不需要启动 `nfs-lock` 和 `nfs-idmapd`，因为系统启动时其它服务会自动启动它们：

```
# systemctl restart rpcbind nfs-server nfs-lock nfs-idmap
# systemctl enable rpcbind nfs-server
```

测试环境和其它前提要求

在这篇指南中我们使用下面的测试环境：

- 客户端机器 [box1: 192.168.0.18]
- NFS / Kerberos 服务器 [box2: 192.168.0.20]（也称为密钥分发中心，简称 KDC）。

注意： Kerberos 服务是至关重要的认证方案。

正如你看到的，为了简便，NFS 服务器和 KDC 在同一台机器上，当然如果你有更多可用机器你也可以把它们安装在不同的机器上。两台机器都在 **mydomain.com** 域。

最后同样重要的是，Kerberos 要求客户端和服务端中至少有一个域名解析的基本方式和网络时间协议 <<http://www.tecmint.com/install-ntp-server-in-centos/>> 服务，因为 Kerberos 身份验证的安全一部分基于时间戳。

为了配置域名解析，我们在客户端和服务端中编辑 /etc/hosts 文件：

host 文件 – 为域添加 DNS

```
192.168.0.18 box1.mydomain.com box1
192.168.0.20 box2.mydomain.com box2
```

在 RHEL 7 中，chrony 是用于 NTP 同步的默认软件：

```
# yum install chrony
# systemctl start chronyd
# systemctl enable chronyd
```

为了确保 chrony 确实在和时间服务器同步你系统的时间，你可能要输入下面的命令两到三次，确保时间偏差尽可能接近 0：

```
# chronyc tracking
```

```
[root@box1 ~]# chronyc tracking
Reference ID      : 66.60.22.202 (argentino.microsulesybernabo.com.ar)
Stratum          : 5
Ref time (UTC)   : Fri Sep  4 00:18:34 2015
System time      : 0.000058842 seconds slow of NTP time
Last offset      : -0.043042619 seconds
RMS offset       : 0.043042619 seconds
Frequency        : 107.031 ppm slow
Residual freq    : -19.210 ppm
Skew             : 528.732 ppm
Root delay       : 0.056379 seconds
Root dispersion  : 0.012710 seconds
Update interval  : 65.2 seconds
Leap status      : Normal
```

1

```
[root@box1 ~]# chronyc tracking
Reference ID      : 66.60.22.202 (argentino.microsulesybernabo.com.ar)
Stratum          : 5
Ref time (UTC)   : Fri Sep  4 00:37:58 2015
System time      : 0.008076809 seconds fast of NTP time
Last offset      : 0.007414413 seconds
RMS offset       : 0.023549324 seconds
Frequency        : 58.135 ppm fast
Residual freq    : 1.626 ppm
Skew             : 103.616 ppm
Root delay       : 0.162798 seconds
Root dispersion  : 0.039265 seconds
Update interval  : 257.2 seconds
Leap status      : Normal
```

2

<http://www.tecmint.com>

用 Chrony 同步服务器时间

安装和配置 Kerberos

要设置 KDC，首先在客户端和服务端安装下面的软件包（客户端不需要 server 软件包）：

```
# yum update && yum install krb5-server krb5-workstation pam_krb5
```

安装完成后，编辑配置文件（/etc/krb5.conf 和 /var/kerberos/krb5kdc/kadm5.acl），像下面那样用 **mydomain.com** 替换所有 example.com。

下一步，确保 Kerberos 能功过防火墙并启动/启用相关服务。

重要：客户端也必须启动和启用 nfs-secure：

```
# firewall-cmd --permanent --add-service=kerberos
# systemctl start krb5kdc kadmin nfs-secure
# systemctl enable krb5kdc kadmin nfs-secure
```

现在创建 Kerberos 数据库（请注意这可能会需要一点时间，因为它会和你的系统进行多次交互）。为了加速这个过程，我打开了另一个终端并运行了 **ping -f localhost 30** 到 45 秒）：

```
# kdb5_util create -s
```

```
[root@box2 ~]# kdb5_util create -s http://www.tecmint.com
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'MYDOMAIN.COM',
master key name 'K/M@MYDOMAIN.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: Enter password twice
Re-enter KDC database master key to verify:
[root@box2 ~]#
```

创建 Kerberos 数据库

下一步，使用 `kadmin.local` 工具为 `root` 创建管理权限：

```
# kadmin.local
# addprinc root/admin
```

添加 Kerberos 服务器到数据库：

```
# addprinc -randkey host/box2.mydomain.com
```

在客户端（`box1`）和服务器（`box2`）上对 NFS 服务同样操作。请注意下面的截图中在退出前我忘了在 `box1` 上进行操作：

```
# addprinc -randkey nfs/box2.mydomain.com
# addprinc -randkey nfs/box1.mydomain.com
```

输入 `quit` 和回车键退出：

```
[root@box2 ~]# kdb5_util create -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'MYDOMAIN.COM',
master key name 'K/M@MYDOMAIN.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key: Enter password twice
Re-enter KDC database master key to verify:
[root@box2 ~]# kadmin.local
Authenticating as principal root/admin@MYDOMAIN.COM with password.
kadmin.local: addprinc root/admin
WARNING: no policy specified for root/admin@MYDOMAIN.COM; defaulting to no policy
Enter password for principal "root/admin@MYDOMAIN.COM": Enter password twice
Re-enter password for principal "root/admin@MYDOMAIN.COM":
Principal "root/admin@MYDOMAIN.COM" created.
kadmin.local: addprinc -randkey host/box2.mydomain.com
WARNING: no policy specified for host/box2.mydomain.com@MYDOMAIN.COM; defaulting to
no policy
Principal "host/box2.mydomain.com@MYDOMAIN.COM" created.
kadmin.local: addprinc -randkey nfs/box2.mydomain.com
WARNING: no policy specified for nfs/box2.mydomain.com@MYDOMAIN.COM; defaulting to
no policy
Principal "nfs/box2.mydomain.com@MYDOMAIN.COM" created.
kadmin.local: quit
[root@box2 ~]#
```

<http://www.tecmint.com>

添加 Kerberos 到 NFS 服务器

为 root/admin 获取和缓存 ticket-granting 票据授权票据 ticket :

```
# kinit root/admin
# klist
```

```
[root@box2 ~]# kinit root/admin
Password for root/admin@MYDOMAIN.COM:
[root@box2 ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: root/admin@MYDOMAIN.COM

Valid starting    Expires    Service principal
09/05/2015 14:08:42  09/06/2015 14:08:42  krbtgt/MYDOMAIN.COM@MYDOMAIN.COM
[root@box2 ~]#
```

<http://www.tecmint.com>

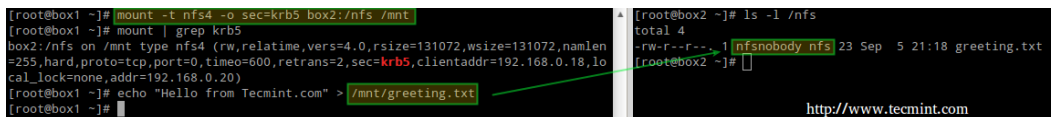
缓存 Kerberos

真正使用 Kerberos 之前的最后一步是保存被授权使用 Kerberos 身份验证的规则到一个密钥表文件 (在服务器中) :

```
# kadmin.local
# ktadd host/box2.mydomain.com
# ktadd nfs/box2.mydomain.com
# ktadd nfs/box1.mydomain.com
```

最后, 挂载共享目录并进行一个写测试 :

```
# mount -t nfs4 -o sec=krb5 box2:/nfs /mnt
# echo "Hello from Tecmint.com" > /mnt/greeting.txt
```



```
[root@box1 ~]# mount -t nfs4 -o sec=krb5 box2:/nfs /mnt
[root@box1 ~]# mount | grep krb5
box2:/nfs on /mnt type nfs4 (rw,relatime,vers=4.0,rsiz=131072,wsiz=131072,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=krb5,clientaddr=192.168.0.18,local_lock=none,addr=192.168.0.20)
[root@box1 ~]# echo "Hello from Tecmint.com" > /mnt/greeting.txt
[root@box1 ~]#
```

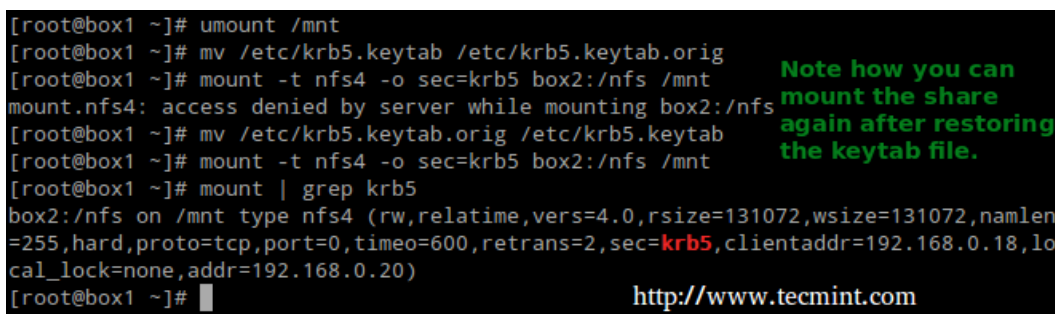
```
[root@box2 ~]# ls -l /nfs
total 4
-rw-r--r-- 1 nfsnobody nfs 23 Sep  5 21:18 greeting.txt
[root@box2 ~]#
```

http://www.tecmint.com

挂载 NFS 共享

现在让我们卸载共享，在客户端中重命名密钥表文件（模拟它不存在）然后试着再次挂载共享目录：

```
# umount /mnt
# mv /etc/krb5.keytab /etc/krb5.keytab.orig
```



```
[root@box1 ~]# umount /mnt
[root@box1 ~]# mv /etc/krb5.keytab /etc/krb5.keytab.orig
[root@box1 ~]# mount -t nfs4 -o sec=krb5 box2:/nfs /mnt
mount.nfs4: access denied by server while mounting box2:/nfs
[root@box1 ~]# mv /etc/krb5.keytab.orig /etc/krb5.keytab
[root@box1 ~]# mount -t nfs4 -o sec=krb5 box2:/nfs /mnt
[root@box1 ~]# mount | grep krb5
box2:/nfs on /mnt type nfs4 (rw,relatime,vers=4.0,rsiz=131072,wsiz=131072,namlen=255,hard,proto=tcp,port=0,timeo=600,retrans=2,sec=krb5,clientaddr=192.168.0.18,local_lock=none,addr=192.168.0.20)
[root@box1 ~]#
```

Note how you can mount the share again after restoring the keytab file.

http://www.tecmint.com

挂载/卸载 Kerberos NFS 共享

现在你可以使用基于 Kerberos 身份验证的 NFS 共享了。

总结

在这篇文章中我们介绍了如何设置带 Kerberos 身份验证的 NFS。和我們在这篇指南中介绍的相比，该主题还有很多相关内容，可以在 [Kerberos 手册](http://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/) <http://web.mit.edu/kerberos/krb5-1.12/doc/admin/admin_commands/> 查看，另外至少可以说 Kerberos 有一点棘手，如果你在测试或实现中遇到了任何问题或需要帮助，别犹豫在下面的评论框中告诉我们吧。

via: <http://www.tecmint.com/setting-up-nfs-server-with-kerberos-based-authentication/>
<<http://www.tecmint.com/setting-up-nfs-server-with-kerberos-based-authentication/>>

作者：Gabriel Cánepa <<http://www.tecmint.com/author/gacanepa/>> 译者：ictlyh
<<http://www.mutouxiaogui.cn/blog/>> 校对：wxy <<https://github.com/wxy>>

本文由 LCTT <<https://github.com/LCTT/TranslateProject>> 原创编译，Linux中国
<<https://linux.cn/>> 荣誉推出