**如何建立一个NFS挂载在Ubuntu 16.04**

**介绍**

NFS或网络文件系统是一种分布式文件系统协议，允许您在服务器上装载远程目录。 这允许您在不同位置管理存储空间，并从多个客户端写入该空间。 NFS提供了通过网络访问远程系统的相对快速和简单的方法，并且在将定期访问共享资源的情况下工作良好。

在本指南中，我们将介绍如何配置NFS安装。

**先决条件**

我们将在本教程中使用两个服务器：一个将与另一个共享其文件系统的一部分。   
要跟进，您将需要：

* **两个Ubuntu的16.04的服务器，每一个非root用户sudo特权**和专用网络，如果是提供给您。
  + 如需帮助建立这些权限的用户，按照我们[与Ubuntu 16.04的初始服务器安装](https://www.howtoing.com/initial-server-setup-with-ubuntu-16-04/)指南。
  + 如需帮助建立专用网络，请参阅[如何设置和使用DigitalOcean专用网络](https://www.howtoing.com/how-to-set-up-and-use-digitalocean-private-networking/) 。

在本教程中，我们指的是它的共享目录作为**主机**和挂载这些目录作为**客户端**的服务器的服务器。 为了保持正常，我们将使用以下IP地址作为主机和客户端值的替代：

* **主机** ：203.0.113.0
* **客户** ：203.0.113.256

您应该用您自己的主机和客户端IP地址替换这些值。

**第1步 – 下载和安装组件**

我们将首先在每个服务器上安装必要的组件。

**在主机上**

在主机服务器上，我们将安装nfs-kernel-server软件包，它将使我们能够分享我们的目录。 因为这是我们与进行第1操作apt在这个环节中，我们将刷新我们在安装之前本地包索引：

sudo apt-get update

sudo apt-get install nfs-kernel-server

安装这些软件包后，切换到客户端服务器。

**在客户端**

在客户端服务器，我们需要安装一个包叫做nfs-common ，它提供了NFS功能，而不包括不需要的服务器组件。 同样，我们将在安装之前刷新本地软件包索引，以确保我们有最新的信息：

sudo apt-get update

sudo apt-get install nfs-common

现在两个服务器都有必要的包，我们可以开始配置它们了。

**第2步 – 在主机上创建共享目录**

我们将共享两个单独的目录，使用不同的配置设置，以说明可以针对超级用户访问配置NFS安装的两个关键方法。

超级用户可以在他们的系统上的任何地方做任何事情。 但是，装载NFS的目录不是安装它们的系统的一部分，因此默认情况下，NFS服务器拒绝执行需要超级用户权限的操作。 此默认限制意味着客户端上的超级用户不能以root身份写入文件，重新分配所有权或在NFS安装上执行任何其他超级用户任务。

然而，有时候，客户端系统上有受信任的用户需要能够在已装载的文件系统上执行这些操作，但不需要在主机上进行超级用户访问。 NFS服务器可以被配置为允许这样做，虽然它引入风险因素，因为这样的用户*可以获得*对整个主机系统根访问。

**示例1：导出通用安装**

在第一个示例中，我们将创建一个通用的NFS安装，它使用默认的NFS行为，使客户机上具有root权限的用户很难与使用这些客户机超级用户权限的主机进行交互。 您可以使用类似的方式来存储使用内容管理系统上传的文件，或者为用户创建容易共享项目文件的空间。

首先，做一个共享目录名为nfs ：

sudo mkdir /var/nfs/general -p

因为我们通过sudo创造它，该目录由root拥有创建在这里的主机上。

ls -la /var/nfs/general

Output4 drwxr-xr-x 2 root root 4096 Jul 25 15:26 .

NFS将翻译任何root在客户机上操作的nobody:nogroup凭证作为一种安全措施。 因此，我们需要更改目录所有权以匹配这些凭据。

sudo chown nobody:nogroup /var/nfs/general

此目录现在可以导出。

**示例2：导出主目录**

在我们的第二个例子中，目标是使存储在主机上的用户主目录在客户机服务器上可用，同时允许这些客户机服务器的受信任管理员具有方便地管理用户所需的访问。

要做到这一点，我们将导出/home目录中。 由于它已经存在，我们不需要创建它。 我们也不会更改权限。 如果我们*这样做* ，它会引起各种问题与该主机上的主目录的任何人。

**第3步 – 在主机服务器上配置NFS导出**

接下来，我们将深入到NFS配置文件中来设置这些资源的共享。

打开/etc/exports在以root权限文本编辑器文件中：

sudo gedit /etc/exports

该文件具有显示每个配置行的一般结构的注释。 语法基本上是：

/ etc / exports

directory\_to\_share client(share\_option1,...,share\_optionN)

我们需要为我们计划共享的每个目录创建一行。 由于我们的例子中客户端的IP 203.0.113.256 ，我们的防线看起来像下面这样。 确保更改IP以匹配您的客户端：

/ etc / exports

/var/nfs/general 203.0.113.256(rw,sync,no\_subtree\_check)

/home 203.0.113.256(rw,sync,no\_root\_squash,no\_subtree\_check)

或

/export 145.144.164.0/24(rw,fsid=0,insecure,no\_subtree\_check,sync ,no\_root\_squash)

我们正在使用的除no\_root\_squash外两个目录相同的配置选项。 让我们来看看每个的意思。

* ro:只读访问。
* **RW：**此选项使客户端计算机的读写访问卷。
* **同步(sync)** ：同步写入资料到内存与硬盘中。 这导致更稳定和一致的环境，因为答复反映了远程卷的实际状态。 但是，它也降低了文件操作的速度。
* **Async NFS在写入数据前可以相应请求**
* **Secure:NFS通过1024以下的安全TCP/IP端口发送**
* **Insecure:NFS通过1024以上的端口发送**
* **Wdelay:如果多个用户要写入NFS目录，则归组写入（默认）**
* **No\_wdelay:如果多个用户要写入NFS目录，则立即写入，当使用async时，无需此设置。**
* **Hide:在NFS共享目录中不共享其子目录。**
* **No\_hide:共享NFS目录的子目录**
* **Subtree\_check:如果共享/usr/bin之类的子目录时，强制NFS检查父目录的权限（默认）**
* **no\_subtree\_check：即使输出目录是一个子目录，nfs服务器也不检查父目录的权限，这样可以提高效率。**
* **all\_squash:**共享文件的UID和GID映射匿名用户anonymous,适合公用目录。
* **no\_all\_squash:**保留共享文件的UID和GID（默认）
* **root\_squash:**root用户的所有请求映射成anonymous用户一样的权限（默认）
* **no\_root\_squash** ：root用户具有根目录的完全管理访问权限
* **anonuid=xxxx指定NFS服务器/etc/passwd文件中匿名用户的UID**
* **anongid=xxxx指定NFS服务器/etc/passwd文件中匿名用户的GID**
* 完成更改后，保存并关闭文件。 然后，要使共享可用于您配置的客户端，请使用以下命令重新启动NFS服务器：

sudo systemctl restart nfs-kernel-server

但是，在实际使用新共享之前，您需要确保防火墙规则允许共享的流量

**第4步 – 调整主机上的防火墙 （备选项）**

首先，让我们检查防火墙状态，看看是否已启用，如果是，请查看目前允许的内容：

sudo ufw status

OutputStatus: active

To Action From

-- ------ ----

OpenSSH ALLOW Anywhere

OpenSSH (v6) ALLOW Anywhere (v6)

在我们的系统上，只允许SSH流量，因此我们需要为NFS流量添加规则。

由于许多应用程序，您可以使用sudo ufw app list并通过名称启用它们，但nfs是不是其中之一。 由于ufw也检查/etc/services的服务的端口和协议，我们仍然可以按名称添加NFS。 最佳做法建议您启用仍然允许要允许的流量的限制性最强的规则，因此，与其启用来自任何地方的流量，我们将具体。

使用以下命令打开主机上的端口2049，确保替换客户端的IP地址：

sudo ufw allow from 203.0.113.0 to any port nfs

您可以通过键入以下内容来验证更改：

sudo ufw status

您应该在输出中看到从端口2049允许的流量：

OutputStatus: active

To Action From

-- ------ ----

OpenSSH ALLOW Anywhere

2049 ALLOW 203.0.113.256

OpenSSH (v6) ALLOW Anywhere (v6)

这确认UFW将仅允许来自客户端计算机的端口2049上的NFS通信。

**第5步 – 在客户端上创建安装点**

现在主机服务器已配置并提供其共享，我们将准备我们的客户端。

为了使远程共享在客户端上可用，我们需要在空客户端目录上安装主机目录。

**注意：**如果有文件和目录的挂载点，只要你挂载NFS共享，他们会被隐藏。 请确保您在已存在的目录中装载该目录为空。

我们将为我们的挂载创建两个目录：

sudo mkdir -p /nfs/general

sudo mkdir -p /nfs/home

**第6步 – 在客户端上安装目录**

现在，我们有一些地方把远程共享，我们已经打开了防火墙，我们可以解决我们的主机服务器，这本指南是安装股203.0.113.0 ，就像这样：

sudo mount 203.0.113.0:/var/nfs/general /nfs/general

sudo mount 203.0.113.0:/home /nfs/home

这些命令应将共享从主机计算机挂载到客户端计算机上。 您可以通过多种方式仔细检查它们是否成功安装。 你可以用一个简单的检查此mount或findmnt命令，但df -h会给你更多的人类可读的输出演示了如何磁盘的使用情况显示不同的NFS共享：

df -h

OutputFilesystem Size Used Avail Use% Mounted on

udev 238M 0 238M 0% /dev

tmpfs 49M 628K 49M 2% /run

/dev/vda1 20G 1.2G 18G 7% /

tmpfs 245M 0 245M 0% /dev/shm

tmpfs 5.0M 0 5.0M 0% /run/lock

tmpfs 245M 0 245M 0% /sys/fs/cgroup

tmpfs 49M 0 49M 0% /run/user/0

203.0.113.0:/home 20G 1.2G 18G 7% /nfs/home

203.0.113.0:/var/nfs/general 20G 1.2G 18G 7% /nfs/general

我们安装的两个股票都出现在底部。 因为它们是从同一个文件系统装入的，所以它们显示相同的磁盘使用情况。 看到多少空间实际上是被每个下使用挂载点，可使用磁盘使用情况命令du和安装的路径。 该-s标志将提供使用情况的总结，而不是显示每个文件的使用。 该-h将打印人类可读的输出。

例如：

du -sh /nfs/home

Output36K /nfs/home

这告诉我们整个主目录的内容只使用20K的可用空间。

**第7步 – 测试NFS访问**

接下来，让我们对每个人写一些内容来测试对共享的访问。

**示例1：通用共享**

首先，写一个测试文件到/var/nfs/general股。

sudo touch /nfs/general/general.test

然后，检查其所有权：

ls -l /nfs/general/general.test

Output-rw-r--r-- 1 nobody nogroup 0 Aug 1 13:31 /nfs/general/general.test

因为我们装这个量不改变NFS的默认行为，并通过创建的文件作为客户机的root用户sudo命令，该文件默认为没有人的所有权：nogroup。 客户端超级用户将无法在此NFS安装的共享上执行典型的管理操作，例如更改文件所有者或为一组用户创建新目录。

**示例2：主目录共享**

要比较通用分享与主目录共享的权限，请以相同的方式创建文件主目录：

sudo touch /nfs/home/home.test

然后查看文件的所有权：

ls -l /nfs/home/home.test

Output-rw-r--r-- 1 root root 0 Aug 1 13:32 /nfs/home/home.test

我们创建home.test通过以root sudo命令，正是我们创造了以同样的方式general.test文件。 然而，在这种情况下，它是由根，因为我们在我们指定的覆盖了默认行为资no\_root\_squash在此安装选项。 这允许我们在客户端计算机上的root用户充当root，并使用户帐户的管理更加方便。 同时，这意味着我们不必给这些用户在主机上的根访问权限。

**第8步 – 在引导时安装远程NFS目录**

我们可以将它们添加到在开机时自动挂载远程NFS共享/etc/fstab在客户端上的文件。

在文本编辑器中以root权限打开此文件：

sudo gedit /etc/fstab

在文件的底部，我们将为每个共享添加一行。 它们将如下所示：

/ etc / fstab

. . .

203.0.113.0:/var/nfs/general /nfs/general nfs auto,nofail,noatime,nolock,intr,tcp,actimeo=1800 0 0

203.0.113.0:/home /nfs/home nfs auto,nofail,noatime,nolock,intr,tcp,actimeo=1800 0 0

**注：**有关我们在这里指定的选项的详细信息可以在描述NFS安装在该手册页中找到fstab与man nfs命令。

客户端服务器将在引导时自动挂载远程分区，尽管可能需要一段时间才能建立连接并且共享可用。

**第9步 – 卸载NFS远程共享**

如果您不再希望将远程目录装载到系统上，您可以通过移出共享的目录结构并卸载来卸载它，如下所示：

cd ~

sudo umount /nfs/home

sudo umount /nfs/general

这将删除远程共享，只保留您的本地存储：

df -h

Output

Filesystem Size Used Avail Use% Mounted on

/dev/vda 59G 1.3G 55G 3% /

none 4.0K 0 4.0K 0% /sys/fs/cgroup

udev 2.0G 12K 2.0G 1% /dev

tmpfs 396M 320K 396M 1% /run

none 5.0M 0 5.0M 0% /run/lock

none 2.0G 0 2.0G 0% /run/shm

none 100M 0 100M 0% /run/user

如果你也想，以防止他们在下次启动时，编辑被重新装入/etc/fstab并删除该行或在该行的首加＃号注释掉。 您也可以通过删除防止自动安装auto选项，这将允许你手动安装它。

**结论**

在本教程中，我们创建了一个NFS主机，并通过创建两个不同的NFS安装来说明一些关键的NFS行为，我们与NFS客户端共享。 如果你正在生产中实现NFS，重要的是要注意协议本身不加密。 如果您要共享旨在公开访问的文件，则不会导致任何严重问题。

但是，如果您使用NFS作为私有数据，则需要决定如何保护该数据。 您可能能够通过SSH或VPN连接路由NFS以创建更安全的体验，但这通常会带来严重的性能损失。 如果性能是一个问题，考虑[SSHFS](https://www.howtoing.com/how-to-use-sshfs-to-mount-remote-file-systems-over-ssh/) 。 它比未加密的NFS流量稍慢，但通常比隧道NFS快得多。 Kerberos认证的NFS加密是另一个选择。