TECHNICAL NOTE

USING NFS FOR STRM BACKUPS

MARCH 2009

This technical note provides guidelines and procedures for using a Network File System (NFS) storage solution in your STRM deployment.

This document includes:

NFS Considerations

While STRM supports NFS for external storage, we recommend that you do not use NFS for storing active data including:

- **Postgres Database** - The Postgres database is stored in the /store/postgres/ directory. When using NFS for the /store/ directory, database corruption can occur when writing Postgres data to the NFS. We recommend that you mount the /store/postgres partition on a local disk, not on NFS.
- **Ariel Database** - The Ariel database is stored on the /store/ariel/ directory. Performance issues can occur if the Ariel data is stored on NFS. A series of distinct files are created by STRM for each minute, which compromises STRM performance. For example, a locally mounted storage can perform up to five times faster than NFS mounted storage.

For these reasons, we recommend that you only use NFS for STRM backups, which are stored in the /store/backup/ directory. To do this, mount your NFS storage as the /store/backup/ partition. For more information about backing up your information, see the *STRM Administration Guide*.

Implementing NFS for Backups

To implement NFS for backups:

Step 1 Log in to STRM as root.

Step 2 Add your NFS server to the /etc/hosts file:

a Edit the following file:

`/etc/hosts`

b Add your NFS server to the /etc/hosts file.

<IP address> nfsserver

Where:

<IP address> is the IP address of your NFS server.

c Save and close the file

Step 3 Edit the iptables firewall to allow the connection to your NFS server.

a Open the following file:

/opt/qradar/conf/iptables.pre

b Add the following line:

-A INPUT -i <interface> -s <IP address> -j ACCEPT

Where:

<IP address> is the IP address of your NFS server.

<interface> is the STRM interface on your NFS network. This is typically ETH0, unless you have a dedicated NFS network and connected ETH1 to that network instead of ETH0.

Step 4 Restart iptables:

/opt/qradar/bin/iptables_update.pl

The NFS services are disabled by default.

Step 5 Add the NFS to be part of the startup:

```
cd /etc/rc3.d/
chkconfig --level 3 portmap on
chkconfig --level 3 nfs on
chkconfig --level 3 nfslock on
```

Step 6 Manually start NFS services:

```
service portmap start
service nfslock start
service nfs start
```

Step 7 Configure the /store/backup directory:

a Edit the following file:

/etc/fstab

b Add the following line:

nfsserver:<shared_directory> /store/backup nfs soft,intr,rw 0 0

Where:

<shared_directory> is the path to your shared directory on the NFS server.

Note: *You may need to adjust the settings on the NFS mount point to accommodate your configuration. For example:* **/nfsshare/qradar/backup /store/backup nfs soft,intr,rw,noac 0 0.** *For more information about common NFS mount options, enter* **man nfs** *to view the Unix man page for NFS.*

Step 8 Migrate existing backup files to the NFS volume:

a Move your backup files from the existing /store/backup directory to a temporary location:

```
cd /store/
mv backup backup.local
```

b Create a new backup directory:

```
mkdir /store/backup
```

c Mount the NFS volume:

```
mount /store/backup
```

d Set the permissions for the NFS volume:

```
chown nobody:nobody /store/backup
```

e Move the backup files from the temporary location into the NFS volume:

```
mv /store/backup.local/* /store/backup
```

Your NFS backup is now mounted and operational. We recommend that you verify that the backup files are in the shared directory from the NFS server.

Part Number 530-030121-01