Monitoring Network Appliance Filers With Nagios
Mike Solinap, Sr. Systems Integrator, SPK and Associates

This document will guide you through the process of setting up Nagios in order to monitor Network Appliance filers.
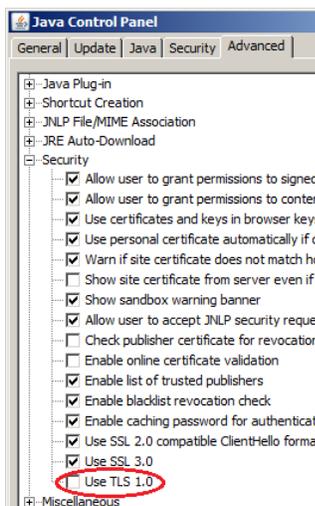
Pre-Requisites:

- Nagios 2.0 or greater
- Network Appliance OnTap 7.0 or greater
- SNMP utilities
  - Redhat Enterprise: `yum install net-snmp-utils`
  - Debian/Ubuntu: `apt-get install snmp`

Enable SNMP in FilerView

Drill down to SNMP -> Configure

* Note: If you're having trouble launching the Java applet, ensure that TLS 1.0 is disabled in the Java Control Panel

Monitoring Network Appliance Filers With Nagios
Mike Solinap, Sr. Systems Integrator, SPK and Associates

Enable SNMP and define a READ-ONLY community ("7a3jhzz" for example).

Verify that SNMP is functioning correctly by walking the tree:

```
[root@spkrh2 bin]# snmpwalk -v1 -c 7a3jhzz filerhost
```

You may also need to set the snmp access to include the Nagios server IP address via the OnTap CLI:

```
filerhost> options snmp.access host=10.2.2.2
```

Install the Network Appliance SNMP MIBS

The SNMP MIBS from Netapp define the different types of objects that we can obtain information about. The MIBS will also let us query for information in a more human readable format.

You can download the MIBS specific to your filer from Netapp's NOW site:

http://now.netapp.com

Unarchive the MIBS to the following path so that the SNMP utilities can pick them up:

```
/usr/share/snmp/mibs/
```

Now query the filer again:

```
[root@spkrh2 bin]# snmpwalk -v1 -c 7a3jhzz \
-m NETWORK-APPLIANCE-MIB filerhost filesys
```

This time, you should see more descriptive results, such as "aggrState.1 = Online".

Monitoring Network Appliance Filers With Nagios
Mike Solinap, Sr. Systems Integrator, SPK and Associates

The Network Appliance MIB has several top level categories. Depending on what item we'd like to monitor, we'll need to know what category it falls in. For instance, disk usage stats are under the top level named "filesys". If we want to determine if any power supplies have failed, we would look under "enclosure". For CPU statistics, we would look under "sysStat". Refer to the NETWORK-APPLIANCE.txt MIB file for a complete listing of objects.

Define a Nagios check

If not already defined, create a "check_snmp" command in your nagios configuration files:

```
# 'check_snmp' command definition
define command{
        command_name     check_snmp
        command_line     $USER1$/check_snmp -H $HOSTADDRESS$ -o $ARG1$ -C $ARG2$ -w
$ARG3$ -c $ARG4$
        }
```

Now we can define checks for any object that the Netapp MIB supports.

For example, to monitor the percent free on a filer's vol0 volume, first determine the appropriate OID:

```
[root@spkrh2 bin]# snmpwalk -v1 -c 7a3jhzz -m NETWORK-APPLIANCE-MIB filerhost filesys
| grep dfFileSys
NETWORK-APPLIANCE-MIB::dfFileSys.1 = STRING: "aggr0"
NETWORK-APPLIANCE-MIB::dfFileSys.2 = STRING: "aggr0/.snapshot"
NETWORK-APPLIANCE-MIB::dfFileSys.3 = STRING: "/vol/vol0/"
NETWORK-APPLIANCE-MIB::dfFileSys.4 = STRING: "/vol/vol0/.snapshot"
```

Here we see that vol0 has the identifier NETWORK-APPLIANCE-MIB::dfFileSys.3. To make the configuration more portable, its best to convert this identifier to its numeric counterpart:

```
[root@spkrh2 bin]# snmpget -v1 -On -c 7a3jhzz filerhost NETWORK-APPLIANCE-
MIB::dfFileSys.3
.1.3.6.1.4.1.789.1.5.4.1.2.3 = STRING: "/vol/vol0/"
```

Now we can take this numeric OID and use it for our service check:

```
# Service definition
define service{
        use                          generic-service
        host_name                    filerhost
        service_description          Vol Percent Used - /vol/vol0
        is_volatile                  0
        check_period                 24x7
        max_check_attempts           3
```

```
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  spk_group
        notification_interval           60
        notification_period             24x7
        notification_options            w,u,c,r
        check_command                   check_snmp!.1.3.6.1.4.1.789.1.5.4.1.6.3!
7a3jhzz!90!95
        }
```