Red Hat Reference Architecture Series

# Monitoring Red Hat Gluster Storage Using Nagios

**Zoltan Porkolab, Infrastructure Consultant**
**RHCE, RHCVA**

**Version 1.0**
**May 2015**

redhat.

1801 Varsity Drive™
Raleigh NC 27606-2072 USA
Phone: +1 919 754 3700
Phone: 888 733 4281
Fax: +1 919 754 3701
PO Box 13588
Research Triangle Park NC 27709 USA



The GPG fingerprint of the security@redhat.com key is:
CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

## Comments and Feedback

In the spirit of open source, we invite anyone to provide feedback and comments on any reference architectures. Although we review our papers internally, sometimes issues or typographical errors are encountered. Feedback allows us to not only improve the quality of the papers we produce, but allows the reader to provide their thoughts on potential improvements and topic expansion to the papers.

Feedback on the papers can be provided by emailing refarch-feedback@redhat.com. Please refer to the title within the email.

## Staying In Touch

Join us on some of the popular social media sites where we keep our audience informed on new reference architectures as well as offer related information on things we find interesting.

**Like us on Facebook:**

https://www.facebook.com/rhrefarch

**Follow us on Twitter:**

https://twitter.com/RedHatRefArch

**Plus us on Google+:**

https://plus.google.com/u/0/b/114152126783830728030/

# Table of Contents

# 1 Executive Summary

Choosing the right solution to provide a reliable, flexible, and high availability storage for file shares is a base requirement for enterprise architectures. Most solutions in the market need expensive hardware or is very costly to purchase and implement. For maintaining good value, the Red Hat Gluster Storage technology is the most appropriate solution to provide a software only, scale-out, massively scalable, and highly available NAS environment.

The new release of Red Hat Storage provides new opportunities to increase performance, manage volume snapshots, and supports Hadoop technologies. This release introduces a sophisticated monitoring using Nagios - an open IT infrastructure monitoring framework.

This reference architecture demonstrates a perfect solution how-to managing Red Hat Gluster Storage Clusters using a centralized management server with Red Hat Storage Console and Nagios Server. Also describes step-by-step implementation and configuration steps as well as best-practices that can help a business achieve high availability.

There is another purpose of this reference architecture to presenting how Storage Console server supports a wide range of storage cluster monitoring capabilities including monitoring of virtual and physical resources, failure alerts, and advanced reporting features. The Monitoring functionality based on Nagios is packaged to work in conjunction with Red Hat Storage Management Console.

# 2 Introduction

## 2.1 Audience

The audience for this document should have a working knowledge of Red Hat Enterprise Linux and understand the concepts of clusters, storage, and server computing. This document applies to Red Hat Consultants, Architects, System Builders, Administrators, and Linux Systems Engineers.

## 2.2 Acronyms

Common acronyms referenced within this document are listed below.

| | |
|---|---|
| **CIFS** | Common Internet File System |
| **EUS** | Extended Update Support |
| **HA** | High Availability |
| **ISCSI** | Internet Small Computer System Interface |
| **NFS** | Network File System |
| **NIC** | Network Interface Controller |
| **NTP** | Network Time Protocol |
| **NRPE** | Nagios Remote Plugin Executor |
| **RHEL** | Red Hat Enterprise Linux |
| **RHN** | Red Hat Network |
| **RHEV** | Red Hat Enterprise Virtualization |
| **RHS** | Red Hat Storage |
| **RHSC** | Red Hat Storage Console |
| **RHSM** | Red Hat Subscription Management |
| **RPM** | Red Hat Package Manager |
| **RPM** | Revolutions per Minute |
| **SM** | Subscription Management |
| **VG** | Logical Volume Group |
| **VIP** | Virtual IP Address |

# 3 Reference Architecture Environment

This reference architecture is made based on a nine nodes RHS production system running at Bristol NHS University Hospitals. IT department uses Red Hat Storage Clusters to provide a high availability file storage solution for customer's data files. The system contains several distributed-replicated Volumes specialized for managing small files. The application servers are connected to the Glusterfs Volumes via CIFS furthermore the infrastructure team is using Red Hat Storage Management Console and Nagios to manage and monitoring the whole environment.

The following architecture diagram shows all the components together.

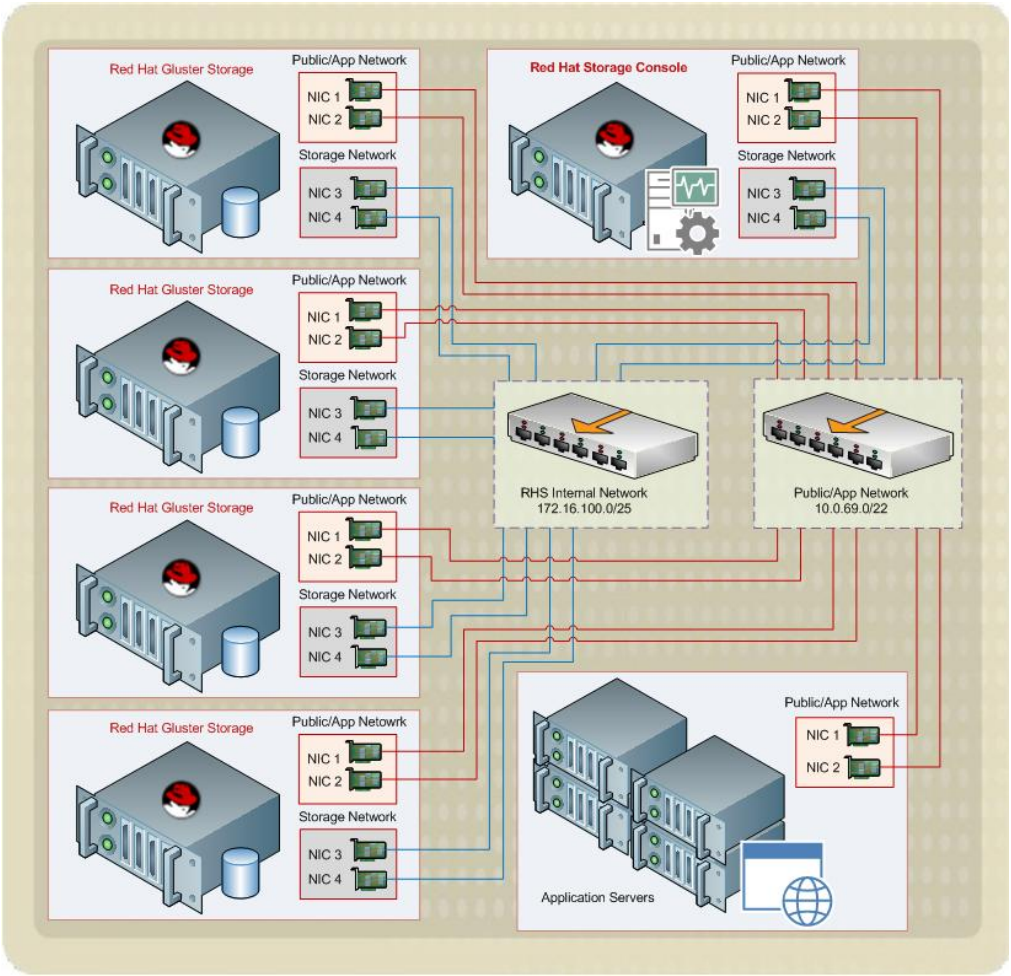


**Figure 3.1: Reference Architecture Overview**

The reference architecture consists of Dell PE servers. Each server has 25TB SSD drives as well as four 1GbE NIC's. The first two network cards are bonded for Public/App networks, the other two NIC's are bonded for the Internal Storage Network. Redundant switches operates to improve high availability on Storage and Public Networks. The architecture is separated in two parts, both parts have four RHS nodes which meets the business expectations. The RHS Console server is running on a standalone virtual server and it is connected to both networks.

Nagios monitoring operates on all system components including switches and routers.

**NOTE:** Using bare metal servers is highly recommended but the Red Hat Gluster Storage architecture can be constructed on virtual environments as well. More details are available in the Supported Virtual Platforms section.

The following table summarizes the main components of the Reference Architecture.

| | | |
|---|---|---|
| **Red Hat Gluster Storage Servers** | Operating System | Red Hat Storage Server 3.0 Update 3 |
| | Host Names | brsrhs0[X].nhs.local |
| | Cluster Host Names | rhs0[X].storage.internal |
| **Red Hat Storage Console Server** | Operating System | Red Hat Enterprise Linux Server release 6.6 |
| | Host Name | brsrhmanager.nhs.local |
| | Cluster Host Name | rhsmanager.storage.internal |

***Table 3.1: Architecture Components***

NOTE: [X] refers to the node number, for example 1, 2, etc.

This table shows the network settings.

| Server | Network | IP/Netmask | Adapters |
|---|---|---|---|
| brsrhmanager.nhs.local | Public Network | 10.0.69.20 / 22 | bond0 (eth0, eth1) |
| | RHS Internal Network | 172.16.100.20 / 24 | bond1 (eth2, eth3) |
| brsrhs01.nhs.local | Public Network | 10.0.69.25 / 22 | bond0 (eth0, eth1) |
| | RHS Internal Network | 172.16.100.11 / 24 | bond1 (eth2, eth3) |
| brsrhs02.nhs.local | Public Network | 10.0.69.26 / 22 | bond0 (eth0, eth1) |
| | RHS Internal Network | 172.16.100.12 / 24 | bond1 (eth2, eth3) |
| brsrhs03.nhs.local | Public Network | 10.0.69.27 / 22 | bond0 (eth0, eth1) |
| | RHS Internal Network | 172.16.100.13 / 24 | bond1 (eth2, eth3) |
| brsrhs04.nhs.local | Public Network | 10.0.69.28 / 22 | bond0 (eth0, eth1) |
| | RHS Internal Network | 172.16.100.14 / 24 | bond1 (eth2, eth3) |

***Table 3.2: Network settings***

All servers are synchronizing their clocks with a dedicated time server through NTP services.

# 4 System Requirements

Red Hat strongly recommends that all customers source their hardware platforms for running Red Hat Storage Server for On-premise based on the criteria specified below to ensure support-ability of production deployments. The Red Hat Storage Management Console must run on separated server. Installing Red Hat Storage Console 3.0 on Red Hat Storage server is not supported. At least two machines are required to support replicated RHS volumes.

## *4.1 Hardware Requirements*

The hardware must be in Red Hat Hardware Compatibility List for Storage Server to ensure it is running on tested, verified, and supported hardware. The Red Hat Hardware Catalog has moved to https://access.redhat.com/certifications

Generic requirements for RHS Server:

- 2-socket (with 4-core, 6-core, or 8-core) servers are recommended.
- Minimum RAM requirements are use case specific. See below.
- Reliable RAID controller shipped by server vendors or from OEM manufacturers.
- RAID 6 and RAID 1+0 Support in hardware RAID controller.
- RAID controller card must be flash-backed or battery-backed.
- 1 x 50 GB SAS disk for RHSS installation.
- 1 x 200 GB disk for /var partition.
- 1 x 10Gig Ethernet NIC for data traffic is recommended. 1Gig NIC may also be used.
- Redundant power supply

Out of band management card is also recommended to manage and monitor RHS nodes even when the server is down.

Optimal recommendations for multiple use cases:

| | | | |
|---|---|---|---|
| **High Performance Computing use-case** | 2u/24 CPU | 15000 RPM 900GB drives (2.5" inch SAS) OR Solid state disks | Minimum RAM 48GB |
| **General Purpose File Serving use-case** | 2u/12 CPU | 7200 or 10000 RPM, up to 6 TB drives (3.5" SAS or SATA) | Minimum RAM 32GB |
| **Archival use-case** | 4u/60 CPU | 7200 or 10000 RPM, up to 6 TB drives (3.5" SAS or SATA) | Minimum RAM 16GB |

***Table 4.1.1: RHS use-ceases***

Separated networks recommended for data and management. Also advisable to use NIC

bonding with 2x 10GigE for increasing throughput and resiliency.

Generic requirements for RHS Management Console Server:

- A quad core CPU or multiple dual core CPU's.
- 16 GB of available system RAM that is not being consumed by existing processes.

## *4.2* Supported Virtual Platforms

| Virtual Platforms | Red Hat Storage supported releases |
|---|---|
| Red Hat Enterprise Virtualization 3.4 | RHS 3, 2.1/U1/U2 (Compatibility Mode) |
| Red Hat Enterprise Virtualization 3.3 | RHS 2.1/U1/U2 (Compatibility Mode) |
| Red Hat Enterprise Virtualization 3.2 | RHS 2.1 /U1 |
| VMware vSphere 5.x | RHS 3, 2x |
| VMWare ESXi 5.x | RHS 3, 2x |
| Red Hat OpenStack Platform 4 | RHS 3, 2.1 |
| Red Hat OpenStack Platform 5 | RHS 3, 2.1 |
| **Virtual Storage** | **Red Hat Storage supported releases** |
| Red Hat Enterprise Linux 6.4+ Hypervisor | RHS 3, 2.1 |

**Table 4.2.1: Supported Virtual Platforms**

More information can be found on the Red Hat Gluster Storage Life Cycle reference page.

## *4.3 Software Components*

### 4.3.1 Gluster File System

GlusterFS is a powerful network/cluster file system written in user space which uses FUSE to hook itself with VFS layer. GlusterFS is a File System but, it uses disk file systems to store data. In Red Hat Gluster Storage environment, XFS is the only supported disk file system for glusterFS bricks/partitions. GlusterFS can scale up to petabytes of storage which is available under a single mount point. A GlusterFS Volume uses separated disk partitions called bricks to add/remove storage capacity as required.

### 4.3.2 Nagios Monitoring

Nagios is an open source network monitoring, computer system monitoring and infrastructure monitoring software application. It provides multiple plugins for advanced monitoring tasks, and offers monitoring and alerting services for servers, switches, applications, services, and databases. The Nagios notification plugin alerts the users when a service status has been changed to wrong or when the problem has been resolved.

# 5 Red Hat Storage Management Console

Red Hat Storage Console application provides a centralized management system to view and manage Red Hat Storage Servers as well as Gluster Volumes. Basically the Console is a graphical user interface to administer Red Hat Storage architectures including physical and logical resources, user sessions, provisioning, and clustering. Furthermore the management server is extended with Nagios Server which is a sophisticated and reliable monitoring solution used by numerous of IT architectures worldwide.

This section provides details on how-to prepare, install and customise a Red Hat Storage Management Server including RHS Console and Nagios Server.

Either Red Hat Enterprise Linux 6.5 or Red Hat Enterprise Linux 6.6 are suitable to run RHS Console. The operating system has to be registered and updated with the latest packages.

## *5.1 Registering RHSC using Subscription Manager*

This section shows a command line registration example but the Red Hat Customer Portal provides a graphical interface for administrators to manage the registered and subscribed RHEL systems.

Red Hat Storage Console Server installation requires the following channels/subscriptions:

- Red Hat JBoss EAP (v 6) for 6Server x86_64
- Red Hat Storage Console 3 (x86_64)
- Red Hat Storage 3 Nagios Server (RHEL 6 for x86_64)

These channels are available via both Subscription Management and RHN Classic. It is recommended to use Subscription Manager to register Red Hat Enterprise Linux systems.

With Red Hat Subscription Manager, the registration and utilization of a subscription is a two-parts process. First register a system, then apply a subscription.

```
# subscription-manager register
Username: rhn_username
Password:
The system has been registered with ID: f7d65862-58c0-4aba.. output omitted
```

Once the system has registered attach the specific Red Hat Gluster Storage subscription using its POOL_ID. Find the suitable ID using the following command.

```
# subscription-manager list --available | grep -A7 -B7  "Red Hat Storage"

Subscription Name: Red Hat Gluster Storage (4 Nodes)
Provides:          Red Hat Beta
                   Red Hat Enterprise Linux Scalable File System (for RHEL
Server)
                   Oracle Java (for RHEL Server) - Extended Update Support
                   JBoss Enterprise Application Platform
                   Oracle Java (for RHEL Server)
                   Red Hat Enterprise Linux Server
```

```
                  Red Hat Storage Nagios Server
                  Red Hat Storage Server for On-premise
                  Red Hat Storage Management Console (for RHEL Server)
SKU:              RS0109273
Contract:         10633819
Pool ID:          8a85f9814b6f0b13014b6f14668d4e1b
Available:        6
Suggested:        1
… output omitted …
```

Add the channel using the specific Pool ID and enable the necessary repositories.

```
# subscription-manager attach --pool=8a85f9814b6f0b13014b6f14668d4e1b
Successfully attached a subscription for: Red Hat Gluster Storage (4 Nodes)
```

```
# subscription-manager repos --enable=rhel-6-server-rpms --enable=jb-eap-6-
for-rhel-6-server-rpms --enable=rhsc-3-for-rhel-6-server-rpms --enable=rhs-
nagios-3-for-rhel-6-server-rpms
Repo 'rhel-6-server-rpms' is enabled for this system.
Repo 'rhs-nagios-3-for-rhel-6-server-rpms' is enabled for this system.
Repo 'rhsc-3-for-rhel-6-server-rpms' is enabled for this system.
Repo 'jb-eap-6-for-rhel-6-server-rpms' is enabled for this system.
```

Verify the enabled repositories.

```
# yum repolist all | grep enabled
```

Systems can also be registered with Customer Portal Subscription Management. Details on how the Red Hat Subscription works are available in the Red Hat Subscription Management document in Appendix C: References.

Another way to system registration is using RHN Classic via Red Hat Customer Portal or RHN Satellite 5 Server. In this case the *rhn_register* command is used to register the system to Red Hat Network (RHN).

```
# rhn_register
# rhn-channel --add --channel rhel-x86_64-server-6-rhs-rhsc-3 --channel
jbappplatform-6-x86_64-server-6-rpm --channel rhel-x86_64-server-6-rhs-
nagios-3
```

Using either RHSM or RHN the Red Hat Network user credentials (username and password) will be necessary for systems registration. Once a node is registered and all specific channels are available update the system with the latest packages. System reboot is recommended if the kernel package has been updated.

## 5.2 Installing Management Console with Nagios Server

This chapter describes the procedure for deploying Nagios and Storage Console together on the same node. Deploying Nagios Server is supported on Red Hat Storage node as well as on Red Hat Enterprise Linux node. For information on deploying Nagios on Red Hat Storage node and Red Hat Enterprise Linux node, see Red Hat Storage 3 Administration Guide.

Console installation requires the rhsc package and its dependencies. The Nagios packages

are part of these dependencies. The installer runs in interactive mode, all settings need to be confirmed or customized during the installation process. Time server services (ntpd) must run and DNS name resolution is required. Set SELinux to permissive for Nagios Server.

The setup process is described below.

```
# yum install rhsc -y
# rhsc-setup
… output omitted …
Host fully qualified DNS name of this server [brsrhmanager.nhs.local]:
brsrhmanager.nhs.local
Do you want Setup to configure the firewall? (Yes, No) [Yes]: Yes
Where is the Engine database located? (Local, Remote) [Local]: Local
Would you like Setup to automatically configure postgresql and create Engine
database, or prefer to perform that manually? (Automatic, Manual)
[Automatic]: Automatic
Engine admin password: Mystr@ngPassword01
Confirm engine admin password: Mystr@ngPassword01
Organization name for certificate [nhs.local]: nhs.local
Do you wish Setup to configure that, or prefer to perform that manually?
(Automatic, Manual) [Automatic]: Automatic
Do you wish to set the application as the default page of the web server?
(Yes, No) [Yes]: Yes
Would you like transactions from the Red Hat Access Plugin sent from the
RHSC to be brokered through a proxy server? (Yes, No) [No]: No
Would you like external monitoring to be enabled? (Yes, No) [Yes]: Yes

          --== CONFIGURATION PREVIEW ==--

          Engine database name                    : engine
          Engine database secured connection      : False
          Engine database host                    : localhost
          Engine database user name               : engine
          Engine database host name validation    : False
          Engine database port                    : 5432
          PKI organization                        : nhs.local
          Application mode                        : gluster
          Firewall manager                        : iptables
          Update Firewall                         : True
          Configure WebSocket Proxy               : False
          Host FQDN                               : brsrhmanager.nhs.local
          Configure local Engine database         : True
          Set application as default page         : True
          Configure Apache SSL                    : True
          Nagios monitoring enabled for gluster hosts: True

          Please confirm installation settings (OK, Cancel) [OK]: OK
… output omitted …
[ INFO  ] Execution of setup completed successfully
```

The installer generates an answer file to */var/lib/ovirt-engine/setup/answers/* folder and the log located at */var/log/ovirt-engine/setup/* directory. If the installer can manage the firewall then the following ports are open: TCP 5432 (postgres), TCP 80 (http), TCP 443 (https), TCP 5667 (Nagios). The RHSC installer supports the Engine database setup on a separated Postgres

database server. Configuration details are available in Red Hat Storage 3 Installation Guide.

Once the installation is completed the Red Hat Storage Administration Portal is accessible at ***https://<server-name>/ovirt-engine***. Click on *Administration Portal* to get Login screen.

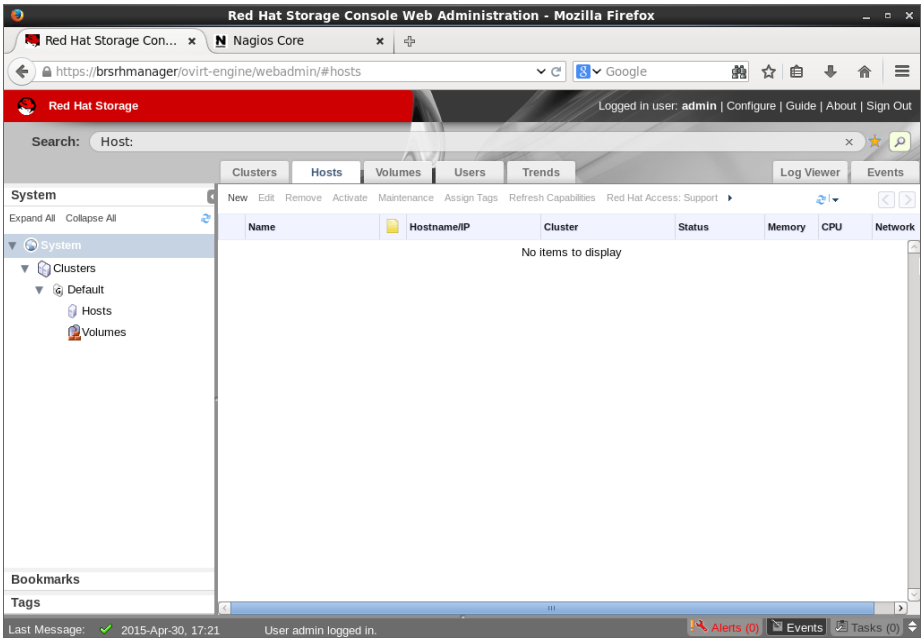


**Figure 5.2.1: Red Hat Storage Console**

The Nagios Dashboard URL is ***https://<server-name>/nagios***. The default admin username and password for Nagios is *nagiosadmin/nagiosadmin*. The password changing process is explained in the Managing Users and Passwords section.

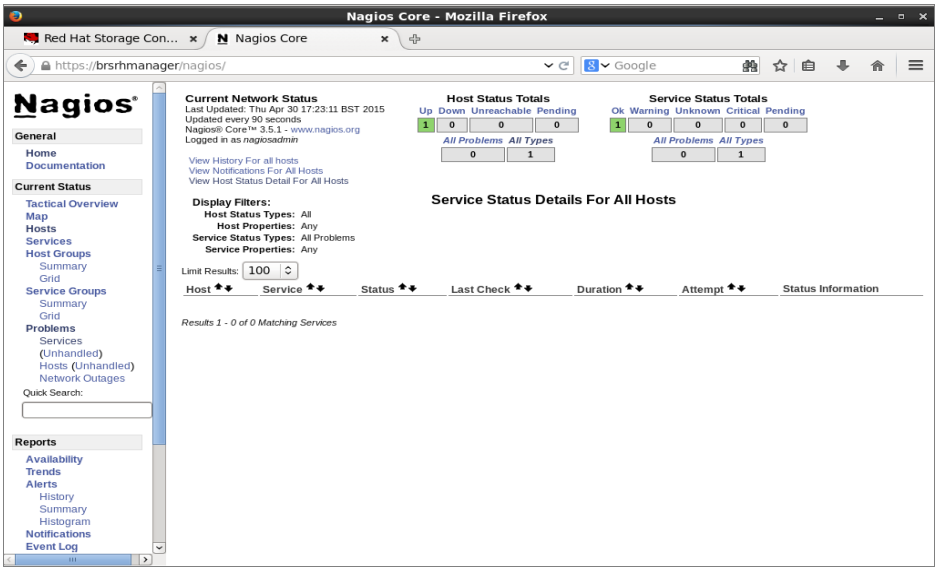


**Figure 5.2.2: Nagios Dashboard**

The installation of Red Hat Storage Management Server is completed. The next section describes how-to configure monitoring for Red Hat Storage nodes.

# 6 Customizing Nagios for Monitoring Red Hat Storage Environments

This section describes how to setup Nagios services for Red Hat Storage Clusters using the Gluster Auto Discover Tool (auto-discovery). To configure Nagios monitoring on Red Hat Storage nodes, the managed nodes have to use Red Hat Storage version 3.0 or above.

Configuration steps:

- Create a Storage Cluster based on the RHS node's version
- Manage Red Hat Storage hosts using Red Hat Storage Console
- Configure NRPE (Nagios Remote Plugin Executor) on RHS Nodes
- Run auto-discovery to setup monitoring for all Red Hat Storage services, nodes and clusters

Before any further steps, set the SELinux mode to Permissive in the */etc/sysconfig/selinux*.

```
SELINUX=permissive
```

Also set the SELinux mode to Permissive on the live system without reboot.

```
# setenforce 0
# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /selinux
Current mode:                   permissive
Mode from config file:          permissive
Policy version:                 24
Policy from config file:        targeted
```

## *6.1 Managing Storage Components Using Console*

There is a prerequisites to setup Nagios monitoring that all Storage Nodes are have to be part of a Cluster managed by the Red Hat Storage Console. Because of this, the first step is add all RHS Hosts to the Console. Once the Hosts are registered, the Console can manage all components including Volumes, Trusted Pools (Clusters), Logical Networks, and Services.

### 6.1.1 Create Storage Clusters

First step is create a new Cluster. The Cluster version must follow the RHS Node software version. To ensure this, check the correct version number on the Red Hat Storage Nodes.

```
# cat /etc/redhat-storage-release
Red Hat Storage Server 3.0 Update 3
```

Next login to the Management Console to define a new cluster. On the left pane, select *Clusters* and click *New*. Specify a name and description for the cluster and select the correct *Compatibility Version* based on the RHS nodes version number (3.3 in this case).

**NOTE**: It is not recommended to use the *Default Cluster* for production environment.

Once a Cluster is created, it shown on the left pane and ready to manage the joined Hosts. In this reference architecture *Storage1* is the name of the created cluster.

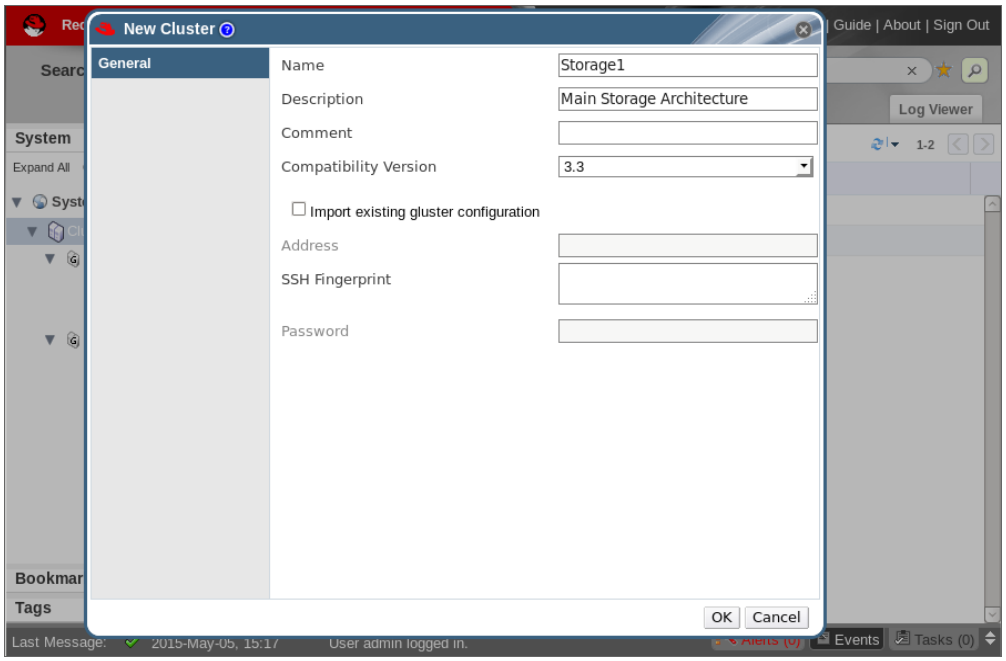


**Figure 6.1.1.1: Create New Cluster**

## 6.1.2 Add Red Hat Gluster Storage Hosts to the Cluster

On the left pane, extract the *Storage1* cluster and select *Hosts*. On the main pane click *New*. Specify the server name, IP address and the root password then click *OK*.

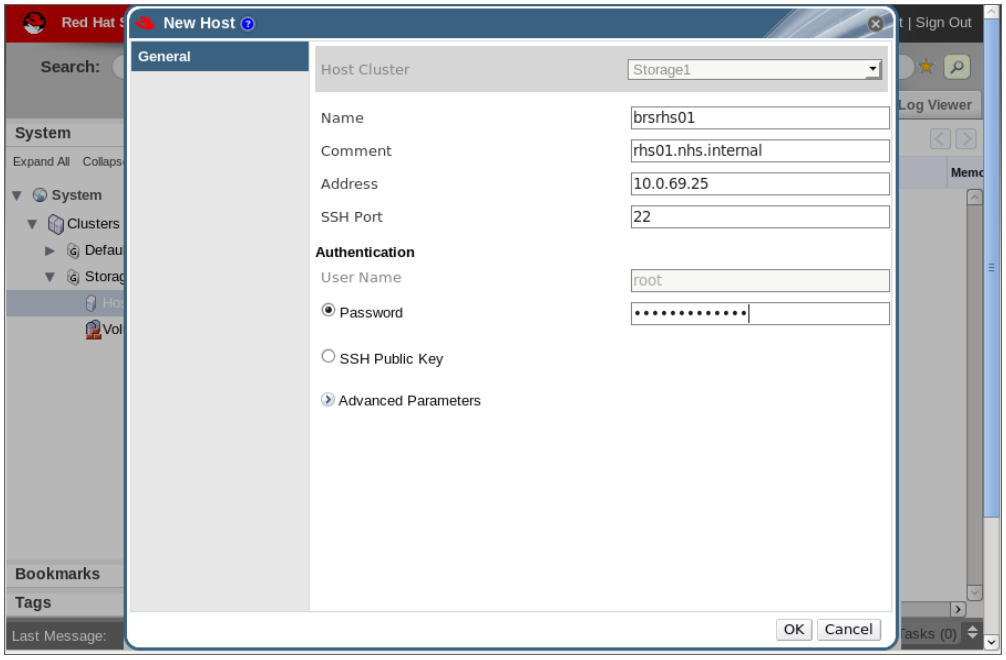


**Figure 6.1.2.1: Add New RHS Host to the Cluster**

The system is going to deploy the new Host automatically. Once it is done, a green sign shows by the host name on the left. The installation logs are in the */var/log/messages*.

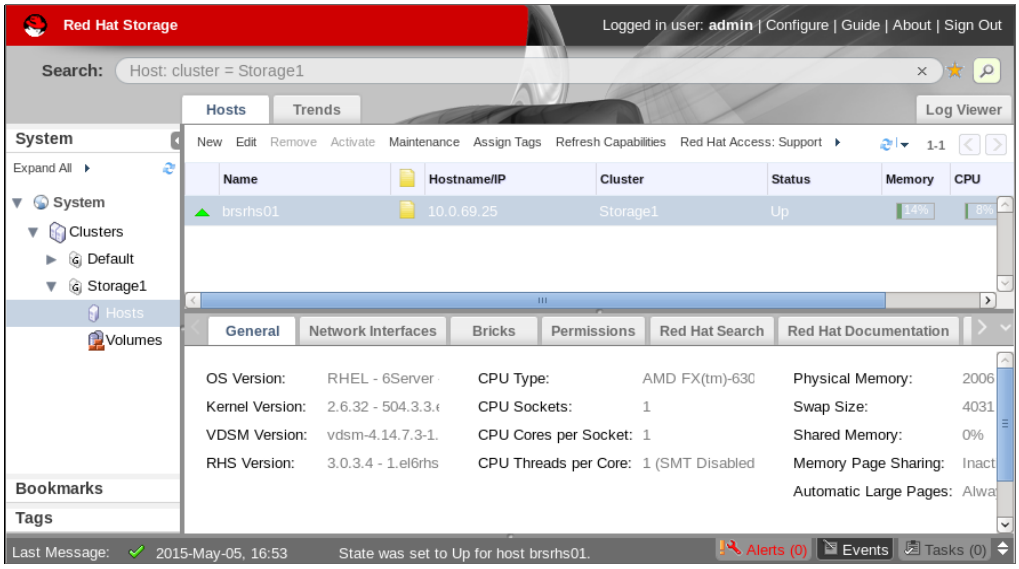


**Figure 6.1.2.2: Manage RHS Hosts using Console**

Click on the host name to check the general descriptions. Use *Network Interfaces* tab to setup networks, and use *Bricks* tab to check all operating bricks.

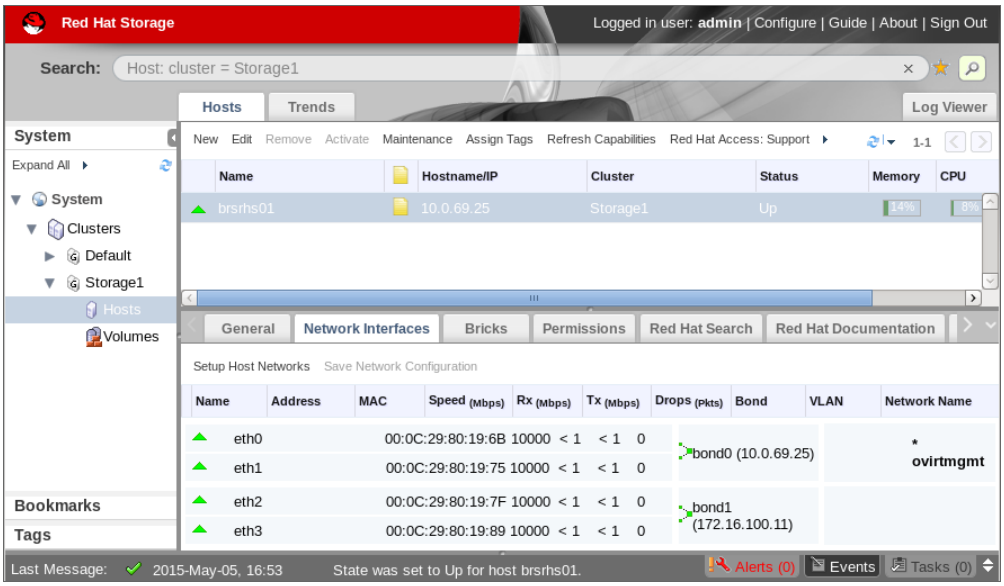


**Figure 6.1.2.3: Manage Network Interfaces**

Repeat these steps above with all remained Red Hat Storage nodes and deploy them to the *Storage1* cluster. More Console administration tasks are described in the Red Hat Storage 3 Console Administration Guide. Once the Console manages all Red Hat Storage hosts within a Cluster, the Gluster Auto Discover Tool is able to configuring all Nagios services automatically. Before running the Nagios auto-configuration tool, the NRPE service (Nagios client) needs to prepared on all Red Hat Storage nodes.

## 6.2 Configuring Nagios Agent on Red Hat Gluster Storage Servers

The Nagios Remote Plugin Executor (NRPE) service is a Nagios Agent (client) designed to execute Nagios Plugins on remote Linux nodes. The NRPE service runs on remote clients and uses TCP 5666 port to provide check results to the Nagios process.

The following diagram shows an overview of NRPE components.

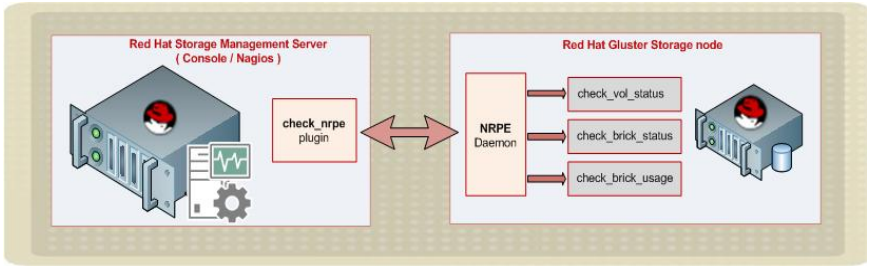


**Figure 6.2.1: NRPE Overview**

In Red Hat Gluster Storage 3, the NRPE package is installed by default as well as all Storage monitoring scripts. Also the Nagios plugins are included to the NRPE configuration file. The Nagios Server IP address or host name is the only thing which needs to be configured.

Open the */etc/nagios/nrpe.cfg* file, add the Red Hat Console (Nagios Server) IP address to the allowed hosts as shown below and restart the nrpe service.

```
allowed_hosts=127.0.0.1, 10.0.69.20
```

```
# service nrpe restart
Shutting down nrpe:                                        [  OK  ]
Starting nrpe:                                             [  OK  ]
```

On each Red Hat Storage nodes, start the Gluster Process Monitoring Service (*glusterpmd*) to monitor glusterd, self heal, smb, quotad, ctdbd, and brick services.

```
# /etc/init.d/glusterpmd start
Starting gluster process monitoring service
# chkconfig glusterpmd on
```

Login to the Nagios Server, and use check_nrpe command to check the availability of NRPE plugins as well as the Nagios agent/server communication.

Usage: check_nrpe -H <RHS_host> -c <command>

```
# /usr/lib64/nagios/plugins/check_nrpe -H 10.0.69.25 -c check_interfaces
OK: bond1:UP,ovirtmgmt:UP |bond1.rxpck=0.03 bond1.txpck=0.00 bond1.rxkB=0.01
bond1.txkB=0.00 ovirtmgmt.rxpck=28.15 ovirtmgmt.txpck=10.65
ovirtmgmt.rxkB=2.23 ovirtmgmt.txkB=2.01
# /usr/lib64/nagios/plugins/check_nrpe -H 10.0.69.25 -c check_swap_usage
OK- 0.00% used(0.00GB out of 3.94GB)|Used=0.00GB;3.15;3.54;0;3.94
```

All check commands are set in the nrpe.cfg file. If no errors, the Red Hat Gluster Storage node is ready to provide system health information to the Nagios Server using NRPE.

## 6.3 Auto-Configuring Nagios Monitoring Services

The *Gluster Auto Discover Tool* is a command line application provided by Red Hat Storage Console which automatically discovers all Hosts and Volumes in the cluster. It also setup all Nagios files automatically to monitor every Storage components.

Prerequisites for auto-discovery usage that all Red Hat Gluster Storage hosts have to be member of a Cluster defined and managed by the Red Hat Storage Console.

Login to the Red Hat Storage Console (Nagios Server) and run *configure-gluster-nagios* command. Usage: *configure-gluster-nagios -c <CLUSTER_NAME> -H <RHS_HOST_IP>*

```
# configure-gluster-nagios -c Storage1 -H 10.0.69.26
Cluster configurations changed

Changes :
Hostgroup Storage1 - ADD
Host Storage1 - ADD
         Service - Volume Utilization - pacs01 -ADD
         Service - Volume Self-Heal - pacs01 -ADD
         Service - Volume Status - pacs01 -ADD
         Service - Volume Utilization - pacs02 -ADD
         Service - Volume Self-Heal - pacs02 -ADD
         Service - Volume Status - pacs02 -ADD
         Service - Cluster Utilization -ADD
         Service - Cluster - Quorum -ADD
         Service - Cluster Auto Config -ADD
Host brsrhs02.nhs.local - ADD
         Service - Brick Utilization - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick Utilization - /xfsbricks/pacs02/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs02/brick1/brick -ADD
Host brsrhs01.nhs.local - ADD
         Service - Brick Utilization - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick Utilization - /xfsbricks/pacs02/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs02/brick1/brick -ADD
Host brsrhs03.nhs.local - ADD
         Service - Brick Utilization - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick Utilization - /xfsbricks/pacs02/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs02/brick1/brick -ADD
Host brsrhs04.nhs.local - ADD
         Service - Brick Utilization - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs01/brick1/brick -ADD
         Service - Brick Utilization - /xfsbricks/pacs02/brick1/brick -ADD
         Service - Brick - /xfsbricks/pacs02/brick1/brick -ADD
Are you sure, you want to commit the changes? (Yes, No) [Yes]: yes
Enter Nagios server address [brsrhmanager.nhs.local]: brsrhmanager.nhs.local
Cluster configurations synced successfully from host 10.0.69.26
Do you want to restart Nagios to start monitoring newly discovered entities?
(Yes, No) [Yes]: Yes
Nagios re-started successfully
```

This command uses a python script named *discovery.py* to discover all RHS nodes and

Volumes automatically. By default, it runs once a day to synchronize the Nagios configuration from Red Hat Storage Cluster configuration. Once the script is completed successfully, the Nagios is able to monitoring all related Gluster services. Open the Nagios dashboard, click *Services* on the left hand pane, and check the service status details for all RHS Hosts.

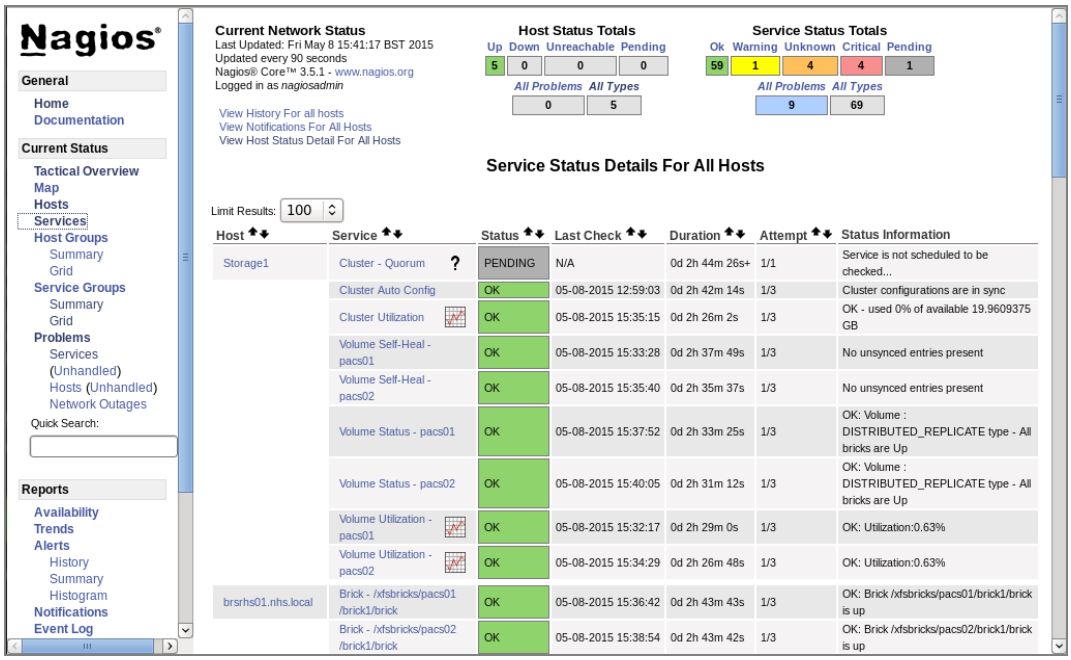


**Figure 6.3.1: Service Status Details**

On the left pane, click *Hosts* to check the host status details for all host groups.

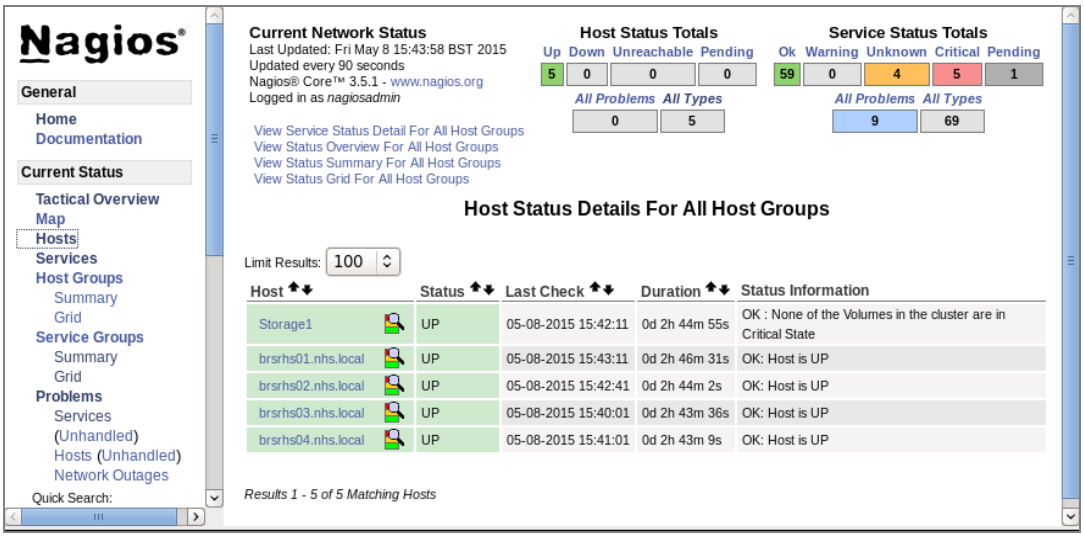


**Figure 6.3.2: Host Status Details**

The Gluster Storage monitoring configuration now is completed but the Nagios Server can be improved with better design, reporting tools, higher security, and graphical configuration tools as well. Most administrators uses the Problems/Services tab on the Nagios Dashboard to focusing on the warnings and critical services only.

# 7 Designing and Administering Nagios

This section shows how-to customize Nagios using different themes and skins. Also explains more about advanced Nagios administration tasks including configuration files, administering tools, notifications and individual services.

## *7.1 Designing Nagios Dashboard*

The Nagios Community has developed a variety of Themes and Web interfaces for Nagios Core. Using a good Nagios Theme makes the monitoring screen sophisticated. Themes, plugins, addons, documentation, and extensions are all downloadable from Nagios Exchange, the website. This architecture uses the Nuvola Style/Theme. Nuvola is a complete image pack for Nagios 3.x including menu, icons, style-sheets, and images.

To implement this theme, download the source (*nagios-nuvola-<version>.tar.gz*) from Nagios Exchange website, extract it and move the "html" folder into the HTML directory of Nagios. It should replace the "*images*" folder, as well as the "*stylesheets*" folder and create a new folder called "*side*". The "*index.html*","main.html" and "*side.html*" should also be replaced. Finally set back the permissions on the modified folders.

This screenshot demonstrates how the new style looks on the Nagios Dashboard.

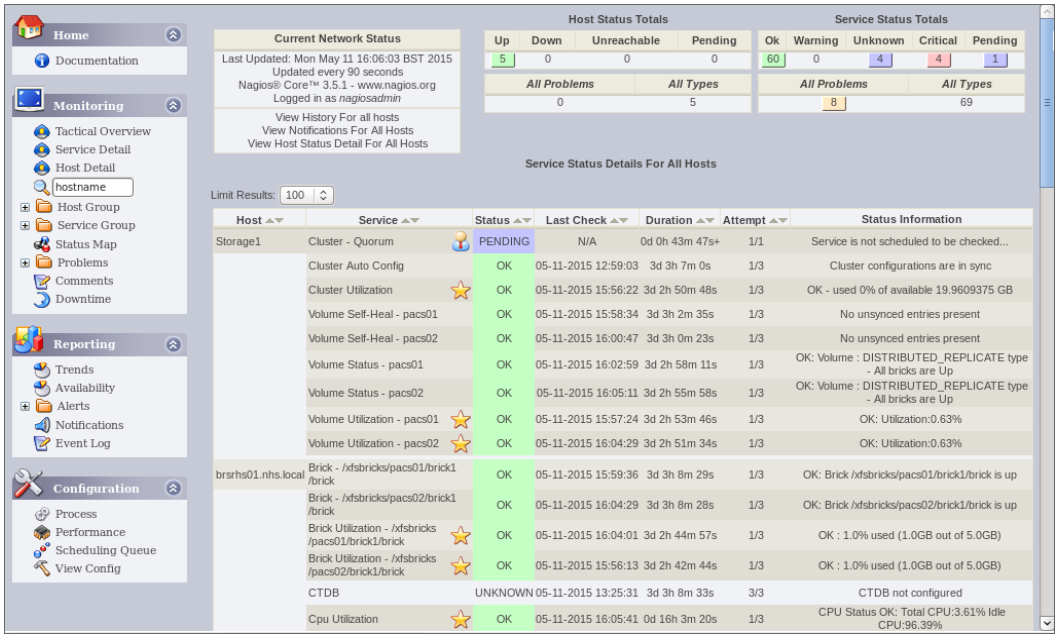


**Figure 7.1.1: Designing Nagios Dashboard**

The following example shows all implementation commands together. In the first step, download the Theme source (*nagios-nuvola-1.0.3.tar.gz*) to the /tmp directory.

```
# mkdir /root/{backup,nagios-theme}
# cp -pr /usr/share/nagios/html /root/backup/
# gzip -d /tmp/nagios-nuvola-1.0.3.tar.gz
# tar -xvzf /tmp/nagios-nuvola-1.0.3.tar  --directory=/root/nagios-theme/
# cp -a /root/nagios-theme/html/* /usr/share/nagios/html/
```

```
# service httpd restart
```

Before restarting *httpd* service, move out the *index.php* and *main.php* from the default HTML directory but leave there all the other files or folders.

**NOTE:** Using a new theme on Nagios dashboard makes the monitoring screen attractive but does not improve anything on the current monitoring services or configuration files.

## 7.2 Managing Users and Passwords

The Nagios Dashboard allows for administrators to do several administration tasks such as enable/disable active monitoring and notifications on specified hosts or services, also manage scheduled downtime or customize reports. Due to unwanted monitoring modifications, the dashboard usage may require a non administrative user access with read-only permissions.

This example shows how-to create a read-only user for Nagios.

```
# htpasswd /etc/nagios/passwd monitoring
New password:
Re-type new password:
Adding password for user monitoring
```

Configure read-only permissions to *monitoring* user in the */etc/nagios/cgi.cfg* configuration file. The *authorized_for_read_only* parameter contains a comma-delimited list of users that have read-only rights only.

```
authorized_for_read_only=monitoring
```

To ensure modifications, restart the *httpd* as well as the *nagios* services.

```
# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
# service nagios restart
Running configuration check...done.
Stopping nagios: .done.
Starting nagios: done.
```

**NOTE:** The read only permission gives a very limited access to the monitoring results, it is recommended to specify other permissions too in the *cgi.cfg* configuration file.

To change the default Nagios administrator (nagiosadmin) password use the following command.

```
# htpasswd -c /etc/nagios/passwd nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin
```

The *cgi.cfg* configuration file allows customizing advanced access permissions for Nagios users. It is also supported to integrating LDAP Authentication with Nagios Dashboard. The authentication setup is described in the Red Hat Storage 3 Administration Guide.

## 7.3 Customizing Monitoring Objects

The Nagios monitoring works with configuration files. The main configuration file is the */etc/nagios/nagios.cfg*. It contains a number of object configuration files that affect how the Nagios daemon operates. Once a new configuration file created it must be specified in the *nagios.cfg*. Objects are all the elements that are involved in the monitoring and notification logic. An object can be defined in one or more configuration files and/or directories.

This section shows brief configuration examples how-to defining objects include: Services, Hosts, Contacts, Check Commands, and Time Periods. Some objects such as Services, Hosts, and Contacts can be collected in a group.

This Service example uses the *check_nrpe* command to get information about Swap usage. The *check_swap_usage* command is defined in the *nrpe.cfg* on the RHS server.

```
define service{
  use                     gluster-service-with-graph
  hostgroup_name          gluster_hosts
  service_description     Swap Utilization
  normal_check_interval 1
  check_command           check_nrpe!check_swap_usage
}
```

The next example defines a Red Hat Gluster Storage Host.

```
define host {
         use             gluster-host
         hostgroups      gluster_hosts,Storage1
         alias           brsrhs02.nhs.local
         host_name       brsrhs02.nhs.local
         _HOST_UUID      5fc4dd0b-89ca-4063-8b87-28b9a8a425d9
         address         10.0.69.26
}
```

There is a Time Period definition example.

```
define timeperiod{
        timeperiod_name workhours
        alias           Normal Work Hours
        monday          09:00-17:00
        tuesday         09:00-17:00
        wednesday       09:00-17:00
        thursday        09:00-17:00
        friday          09:00-17:00
        }
```

This example defines the check_nrpe command which is one of the main check commands.

```
define command{
       command_name check_nrpe
       command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

This check command operates with the *check_nrpe* plugin extended with two arguments. Detailed object configuration examples can be found on the Nagios Community website.

## 7.4 Configuring Email and SMS Notifications

To configuring email notifications, define new contacts in the */etc/nagios/gluster/gluster-contacts.cfg* file. This example has two contacts, *administrator* and *callcenter*.

The contact definition format shown below.

```
define contact {
       contact_name                    administrator
       alias                           Gluster Storage Admin
       email                           admin@nhs.local
       service_notification_period     24x7
       service_notification_options    w,u,c,r,f,s
       service_notification_commands   notify-service-by-email
       host_notification_period        24x7
       host_notification_options       d,u,r,f,s
       host_notification_commands      notify-host-by-email
}

define contact {
       contact_name                    callcenter
       alias                           Call Center Operators
       email                           support@nhs.local
       service_notification_period     workhours
       service_notification_options    w,u,c,r,f,s
       service_notification_commands   notify-service-by-email
       host_notification_period        workhours
       host_notification_options       d,u,r,f,s
       host_notification_commands      notify-host-by-email
}
```

The notification periods are defined in the *timeperiods.cfg*.

Service notification options:

- w = send notifications on a WARNING state,
- u = send notifications on an UNKNOWN state,
- c = send notifications on a CRITICAL state,
- r = send notifications on OK state (recoveries),
- f = send notifications when the service starts and stops flapping,
- s = send notifications when scheduled downtime starts and ends.

Host notification options.

- d = notify on DOWN host states,
- u = notify on UNREACHABLE host states,
- r = notify on host recoveries (UP states),
- f = notify when the host starts and stops flapping,
- s = send notifications when host or service scheduled downtime starts and ends.

Once the Internet connection has crashed, the Nagios cannot send any email alerts to the administrators and the SLA might be violated. Sending SMS notifications to mobile phones could solve this issue also provides high availability for Nagios notifications. This architecture uses an SMS hardware gateway (SMSEagle) to make specified notifications independent from Internet connections. The SMS notification configuration steps are described below.

Download the *notify_eagle_sms.pl* script from Nagios Exchange site, and move it to the /usr/lib64/nagios/plugins/ directory. Next create a new user for this script in SMSEagle. Add *notify-by-sms* and *host-notify-by-sms* commands to the */etc/nagios/objects/commands.cfg*.

```
define command {
command_name notify-by-sms
command_line $USER1$/notify_eagle_sms.pl -s SMSEAGLEIP -u SMSEAGLEUSER -p
SMSEAGLEPASSWORD -d $CONTACTPAGER$ -t "$NOTIFICATIONTYPE$ $SERVICESTATE$
$SERVICEDESC$ Host($HOSTNAME$) Info($SERVICEOUTPUT$) Date($SHORTDATETIME$)"
}

define command {
command_name host-notify-by-sms
command_line $USER1$/notify_eagle_sms.pl -s SMSEAGLEIP -u SMSEAGLEUSER -p
SMSEAGLEPASSWORD -d $CONTACTPAGER$ -t "$NOTIFICATIONTYPE$ $HOSTSTATE$
Host($HOSTALIAS$) Info($HOSTOUTPUT$) Time($SHORTDATETIME$)"
}
```

Script parameters:

- SMSEAGLEIP = IP Address of the SMSEagle device (eg.: 10.0.69.250)
- SMSEAGLEUSER = SMSEagle user
- SMSEAGLEPASSWORD = SMSEagle password

In the */etc/nagios/gluster/gluster-contacts.cfg* file, extend the administrator contact parameters with these two notification commands.

```
define contact {
       contact_name                    administrator
       alias                           Gluster Storage Admin
       email                           admin@nhs.local
       service_notification_period     24x7
       service_notification_options    w,u,c,r,f,s
       service_notification_commands   notify-service-by-email,notify-by-sms
       host_notification_period        24x7
       host_notification_options       d,u,r,f,s
       host_notification_commands      notify-host-by-email,host-notify-by-sms
       pager                           +447654321234
}
```

The "pager" should contain the administrator's mobile number in international format e.g. 44xxxxxxxxx. If the system Administrators are in a contact group then each member's mobile number needs to be configured in his contact definition.

Extend the notification part of all related service definitions with the “administrator” contact and finally restart the Nagios service.

# 8 Using Nagios Server Dashboard

This section describes best practices how-to using Nagios Dashboard including enable or disable monitoring services as well as embedded reporting tools. In Red Hat Gluster Storage environment, the Nagios Server functions are extended with customized Gluster Storage monitoring such as Volume utilization reports and diagrams.

## *8.1 Administering Service Monitoring*

After a successful login, the first screen shows a *Tactical Overview* of Monitoring Performances, Hosts, Services, and some other features.

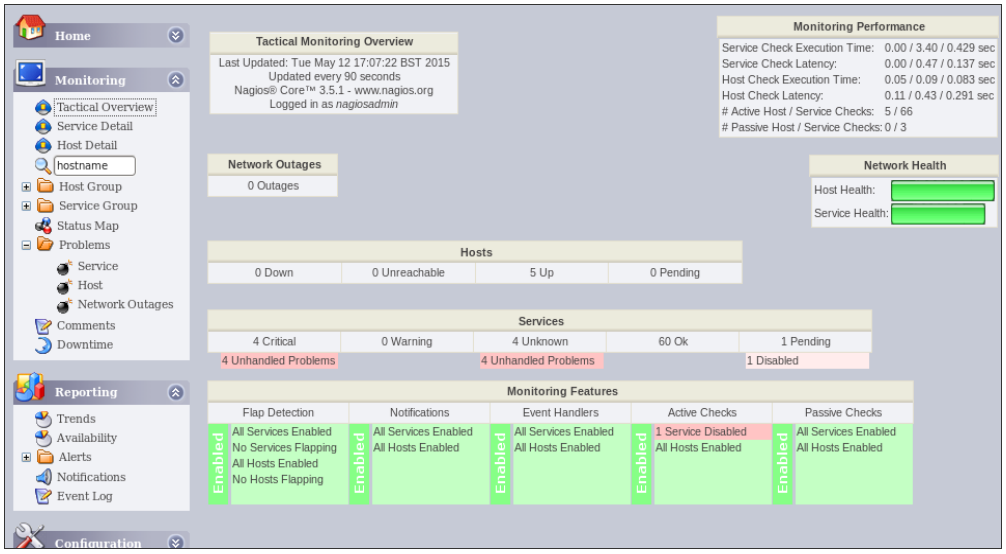


**Figure 8.1.1: Tactical Overview**

The *Service Detail* tab provides a summary of services status grouped by the Hosts.


**Figure 8.1.2: Service Details**

On the left hand pane, click on *Service Detail* to see and manage all monitored services. To manage monitoring via *Service State Information* screen, simply select a service. On the right hand pane all services monitoring can be enabled, disabled, re-scheduled, and commented.

If a Gluster service has known issues, click on "*Disable notifications for this service*" to prevent any further email or sms alert messages from Nagios.

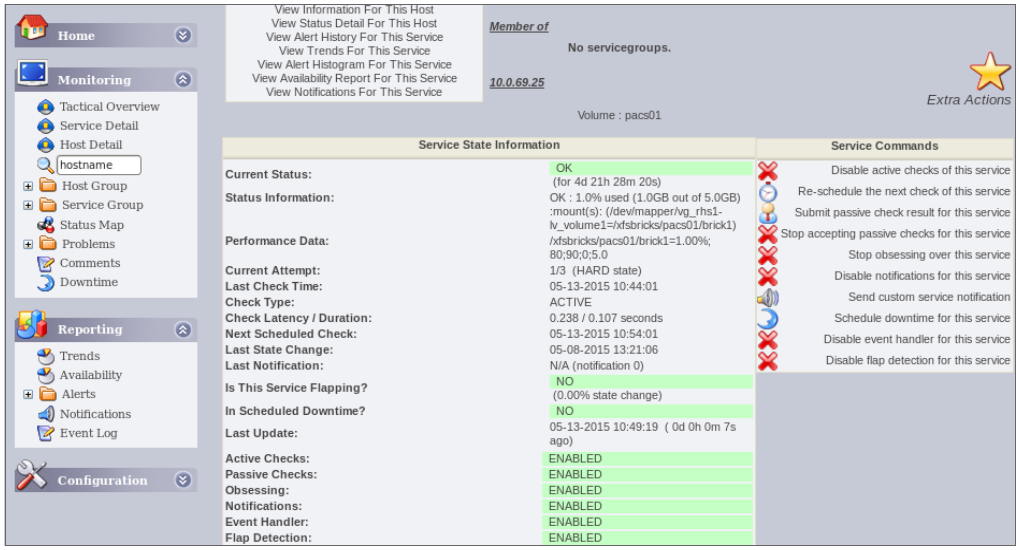


**Figure 8.1.3: Service State Screen**

Select "*Send custom service notification*" to create customized notifications to all involved Nagios users. The *Forced* and *Broadcasts* options allows to override the normal notification logic if sending an important message with priority.

Use links provided in the *Service Information* to get more information for this Service including *Alert History*, *Trends*, *Alert Histogram*, *Availability Report*, and *Notifications*. The next screen shows how the *Service Availability Report* looks like.

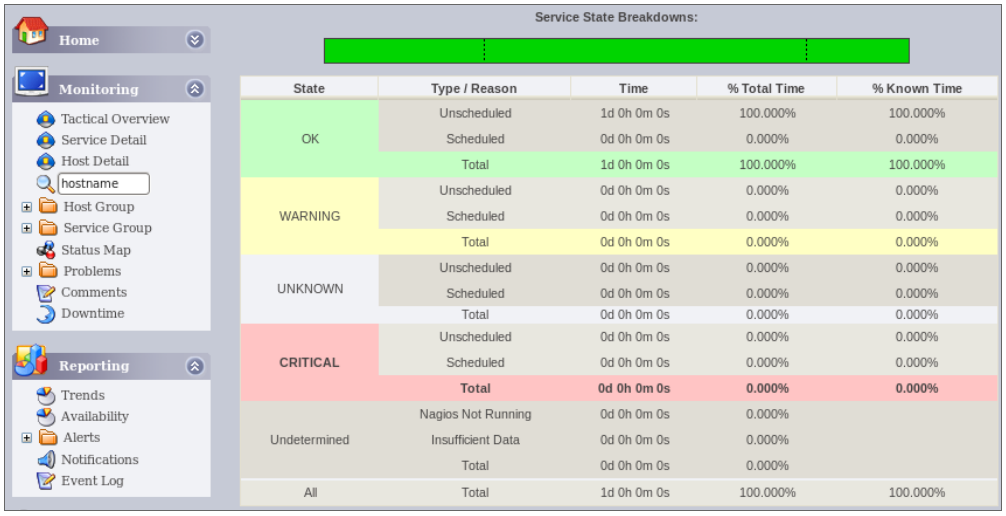


**Figure 8.1.4: Service Availability Report**

# 8.2 Monitoring Red Hat Storage Utilization

By clicking on the gold star beside a service, a new window opens to show extra service actions. This feature displays utilization graphs provided by pnp4nagios which is a Nagios add-on to analyzing performance data and store them automatically.

Click on the appropriate icon in the *Actions* menu and the result of the utilization analysis are downloadable in PDF, XML and some other file formats.

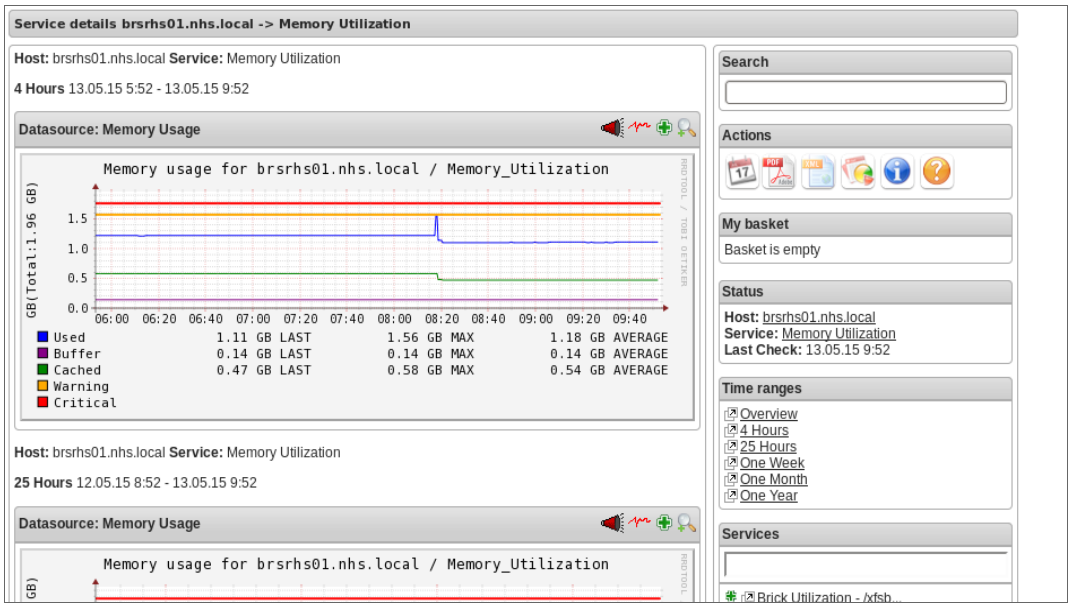


**Figure 8.2.1: Service Details**

The Console can display all of these utilization graphs by clicking on the *Trends* tabs. Login to the Console and select the Storage1 Cluster. Click on *Trends* to get Gluster Volume utilization graphs.

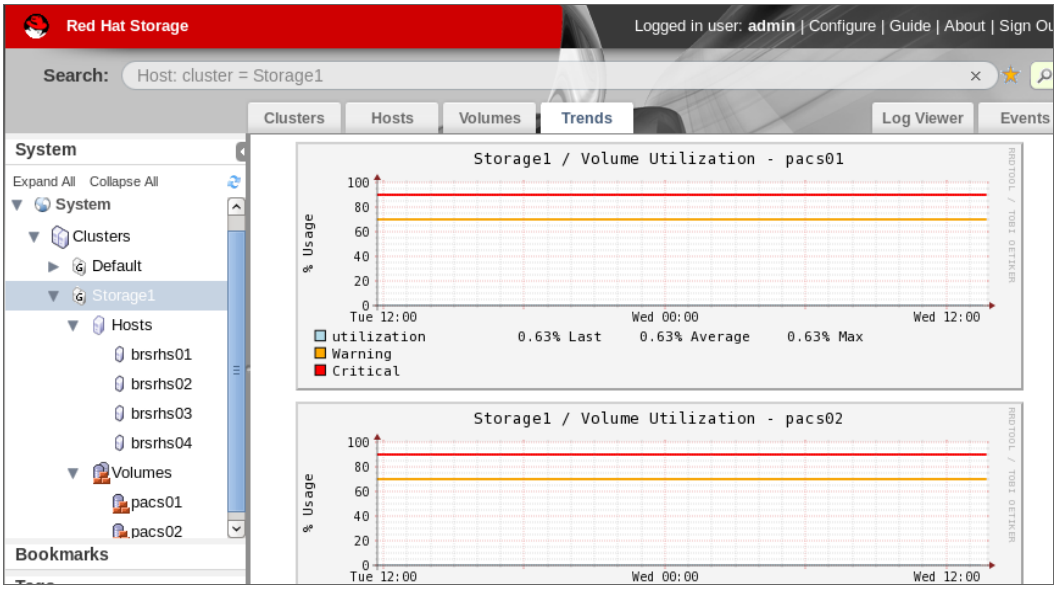


**Figure 8.2.2: Monitor Volume Utilization Using RHS Console**

The Red Hat Storage Console also uses the *pnp4nagios* plugin to display utilization graphs. The *Trends* tab is available if the *rhsc-monitoring* service is running on the Red Hat Storage Console server. To check *rhsc-monitoring* service, run this command.

```
# rhsc-monitoring status
RHSC monitoring is enabled.
Nagios is running
NSCA is running
```

This section presented a brief overview of Nagios Dashboard usage. All functions can be customized, extended or improved using various Nagios plugins or supported scripts. More details about how to use Nagios Dashboard can be found in the Red Hat Storage 3 Console Administration Guide.

## 8.3 Dashboard Best Practices

Use the *Reporting/Alerts/History* screen to check service availability history or use this result for SLA reports. Various filters are available to make reports more sophisticated. Apply *Host Down* or *Service Critical* filters to get a whole picture what happened with critical problems.

To get a fast system configuration overview, use the *Configuration/ViewConfig* menu. This menu provides information for all objects such as Hosts, Host Groups, Services, Service Groups, Contacts, Contact Groups, Time Periods, Commands, and Command Expansion.

The last screenshot in this section shows the output of the *Problems/Service* menu which is the most popular Nagios screen. It displays the unknown, warning, and critical services only.

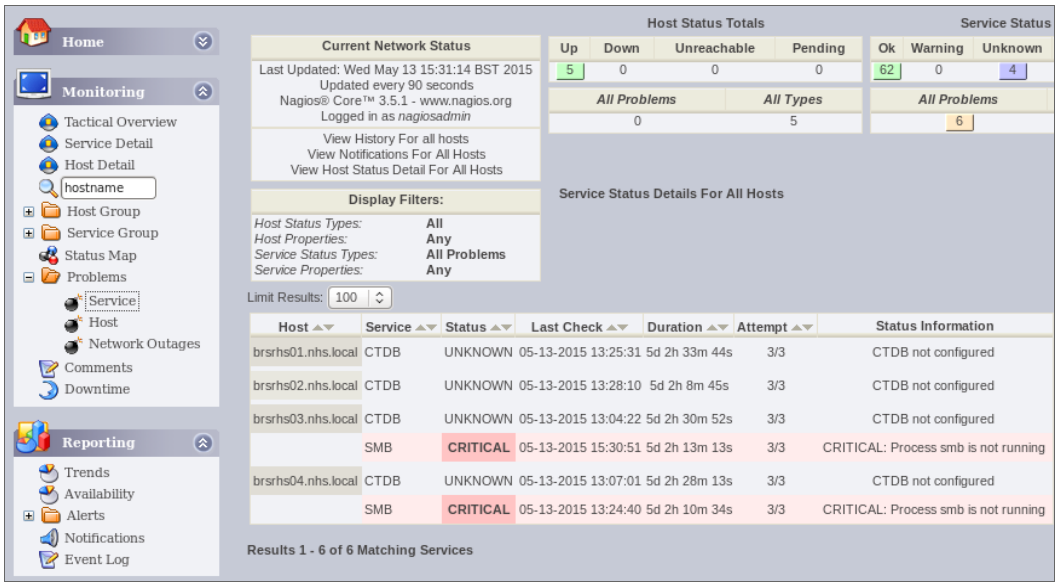


**Figure 8.3.1: Service Problems Screen**

These Nagios Dashboard features above are helps to keep the system healthy as well as the end-users satisfaction with all Storage services.

# 9 Conclusion

Using Red Hat Storage Management Console with Nagios Server presents a great example how easy managing and monitoring serious architectures with the right tool. This is a perfect union which provides a centralized and easy to use management system for system/storage administrators.

The Red Hat Storage Console:

- Manages Clusters, Storage Hosts, Volumes, and Volume lifecycle extensions,
- Supports using multiple Directory Services domains and multilevel administration,
- Provides command line interface tool to manage the whole environment via terminal,
- Displays up-to-date information on the performance and status of storage environment components,
- Uses Nagios plugins to show Host and Cluster utilization graphs,
- Also provides system administration tools to manage backup processes, as well as system logs.

Nagios Server is perfectly fit to extend the Console's rich functionalists with an advanced monitoring solution. The *Red Hat Storage Nagios Server* subscription provides an individual and well prepared Nagios configuration including individual services, service groups, check commands and auto-discovery.

This solution is highly recommended to enterprise companies for whom the main priority is to have a high availability storage solution - without very costly hardware solutions.

# Appendix A: Overview of Nagios Packages

The Red Hat Storage 3 Nagios Server channel (rhs-nagios-3-for-rhel-6-server-rpms) provides individual Nagios packages customized for monitoring Red Hat Storage servers.

The following table provides a brief overview of Nagios related packages.

| Red Hat Software Package (RPM) | Description |
|---|---|
| nagios | Nagios monitors hosts and services and warns if somethings breaks |
| gluster-nagios-common | Common libraries, tools, configurations for Gluster node and Nagios server add-ons |
| nagios-server-addons | Gluster node management add-ons for Nagios |
| rhsc-monitoring-uiplugin | oVirt Engine gluster-nagios-monitoring ui-plugin |
| nagios-common | Provides common directories, uid and gid among nagios-related packages |
| nagios-plugins | Host/service/network monitoring program plugins for Nagios |
| nagios-plugins-dummy | Nagios Plugin - check_dummy |
| nagios-plugins-nrpe | Provides nrpe plugin for Nagios |
| nagios-plugins-ping | Nagios Plugin - check_ping |
| pnp4nagios | Nagios performance data analysis tool |
| pynag | Python modules and utilities for Nagios plugins and configuration |
| check-mk | A new general purpose Nagios-plugin for retrieving data |
| nsca | Nagios Service Check Acceptor |

**Table 9.1: Nagios packages**

Once the Nagios Server is running, the monitoring can be extended with additional plugins and features such as graphical management system, individual skins/themes and advanced reporting tools.

# Appendix B: Configuring Network Bonding Using RHS Console

NIC bonding is a high availability networking solution using two or more network interfaces to provide network redundancy and increase bandwidth. The bonding driver provides a method for aggregating multiple network interfaces into a single logical interface.

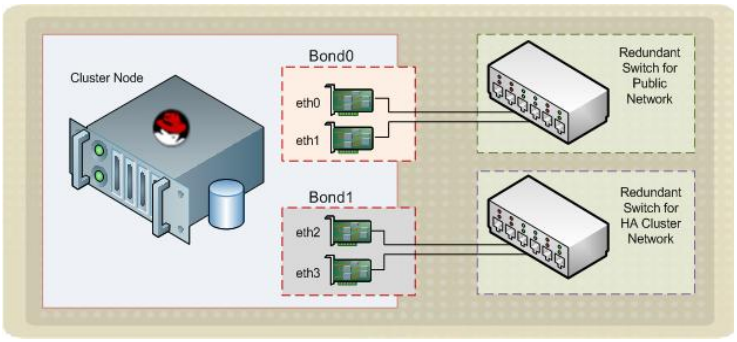


**Figure 9.1: Network Bonding**

All servers in the reference architecture have two pairs of NIC's which provides redundancy for networks using bonding technology. The first two network interfaces ("eth0" and "eth1") is bonded for the Public Network. The other two NIC's ("eth2" and "eth3") deliver redundancy for the RHS Internal network.

The following example describes how to setup network using Red Hat Storage Console.

Login to the RHS Web Administration Console. On the left hand pane, select *Hosts* under the Storage1 Cluster. On the main pane click on the host and select *Network Interfaces* tab in the bottom menu.

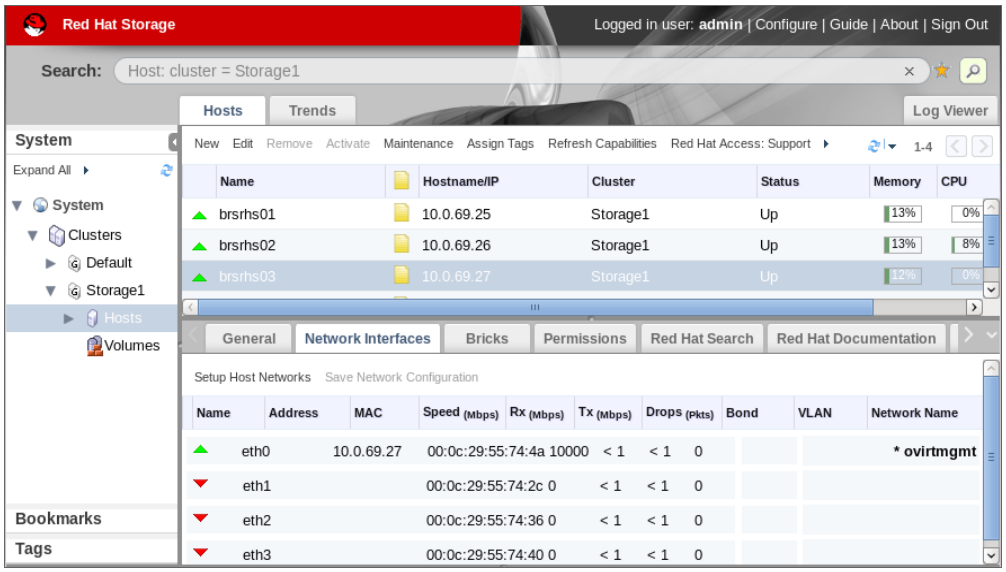


**Figure 9.2: Setup Network**

This RHS Host has four NIC's but only one is configured so far. To configure network bonding, click on *Setup Host Networks* link. In the Setup Host Networks window, right click on *eth1* device and select *Bond eth1 with eth0*.

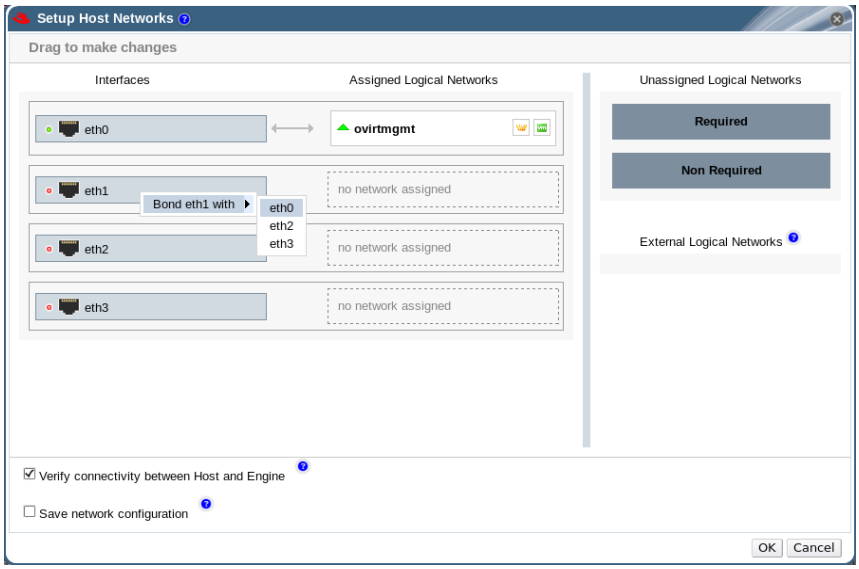


**Figure 9.3: Setup Network Bonding**

New window opens for configuring bonding name and mode. Accept the default and click *OK*. The Bonding Mode defines the bonding policy. Mode 1, 2, 4, and 5 are supported on RHS 3. Now eth0 and eth1 are bounded to the assigned logical network. Click *OK* on the Setup Host Networks window to exit.

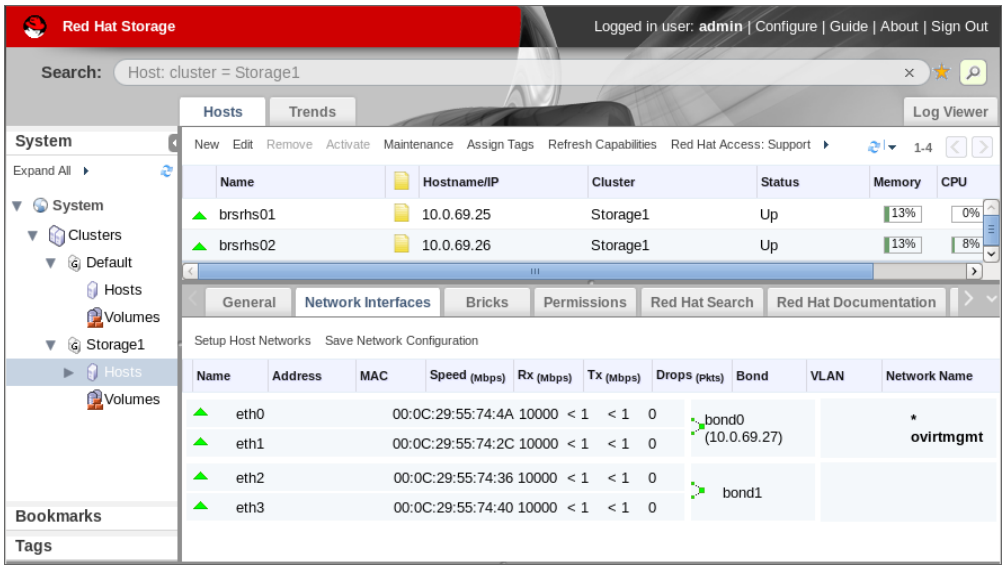


**Figure 9.4: Confirm Network Bonding**

The bonded network becomes activated automatically and a green sign shows on the adapter's left side. Click on *Save Network Configuration* link to confirm the new configuration.

# Appendix C: References

**Red Hat Subscription Management**
This website is collecting together all guides, instructions and recommendations for Red Hat Subscription.

**RHEL Systems Registration Guide**
This article is a guide to find the best registration option for Red Hat Enterprise Linux environments.

**Red Hat Storage 3 Administration Guide**
The official guide for configuring and managing Red Hat Storage environments.

**Red Hat Storage 3 Console Administration Guide**
System Administration of Red Hat Storage Environments using the Administration Portal.

**Red Hat Storage Error Message Guide**
Error description and recommended action for possible errors that occur in the Red Hat Storage Server environment.

**Red Hat Hardware Compatibility List for Storage**
Supported Hardware for a server to be Red Hat Storage Compatible.

**Red Hat Storage Server 3.0 Compatible Platforms**
Up-to-date details about Red Hat Storage Server Compatible Physical Virtual Server and Client OS Platforms.

**Red Hat Storage Server Life Cycle**
Red Hat has established specific life cycle policies for the Red Hat Storage Server product family.

**NRPE Documentation**
NRPE Installation and Configuration Guide from SourceForge.

**Nagios Community Website**
Website for download Nagios Themes, Skins, Plugins, Web interfaces, and documentations.

**Nagios Configuration Examples from SourceForge**
Provides detailed configuration examples for managing Nagios monitoring objects.

**Configuring SMS Notifications via SMSEagle**
Nagios plugin (BSD) created by Radoslaw Janowski.

# Appendix D: Revision History

| | | |
|---|---|---|
| Revision 1.0 | Saturday May 13, 2015 | Zoltan Porkolab |
| Initial Release | | |