Red Hat Storage 3
Console Administration Guide

System Administration of Red Hat Storage Environments using the Administration Portal

Shalaka Harne Anjana Suparna Sriram

Red Hat Storage 3 Console Administration Guide

System Administration of Red Hat Storage Environments using the Administration Portal

Shalaka Harne
Red Hat Engineering Content Services
sharne@redhat.com

Anjana Suparna Sriram
Red Hat Engineering Content Services
asriram@redhat.com

Legal Notice

Abstract

This guide is a step-by-step guide for users to configure and manage Red Hat Storage environment using the Administration Portal. This guide is intended for advanced users, and assumes that you have successfully installed the Red Hat Storage Console and have an understanding of your storage server resources. It describes how to use the Administration Portal, and manage system components and storage infrastructure.

Table of Contents

Chapter 1. Introduction

Red Hat Storage Console is management infrastructure that enables you to create a powerful, scalable storage environment.

It provides IT departments with the tools to meet the challenges of managing complex environments, and enables administrators to reduce the cost and complexity of large deployments. Red Hat Storage Console includes:

- Support to quickly create and manage Red Hat Storage trusted storage pool and volumes.
- Multilevel administration to enable administration of physical infrastructure and virtual objects.

1.1. System Components

The various components work together seamlessly to enable the system administrator to set up, configure, and maintain the storage environment via an intuitive graphical user interface.

1.1.1. Components

Red Hat Storage consists of one or more servers and at least one console. The system and all its components are managed through a centralized management system.

1.1.2. The Console

Red Hat Storage Console is a service that runs on a Red Hat Enterprise Linux 6.5 and Red Hat Enterprise Linux 6.6 servers, providing interfaces for controlling the Red Hat Storage. It manages user session login and logout, high availability and clustering systems.

1.1.3. Hosts

Red Hat Storage Server is a trusted network of storage servers. When you start the first host, the storage pool consists of that host alone. You can add additional storage hosts to the cluster. Red Hat Storage volumes are created on these clusters. The system and all its components are managed through a centralized management system.

1.2. Red Hat Storage Console Resources

The Red Hat Storage Console manages the following resources within the management infrastructure to create a powerful, scalable storage environment.

- **Hosts** - A host is a physical host (a physical machine) running Red Hat Storage 3.0. Servers are grouped into storage clusters. Red Hat Storage volumes are created on these clusters. The system and all its components are managed through a centralized management system.
- **Clusters** - A cluster is a group of linked computers that work together closely, thus in many respects forming a single computer. Hosts in a cluster share the same network infrastructure and the same storage.
- **User** - Red Hat Storage supports multiple levels of administrators and users with distinct levels of permissions. System administrators can manage and administer objects of the physical infrastructure, such as clusters, hosts, and volume.

- **Events and Monitors** - Alerts, warnings, and other notices about activities within the system help the administrator to monitor the performance and operation of various resources.

1.3. Administration of the Red Hat Storage Console

This section provides a high level overview of the tasks and responsibilities of a system administrator for the Red Hat Storage Console. The tasks are divided into two general groups:

- Configuring a new logical cluster is the most important task of the system administrator. Designing a new cluster requires an understanding of capacity planning and definition of requirements. This is typically determined by the solution architect, who provides the requirements to the system architect. Preparing to set up the storage environment is a significant part of the setup, and is usually part of the system administrator's role.
- Maintaining the cluster, including performing updates and monitoring usage and performance to keep the cluster responsive to changing needs and loads.

The procedures to complete these tasks are described in detail in later sections of this guide.

It is assumed that you have already read the material in *Red Hat Storage Console 3 Installation Guide*.

1.3.1. Maintaining the Red Hat Storage Console

This section describes how to maintain a Red Hat Storage Console.

The administrator's tasks include:

- Managing hosts and other physical resources.
- Managing the storage environment. This includes creating, deleting, expanding and shrinking volumes and clusters.
- Monitoring overall system resources for potential problems such as an extreme load on one of the hosts, insufficient memory or disk space, and taking any necessary actions.
- Managing user setup and access, and setting user and administrator permission levels. This includes assigning or customizing roles to suit the needs of the enterprise.
- Troubleshooting for specific users or hosts or for overall system functionality.

These tasks are described in detail in later sections of this guide.

Part I. The Red Hat Storage Console Interface

Chapter 2. Getting Started

The Administration Portal allows you to create, monitor and maintain your Red Hat Storage using an interactive graphical user interface (GUI). The GUI functions in two modes - tree, or flat - allowing you to navigate the system's resources either hierarchically or directly. The powerful search feature enables you to locate any resource in the enterprise, wherever it may be in the hierarchy, and you can use tags and bookmarks to help you to store the results of your searches for later reference.

It is assumed that you have correctly installed Red Hat Storage Console, including hosts, and have logged into the Administration Portal. If you are attempting to set up Red Hat Storage Console, see *Red Hat Storage Console 3 Installation Guide*.

2.1. Graphical User Interface

After you have successfully logged into Red Hat Storage Console, the Administration Portal displays. The GUI consists of a number of contextual panes and menus, and can be used in two modes - tree mode, and flat mode. Tree mode allows you to browse the object hierarchy of a cluster, and is the recommended manner of operation. The elements of the GUI are shown in the figure below.

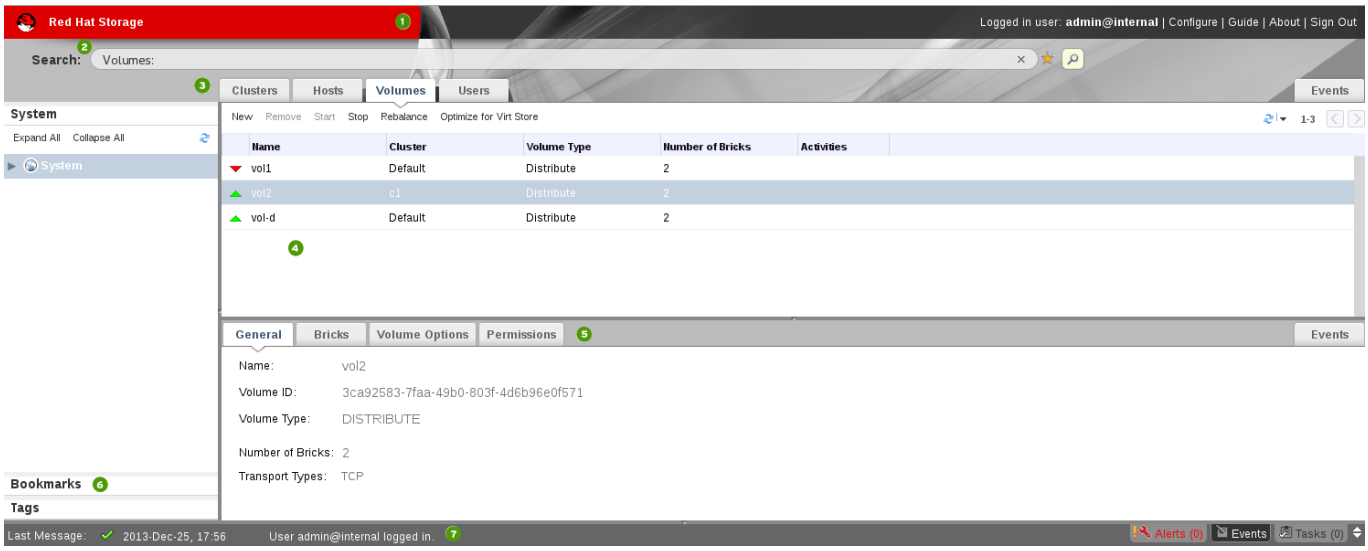


Figure 2.1. Graphical User Interface Elements of the Administration Portal

Graphical User Interface Elements

- **Header**

  The **Header** bar contains the name of the current logged-in user, the **Sign Out** button, the **About** button, and the **Configure** button. The **About** button provides access to version information. The **Configure** button allows you to configure user roles.

- **Search Bar**

  The **Search** bar allows you to quickly search for resources such as hosts and volumes. You can build queries to find the resources that you need. Queries can be as simple as a list of all the hosts in the system, or much more complex. As you type each part of the search query, you will be offered choices to assist you in building the search. The star icon can be used to save the search as a bookmark.

- **Resource Tabs**

All resources, such as hosts and clusters, can be managed using the appropriate tab. Additionally, the **Events** tab allows you to manage and view events across the entire system.

Clicking a tab displays the results of the most recent search query on the selected object. For example, if you recently searched for all hosts starting with "M", clicking the **Hosts** tab displays a list of all hosts starting with "M".

The Administration Portal provides the following tabs: **Clusters**, **Hosts**, **Volumes**, **Users**, and **Events**.

4. **Results List**

   Perform a task on an individual item, multiple items, or all the items in the results list, by selecting the items and then clicking the relevant action button. If multiple selection is not possible, the button is disabled.

   Details of a selected item display in the details pane.

5. **Details Pane**

   The **Details** pane displays detailed information about a selected item in the Results Grid. If multiple items are selected, the **Details** pane displays information on the first selected item only.

6. **Bookmarks Pane**

   Bookmarks are used to save frequently used or complicated searches for repeated use. Bookmarks can be added, edited, or removed.

7. **Alerts/Events Pane**

   The **Alerts** pane lists all events with a severity of **Error** or **Warning**. The system records all events, which are listed as audits in the **Alerts** section. Like events, alerts can also be viewed in the lowermost panel of the **Events** tab by resizing the panel and clicking the **Alerts** tab. This tabbed panel also appears in other tabs, such as the **Hosts** tab.

Important

The minimum supported resolution for viewing the Administration Portal in a web browser is 1024 x 768. When viewed at a lower resolution, the Administration Portal will not render correctly.

2.1.1. Tree Mode and Flat Mode

The Administration Portal provides two different modes for managing your resources - tree mode, and flat mode.

Tree mode displays resources in a hierarchical view for each cluster, from the highest level of the cluster down to the individual volumes. Tree mode provides a visual representation of the storage system. Working in tree mode is recommended for most operations.

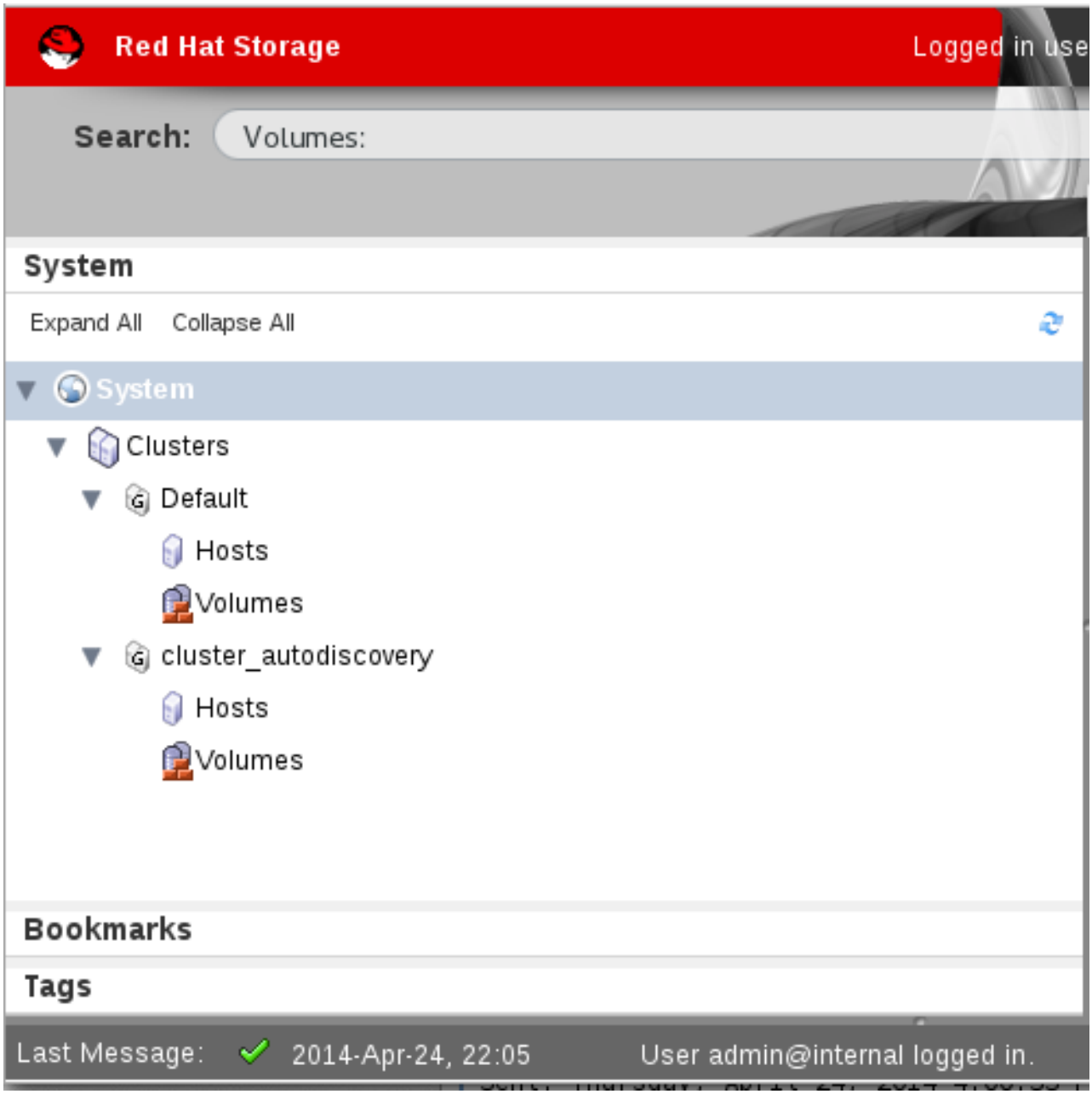


Figure 2.2. Tree Mode

Flat mode offers powerful search functionality, and allows you to customize how you manage your system. It gives you access to any resource, regardless of its position in the enterprise. In this mode, the full power of the search feature can be used. Flat mode does not limit you to viewing the resources of a single hierarchy, allowing you to search across clusters. For example, flat mode makes it possible to find all hosts that are using more than 80% CPU across clusters, or locate all hosts that have the highest utilization. In addition, certain objects are not in the cluster hierarchy, so they will not appear in tree mode. For example, users are not part of the cluster hierarchy, and can be accessed only in flat mode.

To access flat mode, click **System** in the pane on the left-hand side of the screen.

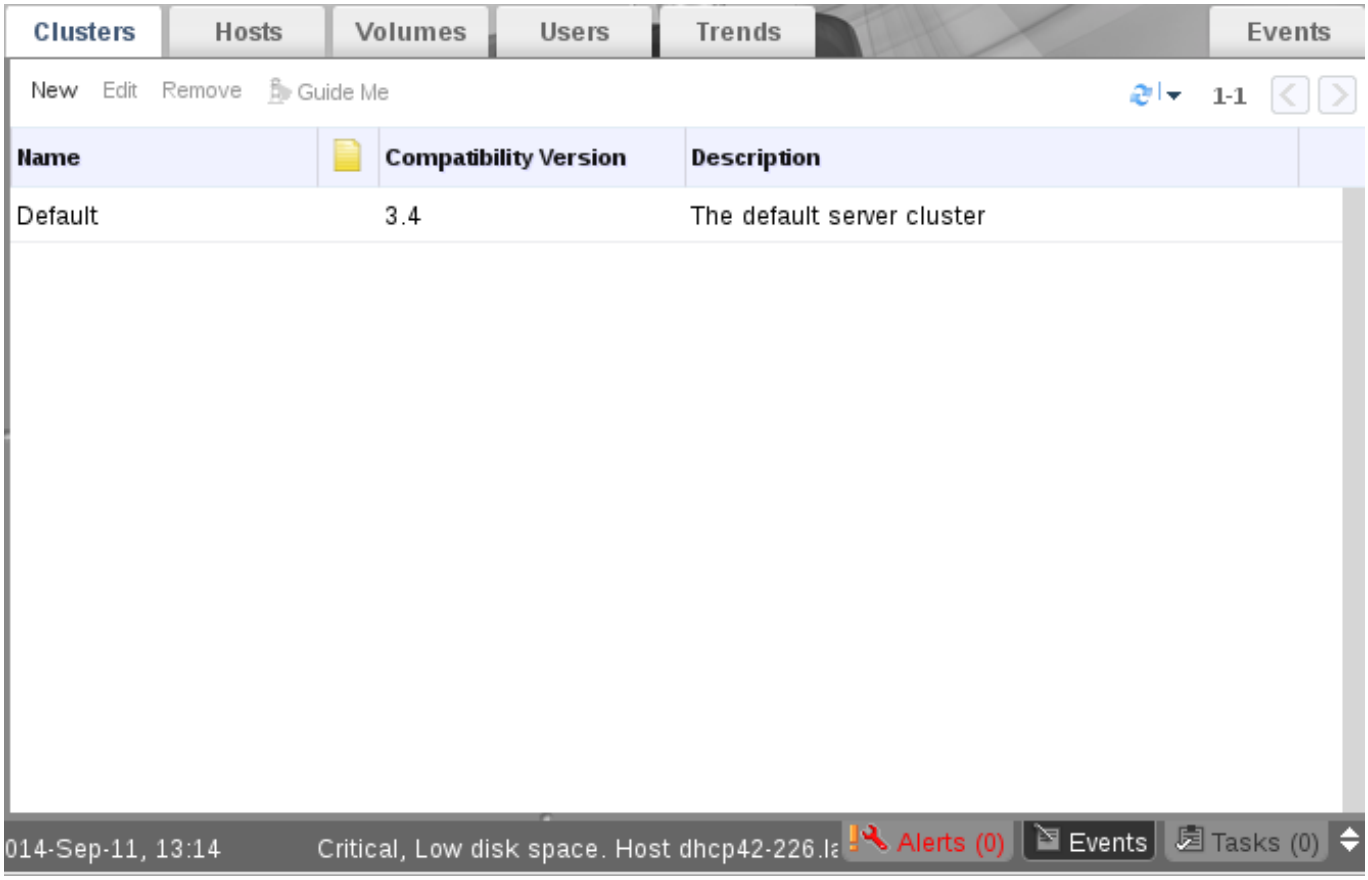


Figure 2.3. Flat Mode

2.2. Search

The Administration Portal is designed to enable the management of thousands of resources, such as volumes, hosts, and clusters. When managing the storage environment, it is recommended that large lists of resources, such as volumes, are reduced to a manageable number (for example, 10). This allows tasks to be performed on a smaller list, or to select specific items on the list on which to perform a given task.

To perform a search, enter the search query (free-text or syntax-based) in the **Search** bar at the top of the Administration Portal. Search queries can be saved as bookmarks for future reuse (Section 2.2.2, “Saving and Accessing Queries as Bookmarks”). This eliminates the need to re-enter a search query each time specific search results are required.

2.2.1. Search Syntax

The syntax of search queries for Red Hat Storage Console resources is as follows:

```
result-type: {criteria} [sortby sort_spec]
```

Syntax Examples

The following examples describe how search queries are used, and help you to understand how Red Hat Storage Console assists with building search queries.

Table 2.1. Example Search Queries

Example	Result
Volumes: status = up	Displays a list of all volumes that are up.
Volumes: cluster = data	Displays a list of all volumes of the cluster data.
Events: severity > normal sortby time	Displays the list of all events whose severity is higher than **Normal**, sorted by time.

2.2.1.1. Auto-Completion

The Administration Portal provides auto-completion to help you create valid and powerful search queries. As you type each part of a search query, a drop-down list of choices for the next part of the search opens below the **Search** bar. You can select from the list and then continue typing or selecting the next part of the search, or ignore the options and continue entering your query manually.

The following table provides examples of how Administration Portal auto-completion assists in constructing a query:

Volumes: status = down

Table 2.2. Example Search Queries using Auto-Completion

Input	List Items Displayed	Action
v	**Volumes** (1 option only)	Select **Volumes** or; Type **Volumes**
Volumes:	All volumes properties	Type **s**
Volumes: s	volume properties starting with **s**	Select **status** or type **status**
Volumes: status	**=** **!=**	Select or type **=**
Volumes: status =	All status values	Select or type **down**

2.2.1.2. Result-Type Options

The result type allows you to search for resources of any of the following types:

- **Host** for a list of hosts
- **Event** for a list of events
- **Users** for a list of users
- **Cluster** for a list of clusters
- **Volumes** for a list of volumes

Each type of resource has a unique set of properties and a set of other resource types that it is associated with, so each search type has a set of valid syntax combinations. However, using the auto-complete feature helps you to easily create valid queries.

2.2.1.3. Search Criteria

You can specify the search criteria after the colon in the query. The syntax of **{criteria}** is as follows:

```
<prop> <operator> <value>
```

or

```
<obj-type>.<prop> <operator> <value>
```

Examples

The following table describes the parts of the syntax:

Table 2.3. Example Search Criteria

Part	Description	Values	Example	Note
prop	The property of the searched-for resource. Can also be the property of a resource type (see **obj-type**), or *tag* (custom tag).	See the information for each of the search types in Section 2.2.1.3.1, "Wildcards and Multiple Criteria".	Status	--
obj-type	A resource type that can be associated with the searched-for resource.	See the explanation of each of the search types in Section 2.2.1.3.1, "Wildcards and Multiple Criteria".	Users	--
operator	Comparison operators.	= != (not equal) > < >= <=	--	Value options depend on obj-type.

Part	Description	Values	Example	Note
Value	What the expression is being compared to.	String Integer Ranking Date (formatted according to regional settings)	Jones 256 normal	▸ Wildcards can be used within strings. ▸ "" (two sets of quotation marks with no space between them) can be used to represent an un-initialized (empty) string. ▸ Double quotation marks should be used around a string or date that contains spaces.

2.2.1.3.1. Wildcards and Multiple Criteria

Wildcards can be used in the **<value>** part of the syntax for strings. For example, to find all users beginning with **m**, enter **m***.

You can perform a search with two criteria by using the Boolean operators **AND** and **OR**. For example:

```
Volumes: name = m* AND status = Up
```

This query returns all volumes whose names begin with "m".

When two criteria are specified without **AND** or **OR**, **AND** is implied. **AND** precedes **OR**, and **OR** precedes implied **AND**.

2.2.1.4. Determining Sort Order

You can determine the sort order of the returned information by using **sortby**. Sort direction (**asc** for ascending, **desc** for descending) can be included.

For example:

```
events: severity > normal sortby time desc
```

This query returns all events whose severity is higher than Normal, sorted by time (descending order).

2.2.2. Saving and Accessing Queries as Bookmarks

Search queries can be saved as bookmarks. This allows you to sort and display results lists with a single click. You can save, edit and remove bookmarks with the Bookmarks pane.

2.2.2.1. Creating Bookmarks

Bookmarks can be created for any type of available search, using a number of criteria.

Procedure 2.1. Saving a query string as a bookmark

1. Enter the search query in the **Search** bar (see Section 2.2.1, “Search Syntax”).
2. Click the star-shaped **Bookmark** button to the right of the **Search** bar.

   The **New Bookmark** dialog box displays. The query displays in the **Search String** field. You can edit it if required.
3. Specify a descriptive name for the search query in **Name**.
4. Click **OK** to save the query as a bookmark.
5. The search query is saved and displays in the **Bookmarks** pane.

2.2.2.2. Editing Bookmarks

Bookmarks can be edited for any type of available search, using an existing bookmark.

Procedure 2.2. Editing a bookmark

1. Select the **Bookmark** pane by clicking the **Bookmarks** tab on the far left side of the screen.
2. Select a bookmark from the **Bookmark** pane.
3. The results list displays the items according to the criteria. Click the **Edit** button on the **Bookmark** pane.

   The **Edit Bookmark** dialog box displays. The query displays in the **Search String** field. Edit the search string to your requirements.
4. Change **Name** and **Search String** as necessary.
5. Click **OK** to save the edited bookmark.

2.2.2.3. Deleting Bookmarks

Bookmarks can be deleted.

Procedure 2.3. Deleting a bookmark

1. Select one or more bookmark from the **Bookmarks** pane.
2. The results list displays the items according to the criteria. Click the **Remove** button at the top of the **Bookmark** pane.

   The **Remove Bookmark** dialog box displays, prompting you to confirm your decision to remove the bookmark.
3. Click **OK** to remove the selected bookmarks.

2.3. Tags

After your Red Hat Storage is set up and configured to your requirements, you can customize the way you work with it using tags. Tags provide one key advantage to system administrators - they allow system resources to be arranged into groups or categories. This is useful when many objects exist in the storage environment and the administrator would like to concentrate on a specific set of them.

This section describes how to create and edit tags, assign them to hosts and search using the tags as criteria. Tags can be arranged in a hierarchy that matches a structure, to fit the requirements of the enterprise.

Administration Portal tags can be created, modified, and removed using the **Tags** pane.

Procedure 2.4. Creating a tag

1. In tree mode or flat mode, click the resource tab for which you wish to create a tag. For example, **Hosts**.
2. Click the **Tags** tab. Select the node under which you wish to create the tag. For example, click the root node to create it at the highest level. The **New** button is enabled.
3. Click **New** at the top of the **Tags** pane. The **New Tag** dialog box displays.
4. Enter the **Name** and **Description** of the new tag.
5. Click **OK**. The new tag is created and displays on the **Tags** tab.

Procedure 2.5. Modifying a tag

1. Click the **Tags** tab. Select the tag that you wish to modify. The buttons on the **Tags** tab are enabled.
2. Click **Edit** on the **Tags** pane. The **Edit Tag** dialog box displays.
3. You can change the **Name** and **Description** of the tag.
4. Click **OK**. The changes in the tag display on the **Tags** tab.

Procedure 2.6. Deleting a tag

1. Click the **Tags** tab. The list of tags will display.
2. Select the tags to be deleted and click **Remove**. The **Remove Tag(s)** dialog box displays.
3. The tags are displayed in the dialog box. Check that you are sure about the removal. The message warns you that removing the tags will also remove all descendants of the tags.
4. Click **OK**. The tags are removed and no longer display on the **Tags** tab. The tags are also removed from all the objects to which they were attached.

Tags can be attached to hosts and users.

Procedure 2.7. Adding or removing a tag to or from one or more object instances

1. Search for the objects that you wish to tag or untag so that they are among the objects displayed in the results list.
2. Select one or more objects on the results list.
3. Click the **Assign Tags** button on the tool bar or right-click menu option.

4. A dialog box provides a list of tags. Select the check box to assign a tag to the object, or deselect the check box to detach the tag from the object.

5. Click **OK**. The specified tag is now added or removed as a custom property of the selected objects.

A user-defined tag can be a property of any object (for example, a host), and a search can be conducted to find it.

To search for objects using tags:

- Follow the search instructions in Section 2.2, “Search” , and enter a search query using “tag” as the property and the desired value or set of values as criteria for the search.

  The objects tagged with the tag criteria that you specified are listed in the results list.

Part II. Managing System Components

Chapter 3. Managing Clusters

The cluster is the highest level entity for all physical and logical resources within a storage environment. This chapter describes how to create and manage clusters.

3.1. Cluster Properties

Use the **Clusters** tab in the Administration Portal to define, manage, and view clusters.

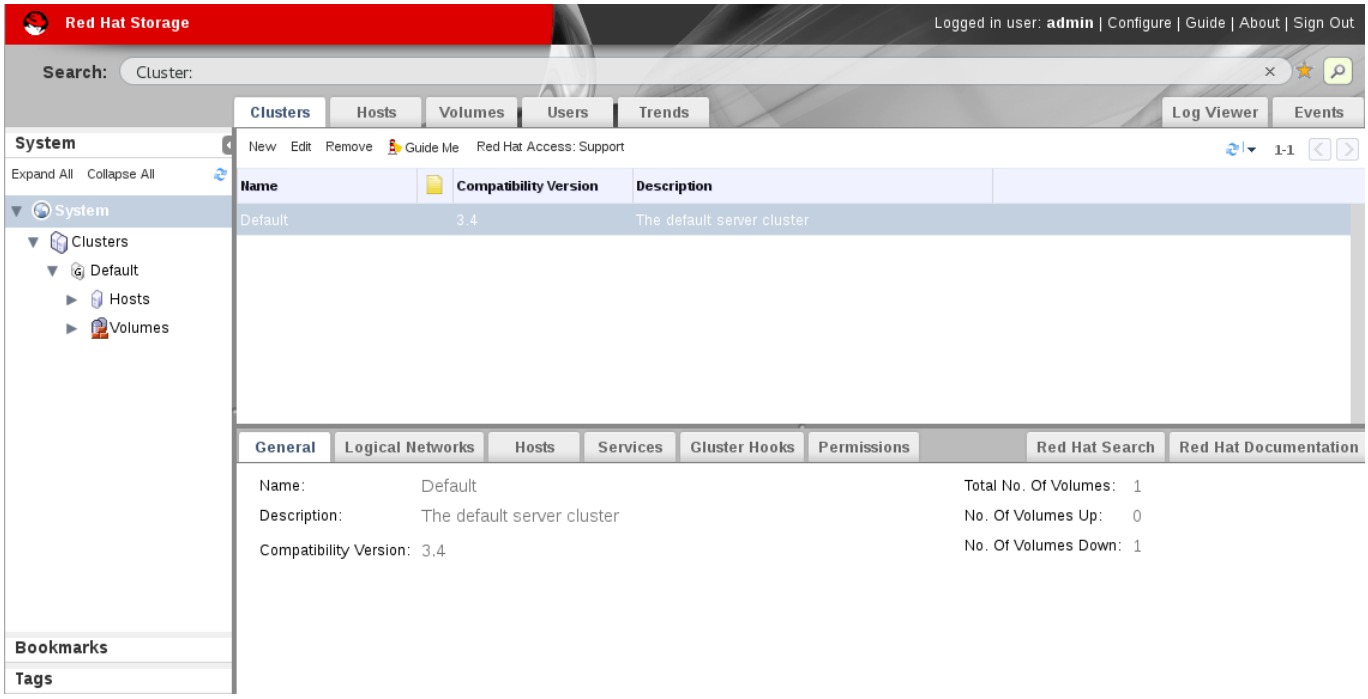


Figure 3.1. Clusters Tab

The following table describes the cluster properties displayed in the **New Cluster** and **Edit Cluster** dialog boxes. Missing mandatory fields and invalid entries are outlined in red when you click **OK** to close the **New Cluster** or **Edit Cluster** dialog box.

Table 3.1. Cluster Properties

Field	Description
Name	The name of the cluster. This must be a unique name and may use any combination of uppercase or lowercase letters, numbers, hyphens and underscores. Maximum length is 40 characters. The name can start with a number and this field is mandatory.
Description	The description of the cluster. This field is optional, but recommended.

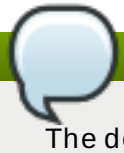
Field	Description
Compatibility Version	The version of Red Hat Storage Console with which the cluster is compatible. All hosts in the cluster must support the indicated version. - Clusters with compatibility version 3.2 can manage Red Hat Storage 2.1 nodes. - Clusters with compatibility version 3.3 can manage Red Hat Storage 2.1 Update 2 nodes. - Clusters with compatibility version 3.4 can manage Red Hat Storage 3.0 nodes.  **Note** The default compatibility version is 3.4.

Table 3.2. Compatibility Matrix

Feature	Compatibility Version 3.2	Compatibility Version 3.3	Compatibility Version 3.4
View advanced details of a particular brick of the volume through the Red Hat Storage Console.	Supported	Supported	Supported
Synchronize brick status with the engine database.	Supported	Supported	Supported
Manage glusterFS hooks through the Red Hat Storage Console. View the list of hooks available in the hosts, view the contents and status of hooks, enable or disable hooks, and resolve hook conflicts.	Supported	Supported	Supported
Display **Services** tab with NFS and SHD service status.	Supported	Supported	Supported
Manage volume rebalance through the Red Hat Storage Console. Rebalance volume, stop rebalance, and view rebalance status.	Not Supported	Supported	Supported
Manage remove-brick operations through the Red Hat Storage Console. Remove-brick, stop remove-brick, view remove-brick status, and retain the brick being removed.	Not Supported	Supported	Supported
Allow using system's root partition for bricks and and re-using the bricks by clearing the extended attributes.	Not Supported	Supported	Supported
Addition of RHS U2 nodes	Not Supported	Supported	Supported
Viewing Nagios Monitoring Trends	Not Supported	Not Supported	Supported

3.2. Cluster Operations

3.2.1. Creating a New Cluster

You can create a new cluster using the **New** option in the **Clusters** tab.

Procedure 3.1. To Create a New Cluster

1. Open the **Clusters** view by expanding the **System** tab and selecting the **Cluster** tab in the **Tree** pane. Alternatively, select **Clusters** from the **Details** pane.
2. Click **New** to open the **New Cluster** dialog box.

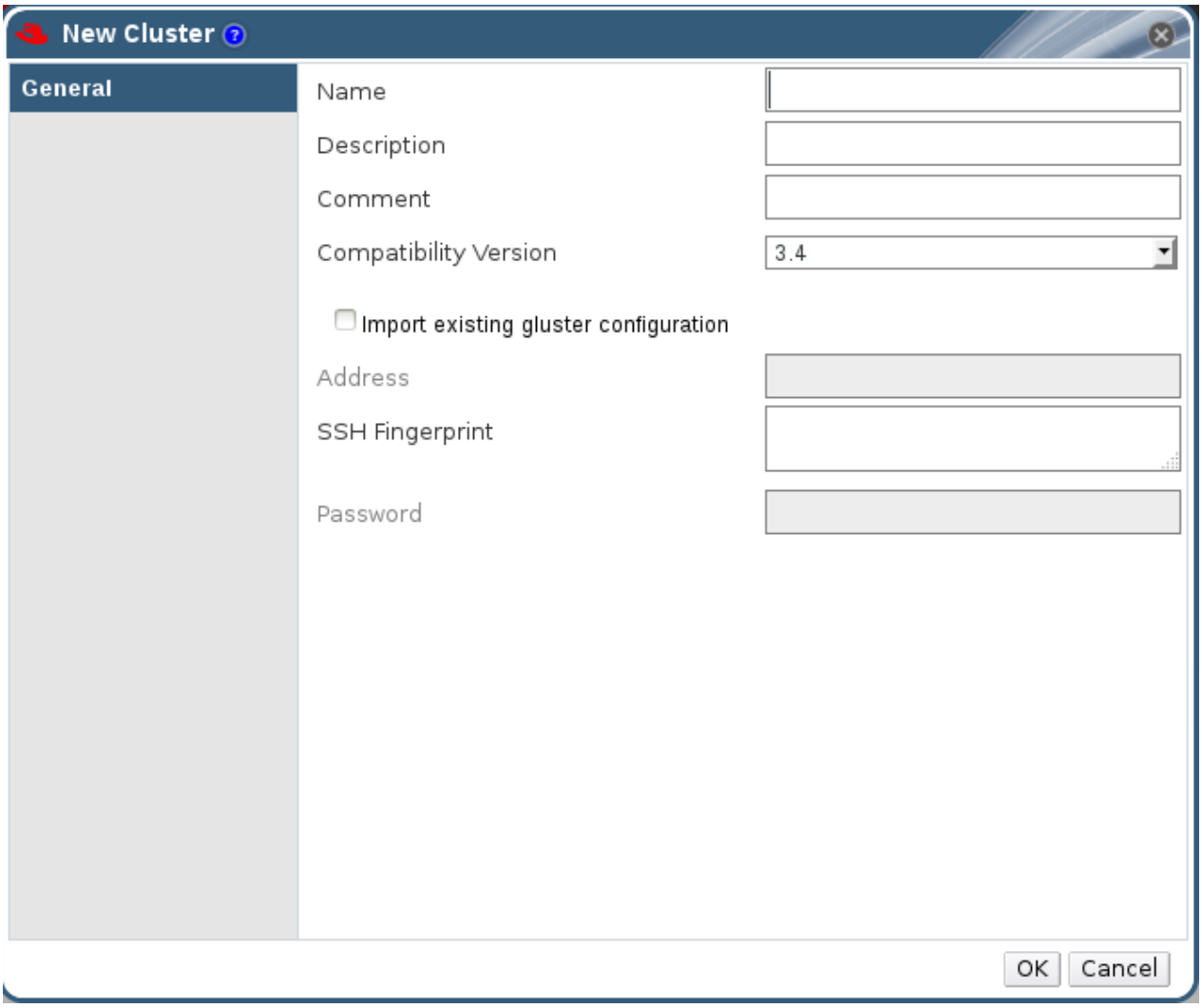


Figure 3.2. New Cluster Dialog Box

3. Enter the cluster **Name**, **Description** and **Compatibility Version**. The name cannot include spaces.
4. Click **OK** to create the cluster. The new cluster displays in the **Clusters** tab.
5. Click **Guide Me** to configure the cluster. The **Guide Me** window lists the entities you need to configure for the cluster. Configure these entities or postpone configuration by clicking **Configure Later**. You can resume the configuration process by selecting the cluster and clicking **Guide Me**. To import an existing cluster, see Section 3.2.2, “Importing an Existing Cluster”.

3.2.2. Importing an Existing Cluster

You can import a Red Hat Storage cluster and all the hosts belonging to the cluster into the Red Hat Storage Console.

When you provide details such as the IP address or host name and password of any host in the cluster, the gluster **peer status** command executes on that host through SSH, then displays a list of hosts that are part of the cluster. You must manually verify the fingerprint of each host and provide passwords for them. If some hosts are not reachable, then import cluster will not add these hosts to the cluster during import.

Procedure 3.2. To Import an Existing Cluster

1. In the **Tree** pane, click **System** tab, then click the **Clusters** tab.
2. Click **New** to open the **New Cluster** dialog box.
3. Enter the cluster **Name**, **Description** and **Compatibility Version**. The name cannot include spaces.
4. Select **Import existing gluster configuration** to import the cluster.
5. In the **Address** field, enter the host name or IP address of a host in the cluster.

   The host **Fingerprint** displays to indicate the connection host. If a host in unreachable or if there is a network error, **Error in fetching fingerprint** displays in the **Fingerprint** field.
6. Enter the **Root Password** for the host in the **Password** field and click **OK**.
7. The **Add Hosts** window opens, and a list of hosts that are part of the cluster displays.
8. For each host, enter the **Name** and **Root Password**. If you wish to use the same password for all hosts, check **Use a common password** and enter a password.
9. Click **Apply** to set the password for all hosts then click **OK** to submit the changes.

3.2.3. Editing a Cluster

Procedure 3.3. To Edit a Cluster

1. Click the **Clusters** tab to display the list of host clusters. Select the cluster that you want to edit.
2. Click **Edit** to open the **Edit Cluster** dialog box.
3. Enter a **Name** and **Description** for the cluster and select the compatibility version from the **Compatibility Version** drop down list.
4. Click **OK** to confirm the changes and display the host cluster details.

3.2.4. Viewing Hosts in a Cluster

Procedure 3.4. To View Hosts in a Cluster

1. Click the **Clusters** tab to display a list of host clusters. Select the desired cluster to display the **Details** pane.

2. Click the **Hosts** tab to display a list of hosts.

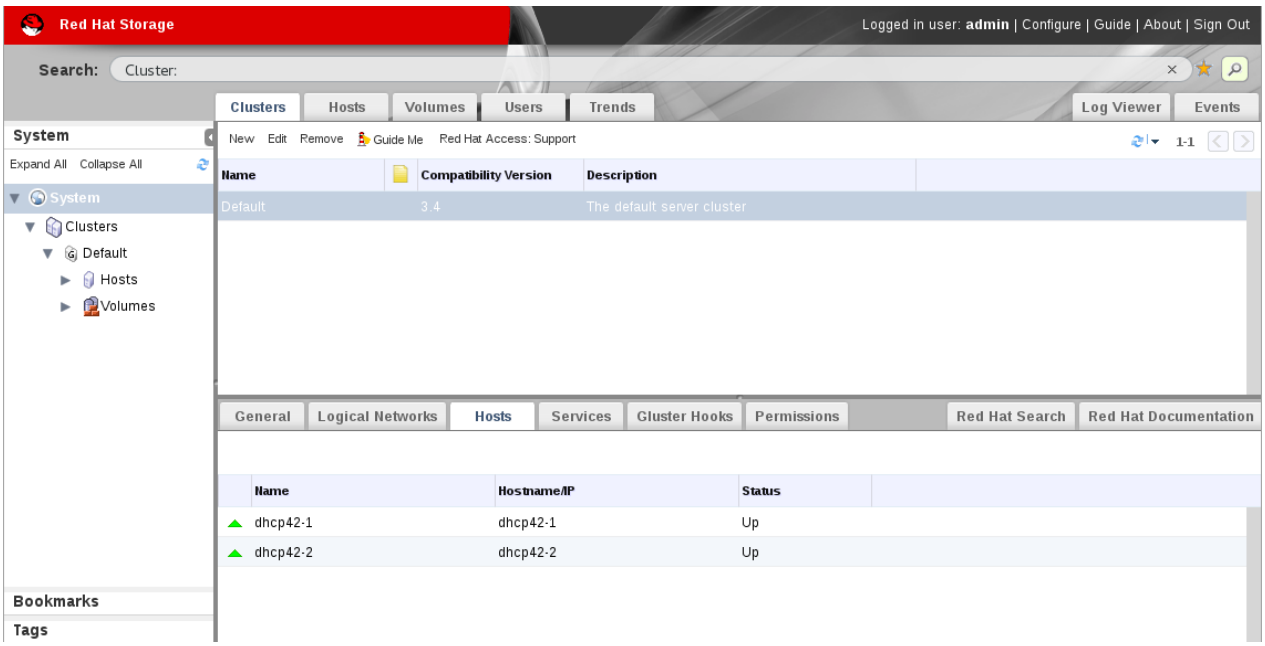


Figure 3.3. The Hosts tab on the Cluster Details pane

3.2.5. Removing a Cluster

You can permanently remove clusters that are not in use. Deleting unused clusters saves system resources, as existing hosts are contacted at regular intervals.

Warning

Red Hat recommends that you do not remove the default cluster.

Procedure 3.5. To Remove a Cluster

1. Click the **Clusters** tab to display a list of clusters. If the required cluster is not visible, perform a search.
2. Select the cluster to be removed. Ensure that there are no running hosts or volumes.
3. Click the **Remove** button.
4. A dialog box lists all the clusters selected for removal. Click **OK** to confirm the removal.

3.3. Cluster Entities

You can configure cluster entities using the Console.

Cluster Entities

A cluster is a collection of hosts. The **Hosts** tab displays all information related to the hosts in a cluster.

Table 3.3. Host Tab Properties

Field	Description
Name	The name of the host.
Hostname/IP	The name of the host/IP address.
Status	The status of the host.

Cluster Logical Networks Entities

Logical networks enable hosts to communicate with other hosts, and for the Console to communicate with cluster entities. You must define logical networks for each cluster.

Table 3.4. Cluster Logical Networks Tab Properties

Field	Description
Name	The name of the logical networks in a cluster.
Status	The status of the logical networks.
Role	The hierarchical permissions available to the logical network.
Description	The description of the logical networks.

Cluster Permissions Entities

Cluster permissions define which users and roles can work in a cluster, and what operations the users and roles can perform.

Table 3.5. Cluster Permissions Tab Properties

Field	Description
User	The user name of an existing user in the directory services.
Role	The role of the user. The role comprises of user, permission level and object. Roles can be default or customized roles.
Inherited Permissions	The hierarchical permissions available to the user.

Gluster Hooks

Gluster Hooks are volume lifecycle extensions. You can manage the Gluster Hooks from Red Hat Storage Console.

Table 3.6. Gluster Hooks Tab Properties

Field	Description
Name	The name of the hook.
Volume Event	Events are instances in the execution of volume commands like create, start, stop, add-brick, remove-brick, set and so on. Each of the volume commands have two instances during their execution, namely Pre and Post. Pre and Post refers to the time just before and after the corresponding volume command has taken effect on a peer respectively.
Stage	When the event should be executed. For example, if the event is *Start Volume* and the *Stage* is *Post*, the hook will be executed after the start of the volume.
Status	Status of the gluster hook.
Content Type	Content type of the gluster hook.

Field	Description

Services

The service running on a host can be searched using the *Services* tab.

Table 3.7. Services Tab Properties

Field	Description
Host	The ip of the host.
Service	The name of the service.
Port	The port number of the host.
Status	The status of the host.
Process Id	The process id of the host.

3.4. Cluster Permissions

A cluster administrator has system administrator permissions for a specific cluster only. This is a hierarchical model, which means that a user assigned the cluster administrator role for a cluster can manage all objects in that cluster. The cluster administrator role permits the following actions:

- Creation and removal of specific clusters.
- Addition and removal of hosts.
- Permission to attach users to hosts within a single cluster.

This is useful when there are multiple clusters, each of which require their own system administrators. A cluster administrator has permissions for the assigned cluster only, not for all clusters.

Note

You can only assign roles and permissions to existing users.

Procedure 3.6. To Add a Cluster Administrator Role

1. Click the **Clusters** tab to display the list of clusters. If the required cluster is not visible, perform a search.
2. Select the cluster that you want to edit. Click the **Permissions** tab in the **Details** pane to display a list of existing users and their current roles and inherited permissions.
3. Click **Add** to display the **Add Permission to User** dialog box. Enter all or part of a name or user name in the **Search** box, then click **Go**. A list of possible matches displays in the results list.
4. Select the user you want to modify. Scroll through the **Role to Assign** list and select **ClusterAdmin**.
5. Click **OK** to display the name of the user and their assigned role in the **Permissions** tab.

Procedure 3.7. To Remove a Cluster Administrator Role

1. Click the **Clusters** tab to display a list of clusters. If the required cluster is not visible, perform a search.
2. Select the cluster that you want to edit. Click the **Permissions** tab in the **Details** pane to display a list of existing users and their current roles and inherited permissions.
3. Select the user you want to modify and click **Remove**. This removes the user from the **Permissions** tab and from associated hosts and volumes.

Chapter 4. Managing Red Hat Storage Hosts

A host is a physical, 64-bit server with an Intel or AMD chipset running Red Hat Storage 3. You can add new hosts to a storage cluster to expand the amount of available storage.

A host on the Red Hat Storage:

- Must belong to only one cluster in the system.
- Can have an assigned system administrator with system permissions.

Important

Red Hat Storage Console uses various network ports for management. These ports must be open on Red Hat Storage hosts. For a full list of ports, see the *Red Hat Storage Console Installation Guide*.

4.1. Hosts Properties

The **Hosts** tab provides a graphical view of all the hosts in the system.

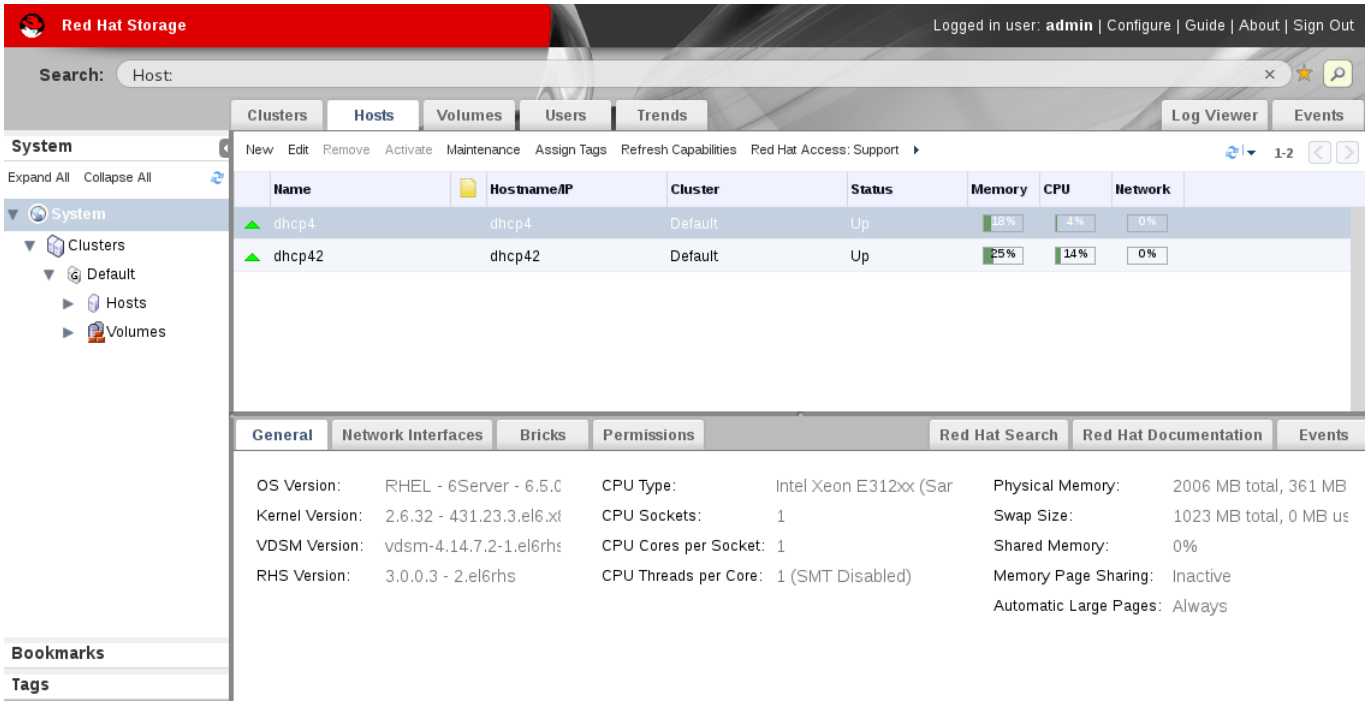


Figure 4.1. Hosts Details Pane

Table 4.1. Hosts Properties

Field	Description
Cluster	The selected cluster.
Name	The host name.
Address	The IP address or resolvable hostname of the host.

4.2. Hosts Operations

4.2.1. Adding Hosts

You must install hosts and configure them with a name and IP address before you can add them to the Red Hat Storage Console.

Important

If you re-install the Red Hat Storage Console, you must remove all hosts and reconnect them with the correct SSH keys for the new installation of Red Hat Storage Console.

Prerequisites

Before you can add a host to Red Hat Storage, ensure your environment meets the following criteria:

- The host hardware is Red Hat Enterprise Linux certified. See https://hardware.redhat.com/ to confirm that the host has Red Hat certification.
- The host should have a resolvable hostname or static IP address.

Procedure 4.1. To Add a Host

Before adding a host, ensure you have the correct IP and password for the host. The process of adding a new host can take some time; you can follow its progress in the **Events** pane.

1. Click the **Hosts** tab to list available hosts.
2. Click **New** to open the **New Host** window.

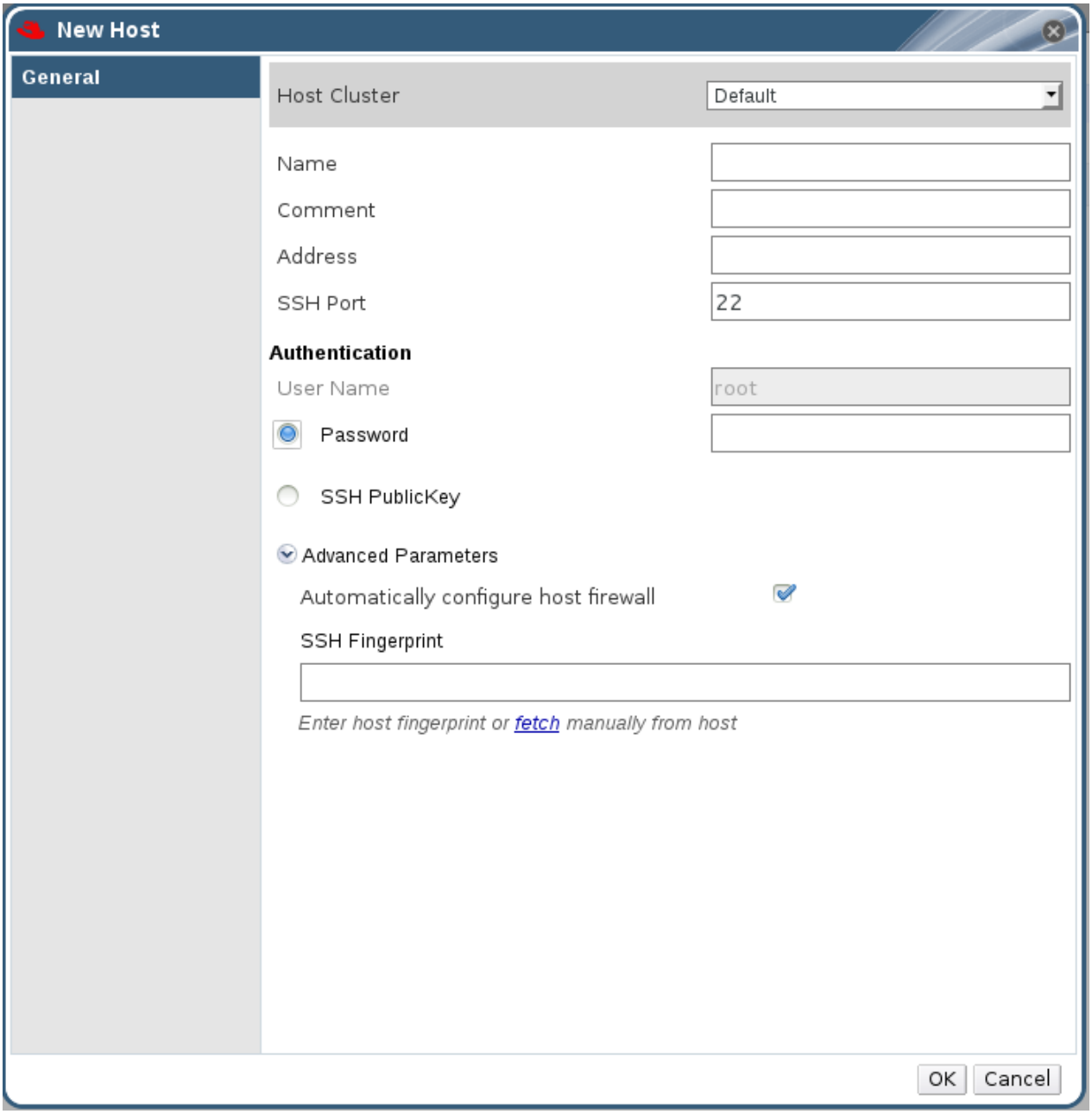


Figure 4.2. New Host Window

3. Select the **Host Cluster** for the new host from the drop-down menu.

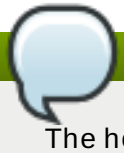
Table 4.2. Add Hosts Properties

Field	Description
Host Cluster	The cluster to which the host belongs.
Name	The name of the host. This text field has a 40-character limit and must be a unique name with any combination of uppercase and lowercase letters, numbers, hyphens, and underscores. If Nagios is enabled, the host name given in **Name** field of **Add Host** window should match the host name given while configuring Nagios.
Address	The IP address or resolvable hostname of the host.

Field	Description
Root Password	The password of the host's root user. This can only be given when you add the host, it cannot be edited afterwards.
SSH Public Key	Copy the contents in the text box to the */root/.ssh/authorized_keys* file on the host if you'd like to use the Manager's ssh key instead of using a password to authenticate with the host.
Automatically configure host firewall	When adding a new host, the Manager can open the required ports on the host's firewall. This is enabled by default. This is an Advanced Parameter. The required ports are opened if this option is selected.
SSH Fingerprint	You can fetch the host's ssh fingerprint, and compare it with the fingerprint you expect the host to return, ensuring that they match. This is an Advanced Parameter.

4. Enter the **Name**, and **Address** of the new host.
5. Select an authentication method to use with the host:
    a. Enter the root user's password to use password authentication.
    b. Copy the key displayed in the **SSH PublicKey** field to **/root/.ssh/authorized_keys** on the host to use public key authentication.
6. The mandatory steps for adding a Red Hat Storage host are complete. Click **Advanced Parameters** to show the advanced host settings:
    a. Optionally disable automatic firewall configuration.
    b. Optionally add a host SSH fingerprint to increase security. You can add it manually, or fetch it automatically.
7. Click **OK** to add the host and close the window.

    The new host displays in the list of hosts with a status of "Installing" and then it goes to "Initialization" state and the host comes up.



Note

The host will be in *Up* status after the status of "Installing" and "Initialization" state. The host will have *Non-Operational* status when the host is not compatible with the cluster compatibility version. The *Non-Responsive* status will be displayed if the host is down or is unreachable.

You can view the progress of the host installation in the **Details** pane.

4.2.2. Activating Hosts

After taking down a host for maintenance, you must reactivate it before using it. When you activate a host, the host's networks are checked and the check if the glusterd is operational is also performed.

Procedure 4.2. To Activate a Host

1. In the **Hosts** tab, select the host you want to activate.
2. Click **Activate**. The host status changes to **Up**.

4.2.3. Managing Host Network Interfaces

The **Network Interfaces** tab in a host's **Details** pane enables you to attach a logical network in the Administration Portal to a host's physical network interface cards.

The management and storage subnets are defined by default in the cluster. Typically, **eth0** is allocated to the management network interface and **eth1** is allocated to the storage network interface, which may display as data. The Administration Portal automatically detects attached subnets and networks, but you must manually match each logical network name to the correct subnet.

Each host can support up to 32 interfaces, and groups these by logical networks. If the default settings are not correct, or you need to add more subnets, use the **Network Interfaces** tab to make changes.

Note

You cannot define new logical networks at the host level.

4.2.3.1. Editing Host Network Interfaces

The **Network Interfaces** tab displays the name, network name, address, MAC address, speed, and link status for each interface. It also provides several options for managing host network interface cards.

Procedure 4.3. To Edit a Host Network Interface

1. Click the **Hosts** tab to display a list of hosts. Select the desired host to display the **Details** pane.
2. Click **Setup Host Networks** to open the **Setup Host Networks** window.

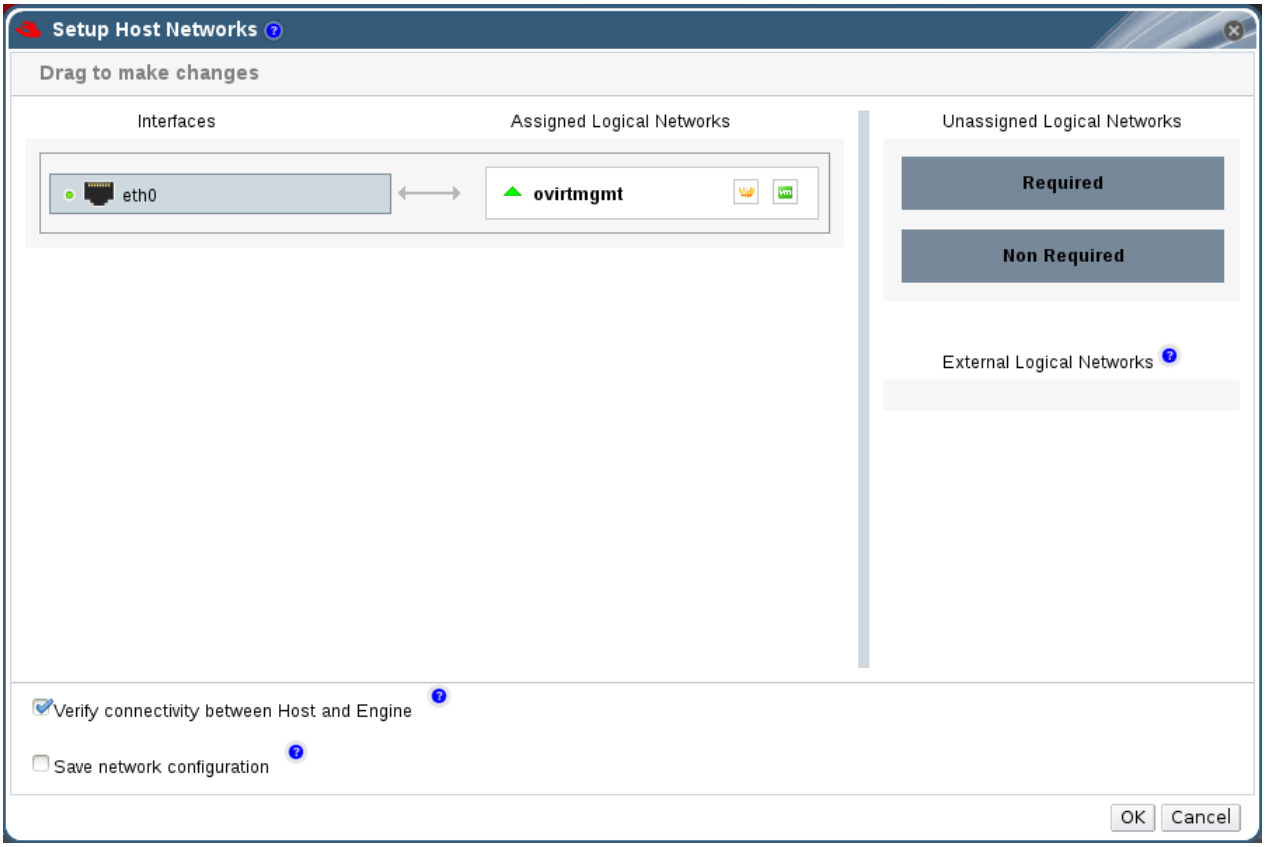


Figure 4.3. Setup Host Networks Window

3. Attach a logical network to a network interface by selecting and dragging the logical network into the **Assigned Logical Networks** area next to the network interface. Alternatively, right-click the logical network and select a network interface from the drop-down menu.
4. Edit the logical networks by hovering over an assigned logical network and clicking the pencil icon to open the **Edit Management Network** window.
5. If your logical network definition is not synchronized with the network configuration on the host, select the **Sync network** check box.
6. Select a **Boot Protocol**:
   - **None**
   - **DHCP**
   - **Static** - provide the **IP** and **Subnet Mask**.
7. Click **OK**.
8. Select **Verify connectivity between Host and Engine** to run a network check.
9. Select **Save network configuration** if you want the network changes to be persistent when you reboot the environment.
10. Click **OK** to implement the changes and close the window.

4.2.3.2. Editing Management Network Interfaces

The **Network Interfaces** tab displays the name, network name, address, MAC address, speed, and link status for each interface. In the course of editing the host network interface cards, you may need to check or edit the management network interface.

Important

Clusters and hosts communicate through the management interface. Changing the properties of the management interface can cause the host to become unreachable.

Procedure 4.4. To Edit a Management Network Interface

1. Click the **Hosts** tab to display a list of hosts. Select the desired host to display the **Details** pane.
2. Edit the logical networks by hovering over an assigned logical network and clicking the pencil icon to open the **Edit Management Network** window.

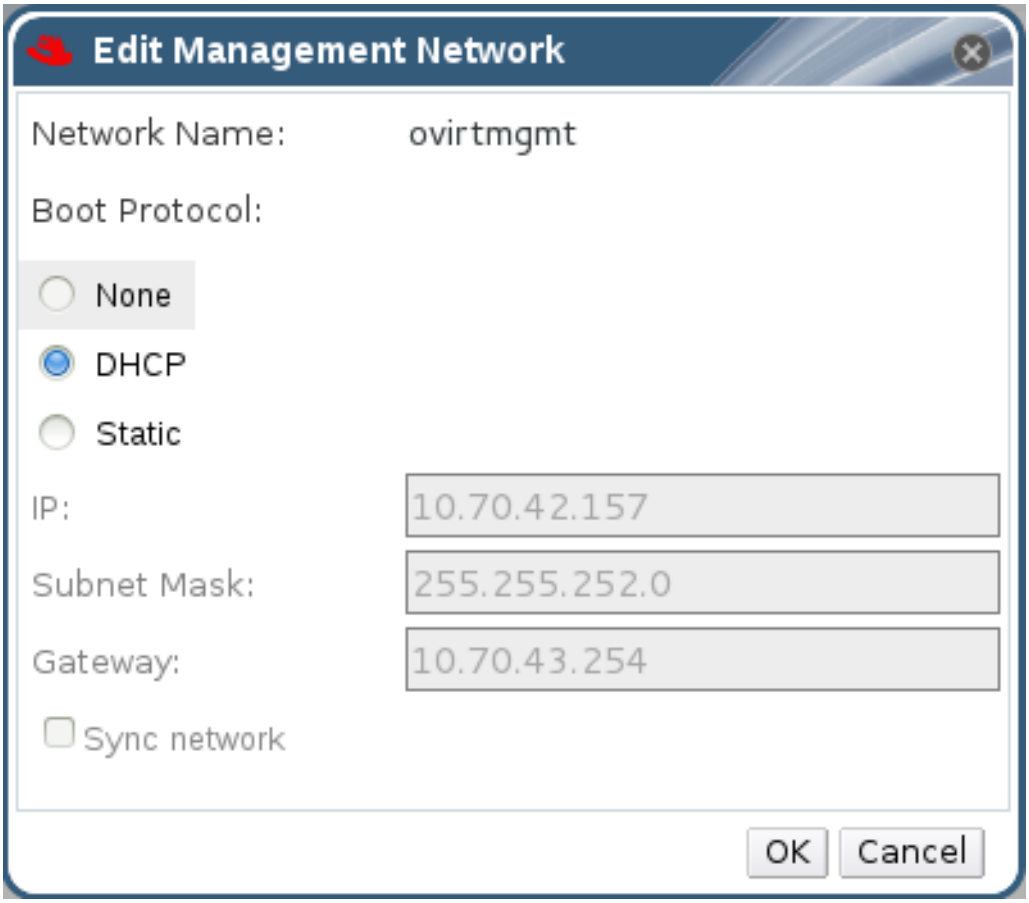


Figure 4.4. Edit Management Network Dialog Box

3. If your logical network definition is not synchronized with the network configuration on the host, select the **Sync network** check box.
4. Select a **Boot Protocol**:
   - **None**
   - **DHCP**

- **Static** - provide the **IP** and **Subnet Mask**.

5. Make the required changes to the management network interface:

    a. To attach the **ovirtmgmt** management network to a different network interface card, select a different interface from the **Interface** drop-down list.

    b. Select the network setting from **None**, **DHCP** or **Static**. For the **Static** setting, provide the IP, Subnet and Default Gateway information for the host.

    c. Click **OK** to confirm the changes.

    d. Select **Verify connectivity between host and engine** if required.

    e. Select **Save network configuration** to make the changes persistent when you reboot the environment.

6. Click **OK**.

7. Activate the host. See Section 4.2.2, “Activating Hosts”.

4.2.4. Configuring Network Interfaces

After connecting physical network interface cards to logical networks, you can perform further configuration. For example, you can aggregate links, separate bonded links, or detach network interface cards from the network. Before performing these actions, Red Hat recommends you save the current network configuration.

4.2.4.1. Saving Host Network Configurations

After connecting physical network interface cards to logical networks, you can perform further configurations. Before performing the configurations, Red Hat recommends you save the current network configuration.

After correctly configuring the network, Red Hat recommends you save the network configuration.

Procedure 4.5. To Save a Host Network Configuration

1. Click the **Hosts** tab to display a list of hosts. Select the desired host to display the **Details** pane.

2. Click **Maintenance** to place the host into maintenance. Click **OK** to confirm the action. The **Status** field of the host changes to *Preparing for Maintenance*, followed by *Maintenance*. The icon changes to indicate that the host is in maintenance mode.

3. Click the **Network Interfaces** tab in the **Details** pane to display the list of network interface cards in the host, their addresses, and other specifications. Select the network interface card that you want to edit.

4. Click **Save Network Configuration** to save the host network configuration. The Events pane displays the message: **Network Changes were saved on Host *HOSTNAME***.

4.2.4.2. Deleting Hosts

You can permanently remove hosts that are not in use. Deleting unused hosts saves system resources, as existing hosts are contacted at regular intervals.

Note

You can not remove hosts if it has volumes in it. Removing a host will detach the host from the cluster.

Procedure 4.6. To Delete a Host

1. Click the **Hosts** tab to display a list of hosts. Select the host you want to remove. If the required host is not visible, perform a search.
2. Click **Maintenance** to place the host into maintenance. Click **OK** to confirm the action. The **Status** field of the host changes to *Preparing for Maintenance*, followed by *Maintenance*. The icon changes to indicate that the host is in maintenance mode.
3. Click **Remove**.
4. Click **OK** to confirm.

4.2.4.3. Managing Gluster Sync

Gluster Sync periodically fetches the latest cluster configuration from glusterFS and synchronizes it with the engine database. The Red Hat Storage Console continuously monitors storage clusters for the addition and removal of hosts. If a change is detected, an action item displays in the **Cluster** tab with the option to **Import** or **Detach** the host.

Procedure 4.7. To Import a Host to a Cluster

1. Click the **Cluster** tab and select a cluster to display the **General** tab with details of the cluster.
2. In **Action Items**, click **Import** to display the **Add Hosts** window.

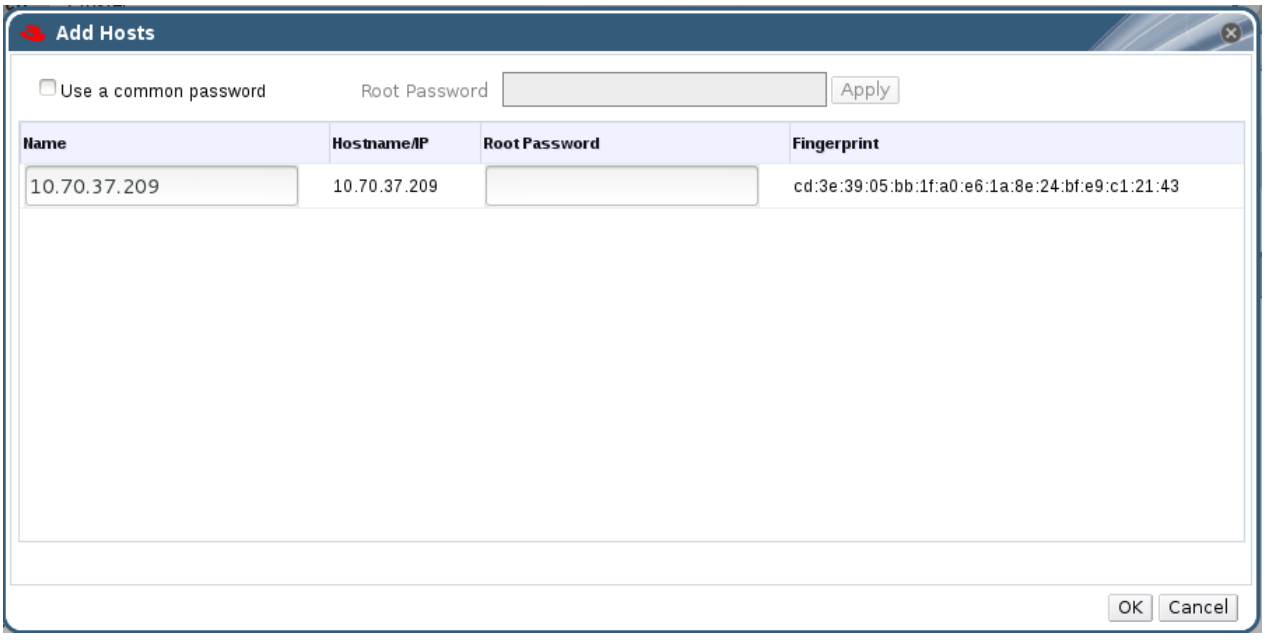


Figure 4.5. Add Hosts Window

3. Enter the **Name** and **Root Password**. Select **Use a common password** if you want to use the same password for all hosts.
4. Click **Apply**.
5. Click **OK** to add the host to the cluster.

Procedure 4.8. To Detach a Host from a Cluster

1. Click the **Cluster** tab and select a cluster to display the **General** tab with details of the cluster.
2. In **Action Items**, click **Detach** to display the **Detach Hosts** window.
3. Select the host you want to detach and click **OK**. Select **Force Detach** if you want to perform force removal of the host from the cluster.

4.3. Maintaining Hosts

You can use the Administration Portal to perform host maintenance tasks, for example changing the network configuration details of a host.

Warning

Editing a host may require shutting down and restarting the host. Plan ahead when performing maintenance actions.

4.3.1. Moving Hosts into Maintenance Mode

To perform certain actions, you need to move hosts into maintenance mode.

Procedure 4.9. To Move a Host into Maintenance Mode

1. Click the **Hosts** tab to display a list of hosts.
2. Click **Maintenance** to place the host into maintenance. Click **OK** to confirm the action. The **Status** field of the host changes to *Preparing for Maintenance*, followed by *Maintenance*. The icon changes to indicate that the host is in maintenance mode.
3. Perform required tasks. When you are ready to reactivate the host, click **Activate**.
4. After the host reactivates, the **Status** field of the host changes to *Up*. If the Red Hat Storage Console is unable to contact or control the host, the **Status** field displays *Non-responsive*.

4.3.2. Editing Host Details

You can edit the details of a host, such as its name, network configuration, and cluster.

Procedure 4.10. To Edit Host Details

1. Click the **Hosts** tab to display a list of hosts.

2. If you are moving the host to a different cluster, first place it in maintenance mode by clicking **Maintenance**. Click **OK** to confirm the action. The **Status** field of the host changes to *Preparing for Maintenance*, followed by *Maintenance*. The icon changes to indicate that the host is in maintenance mode.
3. Click **Edit** to open the **Edit Host** dialog box.
4. To move the host to a different cluster, select the cluster from the **Host Cluster** drop-down list.
5. Make the required edits and click **OK**. Activate the host to start using it. See Section 4.2.2, "Activating Hosts"

4.3.3. Customizing Hosts

You can assign tags to help you organize hosts. For example, you can create a group of hosts running in a department or location.

Note

You can assign tags to a host only if a tag is present. You can not assign the *root* tag to a host. To create a new tag, see Section 2.3, "Tags".

Procedure 4.11. To Tag a Host

1. Click the **Hosts** tab to display a list of hosts. Select the desired host to display the **Details** pane.
2. Click **Assign Tags** to open the **Assign Tags** dialog box.
3. Select the required tags and click **OK**.

4.4. Hosts Entities

4.4.1. Viewing General Host Information

The **General** tab on the **Details** pane provides information on individual hosts, including hardware and software versions, and available updates.

Procedure 4.12. To View General Host Information

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display general information, network interface information and host information in the **Details** pane.
3. Click **General** to display the following information:
   - Version information for OS, Kernel, VDSM, and RHS.
   - Status of memory page sharing (Active/Inactive) and automatic large pages (Always).

- CPU information: number of CPUs attached, CPU name and type, total physical memory allocated to the selected host, swap size, and shared memory.
- An alert if the host is in Non-Operational or Install-Failed state.

4.4.2. Viewing Network Interfaces on Hosts

The **Network Interfaces** tab on the **Details** pane provides information about the logical and physical networks on a host. This view enables you to define the attachment of the logical network in the Administration Portal to the physical network interface cards of the host. See Section 4.2.3, “Managing Host Network Interfaces” for more information on network interfaces.

Procedure 4.13. To View Network Interfaces on a Host

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Network Interfaces** tab.

4.4.3. Viewing Permissions on Hosts

The **Permissions** tab on the **Details** pane provides information about user roles and their inherited permissions.

Procedure 4.14. To View Permissions on a Host

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Permissions** tab.

4.4.4. Viewing Bricks from a Host

The **Events** tab on the **Details** pane provides information about important events such as notifications and errors.

Procedure 4.15. To View Bricks from a Host

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Events** tab.

4.4.5. Viewing Bricks

The **Bricks** tab on the **Details** pane provides information about the bricks as the volume name and the brick directory.

Procedure 4.16. To View Bricks on a Host

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Bricks** tab.

4.5. Hosts Permissions

A host administrator has system administrator permissions for a specific host only. This role is useful when there are multiple hosts, each of which require their own system administrators. A host administrator has permissions for the assigned host only, not for all hosts in the cluster.

Note

You can only assign roles and permissions to existing users.

Procedure 4.17. To Add a Host Administrator Role

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Permissions** tab to display a list of users and their current roles.

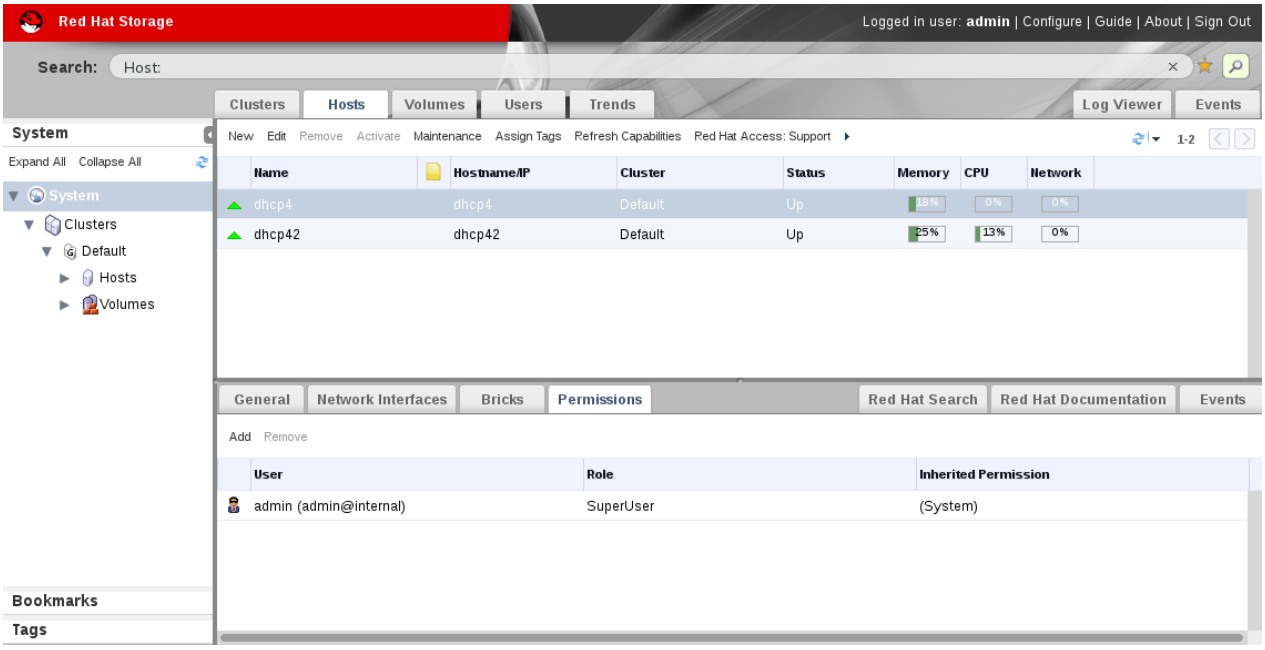


Figure 4.6. Host Permissions Window

4. Click **Add** to display the **Add Permission to User** dialog box. Enter all or part of a name or user name in the **Search** box, then click **Go**. A list of possible matches displays in the results list.
5. Select the user you want to modify. Scroll through the **Role to Assign** list and select **HostAdmin**.

6. Click **OK** to display the name of the user and their assigned role in the **Permissions** tab.

Procedure 4.18. To Remove a Host Administrator Role

1. Click the **Hosts** tab to display a list of hosts. If the required host is not visible, perform a search.
2. Select the desired host to display the **Details** pane.
3. Click the **Permissions** tab to display a list of users and their current roles.
4. Select the desired user and click **Remove**

Chapter 5. Managing Volumes

You can use the console to create and start new volumes featuring a single global namespace. A volume is a logical collection of bricks where each brick is an export directory on a host in the trusted storage pool. Most of the management operations of Red Hat Storage Console happen on the volume.

A volume is the designated unit of administration in Red Hat Storage, so managing them is a large part of the administrator's duties.

The console also enables you to monitor the volumes in your cluster from the **Volumes** tab. To display the volumes, click the **Volumes** node from the **Tree** pane of the console window. The list of volumes is displayed in the right pane of the console window. It also displays the tasks and events for all volumes.

This chapter describes how to manage volumes stored on storage host machines.

5.1. Creating a Volume

You can create new volumes in your storage environment. When creating a new volume, you must specify the bricks that comprise the volume and specify whether the volume is to be **Distribute**, **Replicate**, **Stripe**, **Distributed Replicate**, **Distributed Stripe**, **Striped Replicate**, or **Distributed Striped Replicate**.

Procedure 5.1. Creating a Volume

1. Click the **Volumes** tab. The **Volumes** tab lists all volumes in the system.
2. Click the **New**. The **New Volume** window is displayed.

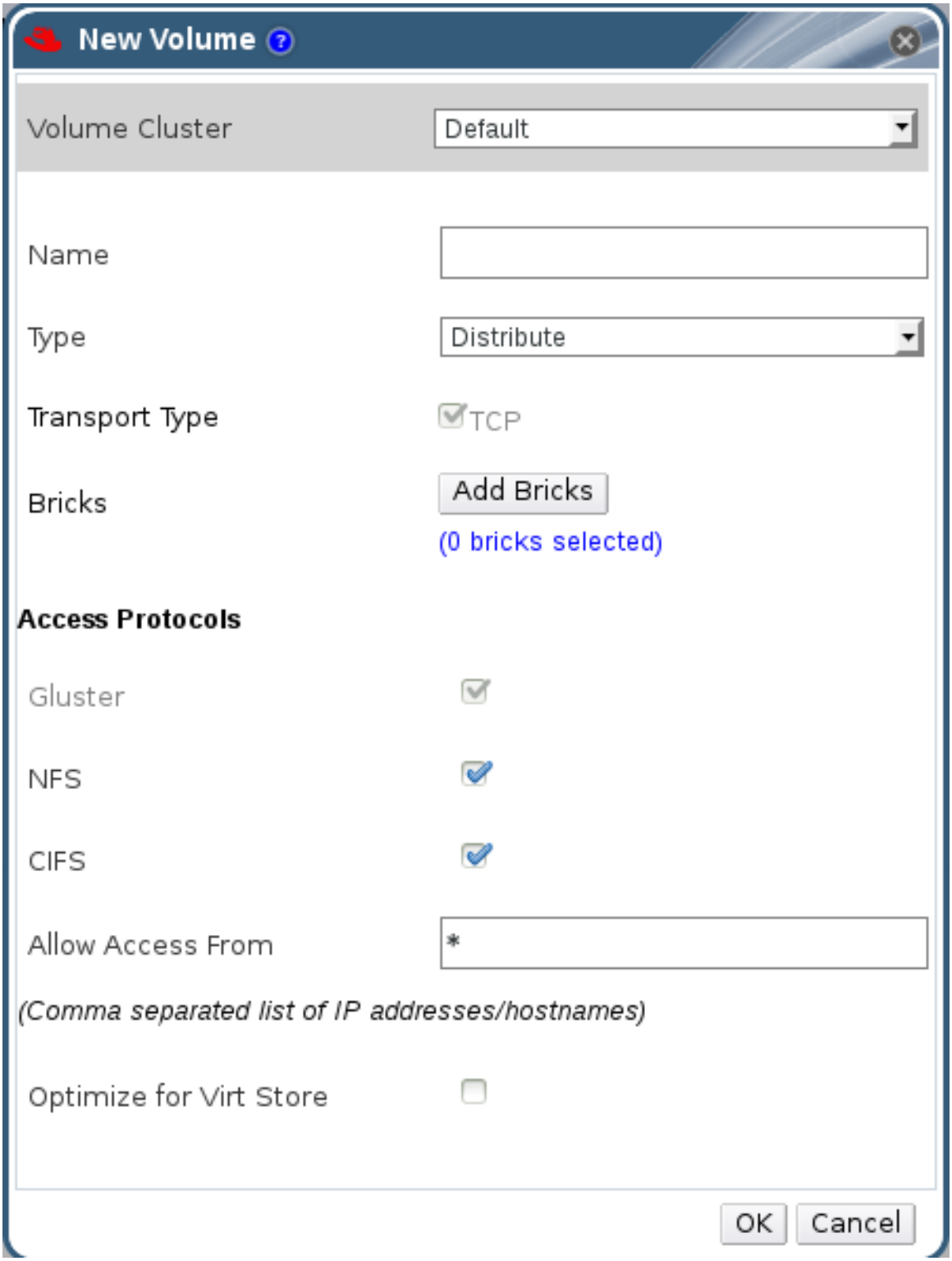
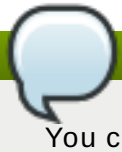


Figure 5.1. New Volume

3. Select the cluster from the **`Volume Cluster`** drop-down list.
4. In the **`Name`** field, enter the name of the volume.



Note

You can not create a volume with the name *volume*.

5. Select the type of the volume from the **Type** drop-down list. You can set the volume type to **Distribute**, **Replicate**, **Stripe**, **Distributed Replicate**, **Distributed Stripe**, **Striped Replicate**, or **Distributed Striped Replicate**.

Note

- The **Stripe**, **Distributed Stripe**, **Striped Replicate**, and **Distributed Striped Replicate** volume types are under technology preview. Technology Preview features are not fully supported under Red Hat subscription level agreements (SLAs), may not be functionally complete, and are not intended for production use. However, these features provide early access to upcoming product innovations, enabling customers to test functionality and provide feedback during the development process.
- Creating replicated volumes with replica count more than 2 is under technology preview.

6. As necessary, click **Add Bricks** to add bricks to your volume.

Note

At least one brick is required to create a volume. The number of bricks required depends on the type of the volume.

For more information on adding bricks to a volume, see Section 5.6.1, “Adding Bricks”.

7. Configure the **Access Protocol** for the new volume by selecting **NFS**, or **CIFS**, or both check boxes.

8. In the **Allow Access From** field, specify the volume access control as a comma-separated list of IP addresses or hostnames.

   You can use wildcards to specify ranges of addresses. For example, an asterisk (*) specifies all IP addresses or hostnames. You need to use IP-based authentication for Gluster Filesystem and NFS exports.

   You can optimize volumes for **virt-store** by selecting **Optimize for Virt Store**.

9. Click **OK** to create the volume. The new volume is added and displays on the **Volume** tab. The volume is configured, and **group** and **storage-owner-gid** options are set.

5.2. Starting Volumes

After a volume has been created or an existing volume has been stopped, it needs to be started before it can be used.

Procedure 5.2. Starting a Volume

1. In the **Volumes** tab, select the volume to be started.

   You can select multiple volumes to start by using the **Shift** or **Ctrl** key.

2. Click the **Start** button.

5.3. Configuring Volume Options

Perform the following steps to configure volume options.

Procedure 5.3. Configuring Volume Options

1. Click the **Volumes** tab.

   A list of volumes displays.

2. Select the volume to tune, and click the **Volume Options** tab from the **Details** pane.

   The **Volume Options** tab lists the options set for the volume.

3. Click **Add** to set an option. The **Add Option** window is displayed. Select the option key from the drop-down list and enter the option value.

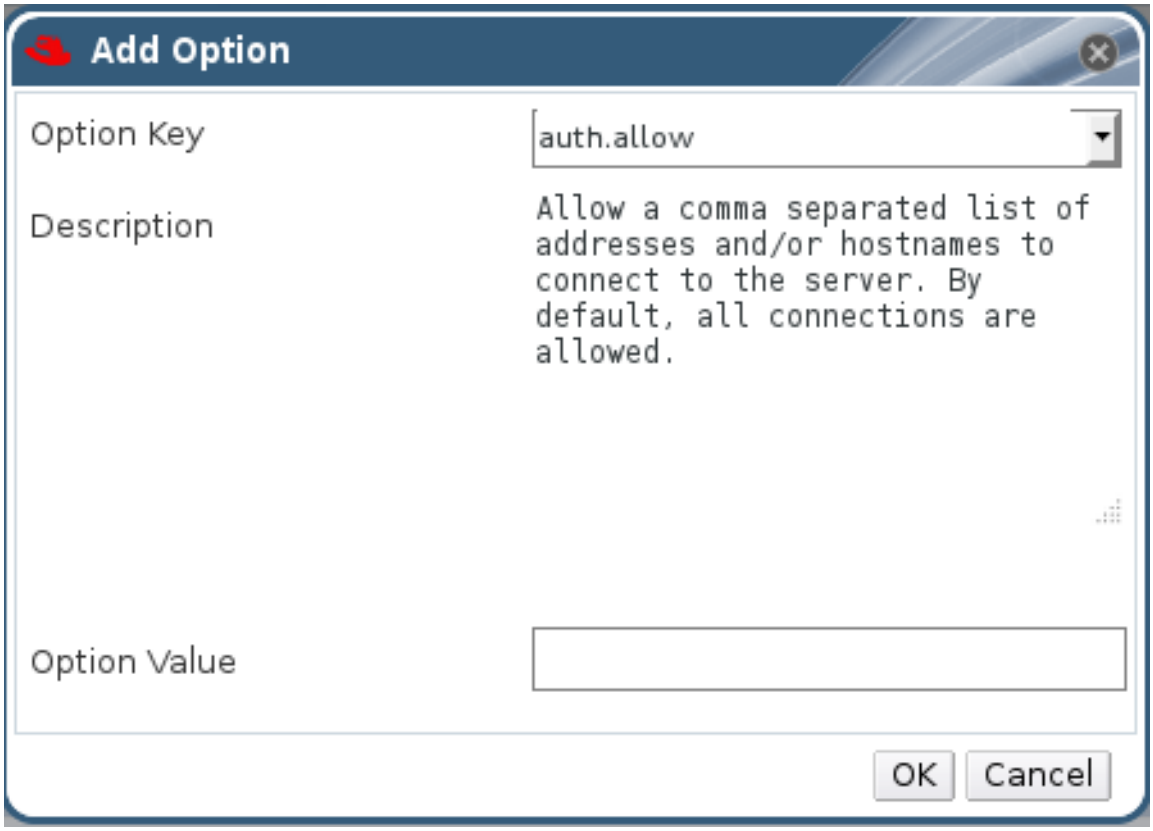


Figure 5.2. Add Option

4. Click **OK**.

   The option is set and displays in the **Volume Options** tab.

For more information about volume options, see *Tuning Volume Options* in *Red Hat Storage Administration Guide*.

5.3.1. Edit Volume Options

Procedure 5.4. Editing Volume Options

1. Click the **Volumes** tab.

A list of volumes displays.

2. Select the volume to edit, and click the **Volume Options** tab from the **Details** pane.

   The **Volume Options** tab lists the options set for the volume.

3. Select the option to edit. Click **Edit**. The **Edit Option** window is displayed. Enter a new value for the option in the **Option Value** field.

4. Click **OK**.

   The edited option displays in the **Volume Options** tab.

5.3.2. Resetting Volume Options

Procedure 5.5. Resetting Volume Options

1. Click the **Volumes** tab.

   A list of volumes is displayed.

2. Select the volume and click the **Volume Options** tab from the **Details** pane.

   The **Volume Options** tab lists the options set for the volume.

3. Select the option to reset. Click **Reset**. **Reset Option** window is displayed, prompting to confirm the reset.

4. Click **OK**.

   The selected option is reset. The name of the volume option reset is displayed in the **Events** tab.

Note

You can reset all volume options by clicking the **Reset All** button. A window is displayed, prompting to confirm the reset option. Click **OK**. All volume options are reset for the selected volume. A message that all volume options have been reset is displayed in the **Events** tab.

5.4. Stopping Volumes

After a volume has been started, it can be stopped.

Note

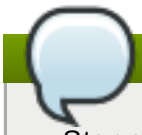
You cannot stop a volume if there are any async tasks such as Rebalance or Remove Brick which are in progress.

Procedure 5.6. Stopping a Volume

1. In the **Volumes** tab, select the volume to be stopped.

   You can select multiple volumes to stop by using the **Shift** or **Ctrl** key.

2. Click **Stop**. A window is displayed, prompting to confirm the stop.



Note

Stopping volume will make its data inaccessible.

3. Click **OK**.

5.5. Deleting Volumes

You can delete a volume or multiple volumes from your cluster.

Procedure 5.7. Deleting a Volume

1. In the **Volumes** tab, select the volume to be deleted.
2. Click **Stop**. The volume stops.
3. Click **Remove**. A window is displayed, prompting to confirm the deletion. Click **OK**. The volume is removed from the cluster.

5.6. Managing Bricks

A brick is the basic unit of storage, represented by an export directory on a host in the storage cluster. You can expand or shrink your cluster by adding new bricks or deleting existing bricks.

Note

When expanding distributed replicated or distributed striped volumes, the number of bricks being added must be a multiple of the replica or stripe count. For example, to expand a distributed replicated volume with a replica count of 2, you need to add bricks in multiples of 2 (such as 2, 4, 6, 8, etc.).

5.6.1. Adding Bricks

You can expand a volume by adding new bricks to an existing volume.

Procedure 5.8. Adding a Brick

1. Click the **Volumes** tab.

   A list of volumes displays.

2. Select the volume to which the new bricks are to be added. Click the **Bricks** tab from the **Details** pane.

   The **Bricks** tab lists the bricks of the selected volume.

3. Click **Add** to add new bricks. The **Add Bricks** window is displayed.

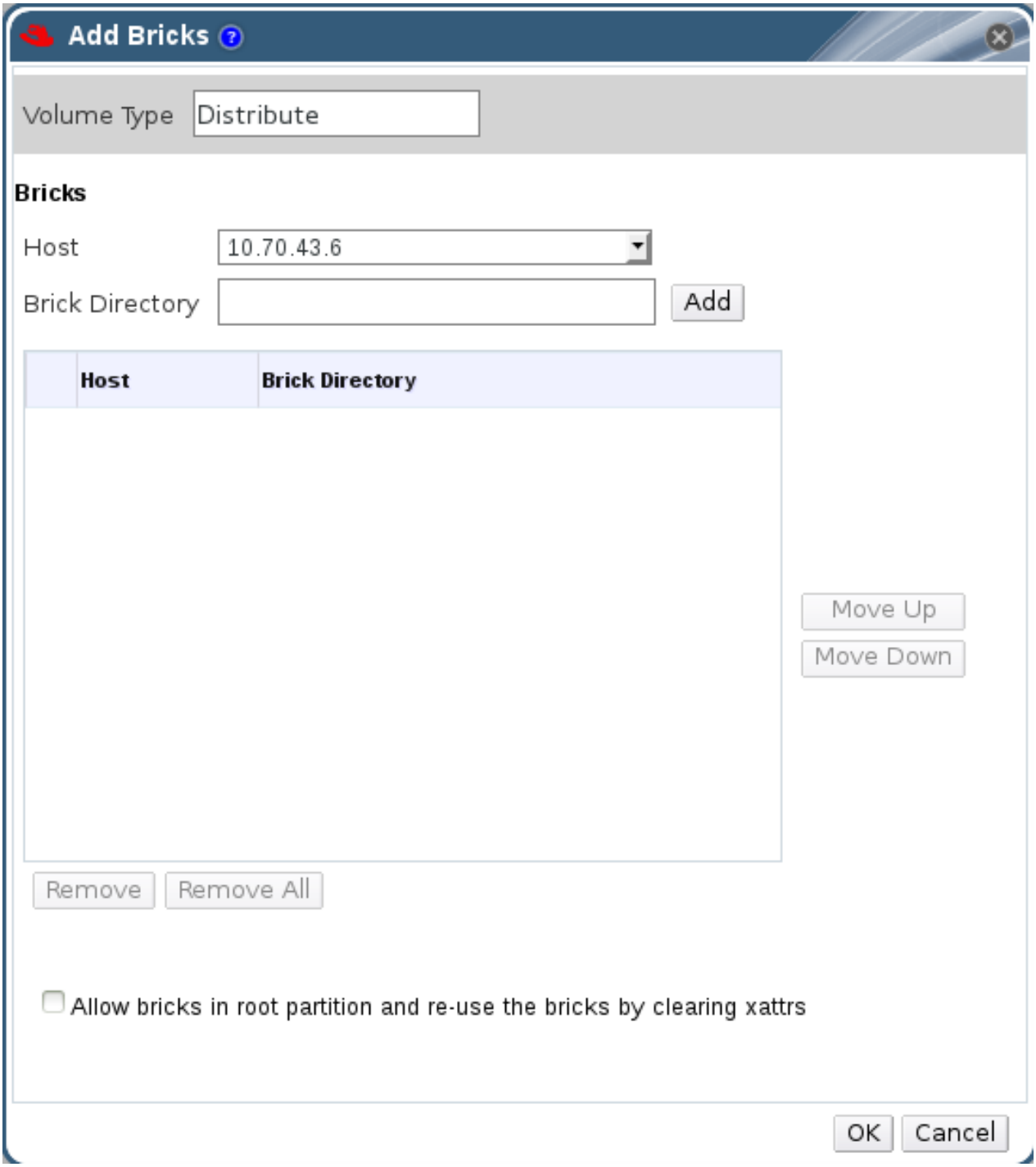


Figure 5.3. Add Bricks

Table 5.1. Add Bricks Tab Properties

Field/Tab	Description/Action
Volume Type	The type of volume.
Replica Count	Number of replicas to keep for each stored item.
Stripe Count	Number of bricks to stripe each file across.
Host	The selected host from which new bricks are to be added.
Brick Directory	The directory in the host.

4. Use the **Host** drop-down menu to select the host on which the brick resides .

5. Select the *Allow bricks in root partition and re-use the bricks by clearing xattrs* to use the system's root partition for storage and to re-use the existing bricks by clearing the extended attributes.

Note

It is recommended that you don't use the system's root partition for storage backend.

6. Enter the path of the **Brick Directory**. The directory must already exist.
7. Click **Add** and click **OK**. The new bricks are added to the volume and is displayed in the **Bricks** tab.

5.6.2. Removing Bricks

You can shrink volumes as needed while the cluster is online and available. For example, to remove a brick that has become inaccessible in a distributed volume due to hardware or network failure.

Note

- When shrinking distributed replicated or distributed striped volumes, the number of bricks being removed must be a multiple of the replica or stripe count. For example, to shrink a distributed striped volume with a stripe count of 2, you need to remove bricks in multiples of 2 (such as 2, 4, 6, 8). In addition, the bricks you are removing must be from the same replica set or stripe set. In a non-replicated volume, all bricks must be available in order to migrate data and perform the remove brick operation. In a replicated volume, at least one of the bricks in the replica must be available.
- You can monitor the status of *Remove Bricks* operation from the **Tasks** pane.
- You can perform *Commit*, *Retain*, view *Status* and *Stop* from remove-brick icon in the *Activities* column of *Volumes* and *Bricks* sub-tab.

Procedure 5.9. Removing Bricks from an Existing Volume

1. Click the **Volumes** tab.

   A list of volumes is displayed.

2. Select the volume from which bricks are to be removed. Click the **Bricks** tab from the **Details** pane.

   The **Bricks** tab lists the bricks for the volume.

3. Select the brick to remove. Click **Remove**. The **Remove Bricks** window is displayed, prompting to confirm the removal of the bricks.

Warning

If the brick is removed without selecting the **Migrate Data from the bricks** check box, the data on the brick which is being removed will not be accessible on the glusterFS mount point. If the **Migrate Data from the bricks** check box is selected, the data is migrated to other bricks and on a successful commit, the information of the removed bricks is deleted from the volume configuration. Data can still be accessed directly from the brick.

4. Click **OK**, remove brick starts.

Note

- Once remove-brick starts, remove-brick icon is displayed in **Activities** column of both **Volumes** and **Bricks** sub-tab.
- After completion of the remove brick operation, the remove brick icon disappears after 10 minutes.

5. In the **Activities** column, ensure that data migration is completed and click on the drop down of the remove-brick icon corresponding to the volume from which bricks are to be removed.

6. Click **Commit** to perform the remove brick operation.

Figure 5.4. Remove Bricks Commit

Note

The **Commit** option is enabled only if the data migration is completed.

The remove brick operation is completed and the status is displayed in the **Activities** column. You can check the status of the remove brick operation by selecting **Status** from the activities column.

5.6.2.1. Stopping a Remove Brick Operation

You can stop a remove brick operation after starting the remove brick operation. The remove brick operation is stopped and the migration of data is stopped.

Note

- Stop remove-brick operation is a technology preview feature. Technology Preview features are not fully supported under Red Hat subscription level agreements (SLAs), may not be functionally complete, and are not intended for production use. However, these features provide early access to upcoming product innovations, enabling customers to test functionality and provide feedback during the development process. As Red Hat considers making future iterations of Technology Preview features generally available, we will provide commercially reasonable efforts to resolve any reported issues that customers experience when using these features.
- Files which were migrated during Remove Brick operation are not migrated to the same brick when the operation is stopped.

Procedure 5.10. Stopping a Remove Brick Operation

1. Click the **Volumes** tab. A list of volumes displays.
2. In the **Activities** column, click on the drop down of the remove-brick icon corresponding to the volume to stop remove brick.
3. Click **Stop** to stop remove brick operation. The remove brick operation is stopped and remove-brick icon in the activities column is updated. The remove brick status is displayed after stopping the remove brick.

   You can also view the status of the *Remove Brick* operation by selecting **Status** from the drop down of the remove-brick icon in the *Activities* column of *Volumes* and *Bricks sub-tab.*.

5.6.2.2. Viewing Remove Brick Status

You can view the status of a remove brick operation when the remove brick operation is in progress.

Procedure 5.11. Viewing Remove Brick Status

1. Click the **Volumes** tab. A list of volumes displays.
2. In the **Activities** column, click the arrow corresponding to the volume.
3. Click **Status** to view the status of the remove brick operation. The **Remove Bricks Status** window displays.

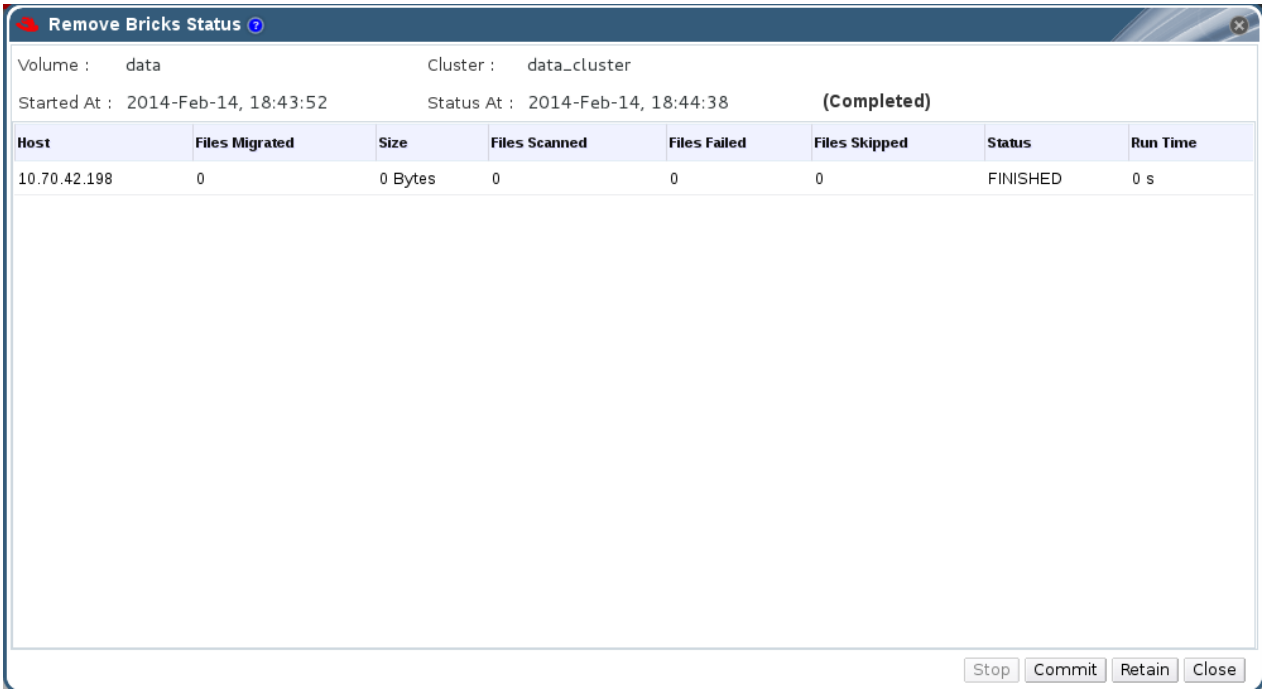


Figure 5.5. Remove Brick Status

4. Click one of the options below for the corresponding results
   - **Stop** to stop the remove brick operation
   - **Commit** to commit the remove brick operation
   - **Retain** to retain the brick selected for removal
   - **Close** to close the remove-brick status popup

5.6.2.3. Retaining a brick selected for Removal

You can retain a brick selected for removal operation when the remove brick operation is in progress. The brick that was selected to be removed will be retained and will not be removed from the volume.

The *Retain* option is enabled only after migration of data to other brick is completed.

Note

When a brick is retained, already migrated data is not migrated back.

Procedure 5.12. Retaining a Brick selected for Removal

1. Click the **Volumes** tab. A list of volumes displays.
2. In the **Activities** column, click the arrow corresponding to the volume.
3. Click **Retain** to retain the brick selected for removal. The brick is not removed and the status of the operation is displayed in the remove brick icon in the *Activities* column.

   You can also check the status by selecting the **Status** option from the drop down of remove-brick icon in the activities column.

5.6.3. Viewing Advanced Details

You can view the advanced details of a particular brick of the volume through Red Hat Storage Console. The advanced view displays the details of the brick, and is divided into four parts. Namely, **General**, **Clients**, **Memory Statistics**, and **Memory Pools**.

Procedure 5.13. Viewing Advanced Details

1. Click the **Volumes** tab. A list of volumes displays.
2. Select the required volume and click the **Bricks** tab from the **Details** pane.
3. Select the brick and click **Advanced Details**. The **Brick Advanced Details** window displays.

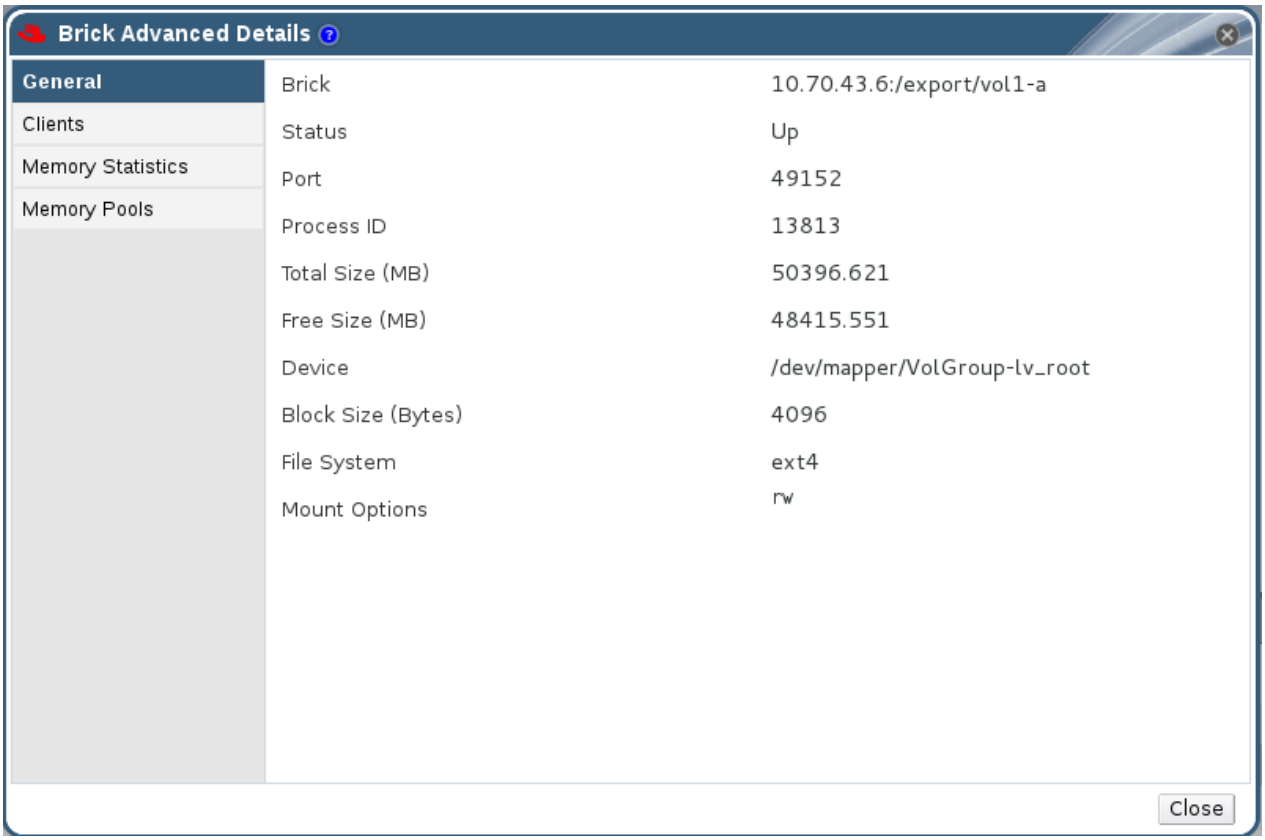


Figure 5.6. Brick Advanced Details

Table 5.2. Brick Details

Field/Tab	Description/Action
General	Displays additional information about the bricks.
Clients	Displays a list of clients accessing the volumes.
Memory Statistics/Memory Pool	Displays the details of memory usage and memory pool for the bricks.

You can view the advanced details of Red Hat Storage volumes through Red Hat Storage Console.

5.7. Volumes Permissions

While the superuser or system administrator of the Red Hat Storage has the full range of permissions, a Storage Administrator is a system administration role for a specific volume only. This is a hierarchical model, meaning that the Cluster Administrator has permissions to manage volumes. However, Storage Administrators have permission for the assigned volumes only, and not for all volumes in the cluster.

Procedure 5.14. Assigning a System Administrator Role for a Volume

1. Click the **Volumes** tab. A list of volumes displays.
2. Select the volume to edit, and click the **Permissions** tab from the **Details** pane.

   The **Permissions** tab lists users and their current roles and permissions, if any.

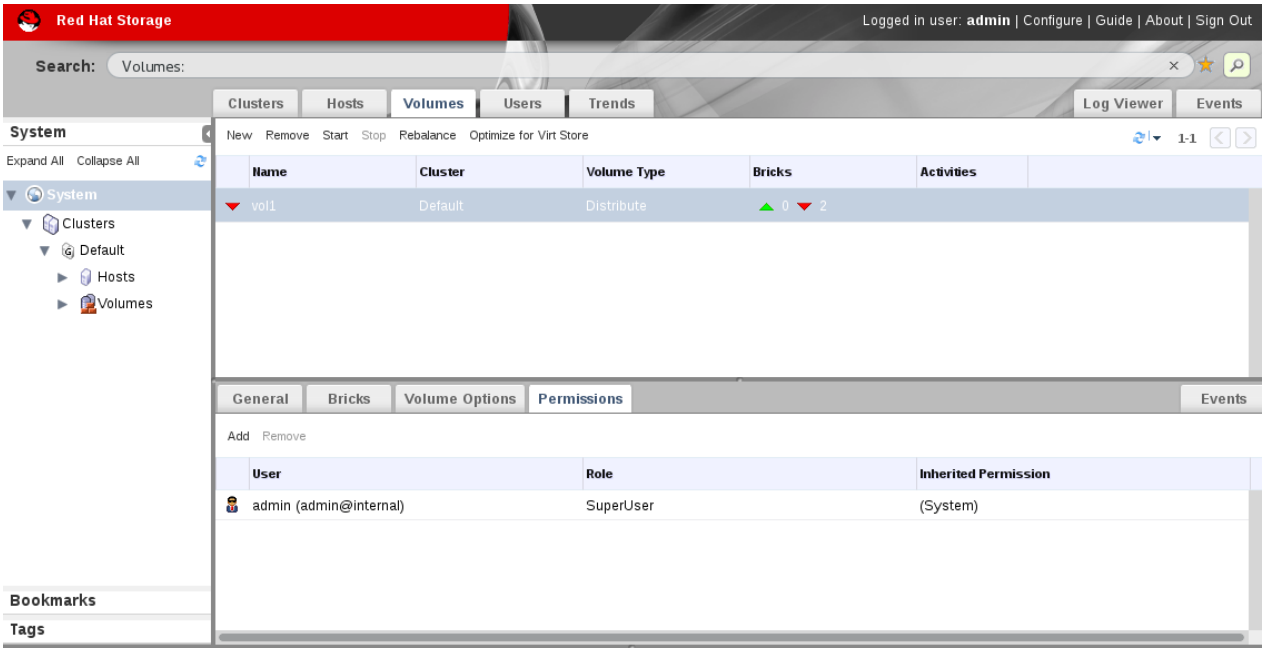


Figure 5.7. Volume Permissions

3. Click **Add** to add an existing user. The **Add Permission to User** window is displayed. Enter a name, a user name, or part thereof in the **Search** text box, and click **Go**. A list of possible matches displays in the results list.
4. Select the check box of the user to be assigned the permissions. Scroll through the **Role to Assign** list and select **GlusterAdmin**.

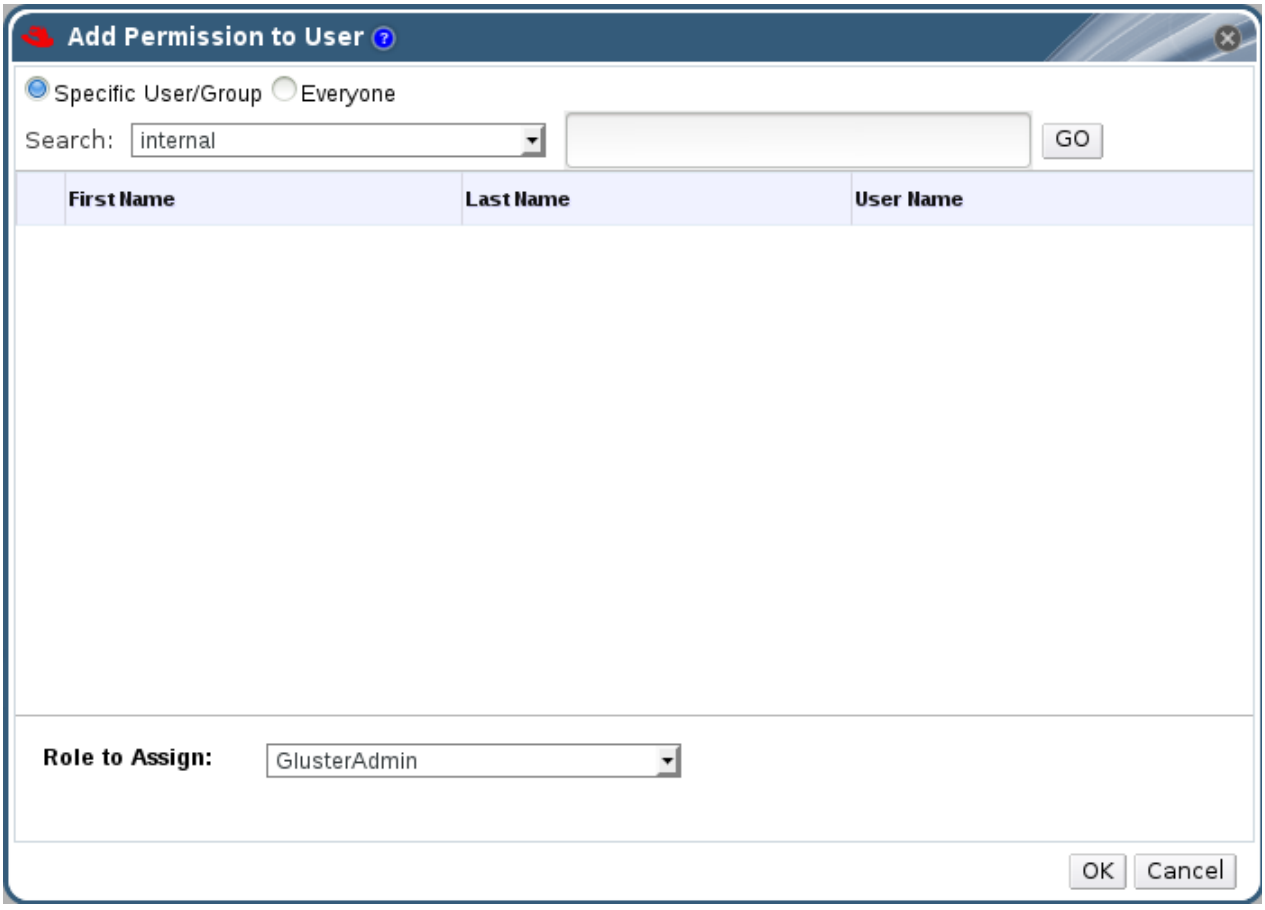


Figure 5.8. Assign GlusterAdmin Permission

5. Click **OK**.

   The name of the user displays in the **Permissions** tab, with an icon and the assigned role.

Note

You can only assign roles and permissions to existing users.

You can also change the system administrator of a volume by removing the existing system administrator and adding a new system administrator as described in the previous procedure.

Procedure 5.15. Removing a System Administrator Role

1. Click the **Volumes** tab. A list of volumes displays.
2. Select the required volume and click the **Permissions** tab from the **Details** pane.

   The **Permissions** tab lists users and their current roles and permissions, if any. The Super User and Cluster Administrator, if any, will display in the **Inherited Permissions** tab. However, none of these higher level roles can be removed.
3. Select the appropriate user.
4. Click **Remove**. A window is displayed, prompting to confirm removing the user. Click **OK**. The user is removed from the **Permissions** tab.

5.8. Rebalancing Volume

Storage volumes are abstracted from hardware, allowing each to be managed independently. Storage can be added or removed from the storage pools while data continues to be available, with no application interruption. Volumes can be expanded or shrunk across machines by adding or removing bricks.

After expanding or shrinking a volume (without migrating data), you need to rebalance the data among the hosts. In a non-replicated volume, all bricks should be online to perform the rebalance operation. In a replicated volume, at least one of the bricks in the replica should be online.

Through Red Hat Storage Console, you can perform the following:

- Start Rebalance
- Stop Rebalance
- View Rebalance Status

Note

You can monitor the status of Rebalance operation from the **Tasks** pane.

5.8.1. Start Rebalance

1. Click the **Volumes** tab. The **Volumes** tab is displayed with the list of all volumes in the system.
2. Select the volume that you want to **Rebalance**.
3. Click the **Rebalance**. The **Rebalance** process starts and the rebalance icon is displayed in the **Activities** column of the volume. A mouseover script is displayed mentioning that the rebalance is in progress. You can view the rebalance status by selecting status from the rebalance drop-down list .

Note

After completion of the rebalance operation, the rebalance icon disappears after 10 minutes.

5.8.2. Stop Rebalance

1. Click the **Volumes** tab. The **Volumes** tab is displayed with the list of all volumes in the system.
2. Select a volume on which Rebalance needs to be stopped.

Note

- You can not stop rebalance for multiple volumes.
- Rebalance can be stopped for volumes only if it is in progress

3. In the **Activities** column, click on the drop-down of the Rebalance icon corresponding to the volume.
4. Click **Stop**. The **Stop Rebalance** window is displayed.
5. Click **OK** to stop rebalance. The **Rebalance** is stopped and the status window is displayed.

   You can also check the status of the *Rebalance* operation by selecting **Status** option from the drop down of Rebalance icon in the activities column.

5.8.3. View Rebalance Status

1. Click the **Volumes** tab. The **Volumes** tab is displayed with the list of all volumes in the system.
2. Select the volume on which Rebalance is in progress, stopped, completed.
3. Click **Status** option from the Rebalance icon drop down list. The **Rebalance Status** page is displayed.

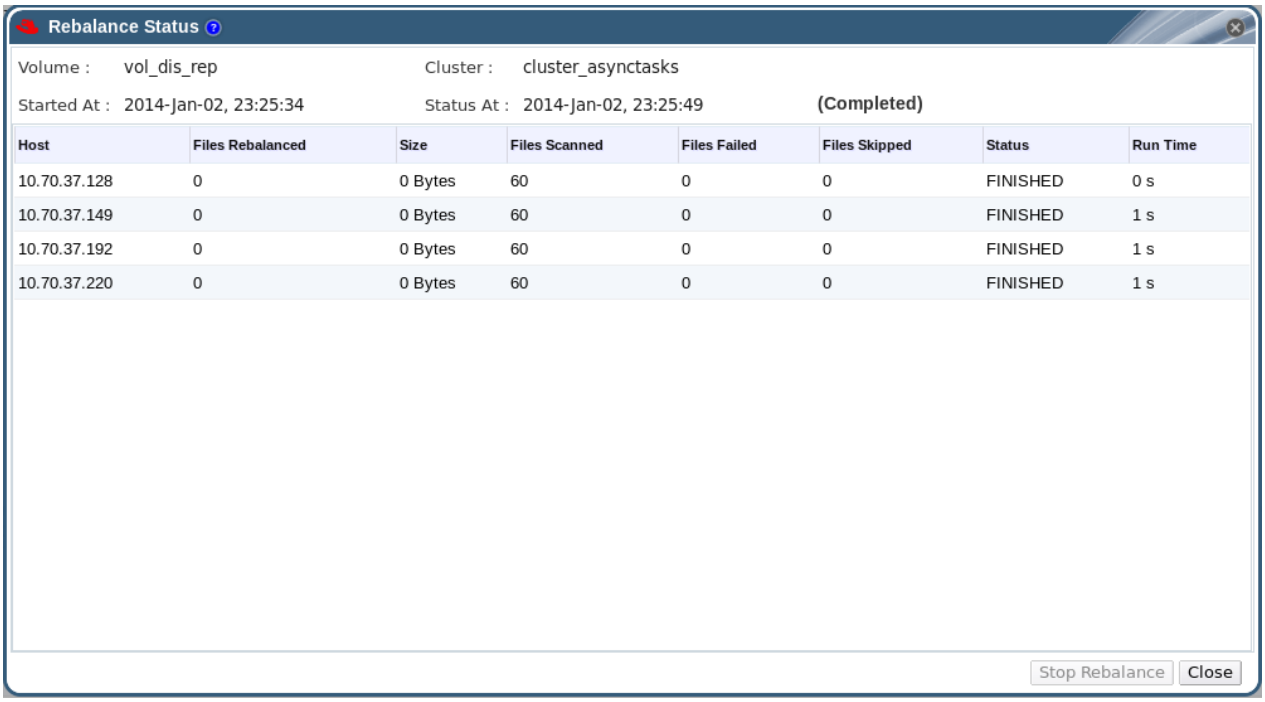


Figure 5.9. Rebalance Status

Note

If the Rebalance Status window is open while Rebalance is stopped using the CLI, the status is displayed as **Stopped**. If the **Rebalance Status** window is not open, the task status is displayed as **Unknown** as the status update depends on gluster CLI.

You can also stop *Rebalance* operation by clicking **Stop** in the **Rebalance Status** window.

Chapter 6. Managing Gluster Hooks

Gluster hooks are volume lifecycle extensions. You can manage Gluster hooks from Red Hat Storage Console. The content of the hook can be viewed if the hook content type is **Text**. Through Red Hat Storage Console, you can perform the following:

- View a list of hooks available in the hosts.
- View the content and status of hooks.
- Enable or disable hooks.
- Resolve hook conflicts.

6.1. Viewing the list of Hooks

Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.

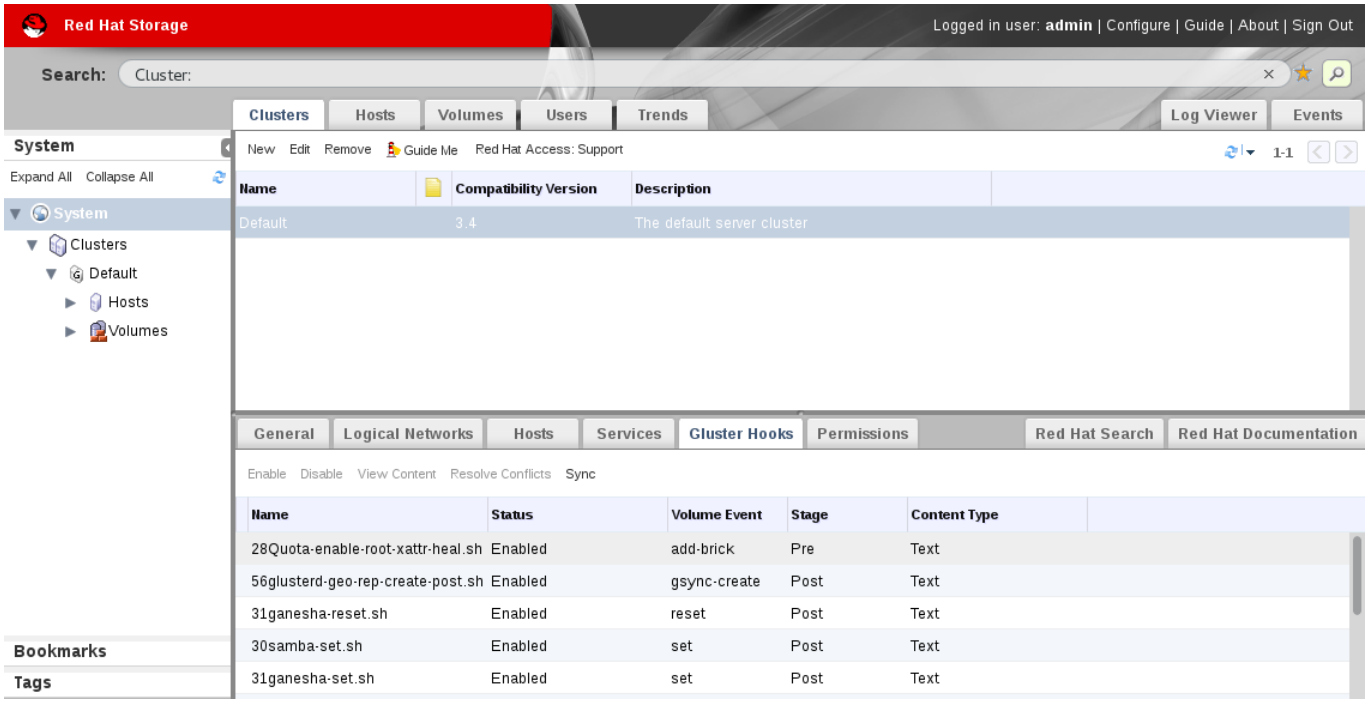


Figure 6.1. Gluster Hooks

6.2. Viewing the Content of Hooks

Procedure 6.1. Viewing the Content of a Hook

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select a hook with content type **Text** and click **View Content**. The **Hook Content** window displays with the content of the hook.

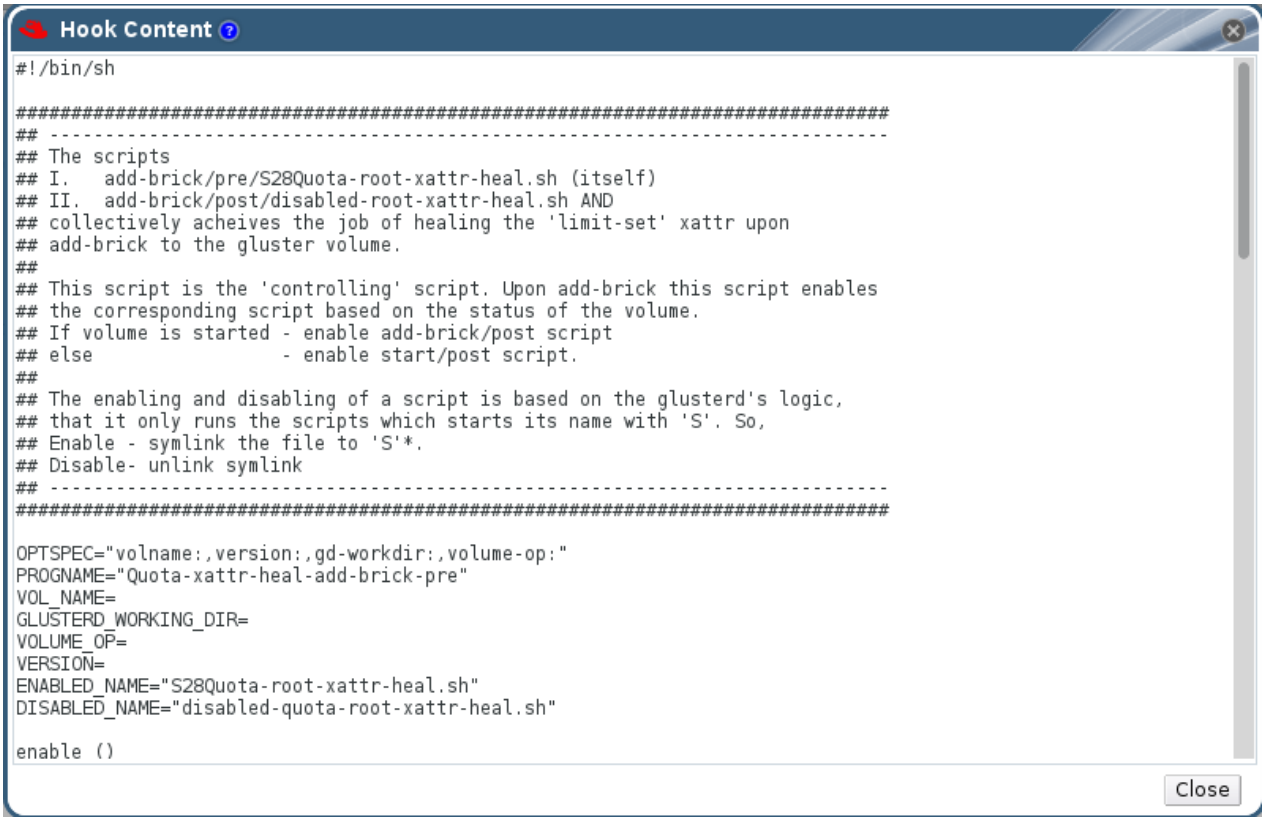


Figure 6.2. Hook Content

6.3. Enabling or Disabling Hooks

Procedure 6.2. Enabling or Disabling a Hook

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select the hook and click **Enable** or **Disable**.

   If **Disable** is selected, *Disable Gluster Hooks* dialog box displays, prompting you to confirm disabling hook. Click *OK* to confirm disabling.

   The hook is enabled or disabled on all nodes of the cluster.

   The enabled or disabled hooks status update displays in the **Gluster Hooks** sub-tab.

6.4. Refreshing Hooks

By default, the Red Hat Storage Console checks for the status of installed hooks on all hosts in the cluster and detects new hooks by running a periodic job every hour. If the user wishes to trigger this job, they can choose to do so by clicking **Sync**.

Procedure 6.3. Refreshing a Hook

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Click **Sync**. The hooks are synchronized and displayed.

6.5. Resolving Conflicts

6.5. Resolving Conflicts

The hooks are displayed in the **Gluster Hooks** sub-tab of the **Cluster** tab. Hooks causing a conflict are displayed with an exclamation mark. This denotes either that there is a conflict in the content or status of the hook across the servers in the cluster, or that the hook script is missing in one or more servers. These conflicts can be resolved via the console. The hooks in the servers are periodically synchronized with engine database and the following conflicts can occur for the hooks:

- Content Conflict - the content of the hook is different across servers.
- Status Conflict - the status of the hook is different across servers.
- Missing Conflict - one or more servers of the cluster do not have the hook.
- Content + Status Conflict - both the content and status of the hook are different across servers.
- Content + Status + Missing Conflict - both the content and status of the hook are different across servers, or one or more servers of the cluster do not have the hook.

6.5.1. Resolving Missing Hook Conflicts

Procedure 6.4. Resolving a Missing Hook Conflict

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select a hook causing a conflict and click **Resolve Conflicts**. The **Resolve Conflicts** window displays.

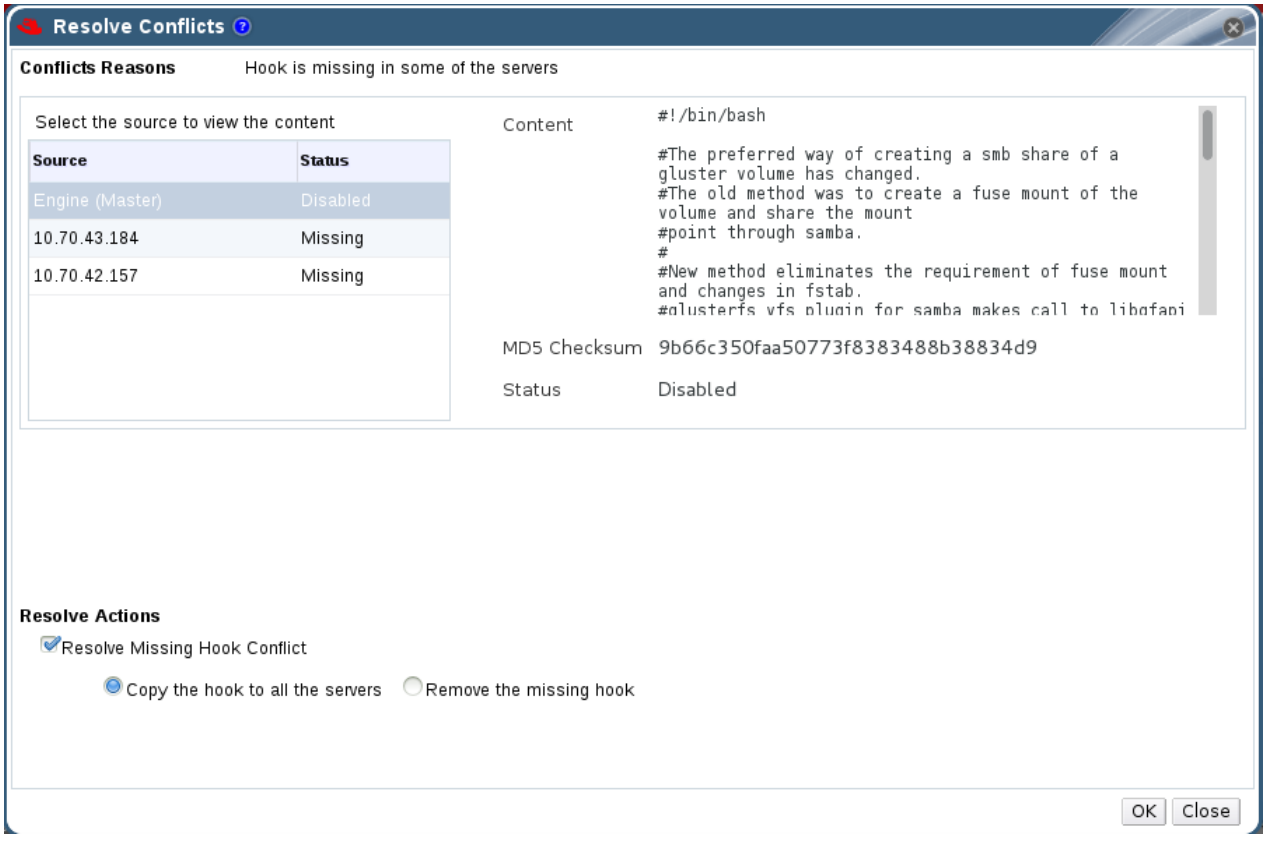


Figure 6.3. Missing Hook Conflict

3. Select one of the options give below:

- **Copy the hook to all the servers** to copy the hook to all servers.
- **Remove the missing hook** to remove the hook from all servers and the engine.

4. Click **OK**. The conflict is resolved.

6.5.2. Resolving Content Conflicts

Procedure 6.5. Resolving a Content Conflict

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select the conflicted hook and click **Resolve Conflicts**. The **Resolve Conflicts** window displays.

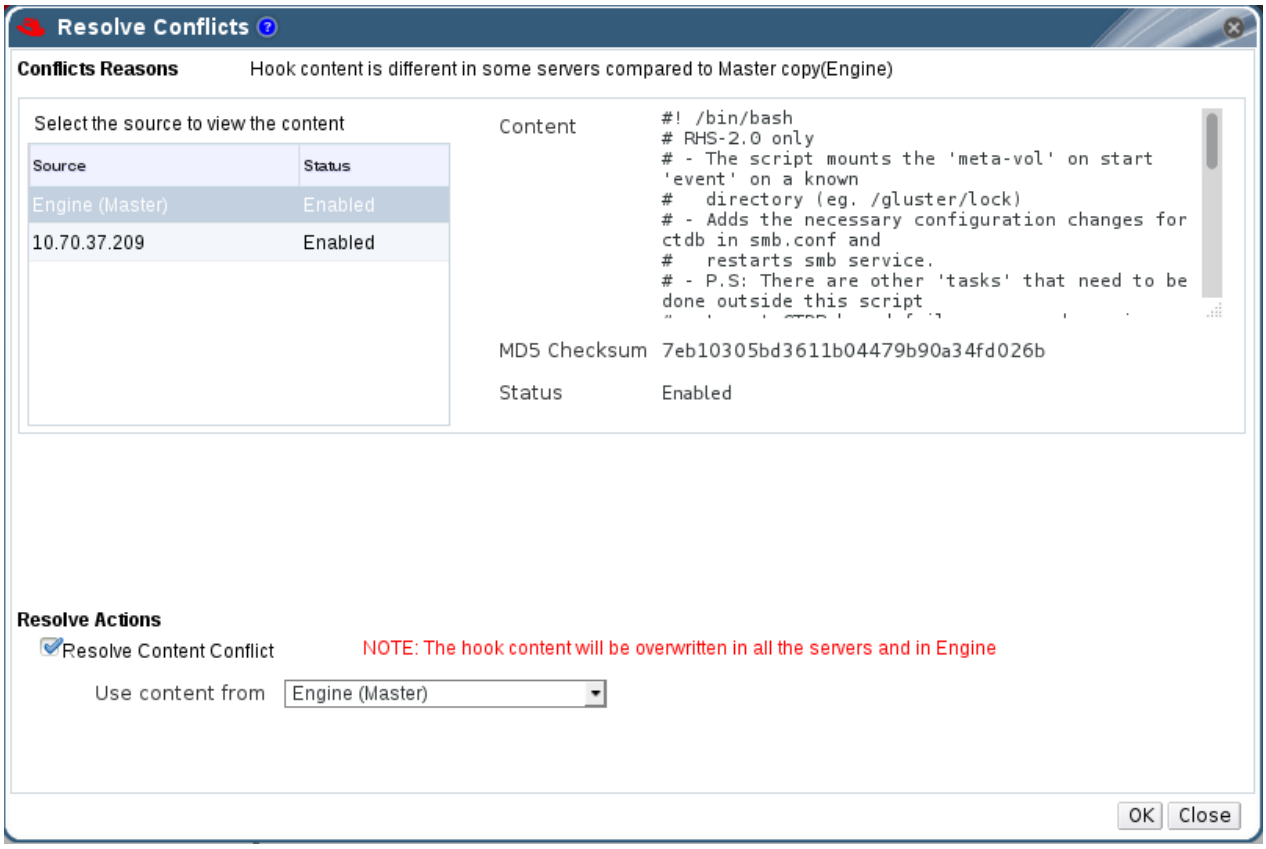


Figure 6.4. Content Conflict

3. Select an option from the **Use Content from** drop-down list:
   - Select a server to copy the content of the hook from the selected server.

     Or

   - Select **Engine (Master)** to copy the content of the hook from the engine copy.

Note

The content of the hook will be overwritten in all servers and in the engine.

4. Click **OK**. The conflict is resolved.

6.5.3. Resolving Status Conflicts

Procedure 6.6. Resolving a Status Conflict

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select the conflicted hook and click **Resolve Conflicts**. The **Resolve Conflicts** window displays.

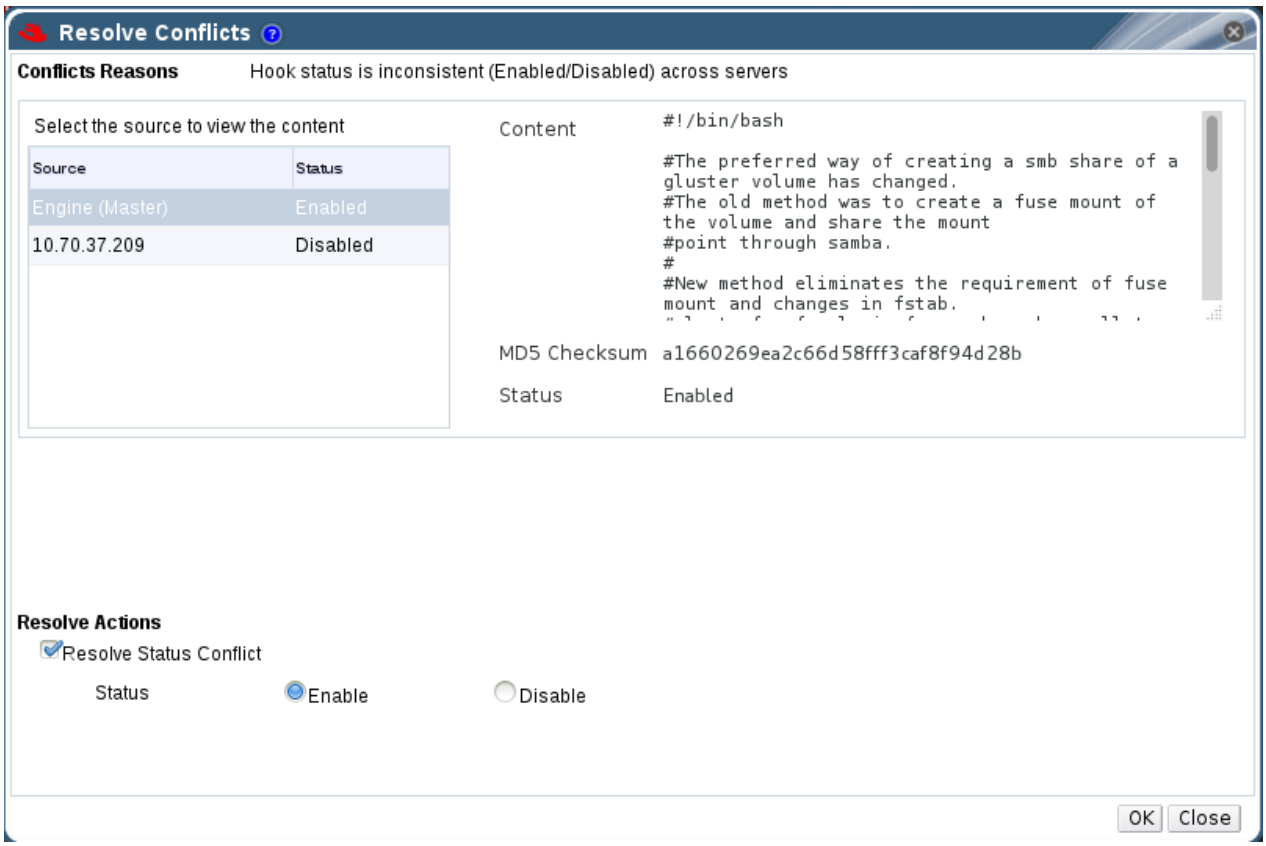


Figure 6.5. Status Conflict

3. Set **Hook Status** to **Enable** or **Disable**.
4. Click **OK**. The conflict is resolved.

6.5.4. Resolving Content and Status Conflicts

Procedure 6.7. Resolving a Content and Status Conflict

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select a hook causing a conflict and click **Resolve Conflicts**. The **Resolve Conflicts** window displays.
3. Select an option from the **Use Content from** drop-down list to resolve the content conflict:
   - Select a server to copy the content of the hook from the selected server.

Or

- Select **Engine (Master)** to copy the content of the hook from the engine copy.

Note

The content of the hook will be overwritten in all the servers and in Engine.

4. Set **Hook Status** to **Enable** or **Disable** to resolve the status conflict.
5. Click **OK**. The conflict is resolved.

6.5.5. Resolving Content, Status, and Missing Conflicts

Procedure 6.8. Resolving a Content, Status and Missing Conflict

1. Click the **Cluster** tab and select a cluster. A **Gluster Hooks** sub-tab displays, listing the hooks in the cluster.
2. Select the conflicted hook and click **Resolve Conflicts**. The **Resolve Conflicts** window displays.
3. Select one of the options given below to resolve the missing conflict:
   - Copy the hook to all the servers.
   - Remove the missing hook.
4. Select an option from the **Use Content from** drop-down list to resolve the content conflict:
   - Select a server to copy the content of the hook from the selected server.

   Or

   - Select **Engine (Master)** to copy the content of the hook from the engine copy.

Note

The content of the hook will be overwritten in all the servers and in Engine.

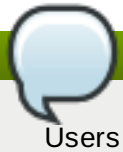
5. Set **Hook Status** to **Enable** or **Disable** to resolve the status conflict.
6. Click **OK**. The conflict is resolved.

Chapter 7. Users

This section describes the users in Red Hat Storage Console, how to set up user roles that control user permission levels, and how to manage users on the Red Hat Storage. Red Hat Storage Console relies on directory services for user authentication and information.

Users are assigned roles that allow them to perform their tasks as required. The role with the highest level of permissions is the admin role, which allows a user to set up, manage, and optimize all aspects of the Red Hat Storage Console. By setting up and configuring roles with permissions to perform actions and create objects, users can be provided with a range of permissions that allow the safe delegation of some administrative tasks to users without granting them complete administrative control.

Red Hat Storage Console provides a rich user interface that allows an administrator to manage their storage infrastructure from a web browser allowing even the most advanced configurations such as network bonding and VLANs to be centrally managed from a graphical console.



Note

Users are not created in Red Hat Storage Console, but in the Directory Services domain. Red Hat Storage Console can be configured to use multiple Directory Services domains.

7.1. Directory Services Support in Red Hat Storage Console

During installation, Red Hat Storage Console creates its own internal administration user, **admin**. This account is intended for use when initially configuring the environment, and for troubleshooting. To add other users to Red Hat Storage Console you will need to attach a directory server to the Console using the Domain Management Tool, **rhsc-manage-domains**.

Once at least one directory server has been attached to the Console you will be able to add users that exist in the directory server and assign roles to them using the Administration Portal. Users will be identified by their User Principle Name (UPN) of the form ***user@domain***. Attachment of more than one directory server to the Console is also supported.

The directory servers currently supported for use with Red Hat Storage Console are:

- Active Directory;
- Identity Management (IdM); and
- Red Hat Directory Server(RHDS).

You must ensure that the correct DNS records exist for your directory server. In particular you must ensure that the DNS records for the directory server include:

- A valid pointer record (PTR) for the directory server's reverse look-up address.
- A valid service record (SRV) for LDAP over TCP port **389**.
- A valid service record (SRV) for Kerberos over TCP port **88**.
- A valid service record (SRV) for Kerberos over UDP port **88**.

If these records do not exist in DNS then you will be unable to add the domain to the Red Hat Storage Console configuration using **rhsc-manage-domains**.

For more detailed information on installing and configuring a supported directory server, refer to the vendor's documentation:

- Active Directory - http://technet.microsoft.com/en-us/windowsserver/dd448614.
- Identity Management (IdM) - https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Identity_Management_Guide/index.html
- Red Hat Directory Server (RHDS) Documentation - https://access.redhat.com/site/documentation/en-US/Red_Hat_Directory_Server/

Important

A user must be created in the directory server specifically for use as the Red Hat Storage administrative user. Do *not* use the administrative user for the directory server as the Red Hat Storage administrative user.

Important

It is not possible to install Red Hat Storage Console (*rhsc*) and IdM (*ipa-server*) on the same system. IdM is incompatible with the *mod_ssl* package, which is required by Red Hat Storage Console.

For information on creation of user accounts in Active Directory refer to http://technet.microsoft.com/en-us/library/cc732336.aspx.

For information on delegation of control in Active Directory refer to http://technet.microsoft.com/en-us/library/cc732524.aspx.

Note

Red Hat Storage Console uses Kerberos to authenticate with directory servers. RHDS does not provide native support for Kerberos. If you are using RHDS as your directory server then you must ensure that the directory server is made a service within a valid Kerberos domain. To do this you will need to perform these steps while referring to the relevant directory server documentation:

- Configure the **memberOf** plug-in for RHDS to allow group membership. In particular ensure that the value of the ***memberofgroupattr*** attribute of the **memberOf** plug-in is set to **uniqueMember**.

  Consult the Red Hat Directory Server *Plug-in Guide* for more information on configuring the **memberOf** plug-in.

- Define the directory server as a service of the form **ldap/*hostname*@*REALMNAME*** in the Kerberos realm. Replace *hostname* with the fully qualified domain name associated with the directory server and *REALMNAME* with the fully qualified Kerberos realm name. The Kerberos realm name must be specified in capital letters.
- Generate a **keytab** file for the directory server in the Kerberos realm. The **keytab** file contains pairs of Kerberos principals and their associated encrypted keys. These keys will allow the directory server to authenticate itself with the Kerberos realm.

  Consult the documentation for your Kerberos principle for more information on generating a **keytab** file.

- Install the **keytab** file on the directory server. Then configure RHDS to recognize the **keytab** file and accept Kerberos authentication using GSSAPI.

  Consult the Red Hat Directory Server *Administration Guide* for more information on configuring RHDS to use an external **keytab** file.

- Test the configuration on the directory server by using the **kinit** command to authenticate as a user defined in the Kerberos realm. Once authenticated run the **ldapsearch** command against the directory server. Use the ***-Y GSSAPI*** parameters to ensure the use of Kerberos for authentication.

7.2. Authorization Model

Red Hat Storage Console applies authorization controls to each action performed in the system. Authorization is applied based on the combination of the three components in any action:

- The user performing the action
- The type of action being performed
- The object on which the action is being performed

Actions

For an action to be successfully performed, the **user** must have the appropriate **permission** for the **object** being acted upon. Each type of action corresponds to a **permission**. There are many different permissions in the system, so for simplicity they are grouped together in **roles**.

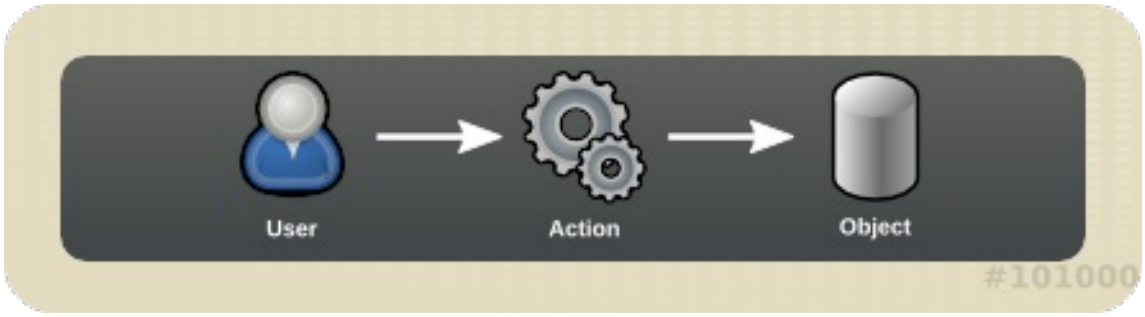


Figure 7.1. Actions

Permissions

Permissions enable users to perform actions on objects, where objects are either individual objects or container objects.

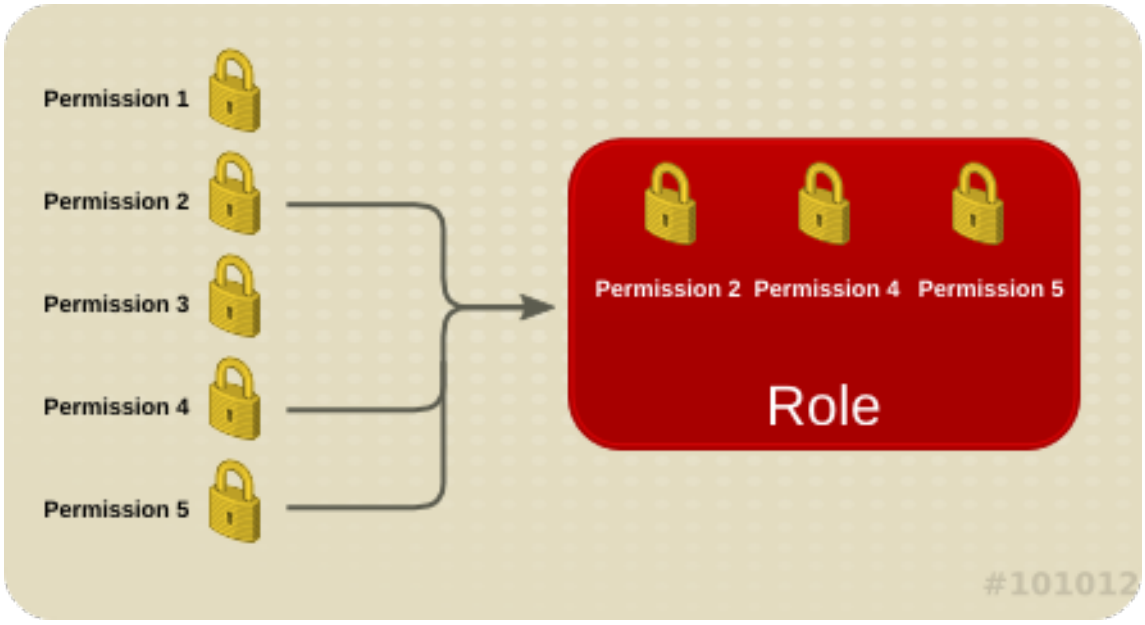


Figure 7.2. Permissions & Roles

Any permissions that apply to a container object also apply to all members of that container.

Important

Some actions are performed on more than one object.

7.3. User Properties

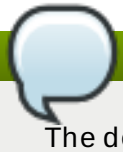
Roles and Permissions can be considered as the properties of the User object. Roles are predefined sets of privileges that can be configured from Red Hat Storage Console, permitting access and management to different levels of resources in the cluster, to specific physical and virtual resources. Multilevel administration includes a hierarchy of permissions that can be configured to provide a finely grained model of permissions, or a wider level of permissions as required by your enterprise. For example, a cluster administrator has permissions to manage all servers in the cluster, while a

server administrator has system administrator permissions to a single server. A user can have permissions to log into and use a single server but not make any changes to the server configurations, while another user can be assigned system permissions to a server, effectively acting as system administrator on the server.

7.3.1. Roles

Red Hat Storage provides a range of pre-configured or default roles, from the Superuser or system administration, to an end user with permissions to access a single volume only. There are two types of system administration roles: roles with system permissions to physical resources, such as hosts and storage; and roles with system permissions to virtual resources such as volumes. While you cannot change the default roles, you can clone them, and then customize the new roles as required.

Red Hat Storage Console has an **`administrator`** role. The privileges provided by this role are shown in this section.



Note

The default roles cannot be removed from the Red Hat Storage, or privileges cannot be modified; however the name and descriptions can be changed.

Administrator Role

- Allows access to the *Administration Portal* for managing servers and volumes.

  For example, if a user has an **`administrator`** role on a cluster, they could manage all servers in the cluster using the *Administration Portal*.

Table 7.1. Red Hat Storage Console System Administrator Roles

Role	Privileges	Notes
SuperUser	Full permissions across all objects and levels	Can manage all objects across all clusters.
ClusterAdmin	Cluster Administrator	Can use, create, delete, and manage all resources in a specific cluster, including servers and volumes.
GlusterAdmin	Gluster Administrator	Can create, delete, configure and manage a specific volume. Can also add or remove host.
HostAdmin	Host Administrator	Can configure, manage, and remove a specific host. Can also perform network-related operations on a specific host.
NetworkAdmin	Network Administrator	Can configure and manage networks attached to servers.

7.3.2. Permissions

The following table details the actions for each object in the cluster, for each of which permission may be assigned. This results in a high level of control over actions at multiple levels.

Table 7.2. Permissions Actions on Objects

Object	Action
System - Configure RHS-C	Manipulate Users, Manipulate Permissions, Manipulate Roles, Generic Configuration
Cluster - Configure Cluster	Create, Delete, Edit Cluster Properties, Edit Network
Server - Configure Server	Create, Delete, Edit Host Properties, Manipulate Status, Edit Network
Gluster Storage - Configure Gluster Storage	Create, Delete, Edit Volumes, Volume Options, Manipulate Status

7.4. Users Operations

Users can be added or removed from the system, assigned roles, and given permissions to various objects, enabling them to effectively perform their required work. The **Users** Details pane displays information on the status and privileges of users, enabling the system administrator to assign or change roles, allot servers, set up event notifications and allocate Directory Service groups. Because of the level of detail that is possible, a multi-level administration system can be defined.

Note

Login to the system is verified against the Directory Service records of the organization.

7.4.1. Adding Users and Groups

Existing users must be added to the Administration Portal before being assigned roles.

Adding Users

1. Click the **Users** tab. The list of authorized users for Red Hat Storage Console displays.
2. Click **Add**. The **Add Users and Groups** dialog box displays.

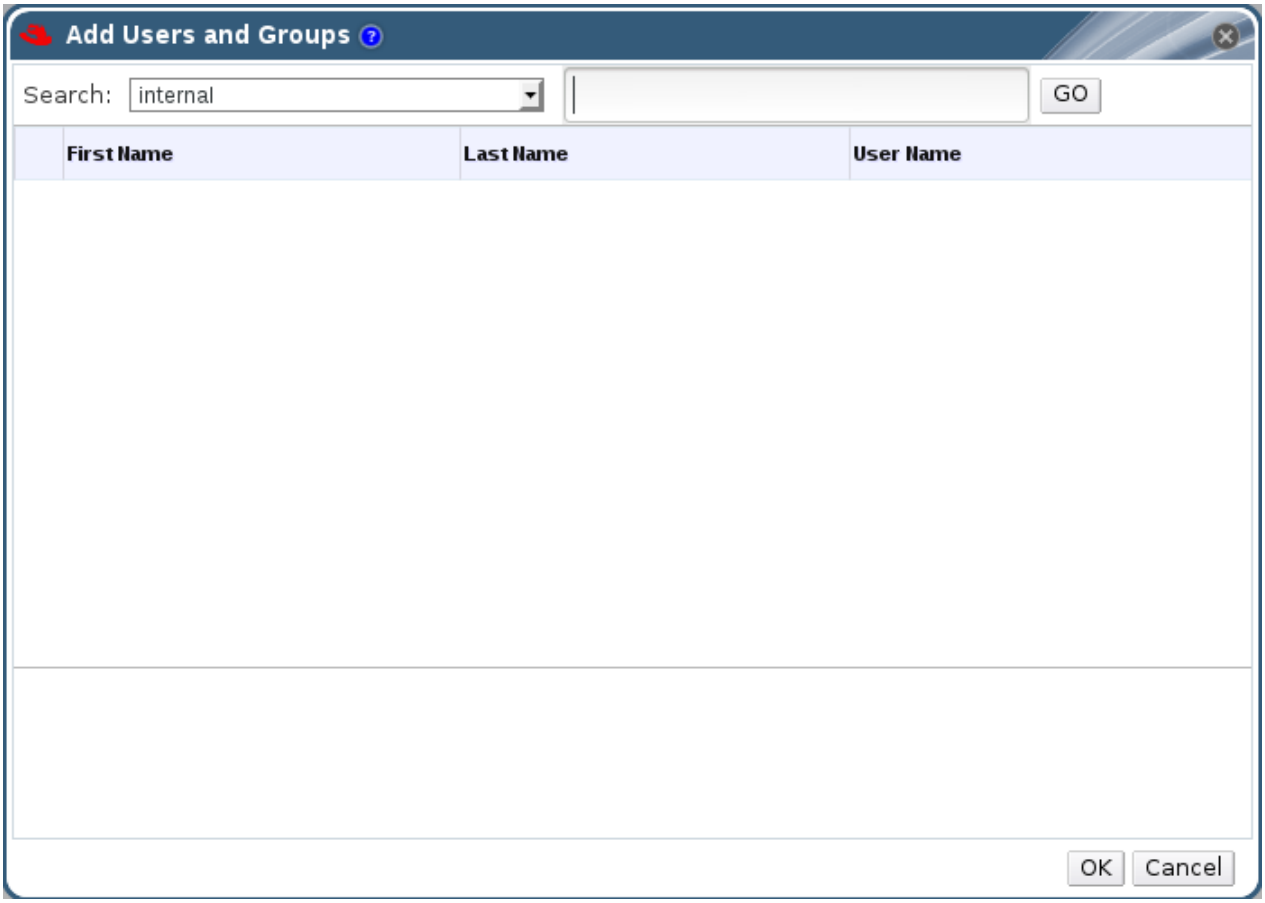


Figure 7.3. Add Users and Groups Dialog Box

3. The default **Search** domain displays. If there are multiple search domains, select the appropriate search domain. Enter a name or part of a name in the search text field, and click **GO**. Alternatively, click **GO** to view a list of all users and groups.
4. Select the group, user or users check boxes. The added user displays on the **Users tab**.

Viewing User Information

Users are not created from within the Red Hat Storage; Red Hat Storage Console accesses user information from the organization's Directory Service. This means that you can only assign roles to users who already exist in your Directory Services domain. To assign permissions to users, use the **Permissions** tab on the Details pane of the relevant resource.

> **Example 7.1. Assigning a user permissions to use a particular server**
>
> To assign a user to a particular server, use the **Permissions** tab on the Details pane of the selected server.

To view general user information:

1. Click the **Users** tab. The list of authorized users for Red Hat Storage Console displays.
2. Select the user, or perform a search if the user is not visible on the results list.
3. The Details pane displays for the selected user, usually with the **General** tab displaying general information, such as the domain name, email, and status of the user.

4. The other tabs allow you to view groups, permissions, and events for the user.

   For example, to view the groups to which the user belongs, click the **Directory Groups** tab.

7.4.2. Removing Users

A system administrator will need to remove users, for example, when they leave the company.

To remove a user:

1. Click the **Users** tab. The list of authorized users for Red Hat Storage Console displays.

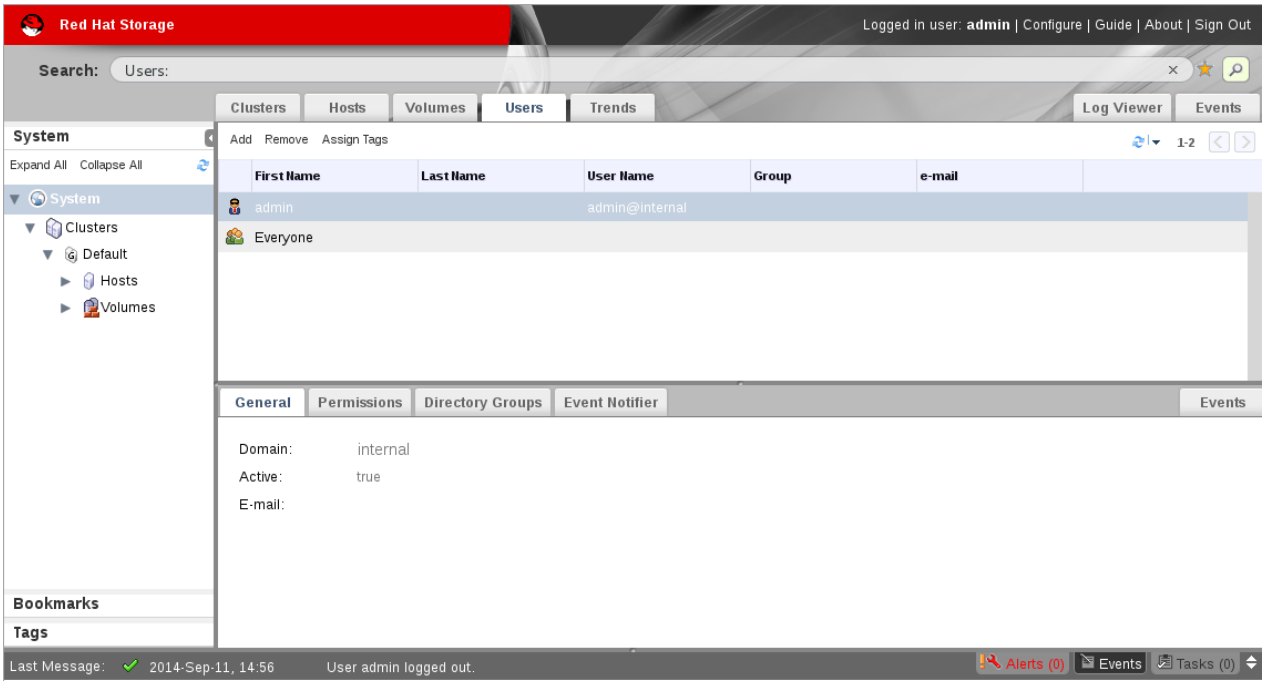


Figure 7.4. Users Tab

2. Select the user to be removed.
3. Click the **Remove** button. A message displays prompting you to confirm the removal.
4. Click **OK**.
5. The user is removed from Red Hat Storage Console.

Note

All user information is read from the Directory Service. Removing a user from the Red Hat Storage Console system deletes the record in the Red Hat Storage Console database, denying the user the ability to log on to the console. It removes the association in the Directory Service between the console and the user. All other user properties remain intact.

7.5. Event Notifications

When troubleshooting problems related to users, the first thing to recall is that users must be correctly added to and authenticated at the Directory Services level, not on the Red Hat Storage Console. Problems with permissions can occur when adequate levels of permissions to all required objects have not been assigned. Users, particularly those with administrator roles, require to be notified when events or triggers occur.

7.5.1. Managing Event Notifiers

This section describes how to set up and manage event notifications for users. Events are displayed on the **Events** tab, however, users can be notified by email about selected events. For example, a system administrator might like to know when there is a problem with storage, or a team lead may want to be notified if a volume is down.

To set up event notifications:

1. Click the **Users** tab. The list of authorized users for Red Hat Storage Console displays.
2. Select the user who requires notification, or perform a search if the user is not visible on the results list.
3. Click the **Event Notifier** tab. The **Event Notifier** tab displays a list of events for which the user will be notified, if any.
4. Click the **Manage Events** button. The **Add Event Notification** dialog box displays a list of events for Services, Hosts, Volumes, Hooks, and General Management events. You can select all, or pick individual events from the list. Click the **Expand All** button to see complete lists of events.

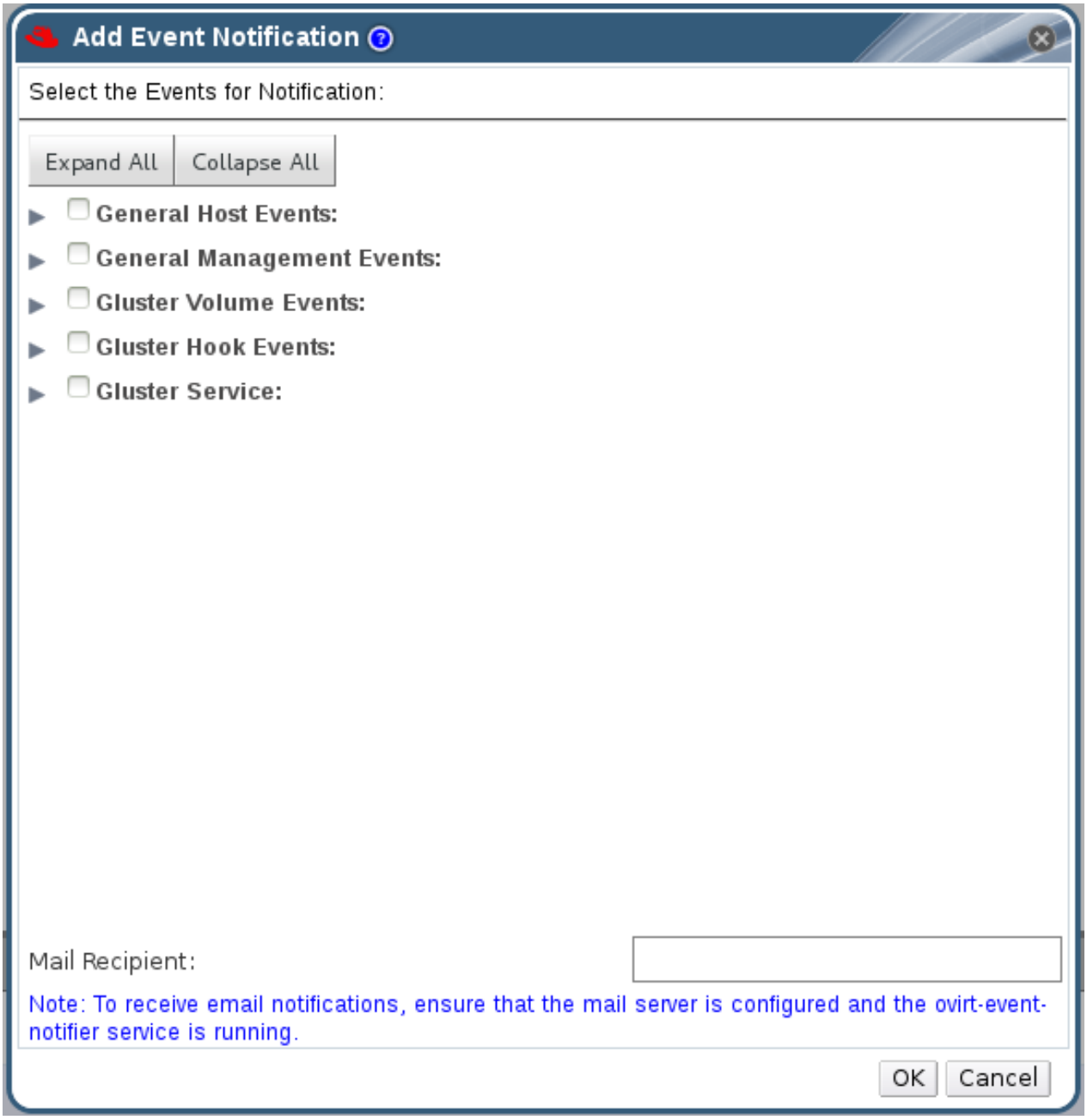


Figure 7.5. The Add Events Dialog Box

5. Enter an email address in the **Mail Recipient:** field.
6. Click **OK** to save changes and close the window. The selected events display on the **Event Notifier** tab for the user.
7. Configure the **ovirt-engine-notifier** service on the Red Hat Storage Console.

Important

The *MAIL_SERVER* parameter is mandatory.

The event notifier configuration file can be found in **/usr/share/ovirt-engine/services/ovirt-engine-notifier/ovirt-engine-notifier.conf**. The parameters for event notifications in *ovirt-engine-notifier.conf* are listed in Table 7.3, "ovirt-engine-notifier.conf variables"

Table 7.3. ovirt-engine-notifier.conf variables

Variable name	Default	Remarks
INTERVAL_IN_SECONDS	120	The interval in seconds between instances of dispatching messages to subscribers.
MAIL_SERVER	none	The SMTP mail server address. Required.
MAIL_PORT	25	The default port of a non-secured SMTP server is 25. The default port of a secured SMTP server (one with SSL enabled) is 465.
MAIL_USER	none	If SSL is enabled to authenticate the user, then this variable must be set. This variable is also used to specify the "from" user address when the MAIL_FROM variable is not set. Some mail servers do not support this functionality. The address is in RFC822 format.
MAIL_PASSWORD	none	This variable is required to authenticate the user if the mail server requires authentication or if SSL is enabled.
MAIL_ENABLE_SSL	false	This indicates whether SSL should be used to communicate with the mail server.
HTML_MESSAGE_FORMAT	false	The mail server sends messages in HTML format if this variable is set to "true".
MAIL_FROM	none	This variable specifies a "from" address in RFC822 format, if supported by the mail server.
MAIL_REPLY_TO	none	This variable specifies "reply-to" addresses in RFC822 format on sent mail, if supported by the mail server.
DAYS_TO_KEEP_HISTORY	none	This variable sets the number of days dispatched events will be preserved in the history table. If this variable is not set, events remain on the history table indefinitely.
DAYS_TO_SEND_ON_STARTUP	0	This variable specifies the number of days of old events that are processed and sent when the notifier starts. If set to 2, for example, the notifier will process and send the events of the last two days. Older events will just be marked as processed and won't be sent. The default is 0, so no old messages will be sent at all during startup.

8. Start the **`ovirt-engine-notifier`** service on the Red Hat Storage Console. This activates

the changes you have made:

```
# /etc/init.d/ovirt-engine-notifier start
```

You now receive emails based on events in your Red Hat Storage Environment. The selected events display on the Event Notifier tab for the user.

To cancel event notification:

1. In the **Users** tab, select the user or the user group.
2. Select the **Event Notifier** tab. The Details pane displays the events for which the user will receive notifications.
3. Click the **Manage Events** button. The **Add Event Notification** dialog box displays a list of events for Servers, Gluster Volume, and General Management events. To remove an event notification, deselect events from the list. Click the **Expand All** button to see the complete lists of events.
4. Click **OK**. The deselected events are removed from the display on the **Event Notifier** tab for the user.

Part III. Monitoring

Chapter 8. Monitoring Red Hat Storage Console

System administrators monitor the management environment to view the overall performance of cluster infrastructure. This helps identify key areas in the cluster environment that require attention or optimization. System administrators gain up-to-date information on the performance and status of storage environment components with the **Events** list.

The **Events** list lists all warnings, errors, and other events that occur in the system.

8.1. Viewing the Event List

The **Events** list displays all system events. You can view the events by clicking on **Events** tab. The type of events that appear in the Events tab are audits, warnings, and errors. The names of the user, host, cluster, and Gluster volume involved in the event are also listed. This information helps determine the cause of the event. Click column headers to sort the event list.

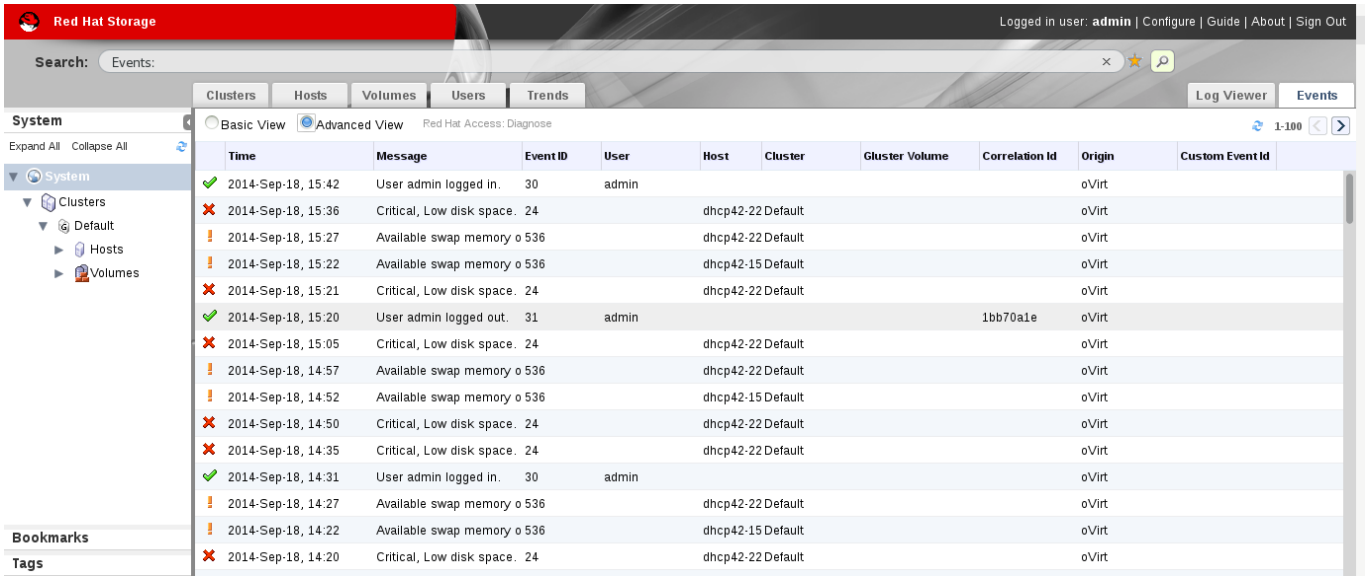


Figure 8.1. Event List - Advanced View

The following table describes the different columns of the **Event** list:

Column	Description
Event	The type of event. The possible event types are: Audit notification (e.g. log on). Warning notification. Error notification.
Time	The time that the event occurred.
Message	The message describing that an event occurred.
User	The user that received the event.
Host	The host on which the event occurred.
Cluster	The cluster on which the event occurred.

8.2. Viewing Alert Information

The **Alerts** pane lists all important notifications regarding the cluster environment.

Alerts display in the lowermost panel on top of the manager interface. Drag the top of the **Alert** pane to resize it or click the minimize/maximize icon in the top right of the pane to show or hide it.

The **Alerts** pane also contains an **Events** list. Click the **Events** tab in the **Alerts** pane to display the **Events** list. See Section 8.1, “Viewing the Event List” for more information about the **Events** list.

Chapter 9. Monitoring Red Hat Storage using Nagios

Red Hat Storage Console provides monitoring of Red Hat Storage trusted storage pool by building on the Nagios platform. You can view the physical and logical resource utilization and status (CPU, Memory, Disk, Network, Swap, Cluster, Volume, Brick) in Trends tab of Red Hat Storage Console. Nagios is installed and enabled in Red Hat Storage Console Server by default to monitor Red Hat Storage nodes. To monitor using Nagios, add hosts to Red Hat Storage Console and configure Nagios using auto-discovery. For more information about adding hosts, see Section 4.2.1, “Adding Hosts”. This chapter describes the procedures for deploying Nagios on Red Hat Storage Console node

For more information on Nagios, see *Nagios Documentation*.

For more information on Changing Nagios Password and Creating Nagios User, see the corresponding sections in *Red Hat Storage Administration Guide*.

The following diagram illustrates deployment of Nagios on Red Hat Storage Console Server.

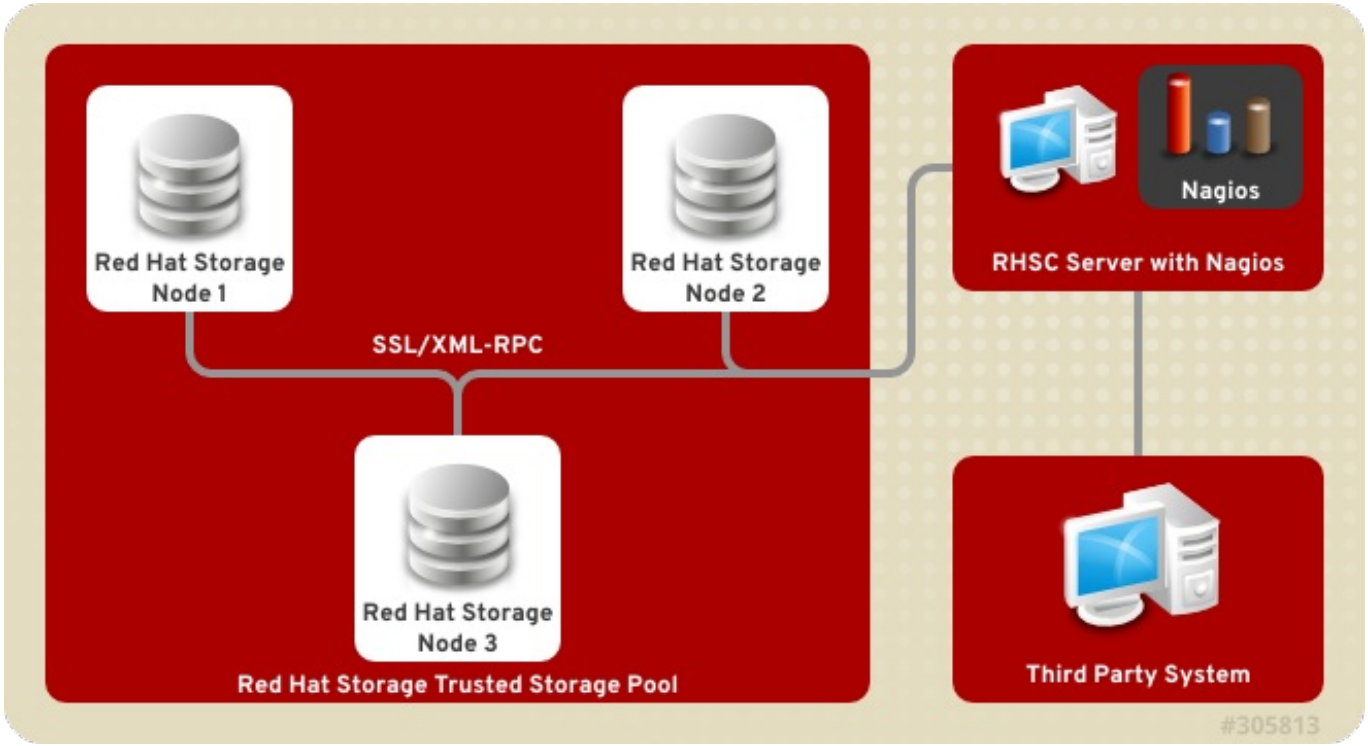


Figure 9.1. Nagios on Red Hat Storage Console Server

9.1. Configuring Nagios using Auto-Discovery

Auto-Discovery is a python script which automatically discovers all the nodes and volumes in the cluster. It also creates Nagios configuration to monitor them. By default, it runs once in 24 hours to synchronize the Nagios configuration from Red Hat Storage Trusted Storage Pool configuration.

For more information on Nagios Configuration files, see Appendix E, *Nagios Configuration Files*

Note

Before configuring Nagios using auto-discovery, ensure that all the Red Hat Storage nodes are configured.

1. Execute **`discovery.py`** script manually only the first time with cluster name and host address on the Nagios server using the following command:

   ```
   # /usr/lib64/nagios/plugins/gluster/discovery.py -c cluster-name -H HostName-or-IP-address
   ```

   For **`-c`**, provide a cluster name (a logical name for the cluster) and for **`-H`**, provide the host name or ip address of a node in the Red Hat Storage trusted storage pool.

2. Perform the steps given below when **`discovery.py`** script runs:

   a. Confirm the configuration when prompted.

   b. Enter the current Nagios server host name or IP address to be configured all the nodes.

   c. Confirm restarting Nagios server when prompted.

   ```
   # /usr/lib64/nagios/plugins/gluster/discovery.py -c demo-cluster -H HostName-or-IP-address
   Cluster configurations changed
   Changes :
   Hostgroup demo-cluster - ADD
   Host demo-cluster - ADD
     Service - Volume Utilization - vol-1 -ADD
     Service - Volume Self-Heal - vol-1 -ADD
     Service - Volume Status - vol-1 -ADD
     Service - Volume Utilization - vol-2 -ADD
     Service - Volume Status - vol-2 -ADD
     Service - Cluster Utilization -ADD
     Service - Cluster - Quorum -ADD
     Service - Cluster Auto Config -ADD
   Host Host_Name - ADD
     Service - Brick Utilization - /bricks/vol-1-5 -ADD
     Service - Brick - /bricks/vol-1-5 -ADD
     Service - Brick Utilization - /bricks/vol-1-6 -ADD
     Service - Brick - /bricks/vol-1-6 -ADD
     Service - Brick Utilization - /bricks/vol-2-3 -ADD
     Service - Brick - /bricks/vol-2-3 -ADD
   Are you sure, you want to commit the changes? (Yes, No) [Yes]:
   Enter Nagios server address [Nagios_Server_Address]:
   Cluster configurations synced successfully from host ip-address
   Do you want to restart Nagios to start monitoring newly discovered entities? (Yes, No) [Yes]:
   Nagios re-started successfully
   ```

   All the hosts, volumes and bricks are added and displayed.

3. Login to the Nagios server GUI using the following URL.

```
https://NagiosServer-HostName-or-IPaddress/nagios
```

Note

- The default Nagios user name and password is *nagiosadmin / nagiosadmin*.
- You can manually update/discover the services by executing the **`discovery.py`** script or by running **`Cluster Auto Config`** service through Nagios Server GUI.
- If the node with which auto-discovery was performed is down or removed from the cluster, run the **`discovery.py`** script with a different node address to continue discovering or monitoring the nodes and services.
- If new nodes or services are added, removed, or if snapshot restore was performed on Red Hat Storage node, run **`discovery.py`** script.

9.2. Configuring Nagios Server to Send Mail Notifications

1. In the **`/etc/nagios/gluster/gluster-contacts.cfg`** file, add contacts to send mail in the format shown below:

   Modify **`contact_name`**, **`alias`**, and **`email`**.

```
define contact {
        contact_name                            Contact1
        alias                                   ContactNameAlias
        email                                   email-address
        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                            Contact2
        alias                                   ContactNameAlias2
        email                                   email-address
        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
}
```

   The **`service_notification_options`** directive is used to define the service states for which notifications can be sent out to this contact. Valid options are a combination of one or more of the following:

- **w**: Notify on WARNING service states
- **u**: Notify on UNKNOWN service states
- **c**: Notify on CRITICAL service states
- **r**: Notify on service RECOVERY (OK states)
- **f**: Notify when the service starts and stops FLAPPING
- **n (none)**: Do not notify the contact on any type of service notifications

The **host_notification_options** directive is used to define the host states for which notifications can be sent out to this contact. Valid options are a combination of one or more of the following:

- **d**: Notify on DOWN host states
- **u**: Notify on UNREACHABLE host states
- **r**: Notify on host RECOVERY (UP states)
- **f**: Notify when the host starts and stops FLAPPING
- **s**: Send notifications when host or service scheduled downtime starts and ends
- **n (none)**: Do not notify the contact on any type of host notifications.

Note

By default, a contact and a contact group are defined for administrators in **contacts.cfg** and all the services and hosts will notify the administrators. Add suitable email id for administrator in **contacts.cfg** file.

2. To add a group to which the mail need to be sent, add the details as given below:

```
  define contactgroup{
        contactgroup_name                    Group1
        alias                                GroupAlias
        members                              Contact1,Contact2
}
```

3. In the **/etc/nagios/gluster/gluster-templates.cfg** file specify the contact name and contact group name for the services for which the notification need to be sent, as shown below:

   Add **contact_groups** name and **contacts** name.

```
define host{
   name                           gluster-generic-host
   use                            linux-server
   notifications_enabled          1
   notification_period            24x7
   notification_interval          120
   notification_options           d,u,r,f,s
   register                       0
```

```
    contact_groups          Group1
    contacts                      Contact1,Contact2
    }

 define service {
    name                          gluster-service
    use                           generic-service
    notifications_enabled        1
    notification_period           24x7
    notification_options          w,u,c,r,f,s
    notification_interval         120
    register                      0
    _gluster_entity               Service
    contact_groups         Group1
    contacts                  Contact1,Contact2

}
```

You can configure notification for individual services by editing the corresponding node configuration file. For example, to configure notification for brick service, edit the corresponding node configuration file as shown below:

```
define service {
  use                             brick-service
  _VOL_NAME                       VolumeName
  __GENERATED_BY_AUTOCONFIG       1
  notes                           Volume : VolumeName
  host_name                       RedHatStorageNodeName
  _BRICK_DIR                      brickpath
  service_description             Brick Utilization - brickpath
  contact_groups          Group1
    contacts                Contact1,Contact2
}
```

4. To receive detailed information on every update when Cluster Auto-Config is run, edit **/etc/nagios/objects/commands.cfg** file add **$NOTIFICATIONCOMMENT$\n** after **$SERVICEOUTPUT$\n** option in **notify-service-by-email** and **notify-host-by-email**command definition as shown below:

```
# 'notify-service-by-email' command definition
define command{
        command_name    notify-service-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios
*****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
Info:\n\n$SERVICEOUTPUT$\n $NOTIFICATIONCOMMENT$\n" | /bin/mail -s
"** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is
$SERVICESTATE$ **" $CONTACTEMAIL$
        }
```

5. Restart the Nagios server using the following command:

```
# service nagios restart
```

The Nagios server sends notifications during status changes to the mail addresses specified in the file.

Note

- By default, the system ensures three occurances of the event before sending mail notifications.
- By default, Nagios Mail notification is sent using **`/bin/mail`** command. To change this, modify the definition for **`notify-host-by-email`** command and **`notify-service-by-email`** command in **`/etc/nagios/objects/commands.cfg`** file and configure the mail server accordingly.

9.3. Verifying the Configuration

1. Verify the updated configurations using the following command:

   ```
   # nagios -v /etc/nagios/nagios.cfg
   ```

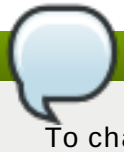
   If error occurs, verify the parameters set in **`/etc/nagios/nagios.cfg`** and update the configuration files.

2. Restart Nagios server using the following command:

   ```
   # service nagios restart
   ```

3. Log into the Nagios server GUI using the following URL with the Nagios Administrator user name and password.

   ```
   https://NagiosServer-HostName-or-IPaddress/nagios
   ```

   Note

   To change the default password, see *Changing Nagios Password* section in *Red Hat Storage Administration Guide.*

4. Click **`Services`** in the left pane of the Nagios server GUI and verify the list of hosts and services displayed.

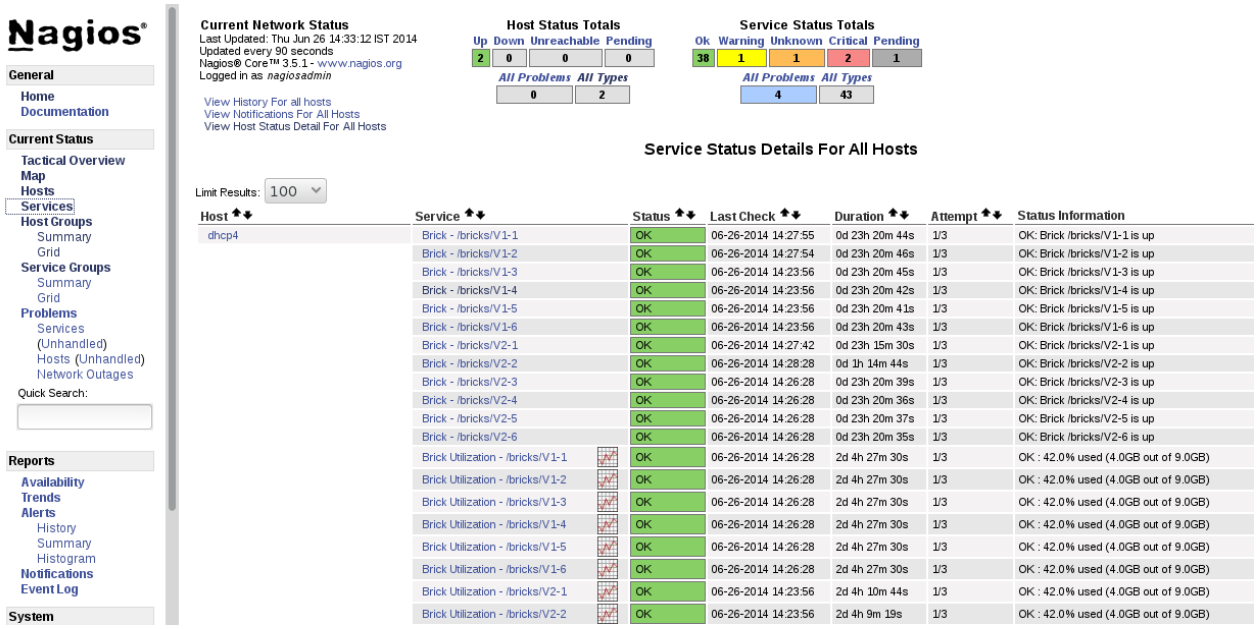


Figure 9.2. Nagios Services

9.4. Using Nagios Server GUI

You can monitor Red Hat Storage trusted storage pool through Nagios Server GUI.

To view the details, log into the Nagios Server GUI by using the following URL.

```
https://NagiosServer-HostName-or-IPaddress/nagios
```

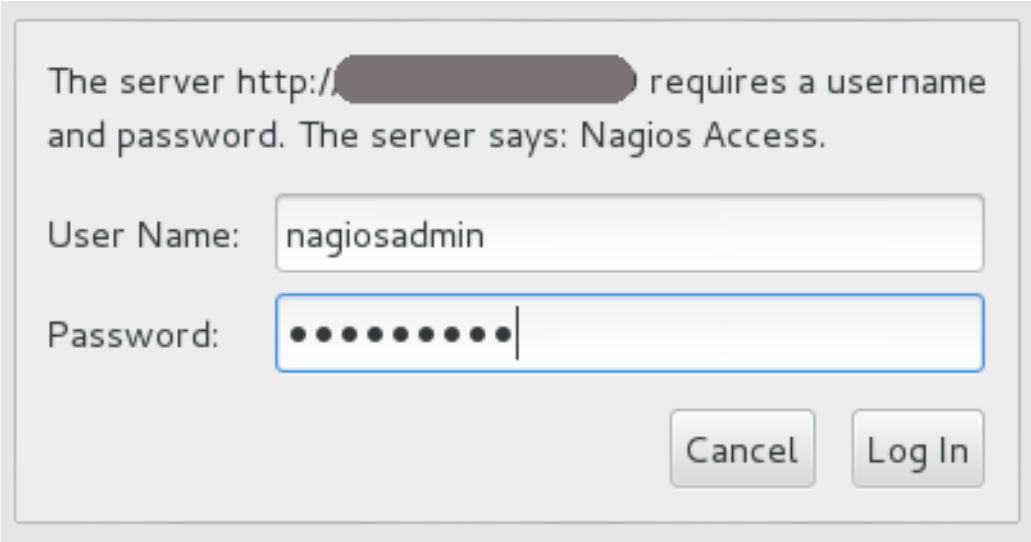


Figure 9.3. Nagios Login

Cluster Overview

To view the overview of the hosts and services being monitored, click **`Tactical Overview`** in the left pane. The overview of Network Outages, Hosts, Services, and Monitoring Features are displayed.

Figure 9.4. Tactical Overview

Host Status

To view the status summary of all the hosts, click **Summary** under **Host Groups** in the left pane.

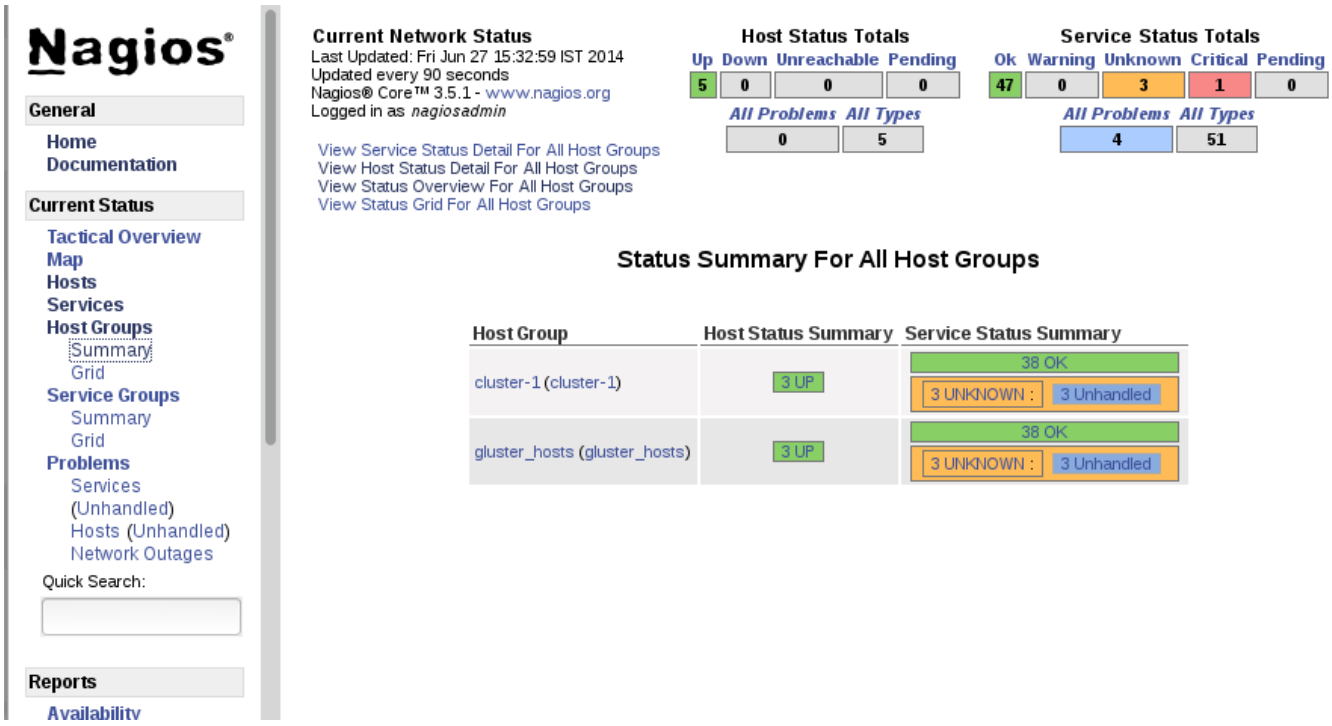


Figure 9.5. Host Groups Summary

To view the list of all hosts and their status, click **Hosts** in the left pane.

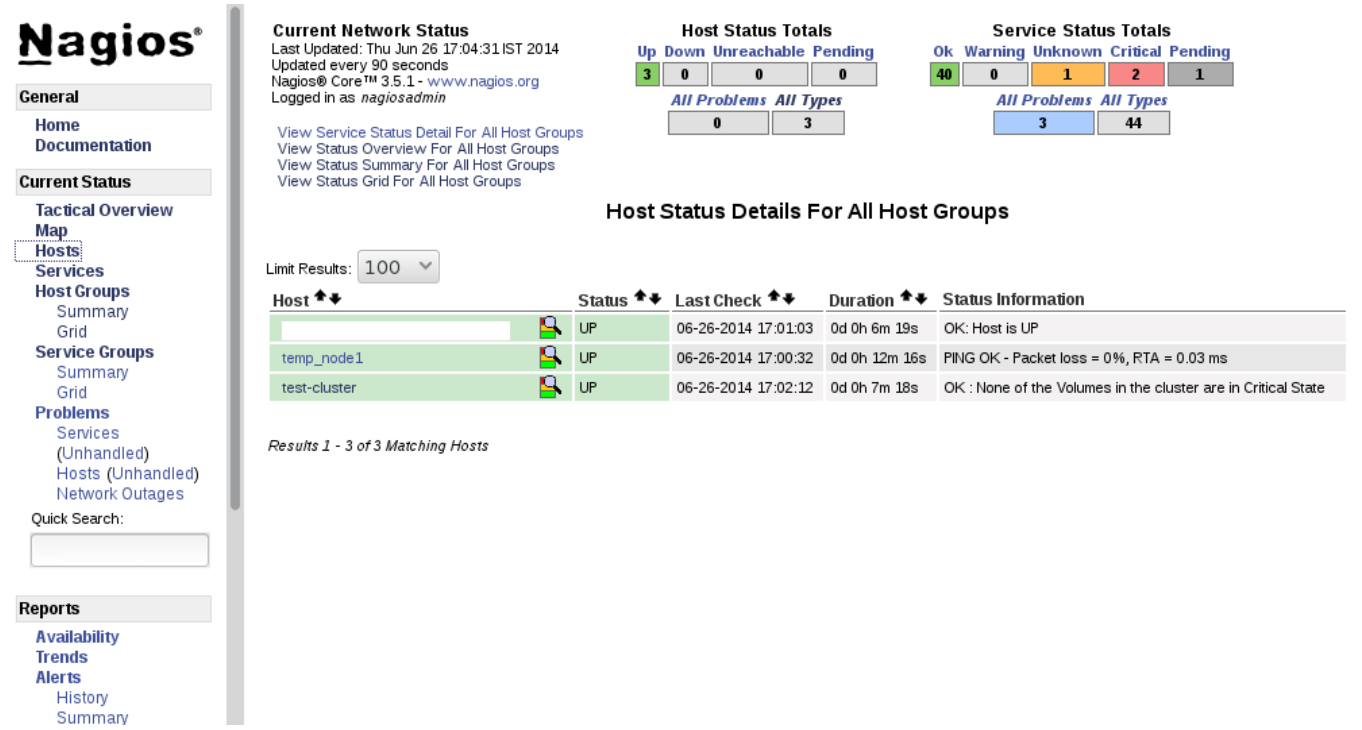


Figure 9.6. Host Status

Service Status

To view the list of all hosts and their service status click **`Services`** in the left pane.

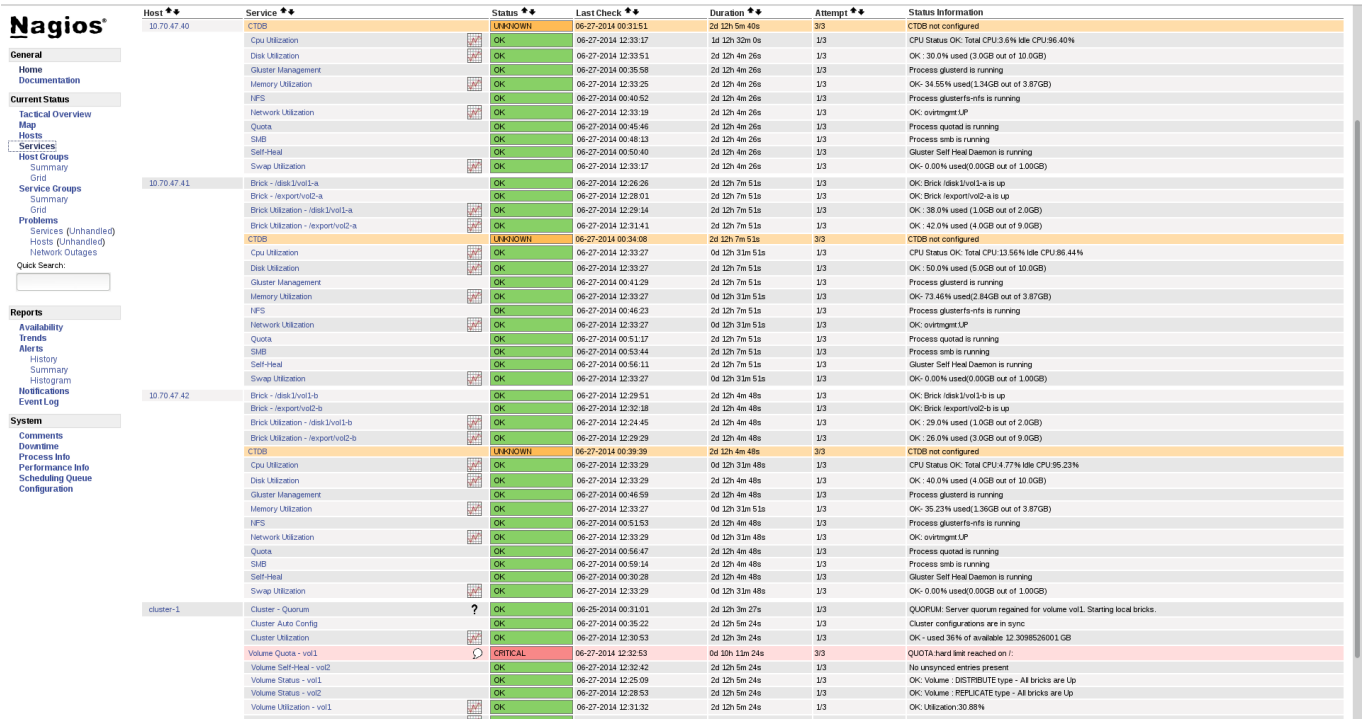


Figure 9.7. Service Status

Note

In the left pane of Nagios Server GUI, click **Availability** and **Trends** under the **Reports** field to view the Host and Services Availability and Trends.

Host Services

1. Click **Hosts** in the left pane. The list of hosts are displayed.
2. Click  corresponding to the host name to view the host details.
3. Click on the service name to view the Service State Information. You can view the utilization of the following services:
   - Memory
   - Swap
   - CPU
   - Network
   - Brick
   - Disk

   The Performance data for services is displayed in the following format: *value[UnitOfMeasurement]*;*warningthreshold*;*criticalthreshold*;*min*;*max*. The *min* and *max* values are optional.

   The Disk Utilization Performance data has two sets of information for every mount point which are disk detail and inode detail of a disk. For example, Performance Data = *disk1-data disk1-inode-data ... diskN-data diskN-inode-data*.
4. To view the utilization graph, click  corresponding to the service name. The utilization graph is displayed.

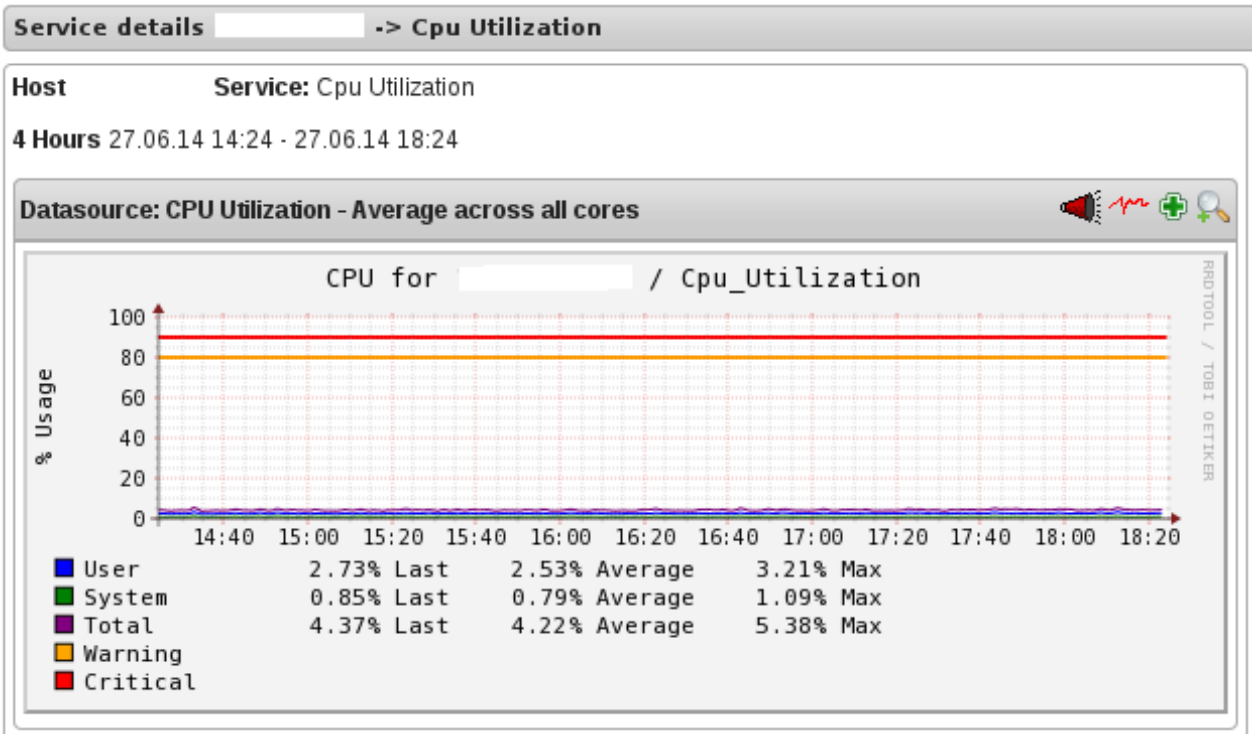


Figure 9.8. CPU Utilization

5. To monitor status, click on the service name. You can monitor the status for the following resources:
   - Disk
   - Network
6. To monitor process, click on the process name. You can monitor the following processes:
   - NFS(NetworkFileSystem)
   - Self-Heal(SelfHeal)
   - GlusterManagement(glusterd)
   - Quota(Quota daemon)
   - CTDB
   - SMB

Note

Monitoring Openstack Swift operations is not supported.

Cluster Services

1. Click **Hosts** in the left pane. The list of hosts and clusters are displayed.
2. Click  corresponding to the cluster name to view the cluster details.

3. To view utilization graph, click  corresponding to the service name. You can monitor the following utilizations:

   - Cluster
   - Volume

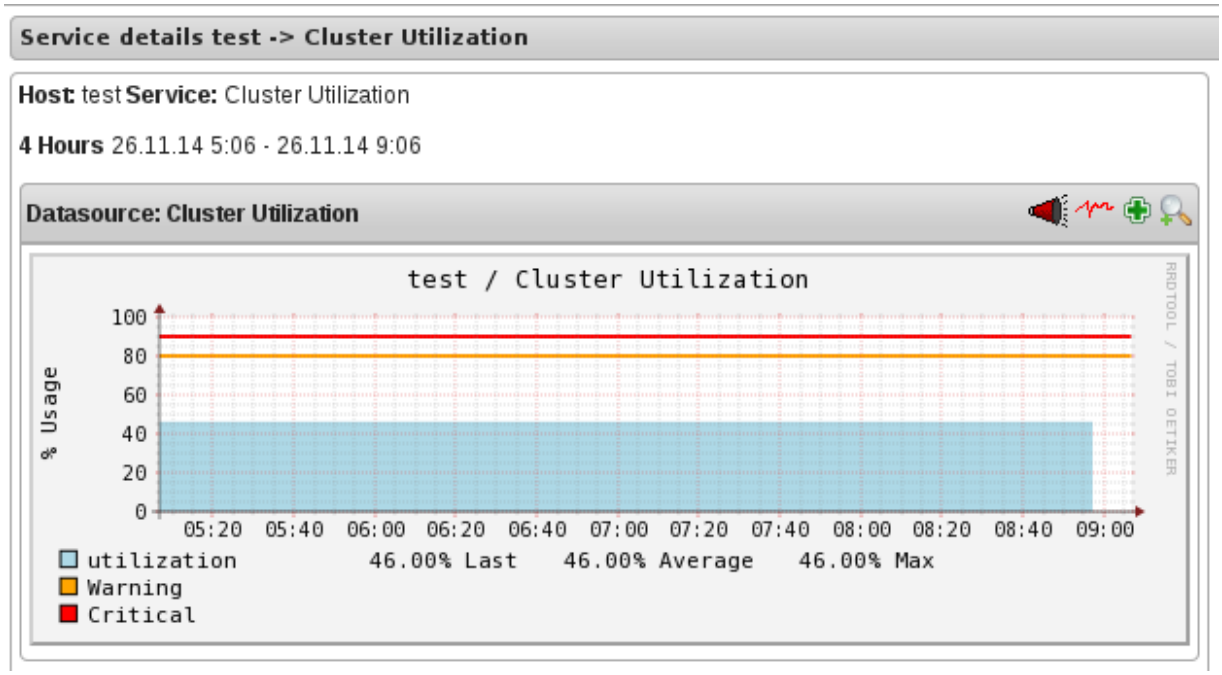


Figure 9.9. Cluster Utilization

4. To monitor status, click on the service name. You can monitor the status for the following resources:

   - Host
   - Volume
   - Brick

5. To monitor cluster services, click on the service name. You can monitor the following:

   - Volume Quota
   - Volume Geo-replication
   - Volume Self Heal
   - Cluster Quorum (A cluster quorum service would be present only when there are volumes in the cluster.)

Rescheduling Cluster Auto config through Nagios Server GUI

If new nodes or services are added or removed, or if snapshot restore was performed on Red Hat Storage node, reschedule the **`Cluster Auto config`** service through Nagios Server GUI or executing the **`discovery.py`** script. To synchronize the configurations through Nagios Server GUI, perform the steps given below:

1. Login to the Nagios Server GUI using the following URL in your browser with nagiosadmin

user name and password.

```
https://NagiosServer-HostName-or-IPaddress/nagios
```

2. Click **Services** in left pane of Nagios server GUI and click **Cluster Auto Config**.

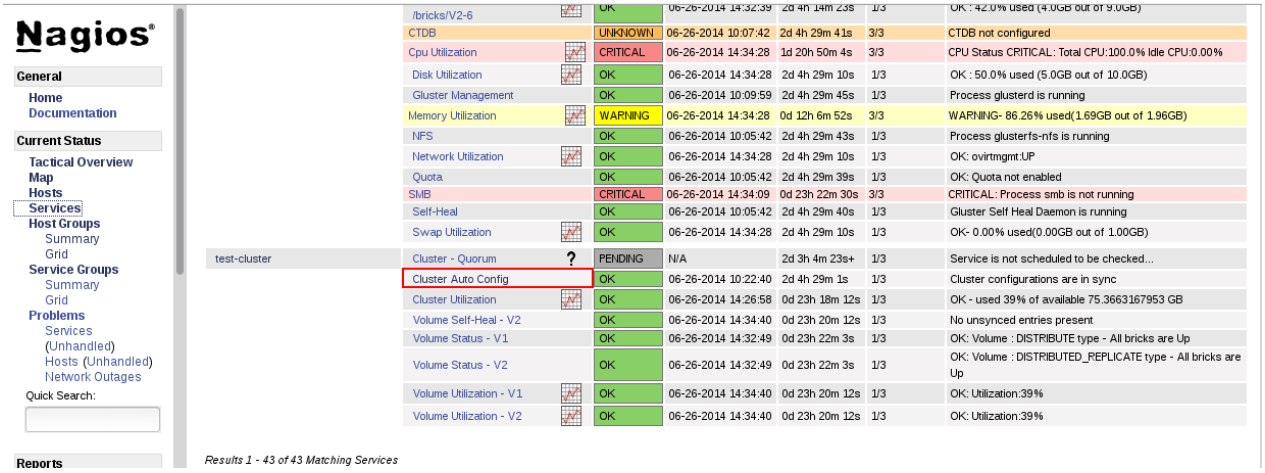


Figure 9.10. Nagios Services

3. In **Service Commands**, click **Re-schedule the next check of this service**. The **Command Options** window is displayed.

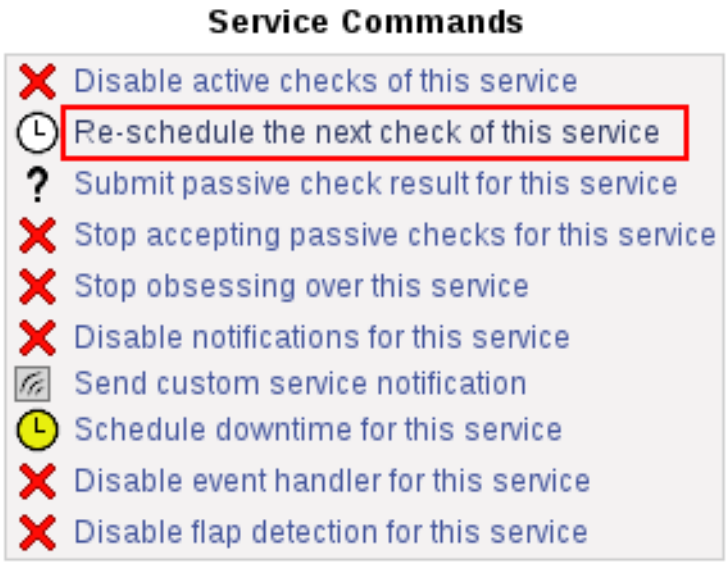


Figure 9.11. Service Commands

4. In **Command Options** window, click **Commit**.

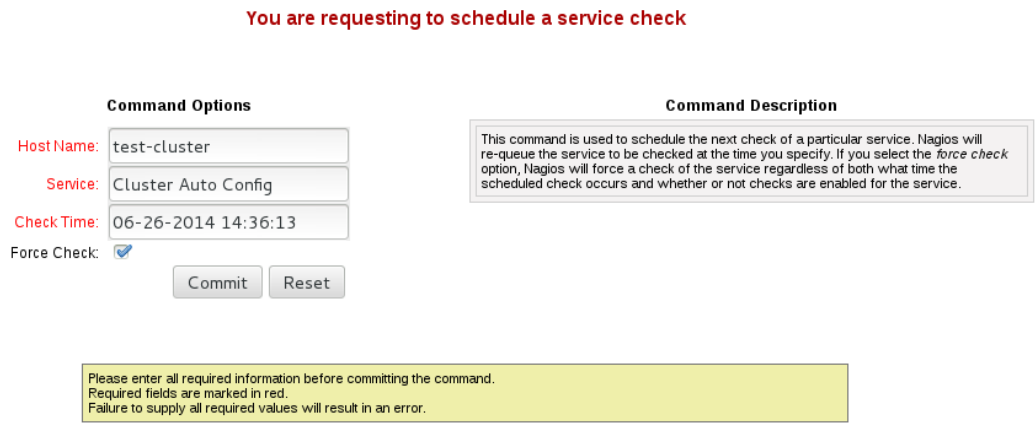


Figure 9.12. Command Options

Monitoring Services Status and Messages

Table 9.1.

Service Name	Status	Messsage	Description
SMB	OK	OK: No gluster volume uses smb	When no volumes are exported through smb.
	OK	Process smb is running	When SMB service is running and when volumes are exported using SMB.
	CRITICAL	CRITICAL: Process smb is not running	When SMB service is down and one or more volumes are exported through SMB.
CTDB	UNKNOWN	CTDB not configured	When CTDB service is not running, and smb or nfs service is running.
	CRITICAL	Node status: BANNED/STOPPED	When CTDB service is running but Node status is *BANNED/STOPPED*.
	WARNING	Node status: UNHEALTHY/DISABLED/PARTIALLY_ONLINE	When CTDB service is running but Node status is *UNHEALTHY/DISABLED/PARTIALLY_ONLINE*.
	OK	Node status: OK	When CTDB service is running and healthy.
Gluster Management	OK	Process glusterd is running	When glusterd is running as unique.
	WARNING	PROCS WARNING: 3 processes	When there are more then one glusterd is running.
	CRITICAL	CRITICAL: Process glusterd is not running	When there is no glusterd process running.

Service Name	Status	Messsage	Description
	UNKNOWN	NRPE: Unable to read output	When unable to communicate or read output
NFS	OK	OK: No gluster volume uses nfs	When no volumes are configured to be exported through NFS.
	OK	Process glusterfs-nfs is running	When glusterfs-nfs process is running.
	CRITICAL	CRITICAL: Process glusterfs-nfs is not running	When glusterfs-nfs process is down and there are volumes which requires NFS export.
Self-Heal	OK	Gluster Self Heal Daemon is running	When self-heal process is running.
	OK	OK: Process Gluster Self Heal Daemon	
	CRITICAL	CRITICAL: Gluster Self Heal Daemon not running	When gluster self heal process is not running.
Auto-Config	OK	Cluster configurations are in sync	When auto-config has not detected any change in Gluster configuration. This shows that Nagios configuration is already in synchronization with the Gluster configuration and auto-config service has not made any change in Nagios configuration.
	OK	Cluster configurations synchronized successfully from host *host-address*	When auto-config has detected change in the Gluster configuration and has successfully updated the Nagios configuration to reflect the change Gluster configuration.

Service Name	Status	Messsage	Description
	CRITICAL	Can't remove all hosts except sync host in 'auto' mode. Run auto discovery manually.	When the host used for auto-config itself is removed from the Gluster peer list. Auto-config will detect this as all host except the synchronized host is removed from the cluster. This will not change the Nagios configuration and the user need to manually run the auto-config.
QUOTA	OK	OK: Quota not enabled	When quota is not enabled in any volumes.
	OK	Process quotad is running	When glusterfs-quota service is running.
	CRITICAL	CRITICAL: Process quotad is not running	When glusterfs-quota service is down and quota is enabled for one or more volumes.
CPU Utilization	OK	CPU Status OK: Total CPU:4.6% Idle CPU:95.40%	When CPU usage is less than 80%.
	WARNING	CPU Status WARNING: Total CPU:82.40% Idle CPU:17.60%	When CPU usage is more than 80%.
	CRITICAL	CPU Status CRITICAL: Total CPU:97.40% Idle CPU:2.6%	When CPU usage is more than 90%.
Memory Utilization	OK	OK- 65.49% used(1.28GB out of 1.96GB)	When used memory is below warning threshold. (Default warning threshold is 80%)
	WARNING	WARNING- 85% used(1.78GB out of 2.10GB)	When used memory is below critical threshold (Default critical threshold is 90%) and greater than or equal to warning threshold (Default warning threshold is 80%).
	CRITICAL	CRITICAL- 92% used(1.93GB out of 2.10GB)	When used memory is greater than or equal to critical threshold (Default critical threshold is 90%)
Brick Utilization	OK	OK : 38.0% used (4.0GB out of 9.0GB)	When used space is lesser than 80%.

Service Name	Status	Messsage	Description
	WARNING	WARNING: 82.0% used (41.0GB out of 50.0GB)	When used space is more than 80% (Default is 80%).
	CRITICAL	CRITICAL : 92.0% used (46.0GB out of 50.0GB)	When used space is more than 90% (Default is 90%).
	CRITICAL	CRITICAL : mount: /bricks/b1=None(Device not found!)	When the brick path/mount not found.
	CRITICAL	CRITICAL : mount: /bricks/b1=None(Unable to access the device)	When the brick is not accessible.
	CRITICAL		When there is any other disk error.
Disk Utilization	OK	OK : 12.0% used (1.0GB out of 7.0GB)	When the disk is in normal state.
	WARNING	WARNING : 82.0% used (6.0GB out of 7.0GB)	When it reaches the warning threshold.
	CRITICAL	CRITICAL : mount: /dev/sda1=None(Unable to access the device)	If the device is not accessible.
	CRITICAL	CRITICAL : mount: /dev/sda2=None(Device not found!)	When the disk path/mount not found.
Network Utilization	OK	OK: tun0:UP,wlp3s0:UP,virbr0:UP	When all the interfaces are UP.
	WARNING	WARNING: tun0:UP,wlp3s0:UP,virbr0:DOWN	When any of the interfaces is down.
	UNKNOWN	UNKNOWN	When network utilization/status is unknown.
Swap Utilization	OK	OK- 0.00% used(0.00GB out of 1.00GB)	When used memory is below warning threshold (Default warning threshold is 80%).
	WARNING	WARNING- 83% used(1.24GB out of 1.50GB)	When used memory is below critical threshold (Default critical threshold is 90%) and greater than or equal to warning threshold (Default warning threshold is 80%).
	CRITICAL	CRITICAL- 83% used(1.42GB out of 1.50GB)	When used memory is greater than or equal to critical threshold (Default critical threshold is 90%).

Service Name	Status	Messsage	Description
Cluster- Quorum	PENDING		When cluster.quorum-type is not set to *server*; or when there are no problems in the cluster identified.
	OK	Quorum regained for volume	When quorum is regained for volume.
	CRITICAL	Quorum lost for volume	When quorum is lost for volume.
Volume Geo-replication	OK	"Session Status: *slave_vol1*-OK .....*slave_voln*-OK.	When all sessions are active.
		Session status :No active sessions found	When Geo-replication sessions are deleted.
	CRITICAL	Session Status: *slave_vol1*-FAULTY *slave_vol2*-OK	If one or more nodes are Faulty and there's no replica pair that's active.
	WARNING	Session Status: *slave_vol1*-NOT_STARTED *slave_vol2*-STOPPED *slave_vol3*-PARTIAL_FAULTY	• Partial faulty state occurs with replicated and distributed replicate volume when one node is faulty, but the replica pair is active. • *STOPPED* state occurs when Geo-replication sessions are stopped. • *NOT_STARTED* state occurs when there are multiple Geo-replication sessions and one of them is stopped.
	WARNING	Geo replication status could not be determined.	When there's an error in getting Geo replication status. This error occurs when **`volfile`** is locked as another transaction is in progress.
	UNKNOWN	Geo replication status could not be determined.	When glusterd is down.
Volume Quota	OK	QUOTA: not enabled or configured	When quota is not set

Service Name	Status	Messsage	Description
	OK	QUOTA:OK	When quota is set and usage is below quota limits.
	WARNING	QUOTA:Soft limit exceeded on *path of directory*	When quota exceeds soft limit.
	CRITICAL	QUOTA:hard limit reached on *path of directory*	When quota reaches hard limit.
	UNKNOWN	QUOTA: Quota status could not be determined as command execution failed	When there's an error in getting Quota status. This occurs when - Volume is stopped or glusterd service is down. - volfile is locked as another transaction in progress.
Volume Status	OK	Volume : *volume type* - All bricks are Up	When all volumes are up.
	WARNING	Volume :*volume type* Brick(s) - *list of bricks* is|are down, but replica pair(s) are up	When bricks in the volume are down but replica pairs are up.
	UNKNOWN	Command execution failed *Failure message*	When command execution fails.
	CRITICAL	Volume not found.	When volumes are not found.
	CRITICAL	Volume: *volume-type* is stopped.	When volumes are stopped.
	CRITICAL	Volume : *volume type* - All bricks are down.	When all bricks are down.
	CRITICAL	Volume : *volume type* Bricks - *brick list* are down, along with one or more replica pairs	When bricks are down along with one or more replica pairs.
Volume Self-Heal	OK		When volume is not a replicated volume, there is no self-heal to be done.
	OK	No unsynced entries present	When there are no unsynched entries in a replicated volume.

Service Name	Status	Messsage	Description
	WARNING	Unsynched entries present : There are unsynched entries present.	If self-heal process is turned on, these entries may be auto healed. If not, self-heal will need to be run manually. If unsynchronized entries persist over time, this could indicate a split brain scenario.
	WARNING	Self heal status could not be determined as the volume was deleted	When self-heal status can not be determined as the volume is deleted.
	UNKNOWN		When there's an error in getting self heal status. This error occurs when: - Volume is stopped or glusterd service is down. - volfile is locked as another transaction in progress.
Cluster Utilization	OK	OK : 28.0% used (1.68GB out of 6.0GB)	When used % is below the warning threshold (Default warning threshold is 80%).
	WARNING	WARNING: 82.0% used (4.92GB out of 6.0GB)	Used% is above the warning limit. (Default warning threshold is 80%)
	CRITICAL	CRITICAL : 92.0% used (5.52GB out of 6.0GB)	Used% is above the warning limit. (Default critical threshold is 80%)
	UNKNOWN	Volume utilization data could not be read	When volume services are present, but the volume utilization data is not available as it's either not populated yet or there is error in fetching volume utilization data.
Volume Utilization	OK	OK: Utilization: 40 %	When used % is below the warning threshold (Default warning threshold is 80%).
	WARNING	WARNING - used *84*% of available *200* GB	When used % is above the warning threshold (Default warning threshold is 80%).

Service Name	Status	Messsage	Description
	CRITICAL	CRITICAL - used *96%* of available *200* GB	When used % is above the critical threshold (Default critical threshold is 90%).
	UNKNOWN	UNKNOWN - Volume utilization data could not be read	When all the bricks in the volume are killed or if glusterd is stopped in all the nodes in a cluster.

9.5. Monitoring Host and Cluster Utilization

9.5.1. Monitoring Host and Cluster Utilization

You can monitor utilization and set alerts and notifications for the utilization changes.

You can monitor Host and Cluster utilization using Nagios plug-in and validate the status of clusters and hosts from the utilization graph through Red Hat Storage Console.

Note

By default, you can view the Utilization report of the last 24 hours.

Procedure 9.1. To Monitor Cluster Utilization

1. Click **System** and select **Clusters** in the Tree pane.
2. Click **Trends** tab.

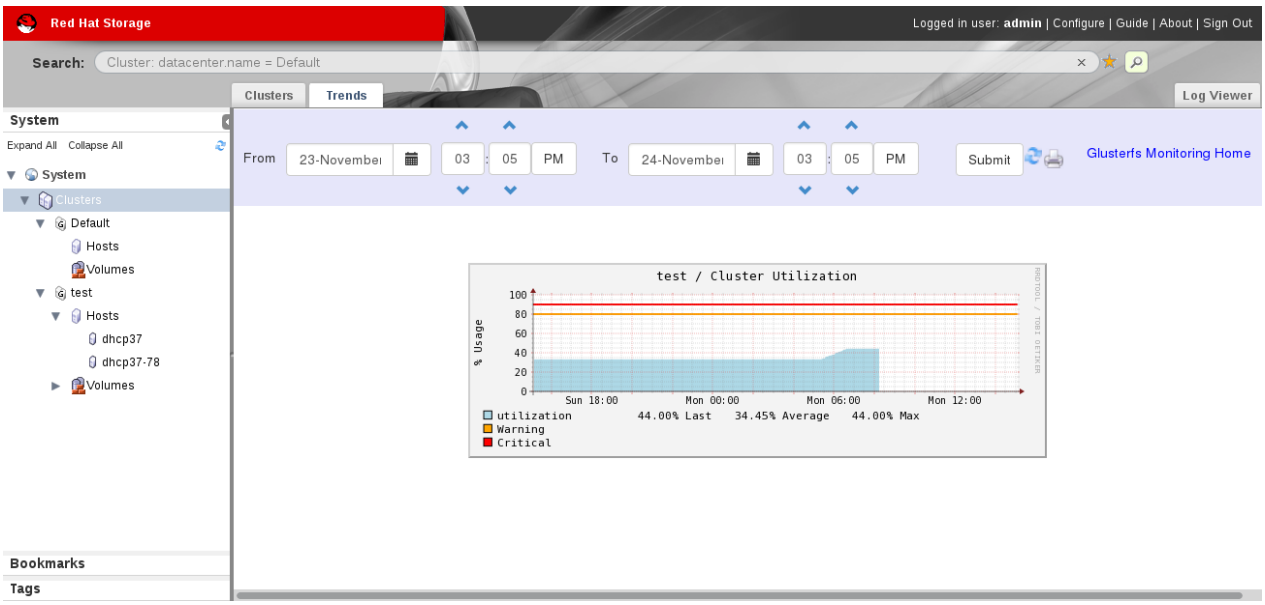


Figure 9.13. Trends

3. Select the date and time duration to view the cluster utilization report.

4. Click **Submit**. The Cluster Utilization graph of all clusters for the selected period is displayed.

   You can refresh the status by clicking the refresh button and also print the report or save as a pdf file by clicking the print button. Click **Glusterfs Monitoring Home** to view the Nagios Home page.

Procedure 9.2. To Monitor Utilization for Hosts

1. Click **System** and select **Clusters** in the Tree pane.
2. Click **Hosts** in the tree pane and click **Trends** tab to view the CPU Utilization for all the hosts.

   To view *CPU Utilization*, *Network Interface Utilization*, *Disk Utilization*,*Memory Uttilization* and *Swap Utilization* for each host, select the Host name from the tree pane and click **Trends** tab.

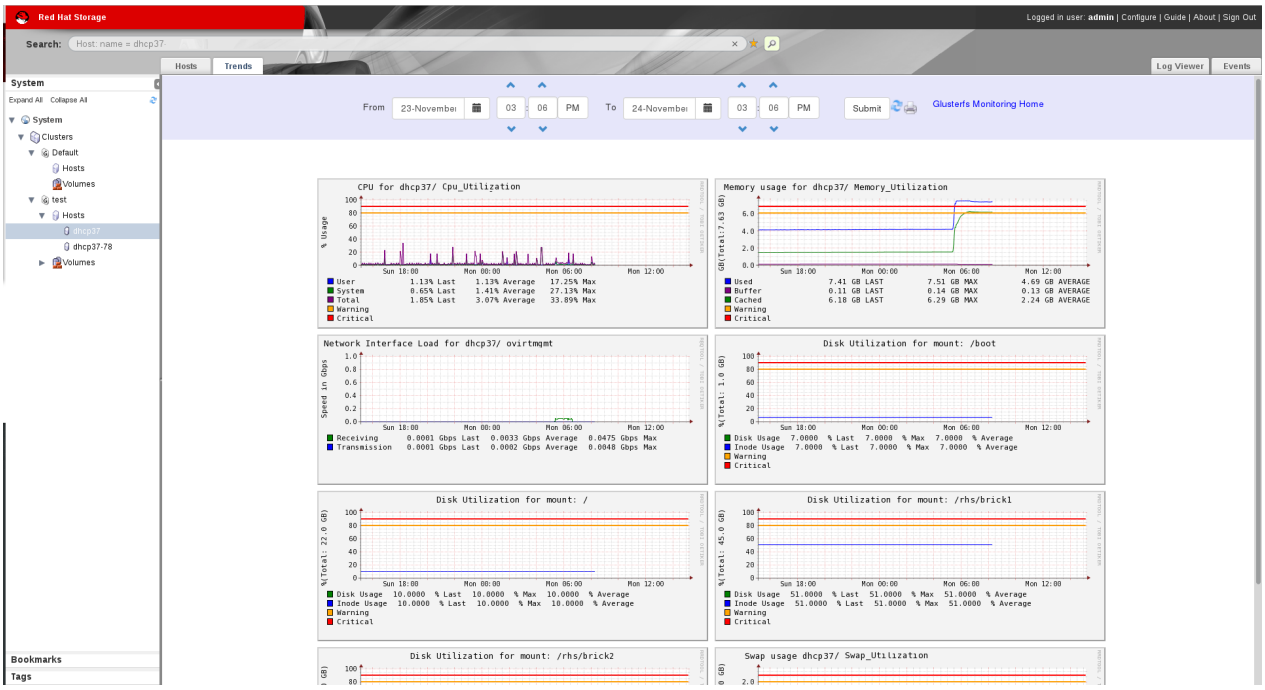


Figure 9.14. Utilization for selected Host

3. Select the date and time to view the Host Utilization report.
4. Click **Submit**. The CPU Utilization graph for all the Hosts for the selected period is displayed.

   You can refresh the status by clicking the refresh button and also print the report or save as a pdf file by clicking the print button. To view the Nagios Home page, click **Glusterfs Monitoring Home**.

Procedure 9.3. To monitor Volume and Brick Utilization

1. Open the **Volumes** view in the tree pane and select **Volumes**.
2. Click **Trends** tab.
3. Select the date and time duration to view the volume and brick utilization report.
4. Click **Submit**. The Volume Utilization graph and Brick Utilization graph for the selected period is displayed.

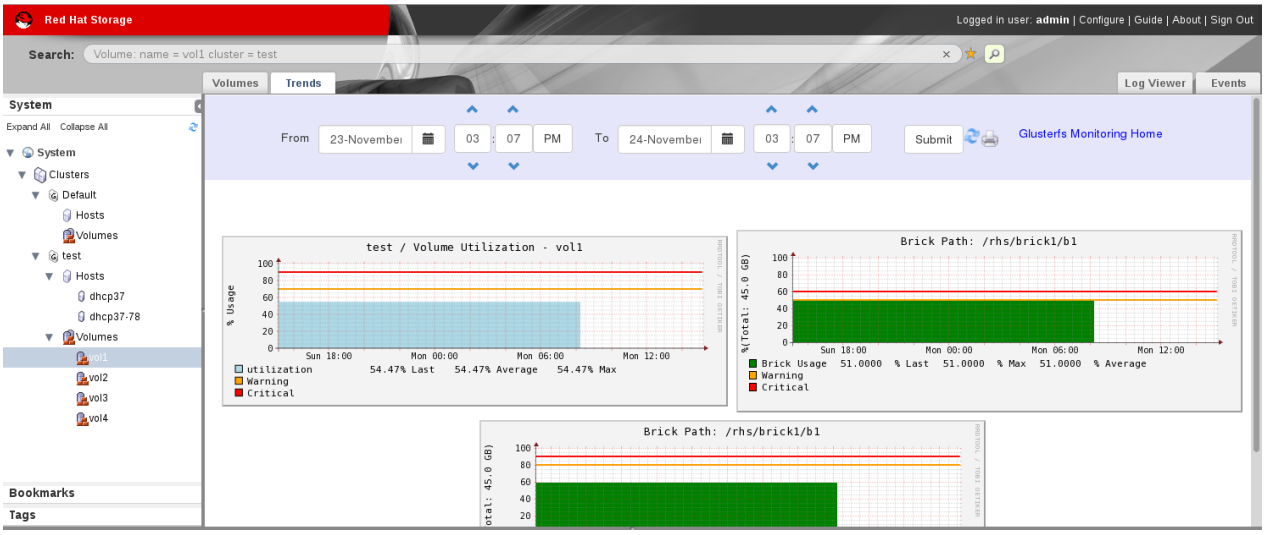


Figure 9.15. Volume and Brick Utilization

You can refresh the status by clicking the refresh button and also print the report or save as a pdf file by clicking the print button. To view the Nagios Home page, click **`Glusterfs Monitoring Home`**.

9.5.2. Enabling and Disabling Monitoring

You can enable and disable monitoring using the command line interface after setting up Red Hat Storage Console. The **`Trends`** tab is displayed with host and cluster utilization details when monitoring is enabled on the server.

Important

You must refresh the browser after enabling or disabling monitoring to view the changes.

- To enable monitoring, run the following command in the Red Hat Storage Console Server :

```
# rhsc-monitoring enable
Setting the monitoring flag...
Starting nagios: done.
Starting nsca: [  OK  ]
INFO: Move the nodes of existing cluster (with compatibilty version >=
3.4) to maintenance and re-install them.
```

The **`Trends`** tab is displayed in the Red Hat Storage Console Administrator portal with the host and cluster utilization details.

- To disable monitoring, run the following command in the Red Hat Storage Console Server:

```
 #rhsc-monitoring disable
Setting the monitoring flag...
Stopping nagios: .done.
Shutting down nsca: [  OK  ]
```

The **Trends** tab is not displayed in the Red Hat Storage Console Administrator portal and the user cannot view host and cluster utilization details. Receiving email and SNMP notifications are disabled. Disabling monitoring also stops Nagios and NSCA services.

Disabling monitoring does not stop the **glusterpmd** service. Run the following commands on all the Red Hat Storage nodes to stop **glusterpmd** service and to remove **chkconfig** for glusterpmd service:

```
# service glusterpmd stop
# chkconfig glusterpmd off
```

9.6. Troubleshooting Nagios

9.6.1. Troubleshooting NSCA and NRPE Configuration Issues

The possible errors while configuring Nagios Service Check Acceptor (NSCA) and Nagios Remote Plug-in Executor (NRPE) and the troubleshooting steps are listed in this section.

Troubleshooting NSCA Configuration Issues

- **Check Firewall and Port Settings on Nagios Server**

  If port 5667 is not opened on the server host's firewall, a timeout error is displayed. Ensure that port *5667* is opened.

  - Log in as root and run the following command on the Red Hat Storage node to get the list of current iptables rules:

    ```
    # iptables -L
    ```

  - The output is displayed as shown below:

    ```
    ACCEPT     tcp  --  anywhere             anywhere             tcp
    dpt:5667
    ```

  - If the port is not opened, add an iptables rule by adding the following line in **/etc/sysconfig/iptables** file:

    ```
    -A INPUT -m state --state NEW -m tcp -p tcp --dport 5667 -j
    ACCEPT
    ```

  - Restart the iptables service using the following command:

    ```
    # service iptables restart
    ```

  - Restart the NSCA service using the following command:

    ```
    # service nsca restart
    ```

- **Check the Configuration File on Red Hat Storage Node**

  Messages cannot be sent to the NSCA server, if Nagios server IP or FQDN, cluster name and hostname (as configured in Nagios server) are not configured correctly.

Open the Nagios server configuration file */etc/nagios/nagios_server.conf* and verify if the correct configurations are set as shown below:

```
# NAGIOS SERVER
# The nagios server IP address or FQDN to which the NSCA command
# needs to be sent
[NAGIOS-SERVER]
nagios_server=NagiosServerIPAddress


# CLUSTER NAME
# The host name of the logical cluster configured in Nagios under
which
# the gluster volume services reside
[NAGIOS-DEFINTIONS]
cluster_name=cluster_auto


# LOCAL HOST NAME
# Host name given in the nagios server
[HOST-NAME]
hostname_in_nagios=NagiosServerHostName
```

If Host name is updated, restart the NSCA service using the following command:

```
# service nsca restart
```

Troubleshooting NRPE Configuration Issues

- **CHECK_NRPE: Error - Could Not Complete SSL Handshake**

  This error occurs if the IP address of the Nagios server is not defined in the **nrpe.cfg** file of the Red Hat Storage node. To fix this issue, follow the steps given below:

  - Add the Nagios server IP address in **/etc/nagios/nrpe.cfg** file in the **allowed_hosts** line as shown below:

    ```
    allowed_hosts=127.0.0.1, NagiosServerIP
    ```

    The **allowed_hosts** is the list of IP addresses which can execute NRPE commands.

  - Save the **nrpe.cfg** file and restart the NRPE service using the following command:

    ```
    # service nrpe restart
    ```

- **CHECK_NRPE: Socket Timeout After n Seconds**

  To resolve this issue perform the steps given below:

  On Nagios Server:

  The default timeout value for the NRPE calls is 10 seconds and if the server does not respond within 10 seconds, Nagios GUI displays an error that the NRPE call has timed out in 10 seconds. To fix this issue, change the timeout value for NRPE calls by modifying the command definition configuration files.

  - Changing the NRPE timeout for services which directly invoke *check_nrpe*

- Changing the NRPE timeout for services which directly invoke *check_nrpe*.

  For the services which directly invoke *check_nrpe* (check_disk_and_inode, check_cpu_multicore, and check_memory), modify the command definition configuration file **/etc/nagios/gluster/gluster-commands.cfg** by adding *-t Time in Seconds* as shown below:

```
define command {
       command_name check_disk_and_inode
       command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c
check_disk_and_inode -t TimeInSeconds
}
```

- Changing the NRPE timeout for the services in **nagios-server-addons** package which invoke NRPE call through code.

  The services which invoke **/usr/lib64/nagios/plugins/gluster/check_vol_server.py** (check_vol_utilization, check_vol_status, check_vol_quota_status, check_vol_heal_status, and check_vol_georep_status) make NRPE call to the Red Hat Storage nodes for the details through code. To change the timeout for the NRPE calls, modify the command definition configuration file **/etc/nagios/gluster/gluster-commands.cfg** by adding *-t No of seconds* as shown below:

```
define command {
      command_name check_vol_utilization
      command_line $USER1$/gluster/check_vol_server.py $ARG1$
$ARG2$ -w $ARG3$ -c $ARG4$ -o utilization -t TimeInSeconds
}
```

  The auto configuration service **gluster_auto_discovery** makes NRPE calls for the configuration details from the Red Hat Storage nodes. To change the NRPE timeout value for the auto configuration service, modify the command definition configuration file **/etc/nagios/gluster/gluster-commands.cfg** by adding *-t TimeInSeconds* as shown below:

```
define command{
        command_name    gluster_auto_discovery
        command_line    sudo $USER1$/gluster/discovery.py -H
$ARG1$ -c $HOSTNAME$ -m auto -n $ARG2$ -t TimeInSeconds
}
```

- Restart Nagios service using the following command:

```
# service nagios restart
```

On Red Hat Storage node:

- Add the Nagios server IP address as described in *CHECK_NRPE: Error - Could Not Complete SSL Handshake* section in *Troubleshooting NRPE Configuration Issues* section.

- Edit the **nrpe.cfg** file using the following command:

```
# vi /etc/nagios/nrpe.cfg
```

- Search for the **command_timeout** and **connection_timeout** settings and change the value. The **command_timeout** value must be greater than or equal to the timeout value set in Nagios server.

  The timeout on checks can be set as *connection_timeout=300* and the *command_timeout=60* seconds.

- Restart the NRPE service using the following command:

```
# service nrpe restart
```

- **Check the NRPE Service Status**

  This error occurs if the NRPE service is not running. To resolve this issue perform the steps given below:

  - Verify the status of NRPE service by logging into the Red Hat Storage node as root and running the following command:

```
# service nrpe status
```

  - If NRPE is not running, start the service using the following command:

```
# service nrpe start
```

- **Check Firewall and Port Settings**

  This error is associated with firewalls and ports. The timeout error is displayed if the NRPE traffic is not traversing a firewall, or if port *5666* is not open on the Red Hat Storage node.

  Enure that port 5666 is open on the Red Hat Storage node.

  - Run **check_nrpe** command from the Nagios server to verify if the port is open and if NRPE is running on the Red Hat Storage Node .

  - Log into the Nagios server as root and run the following command:

```
# /usr/lib64/nagios/plugins/check_nrpe -H RedHatStorageNodeIP
```

  - The output is displayed as given below:

```
NRPE v2.14
```

  If not, ensure the that port 5666 is opened on the Red Hat Storage node.

  - Run the following command on the Red Hat Storage node as root to get a listing of the current iptables rules:

```
# iptables -L
```

  - The output is displayed as shown below:

```
ACCEPT - tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5666
```

- If the port is not open, add iptables rule for it.

- To add iptables rule, edit the **iptables** file as shown below:

```
# vi /etc/sysconfig/iptables
```

- Add the following line in the file:

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 5666 -j
ACCEPT
```

- Restart the iptables service using the following command:

```
# service iptables restart
```

- Save the file and restart the NRPE service:

```
# service nrpe restart
```

- **Checking Port 5666 From the Nagios Server with Telnet**

  Use telnet to verify the Red Hat Storage node's ports. To verify the ports of the Red Hat Storage node, perform the steps given below:

  - Log in as root on Nagios server.
  - Test the connection on port 5666 from the Nagios server to the Red Hat Storage node using the following command:

```
# telnet RedHatStorageNodeIP 5666
```

  - The output displayed is similar to:

```
telnet 10.70.36.49 5666
Trying 10.70.36.49...
Connected to 10.70.36.49.
Escape character is '^]'.
```

- **Connection Refused By Host**

  This error is due to port/firewall issues or incorrectly configured *allowed_hosts* directives. See the sections *CHECK_NRPE: Error - Could Not Complete SSL Handshake* and *CHECK_NRPE: Socket Timeout After n Seconds* for troubleshooting steps.

9.6.2. Troubleshooting General Issues

This section describes the troubleshooting procedures for general issues related to Nagios.

All cluster services are in warning state and status information is displayed as (null).

Set ***SELinux*** to permissive and restart the Nagios server.

Graphs are not displayed in Trends tab

Ensure that the host name given in Name field of Add Host window matches the host name given while configuring Nagios. The host name of the node is used while configuring Nagios server using auto-discovery.

Part IV. Managing Advanced Functionality

Chapter 10. Managing Multilevel Administration

Red Hat Storage Console supports multilevel administration. That is, users can be assigned a variety of permissions for specific objects using a number of default roles. This section describes how to set up user roles that control levels of permissions for different objects and actions in your storage environment. Customized roles can also be created and assigned to users.

Red Hat Storage Console relies on directory services for user authentication. The providers of directory services currently supported for use with the Red Hat Storage Console are Identity (IdM), Active Directory, and Red Hat Directory Server (RHDS).

Note

Users are not created in Red Hat Storage, but in the Directory Services domain. Red Hat Storage Console can be configured to use multiple Directory Services domains. See the *Red Hat Storage Console Installation Guide* for more information.

10.1. Configuring Roles

Roles are predefined sets of privileges that can be configured from Red Hat Storage Console, providing access and management permissions to different levels of resources in the cluster. Permissions enable users to perform actions on objects.

With multilevel administration, any permissions that apply to a container object also apply to all individual objects within that container. For example, when a server administrator role is assigned to a user on a specific server, the user gains permissions to perform any of the available operations, but only on the assigned server. However, if the administrator role is assigned to a user on a cluster, the user gains permissions to perform operations on all servers within the cluster.

10.1.1. Roles

There is one type of role in Red Hat Storage Console, which is the **administrator** role. This role allows access to the Administration Portal for managing server resources. For example, if a user has an **administrator** role on a cluster, they can manage all servers in the cluster using the Administration Portal.

The default roles cannot be removed from the Red Hat Storage, and their privileges cannot be modified. However, you can clone them and then customize the new roles as required.

10.1.2. Creating Custom Roles

In addition to the default roles, you can set up custom roles that permit actions on objects, such as servers and clusters, and assign privileges to specific entities. Use roles to create a granular model of permissions to suit the needs of the enterprise or a group or set of users. Use the **Configure** option to work with roles. You can create a **New** role, or **Edit**, **Clone** or **Remove** an existing role. In each case, the appropriate dialog box displays.

Once the role is set up, you can assign the role to users as required.

Procedure 10.1. Creating a New Role

1. On the header bar of the Red Hat Storage Console menu, click **Configure**. The **Configure** dialog box displays. The dialog box includes a list of Administrator roles, and any custom roles.
2. Click **New**. The **New Role** dialog box displays.
3. Enter the **Name** and **Description** of the new role. This name will display in the list of roles.
4. Select **Admin** as the **Account Type**. If **Admin** is selected, this role displays with the administrator icon in the list.
5. Use the **Expand All** or **Collapse All** buttons to view more or fewer of the permissions for the listed objects in the **Check Boxes to Allow Action** list. You can also expand or collapse the options for each object.
6. For each of the objects, select or deselect the actions you wish to permit/deny for the role you are setting up.
7. Click **OK** to apply the changes you have made. The new role displays on the list of roles.

10.1.3. Editing Roles

While you cannot make changes to the default roles, you may need to change the permissions, names or descriptions of custom roles. To edit custom roles, use the **Edit** button on the **Configure** dialog box.

Procedure 10.2. Editing a Role

1. On the header bar of the Red Hat Storage Console menu, click **Configure**. The **Configure** dialog box displays. The dialog box below shows the list of administrator roles.
2. Click **Edit**. The **Edit Role** dialog box displays.

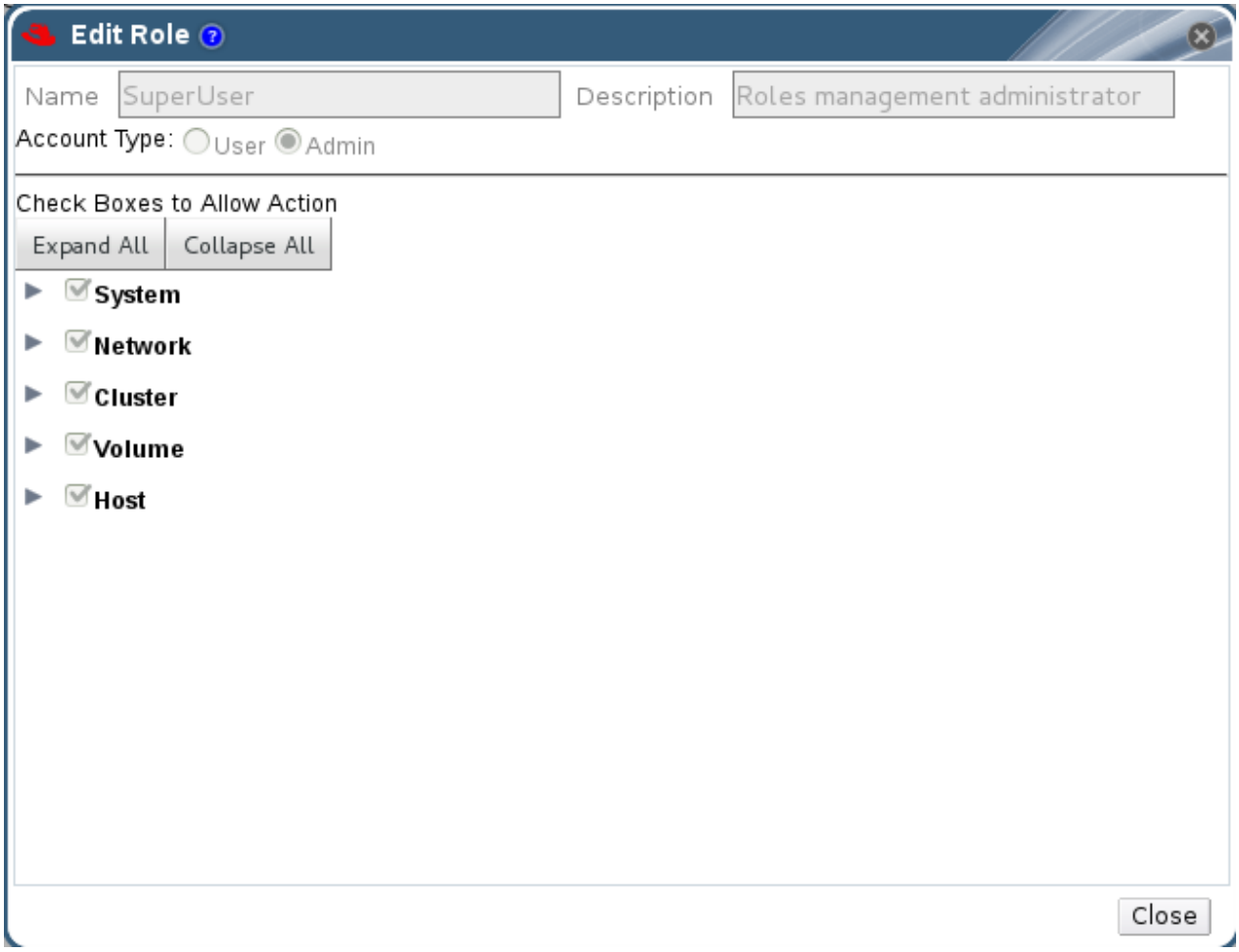


Figure 10.1. The Edit Role Dialog Box

3. If necessary, edit the **Name** and **Description** of the role. This name will display in the list of roles.
4. Use the **Expand All** or **Collapse All** buttons to view more or fewer of the permissions for the listed objects. You can also expand or collapse the options for each object.
5. For each of the objects, select or deselect the actions you wish to permit/deny for the role you are editing.
6. Click **OK** to apply the changes you have made.

10.1.4. Copying Roles

You can create a new role by cloning an existing default or custom role, and changing the permissions set as required. Use the **Copy** button on the Configure dialog box.

Procedure 10.3. Copying a Role

1. On the header bar of the Red Hat Storage Console, click **Configure**. The **Configure** dialog box displays. The dialog box includes a list of default roles, and any custom roles that exist on the Red Hat Storage Console.

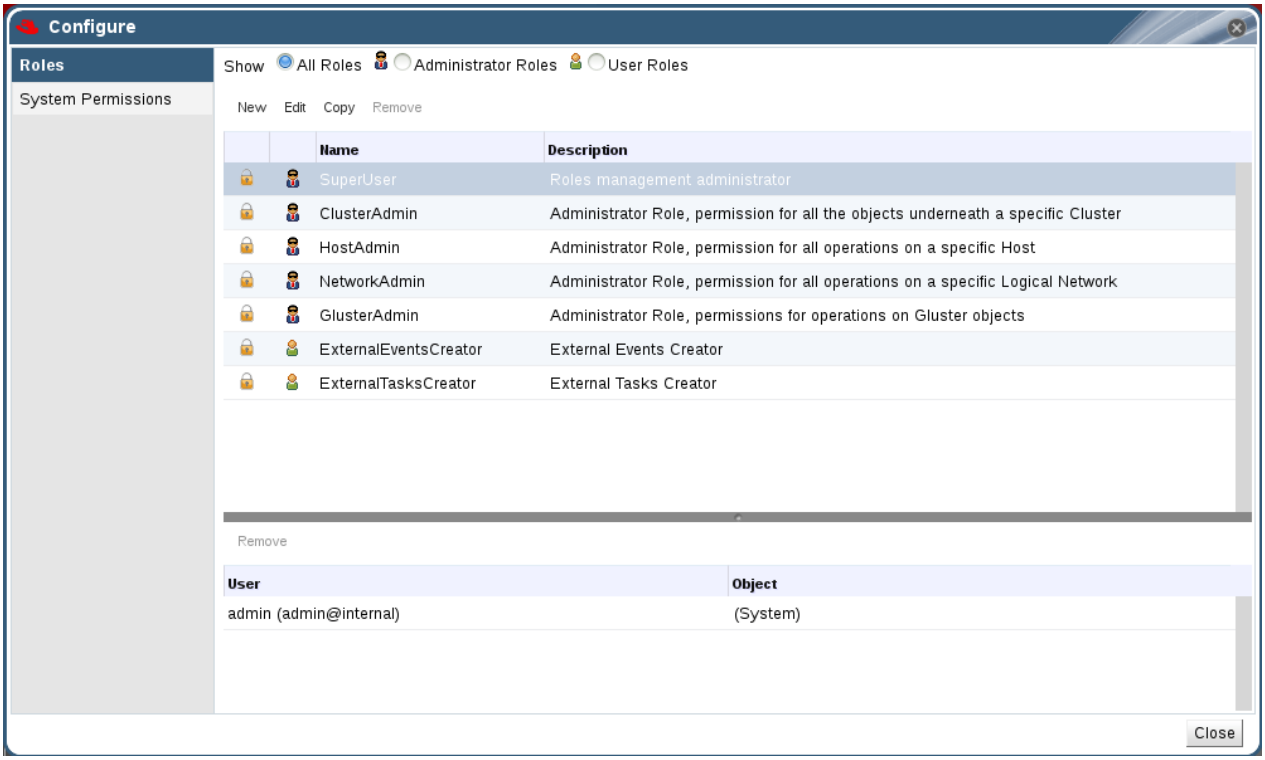


Figure 10.2. The Configure Dialog Box

2. Click **Copy**. The **Copy Role** dialog box displays.
3. Change the **Name** and **Description** of the new role. This name will display in the list of roles.
4. Use the **Expand All** or **Collapse All** buttons to view more or fewer of the permissions for the listed objects. You can also expand or collapse the options for each object.
5. For each of the objects, select or deselect the actions you wish to permit/deny for the role you are editing.
6. Click **Close** to apply the changes you have made.

Chapter 11. Backing Up and Restoring the Red Hat Storage Console

The Red Hat Storage Console maintains important information about the environment and therefore must be regularly backed up. Regular backups ensure that Red Hat Storage Console can recover a previous state simply and quickly.

11.1. Backing Up and Restoring the Red Hat Storage Console

11.1.1. Backing up Red Hat Storage Console - Overview

While taking complete backups of the machine on which the Red Hat Storage Console is installed is recommended whenever changing the configuration of that machine, a utility is provided for backing up only the key files related to the Manager. This utility - the **engine-backup** command - can be used to rapidly back up the engine database and configuration files into a single file that can be easily stored.

11.1.2. Syntax for the engine-backup Command

The **engine-backup** command works in one of two basic modes:

```
# engine-backup --mode=backup
```

```
# engine-backup --mode=restore
```

These two modes are further extended by a set of parameters that allow you to specify the scope of the backup and different credentials for the engine database. A full list of parameters and their function is as follows:

Basic Options

--mode

Specifies whether the command will perform a backup operation or a restore operation. Two options are available - **backup**, and **restore**. This is a required parameter.

--file

Specifies the path and name of a file into which backups are to be taken in backup mode, and the path and name of a file from which to read backup data in restore mode. This is a required parameter in both backup mode and restore mode.

--log

Specifies the path and name of a file into which logs of the backup or restore operation are to be written. This parameter is required in both backup mode and restore mode.

--scope

Specifies the scope of the backup or restore operation. There are two options - **all**, which backs up both the engine database and configuration data, and **db**, which backs up only the engine database.

Database Options

--change-db-credentials

Allows you to specify alternate credentials for restoring the engine database using credentials other than those stored in the backup itself. Specifying this parameter allows you to add the following parameters.

--db-host

Specifies the IP address or fully qualified domain name of the host on which the database resides. This is a required parameter.

--db-port

Specifies the port by which a connection to the database will be made.

--db-user

Specifies the name of the user by which a connection to the database will be made. This is a required parameter.

--db-passfile

Specifies a file containing the password by which a connection to the database will be made. Either this parameter or the ***--db-password*** parameter must be specified.

--db-password

Specifies the plain text password by which a connection to the database will be made. Either this parameter or the ***--db-passfile*** parameter must be specified.

--db-name

Specifies the name of the database to which the database will be restored. This is a required parameter.

--db-secured

Specifies that the connection with the database is to be secured.

--db-secured-validation

Specifies that the connection with the host is to be validated.

Help

--help

Provides an overview of the available modes, parameters, sample usage, how to create a new database and configure the firewall in conjunction with backing up and restoring the Red Hat Storage Console.

11.1.3. Creating a Backup with the engine-backup Command

Summary

The process for creating a backup of the engine database and the configuration data for the Red Hat Storage Console using the **engine-backup** command is straightforward and can be performed while the Manager is active.

Procedure 11.1. Backing up the Red Hat Storage Console

1. Log on to the machine running the Red Hat Storage Console.
2. Run the following command to create a full backup:

   Example 11.1. Creating a Full Backup

   ```
   # engine-backup --scope=all --mode=backup --log=[file name] --
   file=[file name]
   ```

   Alternatively, run the following command to back up only the engine database:

   Example 11.2. Creating an engine database Backup

   ```
   # engine-backup --scope=db --mode=backup --log=[file name] --
   file=[file name]
   ```

Result

A **tar** file containing a backup of the engine database, or the engine database and the configuration data for the Red Hat Storage Console, is created using the path and file name provided.

11.1.4. Restoring a Backup with the engine-backup Command

While the process for restoring a backup using the **engine-backup** command is straightforward, it involves several additional steps in comparison to that for creating a backup depending on the destination to which the backup is to be restored. For example, the **engine-backup** command can be used to restore backups to fresh installations of Red Hat Storage Console, on top of existing installations of Red Hat Storage Console, and using local or remote databases.

Important

Backups can only be restored to environments of the same major release as that of the backup. For example, a backup of a Red Hat Storage Console version 3.0 environment can only be restored to another Red Hat Storage Console version 3.0 environment. To view the version of Red Hat Storage Console contained in a backup file, unpack the backup file and read the value in the **version** file located in the root directory of the unpacked files.

11.1.5. Restoring a Backup to a Fresh Installation

Summary

The **engine-backup** command can be used to restore a backup to a fresh installation of the Red Hat Storage Console. The following procedure must be performed on a machine on which the base operating system has been installed and the required packages for the Red Hat Storage Console have been installed, but the **engine-setup** command has not yet been run. This procedure assumes that the backup file can be accessed from the machine on which the backup is to be restored.

Note

The **engine-cleanup** command used to prepare a machine prior to restoring a backup only cleans the engine database, and does not drop the database, delete the user that owns that database, create engine database or perform the initial configuration of the **postgresql** service. Therefore, these tasks must be performed manually as outlined below when restoring a backup to a fresh installation.

Procedure 11.2. Restoring a Backup to a Fresh Installation

1. Log on to the machine on which the Red Hat Storage Console is installed.
2. Manually create an empty database to which the database in the backup can be restored and configure the **postgresql** service:
   a. Run the following commands to initialize the **postgresql** database, start the **postgresql** service and ensure this service starts on boot:

```
# service postgresql initdb
# service postgresql start
# chkconfig postgresql on
```

   b. Run the following commands to enter the postgresql command line:

```
# su postgres
$ psql
```

   c. Run the following command to create a new user:

```
postgres=# CREATE USER [user name] PASSWORD '[password]';
```

   The password used while creating the database should be same as the one used while taking backup. If the password is different, follow step 3 in Section 11.1.7, “Restoring a Backup with Different Credentials”

   d. Run the following command to create the new database:

```
postgres=# create database [database name] owner [user name]
template template0 encoding 'UTF8' lc_collate 'en_US.UTF-8'
lc_ctype 'en_US.UTF-8';
```

   e. Edit the **/var/lib/pgsql/data/pg_hba.conf** file and add the following lines under the **'local'** section near the end of the file:

   - For local databses:

```
host    [database name]    [user name]    0.0.0.0/0    md5
host    [database name]    [user name]    ::0/0        md5
```

   - For remote databases:

```
host    [database name]    [user name]    X.X.X.X/32   md5
```

Replace *X.X.X.X* with the IP address of the Manager.

f. Run the following command to restart the **postgresql** service:

```
# service postgresql restart
```

3. Restore the backup using the **engine-backup** command:

```
# engine-backup --mode=restore --file=[file name] --log=[file name]
```

If successful, the following output displays:

```
Restoring...
Note: you might need to manually fix:
- iptables/firewalld configuration
- autostart of ovirt-engine service
You can now start the engine service and then restart httpd
Done.
```

4. Run the following command and follow the prompts to set up the Manager as per a fresh installation, selecting to manually configure the database when prompted:

```
# engine-setup
```

Result

The engine database and configuration files for the Red Hat Storage Console have been restored to the version in the backup.

11.1.6. Restoring a Backup to an Existing Installation

Summary

The **engine-backup** command can restore a backup to a machine on which the Red Hat Storage Console has already been installed and set up.

Note

The **engine-cleanup** command used to prepare a machine prior to restoring a backup only cleans the engine database, and does not drop the database, delete the user that owns that database, create engine database or perform the initial configuration of the **postgresql** service. Therefore, these tasks must be performed manually as outlined below when restoring a backup to an existing installation.

Procedure 11.3. Restoring a Backup to an Existing Installation

1. Log on to the machine on which the Red Hat Storage Console is installed.
2. Run the following command and follow the prompts to remove the configuration files for and clean the database associated with the Manager:

```
# engine-cleanup
```

Manually drop the database and create an empty database to which the database in the backup can be restored and configure the **postgresql** service

a. Run the following commands to enter the postgresql command line:

```
# su postgres
$ psql
```

b. Run the following command to drop the database:

```
# postgres=# DROP DATABASE [database name]
```

c. Run the following command to create the new database:

```
# postgres=# create database [database name] owner [user
name] template template0 encoding 'UTF8' lc_collate
'en_US.UTF-8' lc_ctype 'en_US.UTF-8';
```

3. Restore the backup using the **engine-backup** command:

```
# engine-backup --mode=restore --file=[file name] --log=[file name]
```

If successful, the following output displays:

```
Restoring...
Note: you might need to manually fix:
- iptables/firewalld configuration
- autostart of ovirt-engine service
You can now start the engine service and then restart httpd
Done.
```

4. Run the following command and follow the prompts to re-configure the firewall and ensure the **ovirt-engine** service is correctly configured:

```
# engine-setup
```

Result

The engine database and configuration files for the Red Hat Storage Console have been restored to the version in the backup.

11.1.7. Restoring a Backup with Different Credentials

Summary

The **engine-backup** command can restore a backup to a machine on which the Red Hat Storage Console has already been installed and set up, but the credentials of the database in the backup are different to those of the database on the machine on which the backup is to be restored.

Note

The **engine-cleanup** command used to prepare a machine prior to restoring a backup only cleans the engine database, and does not drop the database, delete the user that owns that database, create engine database or perform the initial configuration of the **postgresql** service. Therefore, these tasks must be performed manually as outlined below when restoring a backup with different credentials.

Procedure 11.4. Restoring a Backup with Different Credentials

1. Log on to the machine on which the Red Hat Storage Console is installed.
2. Run the following command and follow the prompts to remove the configuration files for and clean the database associated with the Manager:

```
# engine-cleanup
```

Manually drop the database and create an empty database to which the database in the backup can be restored and configure the **postgresql** service:

a. Run the following commands to enter the postgresql command line:

```
# su postgres
$ psql
```

b. Run the following command to drop the database:

```
# postgres=# DROP DATABASE [database name]
```

c. Run the following command to create the new database:

```
# postgres=# create database [database name] owner [user
name] template template0 encoding 'UTF8' lc_collate
'en_US.UTF-8' lc_ctype 'en_US.UTF-8';
```

3. Restore the backup using the **engine-backup** command with the ***--change-db-credentials*** parameter:

```
# engine-backup --mode=restore --file=[file name] --log=[file name]
--change-db-credentials --db-host=[database location] --db-
name=[database name] --db-user=[user name] --db-password=[password]
```

If successful, the following output displays:

```
Restoring...
Note: you might need to manually fix:
- iptables/firewalld configuration
- autostart of ovirt-engine service
You can now start the engine service and then restart httpd
Done.
```

4. Run the following command and follow the prompts to re-configure the firewall and ensure the **ovirt-engine** service is correctly configured:

```
# engine-setup
```

Result

The engine database and configuration files for the Red Hat Storage Console have been restored to the version in the backup using the supplied credentials.

Utilities

A.1. Domain Management Tool

Red Hat Storage Console uses directory services to authenticate users. During installation, the manager sets up a domain named **internal** that is only used to store the **admin** user. To add and remove other users from the system, you must first add the directory services in which they are found.

The supported directory service is IPA. Red Hat Storage Console includes a domain management tool, **rhsc-manage-domains**, to add and remove domains provided by this service. In this way, you can grant access to the Red Hat Storage environment to users stored across multiple domains.

You will find the **rhsc-manage-domains** command on the machine on which Red Hat Storage Console was installed. The **rhsc-manage-domains** command must be run as the root user.

A.1.1. Syntax

The usage syntax is:

```
# rhsc-manage-domains -action=ACTION [options]
```

The available actions are:

add

Add a domain to the console directory services configuration.

edit

Edit a domain in the console directory services configuration.

delete

Delete a domain from the console directory services configuration.

validate

Validate the console directory services configuration. The command attempts to authenticate to each domain in the configuration using the configured user name and password.

list

List the current directory services configuration of the console.

The options that can be combined with the actions on the command line are:

-domain=DOMAIN

Specifies the domain on which the action must be performed. The ***-domain*** parameter is mandatory for **add**, **edit**, and **delete**.

-user=USER

Specifies the domain user to use. The ***-user*** parameter is mandatory for **add**, and optional for **edit**.

-interactive

Specifies that the domain user's password is to be provided interactively. This option or the ***-passwordFile*** option must be used to provide the password for use with the add action.

-passwordFile=FILE

Specifies that the domain user's password is on the first line of the provided file. This option or the ***-interactive*** option must be used to provide the password for use with the **add** action.

-configFile=FILE

Specifies an alternative configuration file that the command must load. The ***-configFile*** parameter is always optional.

-report

Specifies that all validation errors encountered while performing the validate action will be reported in full.

Common examples of usage are discussed further within this guide. For full information on usage, see the **rhsc-manage-domains** command help output:

```
# rhsc-manage-domains --help
```

A.1.2. Examples

The following examples demonstrate the use of **rhsc-manage-domains** to perform basic manipulation of the Red Hat Storage Console domain configuration.

Changing Passwords in Red Hat Storage Console

This appendix describes how to change passwords for the administrator user in the Administration Portal and Red Hat Storage Console PostgreSQL databases.

B.1. Changing the Password for the Administrator User

The **admin@internal** user account is automatically created on installing and configuring Red Hat Storage Console. This account is stored locally in the Red Hat Storage Console PostgreSQL database and exists separately from other directory services. Unlike IPA domains, users cannot be added to or deleted from the internal domain. The **admin@internal** user is the SuperUser for Red Hat Storage Console, and has administrator privileges over the environment via the Administration Portal.

During installation, you were prompted to set a password for the **admin@internal** user. However, if you have forgotten the password or choose to reset the password, you can use the **rhsc-config** utility.

Procedure B.1. Resetting the Password for the admin@internal User

1. Log in to the Red Hat Storage Console server as the **root** user.
2. Use the **rhsc-config** utility to set a new password for the **admin@internal** user. Run the following command:

   ```
   # rhsc-config -s AdminPassword=interactive
   ```

   After typing the above command, a password prompt displays for you to enter the new password.

   You do not need to use quotes. However, use escape shell characters if you include them in the password.
3. Restart the **ovirt-engine** service to apply the changes. Run the following command:

   ```
   # service ovirt-engine restart
   ```

Search Parameters

This appendix describes the search function in Red Hat Storage Console in detail.

C.1. Search Query Syntax

Each part of the query syntax is explained in greater detail below.

Example	Result
Hosts: cluster = cluster name	Displays a list of all servers in the cluster.
Volumes: status = up	Displays a list of all volumes with status up.
Events: severity > normal sortby time	Displays the list of all events whose severity is higher than **Normal**, sorted by time.

As you type each part of a search query, a drop-down list of choices for the next part of the search opens below the **Search** bar. You can either select from the list and then continue typing or selecting the next part of the search, or ignore the options and continue entering your query manually.

The following table shows how Red Hat Storage Console auto-completion assists in query construction. It shows what the drop-down list will display as the administrator inputs text into the search field.

Hosts: cluster = down

Input	List Items Displayed	Action
h	**Hosts** (1 option only)	Select **Hosts** or; Type **Hosts**
Hosts:	All host properties	Type **c**
Hosts: c	host properties starting with **c**	Select **cluster** or type **cluster**
Hosts: cluster	**=** **=!**	Select or type **=**
Hosts: cluster =		Select or type **cluster name**

C.2. Searching for Resources

This section specifies the unique set of properties for each resource and the set of associated resource types.

C.2.1. Searching for Clusters

The following table describes all search options for clusters.

Property (of resource or resource-type)	Type	Description (Reference)
name	String	The unique name that identifies the clusters on the network.
description	String	The description of the cluster.

Property (of resource or resource-type)	Type	Description (Reference)
initialized	String	A Boolean **True** or **False** indicating the status of the cluster.
sortby	List	Sorts the returned results by one of the resource properties.
page	Integer	The page number of results to display.

Example

```
Clusters: initialized = true or name = Default
```

This above query returns a list of clusters that are:

- Initialized; or
- Named **Default**

C.2.2. Searching for Hosts

The following table describes all search options for hosts.

Property (of resource or resource-type)	Type	Description (Reference)
Events.events-prop	See property types in Section C.2.5, “Searching for Events”	The property of the events associated with the host.
Users.users-prop	See property types in Section C.2.4, “Searching for Users”	The property of the users associated with the host.
name	String	The name of the host.
status	List	The availability of the host.
cluster	String	The cluster to which the host belongs.
address	String	The unique name that identifies the host on the network.
cpu_usage	Integer	The percent of processing power usage.
mem_usage	Integer	The percentage of memory usage.
network_usage	Integer	The percentage of network usage.
load	Integer	Jobs waiting to be executed in the *run-queue* per processor, in a given time slice.
version	Integer	The version number of the operating system.
cpus	Integer	The number of CPUs on the host.
memory	Integer	The amount of memory available.

Property (of resource or resource-type)	Type	Description (Reference)
cpu_speed	Integer	The processing speed of the CPU.
cpu_model	String	The type of CPU.
committed_mem	Integer	The percentage of committed memory.
tag	String	The tag assigned to the host.
type	String	The type of host.
sortby	List	Sorts the returned results by one of the resource properties.
page	Integer	The page number of results to display.

Example

```
Host: cluster = Default
```

The above query returns a list of hosts that:

- Are part of the **Default** cluster.

C.2.3. Searching for Volumes

The following table describes all search options for volumes.

Property (of resource or resource-type)	Type	Description (Reference)
Clusters.clusters prop	See property types in Section C.2.1, “Searching for Clusters”	The property of the clusters associated with the volume.
name	String	The name of the volume.
status	List	The availability of the volume.
type	List	The type of the volume.
transport_type	List	The transport type of the volume.
replica_count	Integer	The replicate count of the volume.
stripe_count	Integer	The stripe count of the volume.
sortby	List	Sorts the returned results by one of the resource properties.
page	Integer	The page number of results to display.

Example

```
Volumes: Cluster.name = Default and Status = Up
```

The above query returns a list of volumes that:

- Belong to the **Default** cluster and the status of the volume is **Up**.

C.2.4. Searching for Users

The following table describes all search options for users.

Property (of resource or resource-type)	Type	Description (Reference)
Hosts.hosts- prop	See property types in Section C.2.2, “Searching for Hosts”	The property of the hosts associated with the user.
Events.events-prop	See property types in Section C.2.5, “Searching for Events”	The property of the events associated with the user.
name	String	The name of the user.
lastname	String	The last name of the user.
usrname	String	The unique name of the user.
department	String	The department to which the user belongs.
group	String	The group to which the user belongs.
title	String	The title of the user.
status	String	The status of the user.
role	String	The role of the user.
tag	String	The tag to which the user belongs.
pool	String	The pool to which the user belongs.
sortby	List	Sorts the returned results by one of the resource properties.
page	Integer	The page number of results to display.

Example

```
Users: Events.severity > normal and Hosts.name = Server name
```

The above query returns a list of users for which:

- Events of a severity greater than **`Normal`** have occurred on their hosts.

C.2.5. Searching for Events

The following table describes all search options you can use to search for events. Auto-completion is offered for many options as appropriate.

Property (of resource or resource-type)	Type	Description (Reference)
Hosts.hosts-prop	See property types in Section C.2.2, “Searching for Hosts”	The property of the hosts associated with the event.
Users.users-prop	See property types in Section C.2.4, “Searching for Users”	The property of the users associated with the event.
type	List	Type of the event.
severity	List	The severity of the Event: Warning/Error/Normal

Property (of resource or resource-type)	Type	Description (Reference)
message	String	Description of the event type.
time	Integer	Time at which the event occurred.
usrname	usrname	The user name associated with the event.
event_host	String	The host associated with the event.
sortby	List	Sorts the returned results by one of the resource properties.
page	Integer	The page number of results to display.

Example

`Events: event_host = gonzo.example.com`

The above query returns a list of events for which:

- The event occurred on the server named **`gonzo.example.com`**.

C.3. Saving and Accessing Queries as Bookmarks

Search queries can be saved as bookmarks. This allows you to sort and display results lists with a single click. You can save, edit and remove bookmarks with the **Bookmarks** pane.

C.3.1. Creating Bookmarks

Bookmarks can be created for any type of available search, using a number of criteria.

Procedure C.1. Saving a Query String as a Bookmark

1. Enter the search query in the **Search** bar (see Appendix D).
2. Click the **Bookmark** button to the right of the **Search** bar.

   The **New Bookmark** dialog box displays. The query displays in the **Search String** field. You can edit the query if required.
3. In **Name**, specify a descriptive name for the search query.
4. Click **OK** to save the query as a bookmark.
5. The search query is saved and displays in the **Bookmarks** pane.

C.3.2. Editing Bookmarks

Bookmarks can be edited for any type of available search, using an existing bookmark.

Procedure C.2. Editing a Bookmark

1. Select a bookmark from the **Bookmarks** pane.

2. The results list displays the items according to the criteria. Click the **Edit** button on the **Bookmark** pane.

   The **Edit Bookmark** dialog box displays. The query displays in the **Search String** field. Edit the search string as required.

3. Change the **Name** and **Search String** as necessary.

4. Click **OK** to save the edited bookmark.

C.3.3. Deleting Bookmarks

Bookmarks can be deleted.

Procedure C.3. Deleting a Bookmark

1. Select one or more bookmark from the **Bookmarks** pane.

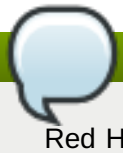
2. The results list displays the items according to the criteria. Click the **Remove** button on the **Bookmark** pane.

   The **Remove Bookmark** dialog box displays.

3. Click **OK** to remove the selected bookmarks.

Red Hat Access Plug-in

The Red Hat Access Plug-in allows you to use Red Hat access services from the Red Hat Storage Administration Portal. You must log in using your Red Hat login credentials. The Red Hat Access Plug-in detects when you are not logged in; if you are not logged in, a login window opens.



Note

Red Hat Storage Administration Portal credentials are not the same as a user's Red Hat login.

This appendix describes how to use the Red Hat Access Plug-in feature. This section shows the procedure to open a new support case, modify an existing case, and to search for Red Hat Storage documentation.

D.1. Using Red Hat Access Plug-in

During installation, you were prompted to set a password for the **admin@internal** user. However, if you have forgotten the password or choose to reset the password, you can use the **rhsc-config** utility.

Procedure D.1. Using Red Hat Access Plug-in

1. In the Red Hat Storage Console, open the Clusters view by expanding the System tab and selecting the Cluster tab in the Tree pane. Alternatively, select Clusters tab.
2. Click **Red Hat Access:Support** to open the *Red Hat Access: Support* dialog box.

   You can select **Red Hat Access:Support** from Hosts tab also.

Note

Red Hat Support Plug-in is available in the details pane as well as in several context menus in the Red Hat Storage Administration Portal.

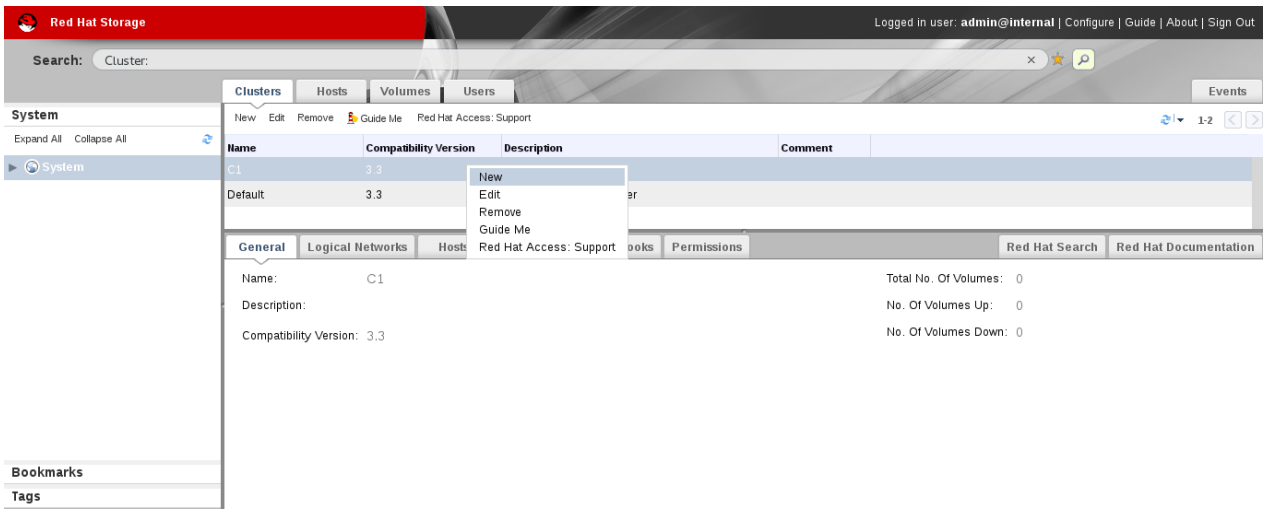


Figure D.1. Selecting Red Hat Access:Support option

3. Log in to **Red Hat Access: Support** with the Red Hat credentials.
4. In the **Search** field you can search for solutions in the knowledge base.

Note

You can also search the Red Hat Access database using the Red Hat Search: field. Search results display in the left-hand navigation list in the details pane.

5. To open a new support case select the **Open New Support Case** radio button in **Red Hat Access: Support** dialog box.

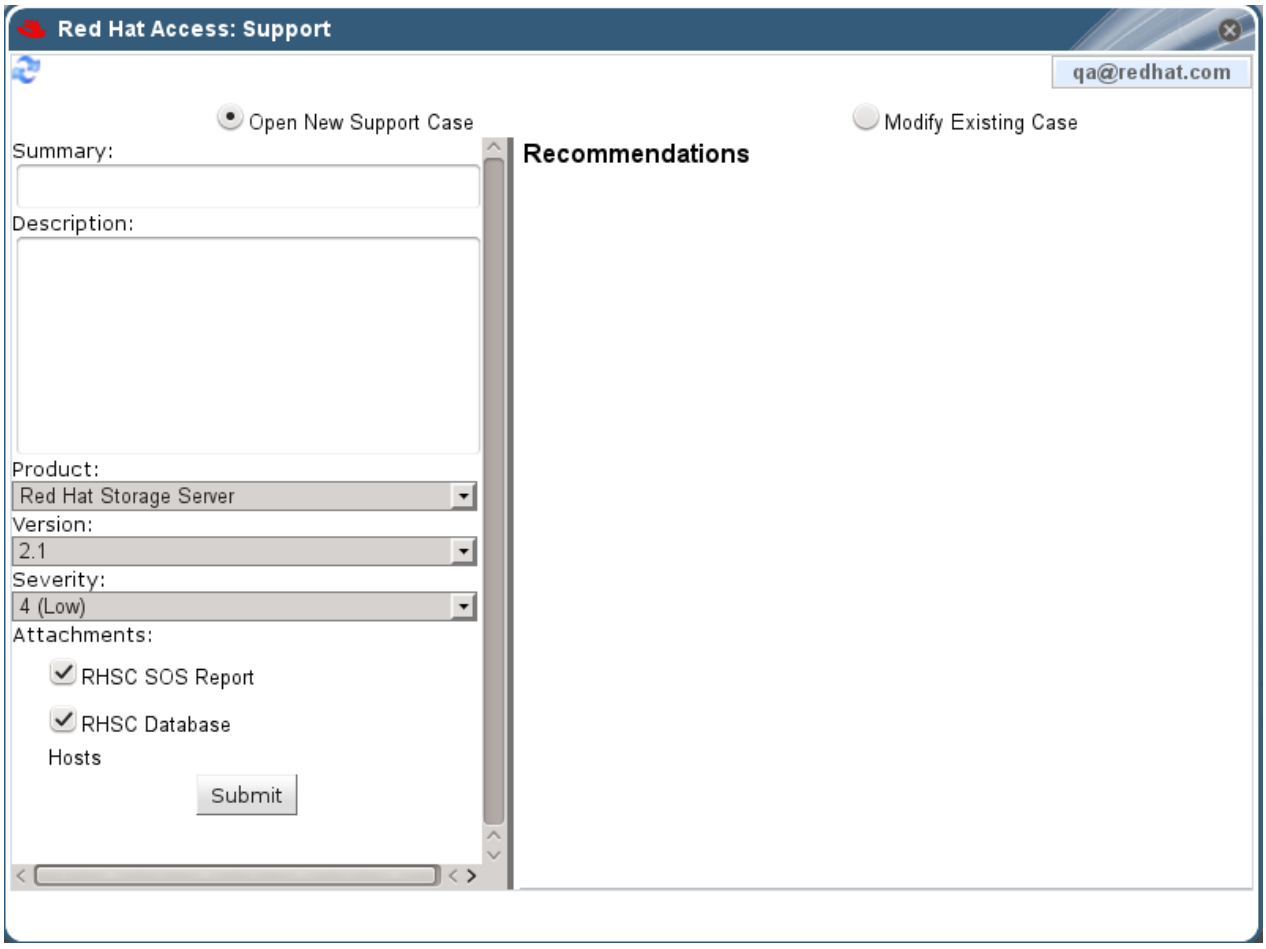


Figure D.2. Red Hat Access: Support Window

6. Enter the Summary, Description and select Product, Version, and Attachments and click **Submit** button.
7. To modify an existing case, select **Modify Existing Case** radio button.
8. Update the details and click **Submit**.
9. To view the documentation relevant to the part of the Administration Portal currently on the screen, click **Red Hat Documentation**.

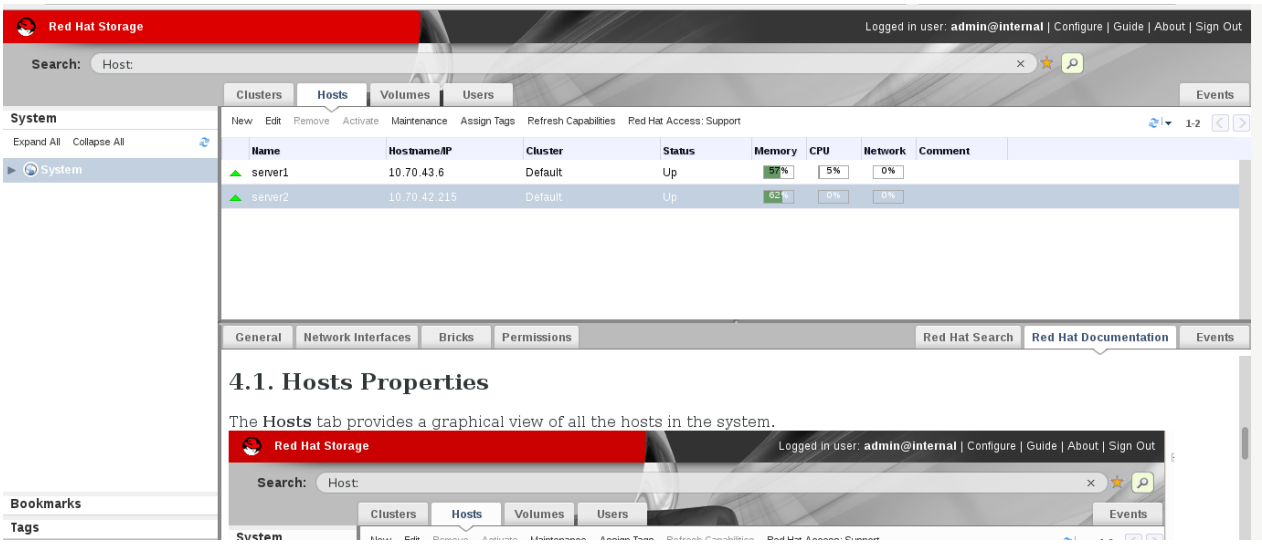


Figure D.3. Red Hat Documentation

Nagios Configuration Files

Auto-discovery creates folders and files as part of configuring Red Hat Storage nodes for monitoring. All nodes in the trusted storage pool are configured as hosts in Nagios. The Host and Hostgroup configurations are also generated for trusted storage pool with cluster name. Ensure that the following files and folders are created with the details described to verify the Nagios configurations generated using Auto-discovery.

- In **/etc/nagios/gluster/** directory, a new directory **Cluster-Name** is created with the name provided as **Cluster-Name** while executing **discovery.py** script for auto-discovery. All configurations created by auto-discovery for the cluster are added in this folder.
- In **/etc/nagios/gluster/*Cluster-Name*** directory, a configuration file, ***Cluster-Name*.cfg** is generated. This file has the host and hostgroup configurations for the cluster. This also contains service configuration for all the cluster/volume level services.

  The following Nagios object definitions are generated in ***Cluster-Name*.cfg** file:

  - A hostgroup configuration with **hostgroup_name** as cluster name.
  - A host configuration with **host_name** as cluster name.
  - The following service configurations are generated for cluster monitoring:
    - A *Cluster - Quorum* service to monitor the cluster quorum.
    - A *Cluster Utilization* service to monitor overall utilization of volumes in the cluster. This is created only if there is any volume present in the cluster.
    - A *Cluster Auto Config* service to periodically synchronize the configurations in Nagios with Red Hat Storage trusted storage pool.
  - The following service configurations are generated for each volume in the trusted storage pool:
    - A Volume Status- *Volume-Name* service to monitor the status of the volume.
    - A Volume Utilization - *Volume-Name* service to monitor the utilization statistics of the volume.
    - A Volume Quota - *Volume-Name* service to monitor the Quota status of the volume, if Quota is enabled for the volume.
    - A Volume Self-Heal - *Volume-Name* service to monitor the Self-Heal status of the volume, if the volume is of type replicate or distributed-replicate.
    - A Volume Geo-Replication - *Volume-Name* service to monitor the Geo Replication status of the volume, if Geo-replication is configured for the volume.
- In **/etc/nagios/gluster/*Cluster-Name*** directory, a configuration file with name ***Host-Name*.cfg** is generated for each node in the cluster. This file has the host configuration for the node and service configuration for bricks from the particular node. The following Nagios object definitions are generated in ***Host-name*.cfg**.
  - A host configuration which has *Cluster-Name* in the **hostgroups** field.
  - The following services are created for each brick in the node:
    - A *Brick Utilization - brick-path* service to monitor the utilization of the brick.
    - A *Brick - brick-path* service to monitor the brick status.

Table E.1. Nagios Configuration Files

File Name	Description
/etc/nagios/nagios.cfg	Main Nagios configuration file.
/etc/nagios/cgi.cfg	CGI configuration file.
/etc/httpd/conf.d/nagios.conf	Nagios configuration for httpd.
/etc/nagios/passwd	Password file for Nagios users.
/etc/nagios/nrpe.cfg	NRPE configuration file.
/etc/nagios/gluster/gluster-contacts.cfg	Email notification configuration file.
/etc/nagios/gluster/gluster-host-services.cfg	Services configuration file that's applied to every Red Hat Storage node.
/etc/nagios/gluster/gluster-host-groups.cfg	Host group templates for a Red Hat Storage trusted storage pool.
/etc/nagios/gluster/gluster-commands.cfg	Command definitions file for Red Hat Storage Monitoring related commands.
/etc/nagios/gluster/gluster-templates.cfg	Template definitions for Red Hat Storage hosts and services.
/etc/nagios/gluster/snmpmanagers.conf	SNMP notification configuration file with the IP address and community name of SNMP managers where traps need to be sent.

Revision History

Revision 3-32	**Tue Dec 23 2014**	**Shalaka Harne**
Bug Fix.		
Revision 3-30	**Mon Nov 17 2014**	**Shalaka Harne**
Bug Fix.		
Revision 3-29	**Wed Nov 12 2014**	**Shalaka Harne**
Version for 3.0.2 release.		