Red Hat Gluster Storage 3.5

Quick Start Guide

Getting Started with Web Administration

Red Hat Gluster Storage 3.5 Quick Start Guide

Getting Started with Web Administration

Red Hat Gluster Storage Documentation Team
Red Hat Customer Content Services

Legal Notice

Abstract

This guide provides essential installation and getting started instructions to set up Red Hat Gluster Storage Web Administration for monitoring purposes. Making open source more inclusive Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message

Table of Contents

CHAPTER 1. OVERVIEW

Red Hat Gluster Storage Web Administration provides monitoring and metrics infrastructure for Red Hat Gluster Storage 3.5 and is the primary method to monitor your Red Hat Gluster Storage environment. The Red Hat Gluster Storage Web Administration environment is based on the Tendrl upstream project and utilizes Ansible automation for installation. The key goal of Red Hat Gluster Storage Web Administration is to provide deep metrics and visualization of Red Hat Storage Gluster clusters and the associated storage elements such as storage nodes, volumes, and bricks.

Key Features

1. Monitoring dashboards for Clusters, Hosts, Volumes, and Bricks

2. Top-level list views of Clusters, Hosts, and Volumes

3. SNMPv3 Configuration and Alerting

4. User Management

5. Importing Gluster cluster

1.1. WEB ADMINISTRATION SYSTEM CONCEPTS

The Red Hat Gluster Storage Web Administration environment consists of the following system components.

Web Administration Server

The Web Administration server system hosts the Web Administration user interface, the API and etcd. The Web Administration server is the system on which the Ansible installation process is run.

Red Hat Gluster Storage Node

The system on which Red Hat Gluster Storage is installed. Web Administration node agents are installed on the storage nodes.

Client System

Any external system that accesses the Web Administration user interface on a compatible web browser.

1.2. WEB ADMINISTRATION ARCHITECTURE

Figure 1.1. Web Administration Architecture
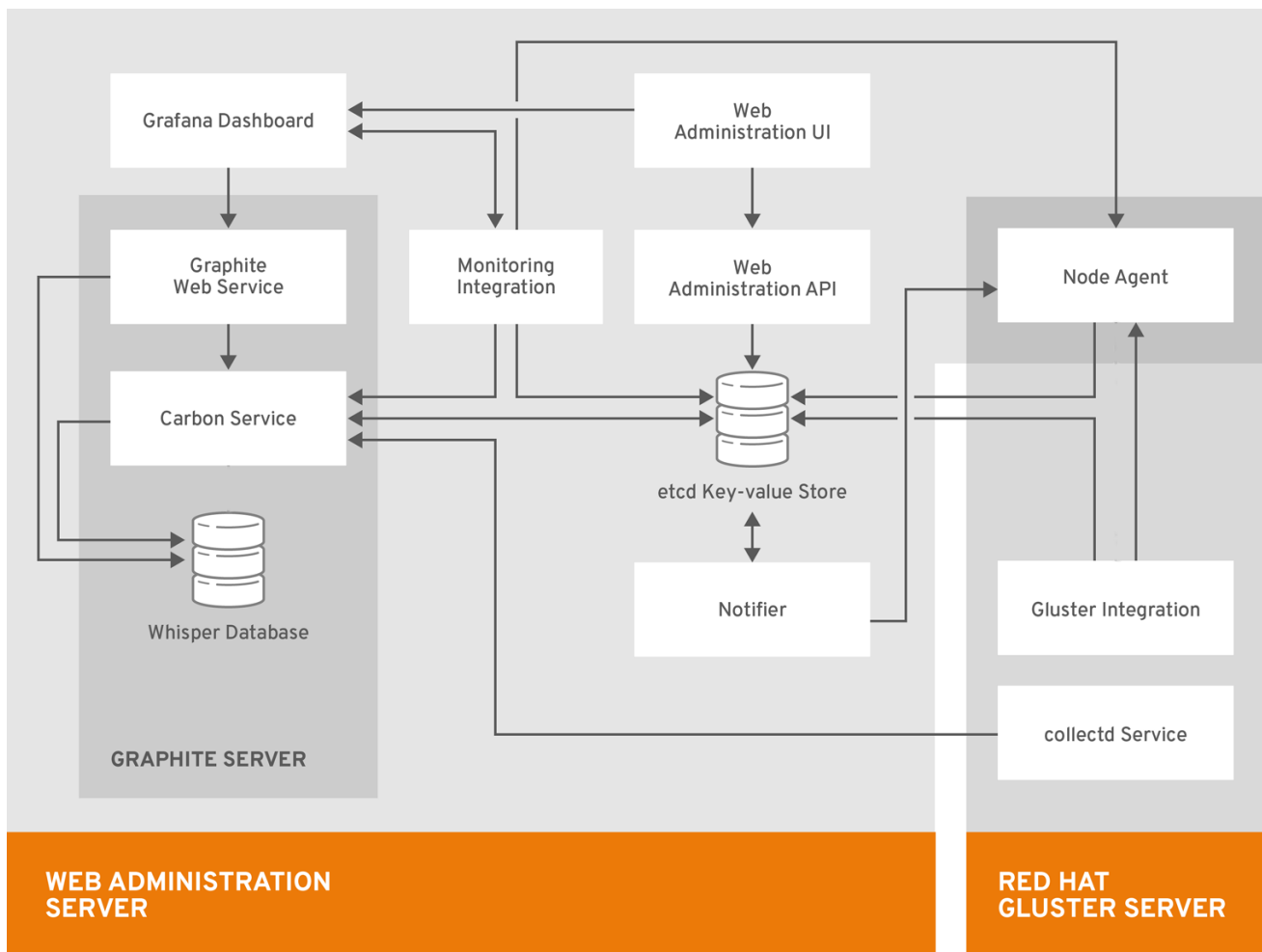
The components of the Web Administration architecture are described below:

Web Administration Server Components

- **Web Administration UI**: the primary user interface for monitoring Red Hat Gluster Storage clusters.

- **Grafana Dashboard**: a third party integrated dashboard that displays real-time metrics and monitoring data.

- **Monitoring Integration**: service that enables monitoring and alerting via integration with external systems such as Graphite and Grafana.

- **Graphite Web Service**: repository of (Gluster) telemetry data collected using collectd.

- **Carbon Service**: set of services dealing with receiving data from collectors (collectd), replication and sharding, and interfacing with Grafana.

- **Whisper Database**: database for storing time-series numeric metrics.

- **Web Administration API**: the Web Administration northbound API.

- **etcd Key-value Store**: central store that contains all the configuration state information for storage subsystems managed by Web Administration

- **Notifier**: notification service that enables various types of notifications and alerts including SMTP and SNMP

Red Hat Gluster Storage Server Components

Red Hat Gluster Storage server is a system with Red Hat Gluster Storage installed. Multiple Red Hat Gluster Storage servers form a Red Hat Gluster Storage cluster. The components are as follows:

- **collectd Service**: host-based system statistics collection daemon that gathers metrics from various sources such as the operating system, applications, log files and devices, Red Hat Gluster Storage clusters, etc.

- **Gluster Integration**: component that fetches data from Red Hat Gluster Storage cluster to be sent to the Web Administration server.

- **Node Agent**: takes care of node-specific flows and tasks to be performed.

CHAPTER 2. SYSTEM REQUIREMENTS

This chapter outlines the minimum hardware and software requirements to install Red Hat Gluster Storage Web Administration.

> **IMPORTANT**
>
> Ensure that all the requirements are met before the installation starts. Missing requirements can result in Red Hat Gluster Storage Web Administration environment not functioning as expected.

The Red Hat Gluster Storage Web Administration environment requires:

- One machine to act as the management server

- One or more machines to act as storage servers. At least three machines are required to support replicated volumes

- One or more machines to be used as clients to access the Web Administration interface

2.1. REQUIREMENTS FOR WEB ADMINISTRATION SERVER SYSTEM

On the system to be designated as the Web Administration server, verify that these recommended hardware and software requirements are met.

2.1.1. Hardware Requirements

The following are the different hardware requirements based on different cluster configurations:

2.1.1.1. Small Cluster Configuration

- Number of nodes: upto 8 nodes

- Number of volumes: upto 6-8 volumes per cluster

- Number of bricks per node for replicated volumes: upto 2-3 bricks

- Number of bricks per node for Erasure Coded volumes: upto 12-36 bricks

Recommended Requirements

- 4 vCPUs

- 4 GB of available system RAM

- One Network Interface Card (NIC) with bandwidth of at least 1 Gbps

Additional Storage Devices

For hosting etcd data directory:

- Storage disk size: 20 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/etcd**

For hosting time-series data from Graphite, Carbon, and Whisper applications:

- Storage disk size: 200 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/carbon**

> **NOTE**
>
> For more information on how to prepare and mount the additional disks, see the Creating a Partition and Mounting a File System sections in the *Red Hat Enterprise Linux Storage Administration Guide*.

2.1.1.2. Medium Cluster Configuration

- Number of nodes: 9-16 nodes

- Number of volumes: upto 6-8 volumes per cluster

- Number of bricks per node for replicated volumes: upto 2-3 bricks

- Number of bricks per node for Erasure Coded volumes: upto 12-36 bricks

Recommended Requirements

- 4 vCPUs

- 6 GB of available system RAM

- One Network Interface Card (NIC) with bandwidth of at least 1 Gbps

Additional Storage Devices

For hosting etcd data directory:

- Storage disk size: 20 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/etcd**

For hosting time-series data from Graphite, Carbon, and Whisper applications:

- Storage disk size: 350 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/carbon**

2.1.1.3. Large Cluster Configuration

- Number of nodes: 17-24 nodes

- Number of volumes: upto 6-8 volumes per cluster

- Number of bricks per node for replicated volumes: upto 2-3 bricks

- Number of bricks per node for Erasure Coded volumes: upto 12-36 bricks

Recommended Requirements

- 6 vCPUs

- 6 GB of available system RAM

- One Network Interface Card (NIC) with bandwidth of at least 1 Gbps

Additional Storage Devices

For hosting etcd data directory:

- Storage disk size: 20 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/etcd**

For hosting time-series data from Graphite, Carbon, and Whisper applications:

- Storage disk size: 500 GB per cluster

- Filesystem format: XFS

- Mounting directory: **/var/lib/carbon**

2.1.2. Software Requirements

Red Hat Gluster Storage Web Administration is supported on Red Hat Enterprise Linux 7.5 or later 64-bit version.

Table 2.1. Software Requirements

Software	Name and Version
Operating System	Red Hat Enterprise Linux 7.5 or later

2.2. REQUIREMENTS FOR RED HAT GLUSTER STORAGE NODES

Ensure the following requirements are met on the Red Hat Gluster Storage nodes:

> **NOTE**
>
> Red Hat Gluster Storage Web Administration is not supported on new installations of Red Hat Gluster Storage 3.5.2 on Red Hat Enterprise Linux 8. Red Hat Gluster Storage server on Red Hat Enterprise Linux 8 and Red Hat Gluster Storage Web Administration on Red Hat Enterprise Linux 7 is not supported.

1. Red Hat Enterprise Linux 7.5 or later.

2. Red Hat Gluster Storage servers updated to the latest Red Hat Gluster Storage version 3.5 or greater. For detailed instructions on the upgrade process, see the Upgrading Red Hat Storage section in the Red Hat Gluster Storage Installation Guide.

3. Minimum hardware requirements

> **NOTE**
>
> For more information, see the knowledge base article on Red Hat Gluster Storage Hardware Compatibility.

4. Network Time Protocol (NTP) setup

5. Firewall access to ports

For detailed information on prerequisites and setting up Red Hat Gluster Storage server, see the *Red Hat Gluster Storage 3.5 Installation Guide*.

2.3. REQUIREMENTS FOR THE CLIENT SYSTEM

The Red Hat Gluster Storage Web Administration environment can be accessed by a client machine with the following web browser compatibility:

Table 2.2. Web Browser Compatibility

Software	Name and Version
Web Browser	Mozilla Firefox 38.7.0 or later
Web Browser	Google Chrome 46 or later

2.4. FIREWALL CONFIGURATION

Automated Firewall Setup

In this version of Red Hat Gluster Web Administration, firewall configuration is automated by Ansible automation. The tendrl-ansible installer configures the firewall during Web Administration installation as the variable **configure_firewalld_for_tendrl** is set to **True** by default. This automation opens all the required ports for the Web Administration environment.

To automatically configure the firewall, follow the Web Administration installation process. See the Web Administration installation section in the Quick Start Guide for details.

> **NOTE**
>
> For tendrl-ansible to automate firewall setup, ensure the firewalld service is configured and enabled. For instructions, see Using firewalls in the Red Hat Enterprise Linux 7 *Security Guide*.

Manual Firewall Setup

To manually configure firewall for Web Administration services:

1. Open the required ports before continuing the installation process

2. Set the variable **configure_firewalld_for_tendrl** to False in the **[all:vars]** section of the inventory file which will be applied to both the groups: **tendrl_server** and **gluster_servers**. See sample variables described in **Sample Inventory Variables** at the end of 3.5 Web Administration Installation procedure of this guide.

NOTE

The inventory file is created as part of the Web Administration Ansible installation process.

3. Follow Web Administration Installation procedure of this guide.

The list of the ports and the port numbers are given in the table below:

Table 2.3. Web Administration Port Numbers

TCP Port Numbers	Usage
2379	For etcd
2003	For Graphite
80 or 443	For tendrl http or https
8789	For tendrl–monitoring–integration

NOTE:

- If you are updating to Web Administration **3.5 Update 2** or higher from previous versions, you no longer need to open TCP port 3000 on the Web Administration server.

- If you are updating to Web Administration **3.5 Update 3** or higher from previous versions, you no longer need to open TCP port 10080 on the Web Administration server. Access to **Graphite-web** TCP port 10080 is unencrypted, you can open it if required.

To use Firewalld to open a particular port, run:

```
# firewall-cmd --zone=zone_name --add-port=5667/tcp
# firewall-cmd --zone=zone_name --add-port=5667/tcp --permanent
```

To use iptables to open a particular port, run:

```
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 5667 -j ACCEPT
# service iptables save
```

NOTE

To be able to execute the iptables commands successfully, ensure the **iptables-services** package is installed. To install the **iptables-services** package, run **yum install iptables-services**.

CHAPTER 3. INSTALLING WEB ADMINISTRATION

This chapter covers installing Red Hat Gluster Web Administration using Ansible automation.

3.1. PREREQUISITES

Before installing Red Hat Gluster Web Administration, ensure the following prerequisites are met:

1. Enable the following repositories on the Web Administration server and all the Gluster storage servers:

   ```
   # subscription-manager repos --enable=rhel-7-server-rpms

   # subscription-manager repos --enable=rhel-7-server-ansible-2-rpms
   ```

2. Enable the following repository on the Web Administration server:

   ```
   # subscription-manager repos --enable=rh-gluster-3-web-admin-server-for-rhel-7-server-rpms
   ```

3. Enable the following repositories on all the Gluster storage servers:

   ```
   # subscription-manager repos --enable=rh-gluster-3-for-rhel-7-server-rpms
   # subscription-manager repos --enable=rh-gluster-3-web-admin-agent-for-rhel-7-server-rpms
   ```

4. Set up SSH password–less connection from the Web Administration server system to the remote Gluster servers in addition to localhost (SSH to localhost).

   > **NOTE**
   >
   > For information on how to set up SSH key–based authentication, see the Using Key–based Authentication section in the *Red Hat Enterprise Linux System Administrator's Guide*.

5. If the **httpd** package is already installed on the Web Administration server, stop the **httpd** service before continuing with the installation:

   ```
   # systemctl stop httpd
   ```

3.2. INSTALLATION WORKFLOW

To install Web Administration, follow the sequence outlined below. For detailed instructions to execute the following sequence, see the next section entitled Web Administration Installation of this Guide.

1. Installing the latest version of Ansible and tendrl–ansible on the Web Administration server.

2. Creating inventory file with required groups: tendrl_server and gluster_servers with mandatory and optional ansible variables.

3. Executing the **site.yml** playbook and accessing the Web Administration environment.

> **NOTE**
>
> See also the README file from tendrl-ansible package available at the following path: **/usr/share/doc/tendrl-ansible-1.6.3/README.md**

Ansible Groups

The **site.yml** playbook from tendrl-ansible package expects the hosts to be divided into two groups according to its functionality:

1. **tendrl_server**: contains one machine acting as Web Administration server.

2. **gluster_servers**: contains all the Red Hat Gluster Storage nodes.

Ansible Roles

The tendrl-ansible package contains two Ansible roles with tasks intended for a particular component:

1. **tendrl-ansible.tendrl-server**: contains tasks for Web Administration server belonging to the tendrl_server group in the inventory file.
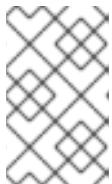
   > **NOTE**
   >
   > For more information about this role and the variables, see the README file from tendrl-ansible package available at the following path: **/usr/share/ansible/roles/tendrl-ansible.tendrl-server/README.md**

2. **tendrl-ansible.tendrl-storage-node**: contains tasks for Red Hat Gluster Storage nodes belonging to the gluster_servers group in the inventory file.

> **NOTE**
>
> For more information on this role and the variables, see the README file from tendrl-ansible package available on the following path: **/usr/share/ansible/roles/tendrl-ansible.tendrl-storage-node/README.md**
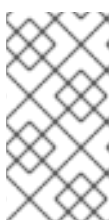
3.3. WEB ADMINISTRATION INSTALLATION

The following procedure outlines the steps to install Web Administration the Ansible way.

Procedure. Installing Web Administration

1. Install the latest version of Ansible and tendrl-ansible on the Web Administration server:

   ```
   # yum install tendrl-ansible
   ```

   > **NOTE**
   >
   > Verify that the latest Ansible package is obtained from the **rhel-7-server-ansible-2-rpms** channel before executing the following steps. Additionally, ensure that the Ansible version is the same on the Web Administration server as available on the storage nodes.

> **NOTE**
>
> Latest version of Web Administration is compatible with the latest version of Ansible. Web Administration is not compatible with versions below Ansible 2.5.
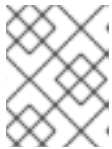
2. Create an Ansible inventory file with two Ansible groups: **tendrl_server** and **gluster_servers**. Ensure to use FQDNs for all the hosts in the inventory file as shown in the following example:
   Sample Inventory groups

   ```
   [tendrl_server]
   tendrl.example.com

   [gluster_servers]

   gl1.example.com
   gl2.example.com
   gl3.example.com
   gl4.example.com
   ```

   > **NOTE**
   >
   > For instructions on setting up an inventory file, see Ansible Inventory file setup in Ansible documentation.

3. Add the following required Ansible variables with their corresponding values in the inventory file:

   - etcd_ip_address: configures where etcd instance is listening

   - etcd_fqdn: configures Web Administration components to be able to connect to the etcd

   - graphite_fqdn: configures Web Administration components to be able to connect to graphite
     Sample Inventory variables

     ```
     [all:vars]

     etcd_ip_address=192.0.2.1
     etcd_fqdn=tendrl.example.com
     graphite_fqdn=tendrl.example.com
     ```

     > **NOTE**
     >
   > For more detail, see the Sample Inventory variables at the end of this installation workflow.

4. Add any other optional variables in the inventory file as required. The other variables are listed in the Ansible roles README files at the following paths. Enable or disable features by specifying values to the variables such as etcd-tls client authentication. For detailed TLS configuration instructions, see Chapter 5. TLS Encryption Configuration of this Guide.

   ```
   # /usr/share/ansible/roles/tendrl-ansible.tendrl-server/README.md
   # /usr/share/ansible/roles/tendrl-ansible.tendrl-storage-node/README.md
   ```

> **NOTE**
>
> The firewall configuration variable is enabled by default.
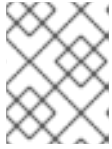
> **NOTE**
>
> For detailed inventory file configuration, see the README.md file provided with the installation at the following path:

```
# less /usr/share/doc/tendrl-ansible-1.6.3/README.md
```
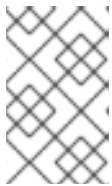
5. Copy the **site.yml** playbook into the working directory where the inventory file is stored.

```
# cp /usr/share/doc/tendrl-ansible-1.6.3/site.yml .
```

6. Copy the **prechecks.yml** file into the inventory file directory:

```
# cp /usr/share/doc/tendrl-ansible-1.6.3/prechecks.yml .
```

7. Set up SSH password-less connection from the Web Administration server system to the remote Gluster servers.

> **NOTE**
>
> For information about how to set up SSH key-based authentication, see the Using Key-based Authentication section in the *Red Hat Enterprise Linux System Administrator's Guide*.

8. Verify SSH connection to all the nodes from the inventory file without asking for password or validation of public key by running:

```
# ansible -i <inventory_file> -m ping all
```

Example

```
# ansible -i <inventory_file> -m ping all
gl3.example.com | SUCCESS => {
    "changed": false,
    "failed": false,
    "ping": "pong"
}
```

> **NOTE**
>
> Ansible should return **SUCCESS** and **pong** message for all the nodes as shown in the example above. Do not proceed until the SSH connection is successfully established.

9. To check if Web Administration minimal requirements and setup are met, run the prechecks playbook:

```
# ansible-playbook -i <inventory_file> prechecks.yml
```
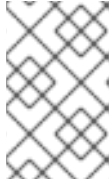
> **NOTE**
>
> If there are any missing requirements, the prechecks playbook will detect it immediately, and direct your attention to the specific problem before running the installation.

10. Run the prepared **site.yml** playbook using the following command to set up the Web Administration server and the Storage nodes:

```
# ansible-playbook -i <inventory_file> site.yml
```

11. Log in to the Web Administration environment. For login instructions, see the Web Administration Login chapter of this guide.

> **NOTE**
>
> The tendrl-ansible.tendrl-server role creates the default user as **admin** and default password as **adminuser**. The default password is stored in the **/root/password** file of the Web Administration server.

Sample Inventory Variables

If there is a single network interface on all machines, the example inventory variables would be as follows:

```
[all:vars]

etcd_ip_address=192.0.2.1
etcd_fqdn=tendrl.example.com
graphite_fqdn=tendrl.example.com
```

In the above example:

- 192.0.2.1 is the IP address of the Web Administration server

- tendrl.example.com is the hostname of the Web Administration server

- tendrl.example.com hostname is translated to IP address 192.0.2.1.

See the full description in the README file of tendrl-ansible.tendrl-server role and pay attention to the values you specify there when you use multiple network interfaces on the machines.

You can define these variables in variable files or from the command line directly, but including them into the inventory file provides you with a single file with a full description of tendrl-ansible setup for future reference.

The consolidated variables in the inventory file can be used for the cluster expansion process and also to ensure the installation configuration is intact. The inventory file does not contain the grafana admin password which is stored in the grafana_admin_passwd file generated during tendrl-ansible execution.

CHAPTER 4. UPGRADING RED HAT GLUSTER STORAGE WEB ADMINISTRATION

4.1. RED HAT GLUSTER STORAGE WEB ADMINISTRATION 3.4 TO 3.5

This chapter describes the procedure to upgrade Web Administration to version 3.5 from previous versions.

To upgrade your Web Administration environment to version 3.5, execute the following actions on the Gluster nodes and the Web Administration server:

On Gluster storage nodes

1. Stop and disable all Web Administration services on storage nodes.

2. Enable the Ansible repository and ensure the other required repositories are enabled.

3. Upgrade Red Hat Gluster Storage to version 3.5.

On Web Administration Server

1. Upgrade Red Hat Enterprise Linux on the Web Administration Server.

2. Import the Gluster 3.5 cluster.

On Gluster storage nodes

Stopping and disabling Web Administration Services

Stop and disable the following services on the storage nodes by executing the commands given below.

To stop and disable the tendrl–node–agent service:

```
# systemctl stop tendrl-node-agent
```

```
# systemctl disable tendrl-node-agent
```

To stop and disable the collectd service:

```
# systemctl stop collectd
```

```
# systemctl disable collectd
```

To stop and disable the tendrl–gluster–integration service:

```
# systemctl stop tendrl-gluster-integration
```

```
# systemctl disable tendrl-gluster-integration
```

> **NOTE**
>
> The **tendrl-node-agent** service is enabled and started during execution of the tendrl-ansible site.yml playbook. The **collectd** and **tendrl-gluster-integration** services are enabled and started after importing a cluster into the Web Administration environment.

Enabling Web Administration Repositories

Enable the Ansible repository by running the following command:

```
# subscription-manager repos --enable=rhel-7-server-ansible-2-rpms
```

Additionally, ensure that the other required Web Administration repositories are enabled. Run the following command to check if all the required repositories are enabled:

```
# yum repolist
```

> **NOTE**
>
> To check the required repositories, see the Prerequisites section of the Quick Start Guide.

After the repositories are enabled, clear yum cache:

```
# yum clean all
```

Upgrading Red Hat Gluster Storage

After enabling the required repositories, upgrade your Red Hat Gluster Storage environment to 3.5. For detailed upgrade instructions, see the Upgrading to Red Hat Gluster Storage 3.5 chapter in the Red Hat Gluster Storage 3.5 Installation Guide. After a successful upgrade, resume the following steps.

On Web Administration server

1. Stop all Web Administration services:

   a. To stop the tendrl-monitoring-integration service:

      ```
      # systemctl stop tendrl-monitoring-integration
      ```

   b. To stop the tendrl-node-agent service:

      ```
      # systemctl stop tendrl-node-agent
      ```

   c. To stop the tendrl-notifier service:

      ```
      # systemctl stop tendrl-notifier
      ```

   d. To stop the tendrl-api service:

      ```
      # systemctl stop tendrl-api
      ```

e. To stop the etcd service:

```
# systemctl stop etcd
```

f. To stop the carbon-cache service:

```
# systemctl stop carbon-cache
```

2. Update all packages on the Web Administration server:

```
# yum update
```

3. Run the tendrl-upgrade script:

```
# tendrl-upgrade
```

4. Run the tendrl-ansible playbooks with the same initial installation configuration. For instructions, see section Web Administration Installation, steps 2 to 9.

5. If updates to the kernel package occurred, reboot the server system. If not, restart the Web Administration services:

```
# systemctl restart httpd
# systemctl restart etcd
# systemctl restart carbon-cache
# systemctl restart tendrl-node-agent
# systemctl restart tendrl-monitoring-integration
# systemctl restart tendrl-notifier
# systemctl restart tendrl-api
```

After upgrading, import the Gluster 3.5 cluster in the Web Administration environment. For detailed import procedure, see the Import Cluster chapter of the Web Administration 3.5 Monitoring Guide.

CHAPTER 5. TLS ENCRYPTION CONFIGURATION

Red Hat Gluster Storage Web Administration supports Transport Layer Security (TLS) based security model. This model is used for the following purposes:

- Authentication and encryption of **etcd** communication between storage nodes and Web Administration server

- HTTPS encryption between Web Administration server and web browser

5.1. GENERAL PREREQUISITES

You need to have Certificate Authority (CA) to be able to generate and sign certificates. The CA can be either self-signed or a trusted CA. For instructions about generating a CA certificate, see the Creating Your Own Certificates section of the Red Hat AMQ Security Guide.

CA is used to sign certificates for the storage nodes and Web Administration server for TLS-based client server **etcd** authentication. CA is also used to sign the certificate that is used for the **https** setup on Web Administration server. However, CA for TLS **etcd** setup can be different from CA for **https** setup.

Red Hat Gluster Storage Web Administration or tendrl-ansible neither generates nor deploys certificate files or keys.

5.2. ENABLING TLS FOR ETCD

Red Hat Gluster Storage Web Administration supports **etcd's** TLS-based security model. This model supports authentication and encryption of traffic between **etcd** and Web Administration system components.

By default, **etcd** functions without authentication and encryption but it is recommended to use TLS authentication for client-server encryption.

5.2.1. Prerequisites for TLS Encryption

Before setting up the TLS encryption, ensure that the general prerequisites are met. See Section 5.1, "General Prerequisites".

- Generate a private key and a client certificate for each storage node and the Web Administration server. For more information, see the Creating and Managing Encryption Keys section of the *Red Hat Enterprise Linux Security Guide* . On each Web Administration managed storage node, and on the Web Administration server, place the PEM-encoded private key and the client/CA certificates in a secure place that is only accessible by the Web Administration server's **root** user.

- Configuration of TLS encryption for **etcd** is automated using tendrl-ansible. Hence, you need to have tendrl-ansible installed and the inventory file created. See Chapter 3, *Installing Web Administration* chapter.

> **NOTE**
>
> Configuration of TLS encryption for **etcd** is performed either during the installation of Web Administration (when tendrl-ansible is run for the first time) or later by rerunning tendrl-ansible.

5.2.2. Configuring TLS Encryption for `etcd`

After generating and placing the TLS certificate files in the preferred directory, update the value of the Ansible variables in the inventory file with the respective file paths of the certificate files.

Add and modify the following **etcd** TLS variables in the **[all:vars]** section of the inventory file.

Variable	Description
etcd_tls_client_auth	Variable used to enable or disable TLS authentication.
etcd_cert_file	Certificate used for SSL/TLS connections to **etcd**. When this option is turned on, **advertise-client-urls** can use the HTTPS schema.
etcd_key_file	Key for the certificate that has to be unencrypted.
etcd_trusted_ca_file	Trusted Certificate Authority.

1. Open the inventory file.

2. Set the value for **etcd_tls_client_auth** variable to **True**. By default, the value of this variable is **False**.

3. Edit the file path for the **etcd_cert_file** variable as required. The default value is **/etc/pki/tls/certs/etcd.crt**.

4. Edit the file path for **etcd_key_file** variable as required. The default value is **/etc/pki/tls/private/etcd.key**.

5. Edit the file path for the **etcd_trusted_ca_file** variable. The default value is **/etc/pki/tls/certs/ca-etcd.crt**.

6. Continue the Web Administration installation process by following the Web Administration Installation chapter.

5.3. ENABLING HTTPS FOR WEB ADMINISTRATION COMPONENTS

This section describes how to set up SSL access for Web Aadministration UI, REST API, and Grafana based dashboard.

Overview of Enabling HTTPS

- Web Administration UI, API and Grafana dashboard, which are provided by the apache server, are secured with SSL by reconfiguration of apache.

- Access to unencrypted **http** port is redirected to encrypted **https** port.

- Web Administration contains sample configuration files for the apache to simplify the SSL setup.

5.3.1. Prerequisites for Enabling HTTPS

- **mod_ssl** package must be installed and the default configuration in **/etc/httpd/conf.d/ssl.conf** must be left unmodified.

- SSL key and certificate files need to be deployed on the Web Administration server. See Section 5.1, "General Prerequisites".

> **NOTE**
>
> Enabling HTTPS for Web Administration components must be done after the Web Administration installation.

5.3.2. Limitations

- Access to Grafana dashboard is not authenticated, which means that anyone who has access to Web Administration login page can access and read all panels in the dashboard without any password. They also can learn about the cluster structure, current workload, and historic trends. This is because Web Administration uses anonymous access to Grafana dashboard.

- Web Administration server listens on a few ports that are not secured but needed for internal communication. For example, Web Administration server receives metrics data from storage machines.

- Nothing else is secured or restricted compared to the default setup without HTTPS enabled.

5.3.3. Configuring HTTPS for Web Administration Components

On a machine where Web Administration server is installed, perform the following steps.

1. Create a new **00_tendrl-ssl.conf** file using the sample configuration file:

   ```
   # cp /etc/httpd/conf.d/00_tendrl-ssl.conf.sample /etc/httpd/conf.d/00_tendrl-ssl.conf
   ```

2. Make the following changes to the **/etc/httpd/conf.d/00_tendrl-ssl.conf** file:

   - Set **ServerName** to host name (**fqdn**) of Web Administration server.

   - Edit the file path for the **SSLCertificateFile** variable if you want to use your own certificate instead of default self–signed **/etc/pki/tls/certs/localhost.crt** generated by the **mod_ssl** package.

   - Edit the file path for the **SSLCertificateKeyFile** variable if you have changed certificate file in the previous step. The default value is **/etc/pki/tls/private/localhost.key**.

3. Make the following changes to the **/etc/httpd/conf.d/tendrl.conf** file:

   - Uncomment the line which has the Redirect rule and replace **%ssl_virtualhost_fqdn%** with the fully qualified domain name of Web Administration server.

   - Comment the lines (put a # at the beginning of each line) that have the **DocumentRoot**, **ProxyPass**, and **ProxyPassReverse** directives.

4. Check if the configuration is valid.

   ```
   # apachectl -t
   ```

■

5. Reload the **httpd** daemon.

```
# systemctl reload httpd.service
```

6. Ensure that the **https** port is open.

```
# firewall-cmd --add-service=https
# firewall-cmd --add-service=https --permanent
```
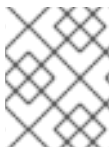
> **NOTE**
>
> Reload the web browser if you have the browser open with the Web Administration UI or Grafana dashboard.
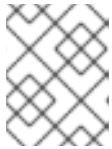
CHAPTER 6. WEB ADMINISTRATION LOGIN

The Web Administration interface is accessed on a client system using a compatible web browser.

Procedure. Logging in the Web Administration interface

1. Open the following URL in a web browser.

   > http://web-admin-server.example.com

   NOTE

   Replace web-admin-server.example.com with the hostname or FQDN of the Web Administration server.

2. The login page is displayed. Enter the default username **admin** and the default password **adminuser**, and click **Log in**.

Figure 6.1. Login Page

3. The Clusters interface is displayed after logging in to the Web Administration interface. This interface is the starting point to initiate a cluster import.

Figure 6.2. Landing Page
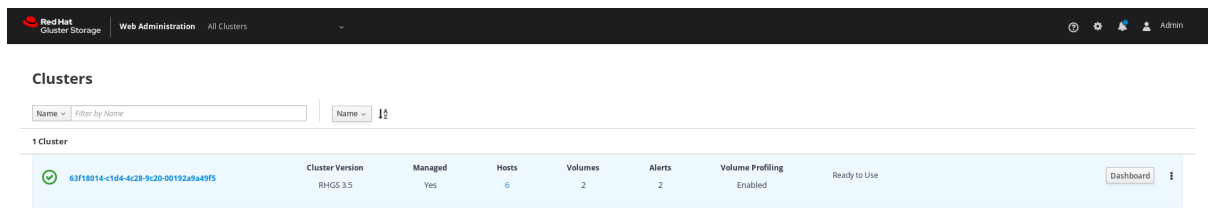
> **NOTE**
>
> For instructions on how to import a Gluster cluster, see the import cluster chapter in the Red Hat Gluster Storage Web Administration Monitoring Guide .

CHAPTER 7. WEB ADMINISTRATION INTERFACE NAVIGATION

7.1. WEB ADMINISTRATION DEFAULT LANDING INTERFACE

After logging in to the Web Administration interface, all the managed and unmanaged clusters are displayed in a rows format with the corresponding cluster attributes.

> **NOTE**
>
> To identify the version of Red Hat Gluster Storage installed, see the Cluster Version attribute.

Managed cluster are the clusters that are successfully imported by Web administration for monitoring purposes. Unmanaged clusters are the clusters that are ready to be imported by Web Administration.

Cluster Attributes

Cluster Version	Managed	Hosts	Volumes	Alerts	Volume Profiling	Ready to Use
RHGS 3.5	Yes	6	2	2	Enabled	

The following are the cluster attributes that are displayed in the cluster row:

- **Cluster name**: the name of the cluster

- **Cluster Version**: the version of Red Hat Gluster Storage installed

- **Managed**: whether the cluster is imported or ready to be imported

- **Hosts**: the number of hosts or nodes part of the cluster

- **Volumes**: the number of volumes part of the hosts

- **Alerts**: the number of alerts generated by the system for different tasks

- **Volume Profiling**: whether Enabled, Disabled or Mixed
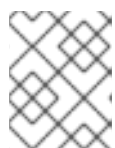
  > **NOTE**
  >
  > **Mixed** cluster attribute signifies a cluster containing at least one volume with profiling enabled and at least one with profiling disabled.

- **Cluster Status**: whether the cluster is ready for use or ready to be imported. The cluster state from the following:

  - Ready for Use

  - Ready to be Imported

  - Ready for expansion

  - Tasks in progress

- **Actionable Buttons**: the Import button, monitoring Dashboard button and an inline menu for the following administrative operations:

    - Enable and disable volume profiling

    - Unmanage Cluster

    - Expand Cluster

To identify managed and unmanaged clusters, view the cluster attributes.

Unmanaged Cluster: An unmanaged cluster displays the **Managed** attribute as **No**.

Managed Cluster: A managed cluster displays the **Managed** attribute as **Yes**.

Accessing Monitoring Dashboard

The Clusters tab provides a shortcut button to access the Grafana Monitoring Dashboard. At the right hand side of a cluster row, click on **Dashboard** and you will be redirected to the Grafana Monitoring dashboard.

7.2. WEB ADMINISTRATION INTERFACE SWITCHER

The Web Administration interface provides a menu to select and switch interface views displaying a common clusters interface and a cluster-specific interface.
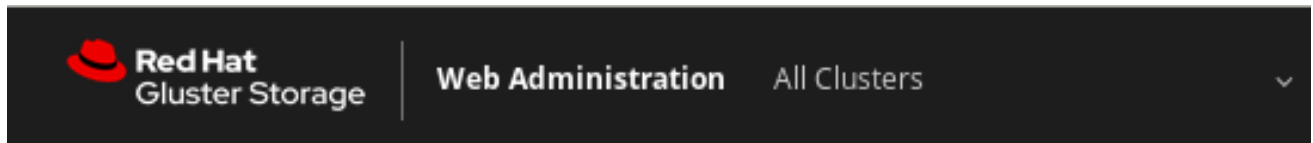
Accessing Interface Switcher

At the top left of the default landing page, next to the label Red Hat Gluster Storage Web Administration, a drop-down menu is available.
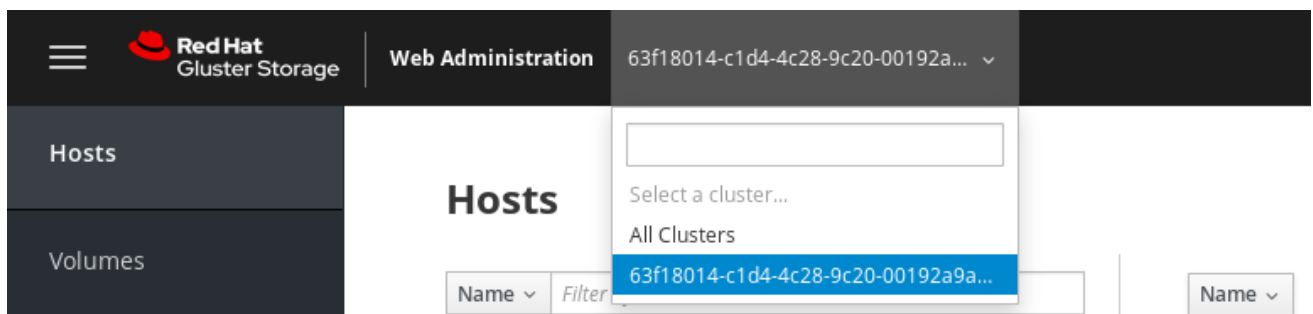
The drop-down menu provides:

- All Clusters view: the default selection after logging in that displays all managed and unmanaged clusters.

- Cluster-specific view: option to select a specific managed cluster.

To select a cluster-specific Interface, click on the down-down menu and select the specific managed cluster.

NOTE

Only managed clusters are available to select in the drop-down menu

The cluster-specific interface is displayed with a left navigation pane for Hosts, Volumes, Tasks, and Events associated with the selected cluster.

To switch back to the default landing interface view displaying all clusters, select **All Clusters** from the drop-down menu.

7.3. WEB ADMINISTRATION CLUSTER-SPECIFIC INTERFACE NAVIGATION

The cluster-specific interface provides a vertical navigation pane available at the left hand side of the interface to conveniently access the different elements of the clusters.
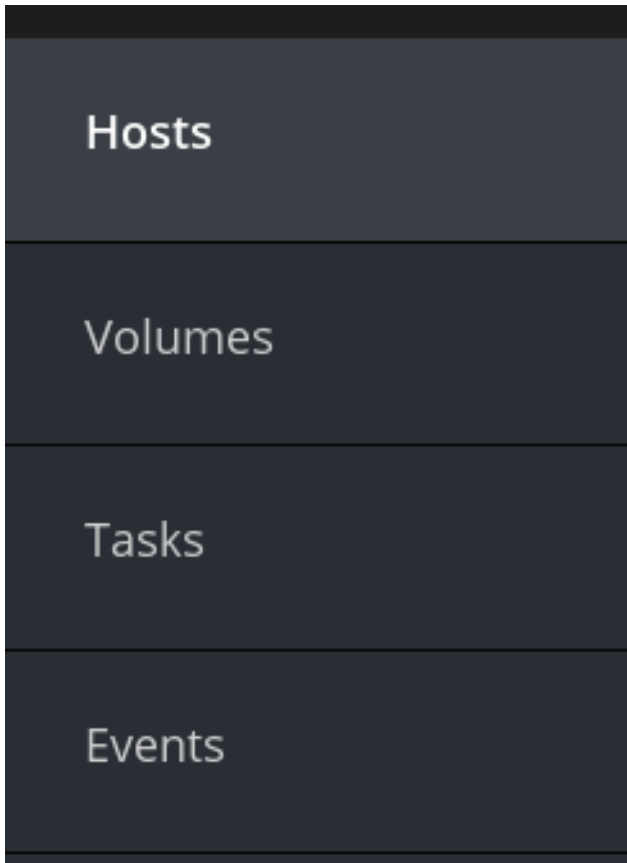
The navigation pane provides access to the following menus:

- Hosts: hosts view and monitoring dashboard shortcut

- Volumes: Volumes view and monitoring dashboard shortcut

- Tasks: view completed and failed system tasks

- Events: view all the system-wide events

7.3.1. Clusters View and Monitoring Dashboard Shortcut

The Clusters tab in the navigation pane lists all the imported clusters in a rows format. Each row shows the individual cluster attributes such as the version of the cluster, whether managed or unmanaged and the status of Volume Profiling whether enabled or disabled.

Figure 7.1. Clusters View

Accessing Monitoring Dashboard

The Clusters tab provides a shortcut button to access the Grafana Monitoring Dashboard. At the right hand side of a cluster row, click on **Dashboard** and you will be redirected to the Grafana Monitoring dashboard.

7.3.2. Hosts View and Monitoring Dashboard Shortcut

The Hosts tab in the navigation pane lists all the accepted hosts assigned to different clusters. The Hosts can be filtered by the Host Name or Status.

Figure 7.2. Hosts View

Accessing Monitoring Dashboard

The Hosts tab provides a shortcut button to access the Grafana Monitoring Dashboard. At the right hand side of a Host row, click on **Dashboard**, and you will be redirected to the Grafana Monitoring dashboard.

7.3.3. Events View

The Events view lists all the events occurred in the system. To view more detail of a specific event: copy the task ID or the job ID if available in the event listing to the task ID filter of the Tasks view interface.

Figure 7.3. Events View

7.3.4. Tasks View

The Web Administration consists of a sizeable number of user-initiated actions to accomplish operations such as importing clusters. It is crucial for Web Administration users to monitor and view the status of the actions they initiated.

A user can view the following task information:

- The status of an initiated task whether completed or failed

- The details of all past and present cluster-wide initiated actions

- The timestamp of the initiated task

- Retrieve a specific task by using the available filters

Figure 7.4. Tasks View

2 Tasks

	ImportCluster Task ID: b7b9a54c-05fe-4d67-ba22-2e6e19f9fd34	Submitted 16 Nov 2017 18:58:20	Completed 16 Nov 2017 19:00:28	Details
	ImportCluster Task ID: 11833313-6d6a-454f-8a56-f4594e66fa25	Submitted 16 Nov 2017 18:51:28	Completed 16 Nov 2017 18:56:47	Details

Tasks can filtered by Task ID, Task name, the status of the task and the time interval.

> **NOTE**
>
> The Task details will remain in the Web Administration interface for not more than the default **Time to live** (**TTL**) of 2 days. Once the timespan has elapsed, the task details will be discarded from the system.

7.3.5. Admin and Users

The Users tab lists all the users created to access the Web Administration interface. The interface provides user tasks such as adding, editing and deleting a user. For more user administration actions, see the Users and Roles Administration chapter of the *Red Hat Gluster Storage Web Administration Monitoring Guide.*

| User ID	Name	Role	Notification	Email	Actions	
admin	Admin	Admin	⊗ Disabled	admin@tendrl.org	Edit	⋮
administrator	John Smith	Normal	⊘ Enabled	jsmith@org.com	Edit	⋮

7.3.6. Alerts and User Settings

To view system-wide notifications and to change the user password, a menubar is available at the top right corner of the interface.
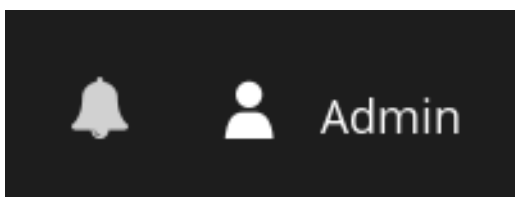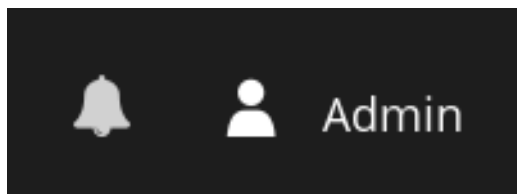
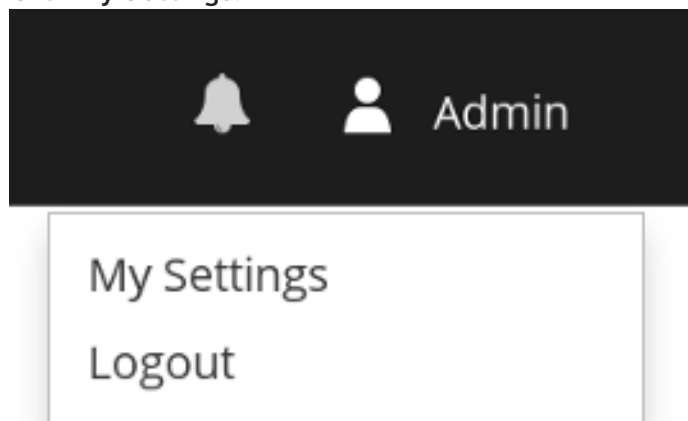To view system-wide alerts, click on the bell icon at the top right menubar of the interface.
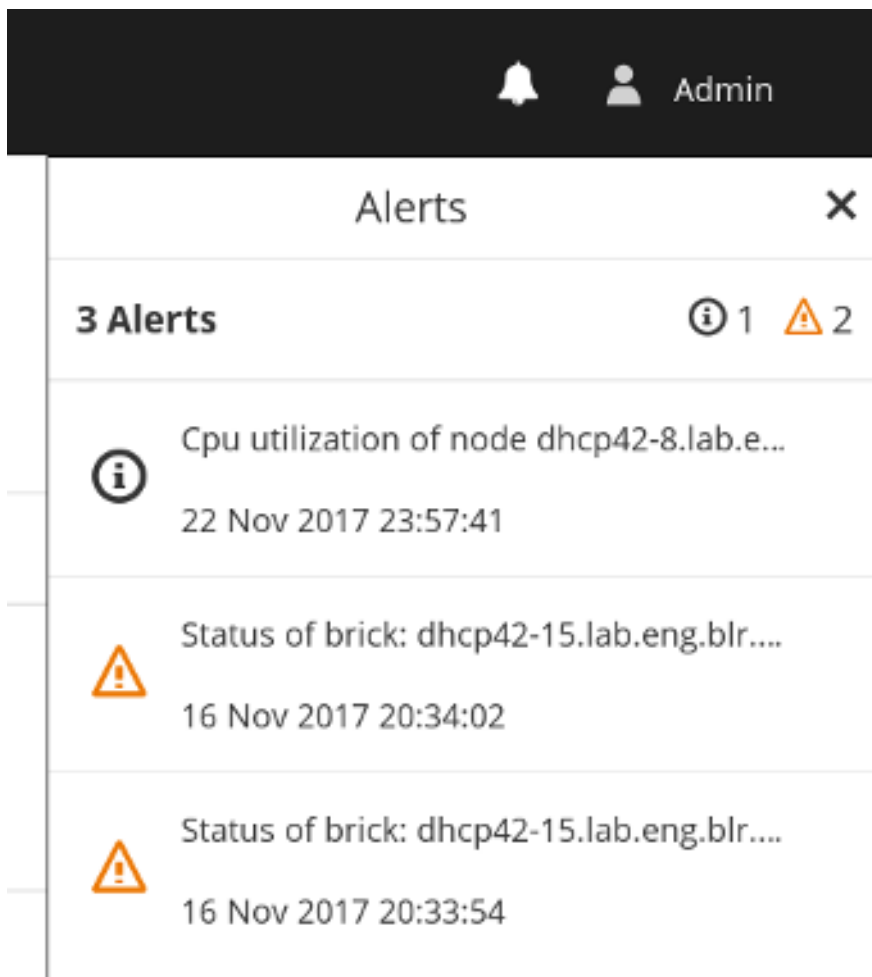
Changing User Password

To change the user password:

1. Click on the user icon from the menu bar.

2. Click **My Settings**.

3. A dialog window is opened. Enter the new password twice and click **Save**.

NOTE

Email notifications are disabled by default. To enable, check the **Email Notifications** box. For email notifications configuration instructions, see the SMTP Notifications Configuration section of the *Red Hat Gluster Storage Web Administration Monitoring Guide*.

Logging out from the interface

To log out from the interface:

1. Click on the user icon from the menu bar.

2. Click **Logout**.