Overland Storage

SnapScale™

Administrator's Guide

For a Clustered Network Running
RAINcloudOS™ Version 3.0

December 2012
10400405-002

FW 3.0.163 (R2).

Overland Storage, Inc.
9112 Spectrum Center Blvd.
San Diego, CA 92123
U.S.A.

Tel: 1.877.654.3429 (toll-free U.S.)
Tel: +1.858.571.5555, Option 5 (International)
Fax: +1.858.571.0982 (general)
Fax: +1.858.571.3664 (sales)
www.overlandstorage.com

Preface

Audience and Purpose

This guide is intended for system and network administrators charged with installing and maintaining a SnapScale cluster running RAINcloudOS 3.0 on their network. It provides information on the installation, configuration, security, and maintenance of the SnapScale cluster and nodes.

It is assumed that the administrator is familiar with the basic concepts and tasks of multi-platform network administration.

This guide also provides information on the following utilities and software components:

- SnapScale node setup and configuration.
- SnapScale cluster setup, configuration, and usage.
- The RAINcloudOS 3.0 Web Management Interface usage.

Product Documentation

SnapScale product documentation and additional literature are available online, along with the latest release of the RAINcloudOS 3.0 software.

Point your browser to:

http://docs.overlandstorage.com/snapscale

Follow the appropriate link on that page to download the **latest** software file or document.

For additional assistance, search at http://support.overlandstorage.com.

Overland Technical Support

For help configuring and using your SnapScale cluster, email our technical support staff at techsupport@overlandstorage.com.

You can get additional technical support information on the Contact Us web page:

http://docs.overlandstorage.com/support

For a complete list of support times depending on the type of coverage, visit our website at:

http://docs.overlandstorage.com/care

Conventions

This document exercises several alerts and typographical conventions.

Alerts

Convention	Description & Usage
IMPORTANT	An *Important* note is a type of note that provides information essential to the completion of a task or that can impact the product and its function.
CAUTION	A *Caution* contains information that the user needs to know to avoid damaging or permanently deleting data or causing physical damage to the hardware or system.
WARNING	A *Warning* contains information concerning personal safety. Failure to follow directions in the warning could result in bodily harm or death.
ADVERTISSEMENT	Un Canadien *avertissement* comme celui-ci contient des informations relatives à la sécurité personnelle. Ignorer les instructions dans l'avertissement peut entraîner des lésions corporelles ou la mort.

Typographical Conventions

Convention	Description & Usage
Button_name	Words in this special boldface font indicate the names of command buttons found in the Web Management Interface.
Ctrl-Alt-r	This type of format details the keys you press simultaneously. In this example, hold down the Ctrl and Alt keys and press the r key.
NOTE	A Note indicates neutral or positive information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases, for example, memory limitations or details that apply to specific program versions.
Menu Flow Indicator (>)	Words with a greater than sign between them indicate the flow of actions to accomplish a task. For example, Setup > Passwords > User indicates that you should press the Setup button, then the Passwords button, and finally the User button to accomplish a task.
Courier Italic	A variable for which you must substitute a value
Courier Bold	Commands you enter in a command-line interface (CLI)

Information contained in this guide has been reviewed for accuracy, but not for product warranty because of the various environments, operating systems, or settings involved. Information and specifications may change without notice.

Software Updates

The latest release of the RAINcloudOS software can be obtained from the Downloads and Resources (SnapScale Solutions) page at the Overland Storage website:

http://docs.overlandstorage.com/snapscale

Follow the appropriate instructions to download the **latest** software file.

For additional assistance, search at http://support.overlandstorage.com/.

Contents

Chapter 4 - Storage Options

Chapter 5 - Security Options

Chapter 6 - System Monitoring

Chapter 7 - Maintenance

Overview

SnapScale is a flexible, scalable, low-maintenance network-attached storage cluster composed of a redundant array of independent nodes running RAINcloudOS. This guide applies to SnapScale nodes running RAINcloudOS version 3.0.

A SnapScale cluster provides the following benefits:

- Increase IT agility by providing storage capacity on demand.
- Simple to configure and administer.
- Higher availability:
  - Data balanced across cluster.
  - Data mirroring so no single point of failure.
  - Improved reliability as nodes are added.
  - Increased availability of data in case of disk, node or network failures.
- Start small and expand capacity incrementally and non-disruptively as needed to hundreds of terabytes across multiple nodes.
- Uses a single global namespace.
- Minimize overall system and management costs.
- Support private cloud storage implementations.

With a SnapScale cluster, volumes can be configured, created, provisioned, and grown on demand. Files can be accessed either through NFS or CIFS/SMB protocols.

Topics in Overview:

SnapScale Conventions

The SnapScale cluster supports three or more redundant (mirrored) nodes for data protection. An Administrator can configure, add, or remove nodes on demand to change storage requirements. The overall storage system is able to easily grow from three nodes to meet your needs.

Peer sets are created using two or three drives (based on redundancy choices) located on different nodes. Each peer set member has the same data and metadata as its peers.

There are three different states for SnapScale nodes:

- **Uninitialized node** – an uninitialized node that has not been joined to a SnapScale cluster.
- **SnapScale node** – a healthy node that is a member of a fully-configured SnapScale cluster.
- **Management node** – a SnapScale node with special duties involved in managing the cluster. The Management node is selected automatically by the RAINcloudOS when the cluster boots. Should that management node fail, another currently available node is automatically chosen to become the new Management node.

Other key concepts include:

- **Management IP** – the IP address through which the administrator accesses the Web Management Interface of the current Management node.
- **Peer set** – a set of two or three disks (each on a separate node) that have mirrored data for redundancy.
- **Cluster Name** – the name visible to network clients and used to connect to the cluster (similar to a server name), and resolvable to node IP addresses via DNS round robin.
- **Cluster Management Name** – the hostname resolvable to the Management IP for Web Management Interface access or Snap EDR configuration.
- **Data Replication Count** – an administrator-specified, cluster-wide count of the number of mirrored copies of data within the cluster. The Data Replication Count can be either "2" or "3" and determines the number of drives in a peer set.

A SnapScale cluster consists of two separate networks:

- **Client Network** – used exclusively for client access. Clients can connect to any node to access data anywhere on the cluster.
- **Storage Network** – an isolated network used exclusively by the cluster for inter-node communications. This includes:
  - Heartbeat (node health/presence) sensing.
  - Synchronization of peer set members.
  - Data transfer between nodes to facilitate clients reading from and writing to files.

SnapScale Node Requirements

The following table details the basic requirements for cluster nodes:

Requirement	Detailed Description
Minimum number of nodes	A SnapScale cluster must have a minimum of three (3) nodes to operate normally.
Maximum number of nodes	The maximum number of nodes supported in RAINcloudOS 3.0 is 100 nodes.
Limit one cluster per subnet	Only one cluster can exist on a subnet and all the nodes on that subnet can only attach to that cluster. To create a new cluster, all the nodes must reside on a subnet without a SnapScale cluster.
No expansion units	A SnapScale node cannot have any expansion units attached to it.
Minimum number of disks per node	Each node must have a minimum of four disks. Additional disks can be added as needed.

Requirement	Detailed Description
Maximum size of file on cluster	While the system reports total free space across the entire cluster, the maximum file size at any given time is dictated by free space on the least-utilized peer set.
Common Storage network	To form or join a SnapScale cluster, each Uninitialized node must be connected to the same Storage network as the other nodes.
Storage network Links	To form or join a SnapScale cluster each Uninitialized node must have connectivity (active link) on both Storage network ports.
Storage network usage	Only a single cluster can use a given Storage network.
Client network separate from Storage network	The Client and Storage networks must be on different (independent) networks, and the Storage network must be isolated from all other networks.
Nodes must have same RAINcloudOS version	To form a SnapScale cluster, all nodes must be running the same version of RAINcloudOS. To join an already configured SnapScale cluster, an Uninitialized node must have the same version of RAINcloudOS as the other SnapScale nodes: • If the Uninitialized node has an older version of the RAINcloudOS, the Uninitialized node must be upgraded to the later version. • If the Uninitialized node has a newer version of the RAINcloudOS, then all SnapScale nodes must be upgraded to the later version. (The node can be reinstalled with a version matching the cluster if the hardware supports it.)
Adding nodes	When adding nodes to an existing cluster, the number of nodes added at one time should be at least the same number as the Data Replication Count in order to use them to efficiently increase cluster storage space.
Disk requirements	All disks in the cluster must be the same type of disk (such as SAS) and same rotational speed. There must not be any empty slots between disks on a node as populated from left to right, top to bottom.

RAINcloudOS Specifications

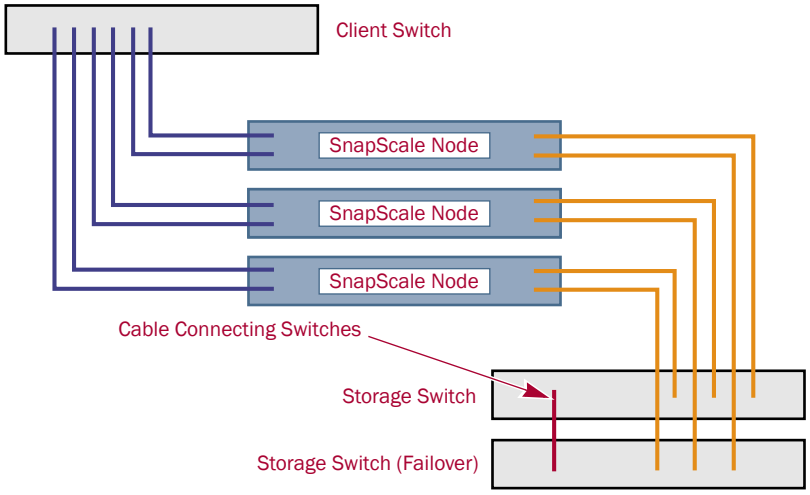
These specifications apply to all SnapScale nodes running RAINcloudOS 3.0:

Feature	Specification
Network Transport Protocols	TCP/IP (Transmission Control Protocol/Internet Protocol) UDP/IP (User Datagram Protocol/Internet Protocol)
Network File Protocols	Microsoft Networking (CIFS/SMB) UNIX Network Filesystem (NFS) 3.0 only Hypertext Transfer Protocol (HTTP/HTTPS)

Feature	Specification
Network Client Types	Microsoft Windows 2003/2003 R2/2008 SP2/2008 R2 /XP SP3/Vista SP2/7 Mac OS X 10.5/10.6/10.7/10.8 (via CIFS/SMB) Sun Solaris 10 and 11 HP-UX 11 AIX 5.3/6 Red Hat Enterprise Linux (RHEL) 4.x/5.x/6.x Novell SuSE Linux Enterprise Server (SLES) 10.x/11.x
Network Security	• Microsoft Active Directory Service (ADS) (member server) • UNIX Network Information Service (NIS) • File and Folder Access Control List (ACL) Security for Users and Groups • Secure Sockets Layer (SSL v2/3) 128-bit Encryption • SMTP Authentication and support for email encryption (STARTTLS and TLS/SSL encryption protocols)
Data Protection	• Snapshots for immediate or scheduled point-in-time images of the cluster filesystem • Support for network backup via CIFS/SMB • APC® brand Uninterruptible Power Supply (UPS) with Network Management Cards, a USB interface, or a serial interface (with USB-to-Serial adapter) are supported for graceful system shutdown
System Management	• Browser-based administration tool called the Web Management Interface • Read-only CLI support • Environmental monitoring • Email event notification • Data importation (migration)
DHCP Support	Only supports Dynamic Host Configuration Protocol (DHCP) in an Uninitialized node for configuring or adding to a cluster.

SnapScale Client and Storage Networks

Each SnapScale node has two 1-gigabit Ethernet (GbE) ports on the motherboard (next to the USB ports at the rear) that are dedicated for connections (blue lines) to a switch on the Client network. The two 1GbE ports on a card in slot 2 are dedicated for connections (orange lines) to two switches on the cluster's private Storage network for communication between nodes.



SnapScale 10Gb nodes feature an upgrade to a 10GbE card for the Client network in slot 1 and a 10GbE card for the Storage network in slot 2. (The motherboard 1GbE ports are not used with a 10GbE system.)

For connections between 10GbE cards and 10GbE switches, use either direct-attached copper cables or fibre cables with SFP+ modules pre-installed in the card and switch ports.

IMPORTANT: If using fibre cables, you must use Overland-approved SFP+ modules. With the node powered off, insert the modules into the card and switch ports. Connect the fibre cable between the two SFP+ modules.

When the two switches on the Storage network are connected together using an Ethernet or 10GbE cable between the switches, failover is enabled. To support high availability (HA), each Storage network port on the node needs to be connected to a separate storage switch.

Japanese Voluntary Control Council for Interference (VCCI)

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

(Translation: This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.)

Chapter 220

Setup and Configuration

This section covers the initial setup and configuration of an individual SnapScale node running RAINcloudOS 3.0. It also addresses how to use that node to set up a SnapScale cluster of three or more nodes, or to add the node to an existing SnapScale cluster.

NOTE: For information concerning the installation and wiring of the SnapScale node hardware, refer to the *SnapScale Quick Start Guide*.

Topics in Setup and Configuration:

Connecting for the First Time

NOTE: Uninitialized nodes are configured to acquire their IP address from a DHCP server. If no DHCP server is found on the network, the node defaults to an IP address in the range of 169.254.xxx.xxx and is labeled "ZeroConf" in SnapServer Manager (SSM). You may not be able to see Uninitialized nodes on your network until you discover them using either the default node name or the SSM utility and optionally assign them an IP address.

Connect Using the Node Name

This procedure requires that name resolution services (via DNS or an equivalent service) be operational.

NOTE: Any node that is earmarked to be part of a cluster can be used to create the cluster.

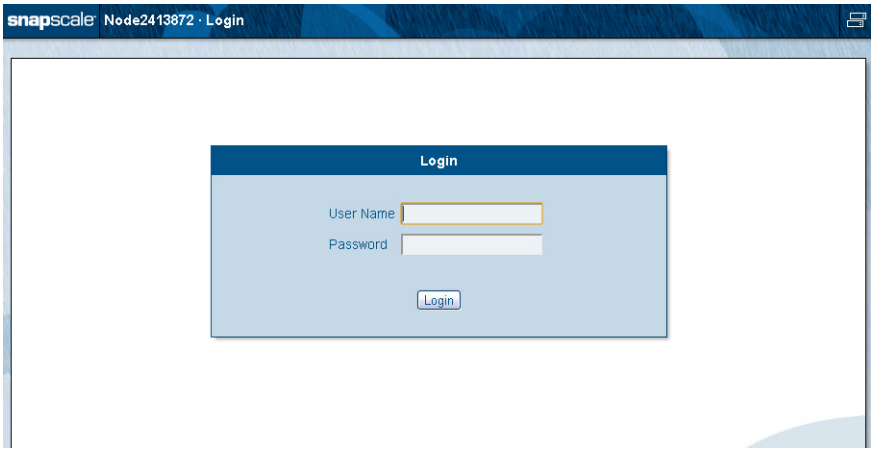
1. Find the **node name** of an Uninitialized node that is to be used to create a new SnapScale cluster.

   A SnapScale node name is of the format "Node*nnnnnnn*," where *nnnnnnn* is the node chassis number. The node number is a unique, numeric-only string that appears on a label affixed to the bottom of the appliance.

2. In a web browser, enter the **URL** to connect to the node.

   For example, enter "http://Node*nnnnnnn*" (using the node name).

3. Press **Enter** to connect to the Web Management Interface.



4. In the login dialog box, enter **admin** as the user name and **admin** as the password (the system defaults), then click **OK**.
5. Complete the **Initial Setup Wizard** to either create a new SnapScale cluster or join an existing cluster.

Connect Using SSM

1. Launch **SSM**.

   SSM discovers all SnapServers, SnapScale clusters, and SnapScale nodes on its local network segment and displays their names, IP addresses, and other status information in the main console. If you do not have a DHCP server, there might be a delay before the node appears on the network.

   NOTE: To distinguish multiple SnapServers or SnapScale nodes, you may need to find their default names as explained in "Connect Using the Node Name."

2. If using a DHCP server, proceed to Step 3; otherwise, assign an **IP address** to one of the nodes to be configured in the cluster.

   NOTE: Only one node needs to be configured with an IP address in order to create the cluster.

   a. In SSM, right-click the **node name**.

   b. Select **Set IP Address**.

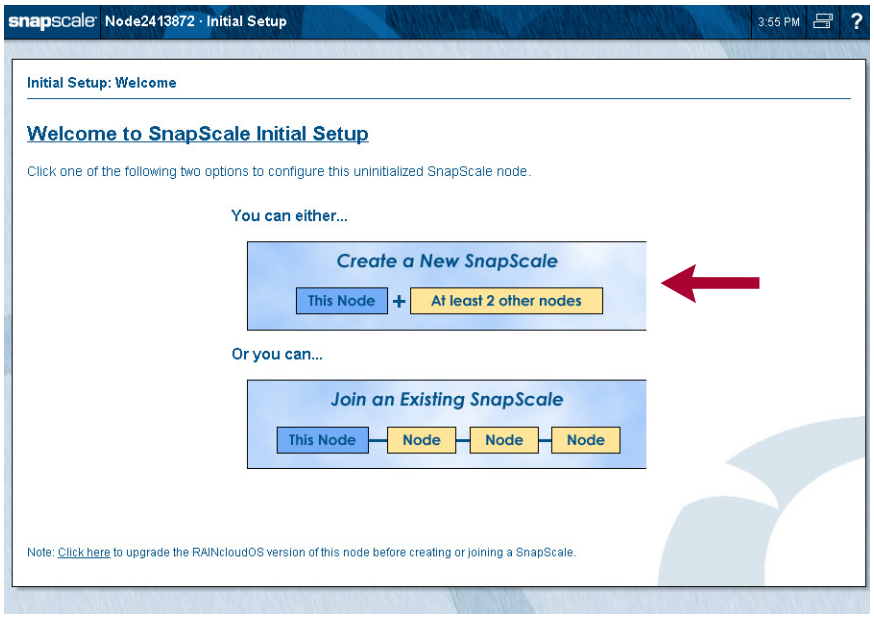
   c. Enter an IP address and a subnet mask, then click **OK**.

3. In SSM, right-click the node name and select **Launch Web Administration**.
4. Log into the Web Management Interface.

   In the login dialog box, enter **admin** as the user name and **admin** as the password (the system defaults), then click **OK**.
5. Complete the **Initial Setup Wizard** to either create a new SnapScale cluster or join an existing cluster.

Create a New SnapScale Cluster (via Wizard)

On a new node, once you log in, the Initial Setup Wizard runs displaying the Welcome page. From the Initial Setup Wizard, you can use this node to create a new SnapScale cluster by connecting to two or more other nodes. Click the **Create a New SnapScale** button to start the wizard.



The Initial Setup Wizard for **creating** a new SnapScale cluster consists of seven steps:

Step 1: Select the nodes to be included in the cluster.

Step 2: Review the Client network information.

Step 3: Choose the static TCP/IP settings for the Client network.

Step 4: Populate the Static IP addresses for the nodes.

Step 5: Enter the basic SnapScale properties.

Step 6: Set the date and time.

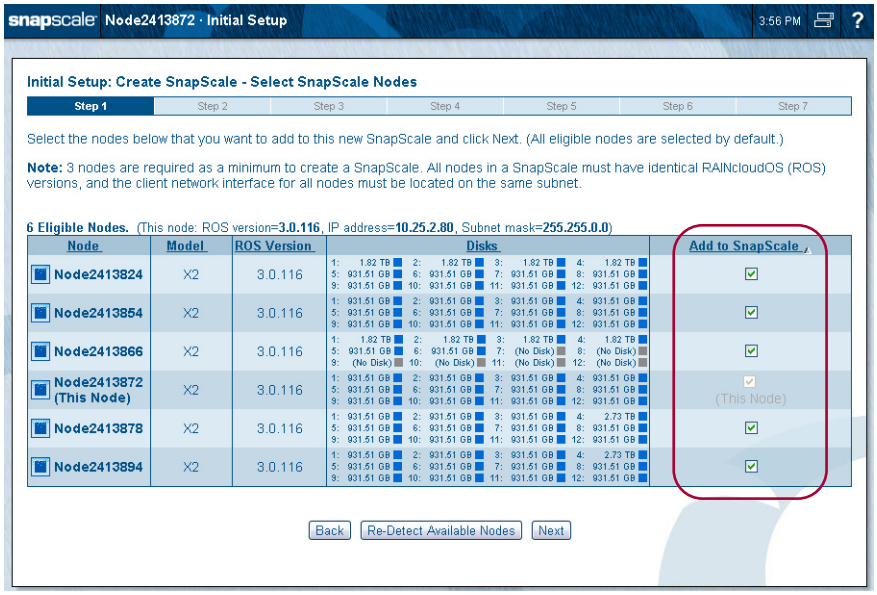
Step 7: Verify the settings and create a SnapScale cluster.

NOTE: After the cluster is created, you are asked to configure the Administrator's password as part of Step 7.

Step 1 – Select SnapScale Nodes

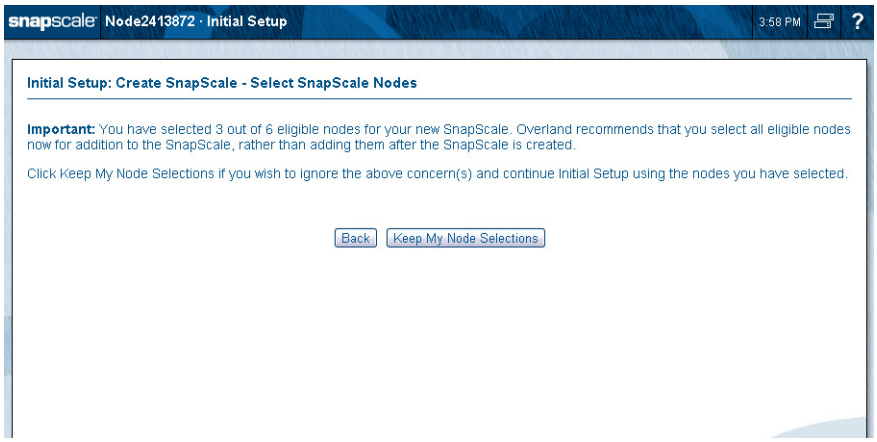
Select the nodes you want to use from the list of eligible nodes.

IMPORTANT: At least three nodes are required to create a SnapScale clustered network. All nodes must have the identical version of RAINcloudOS (ROS). The Client network interfaces for all the nodes must be located on the same public network subnet, and the Storage network interfaces for all nodes must be located on the same private Storage network subnet. The nodes cannot have any expansion units attached.



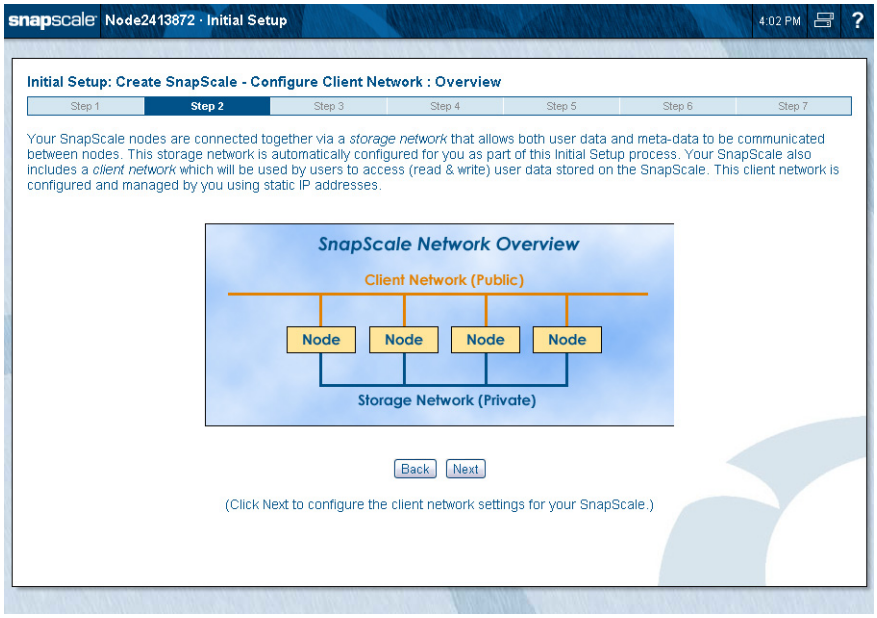
Verify that the boxes in the Add to SnapScale column for the nodes you want to use are checked. Click **Re-Detect Available Nodes** to refresh the list. When ready, click **Next**.

NOTE: If you deselect one or more of the detected nodes, when you click Next a message page is displayed recommending that you add all the nodes at once.



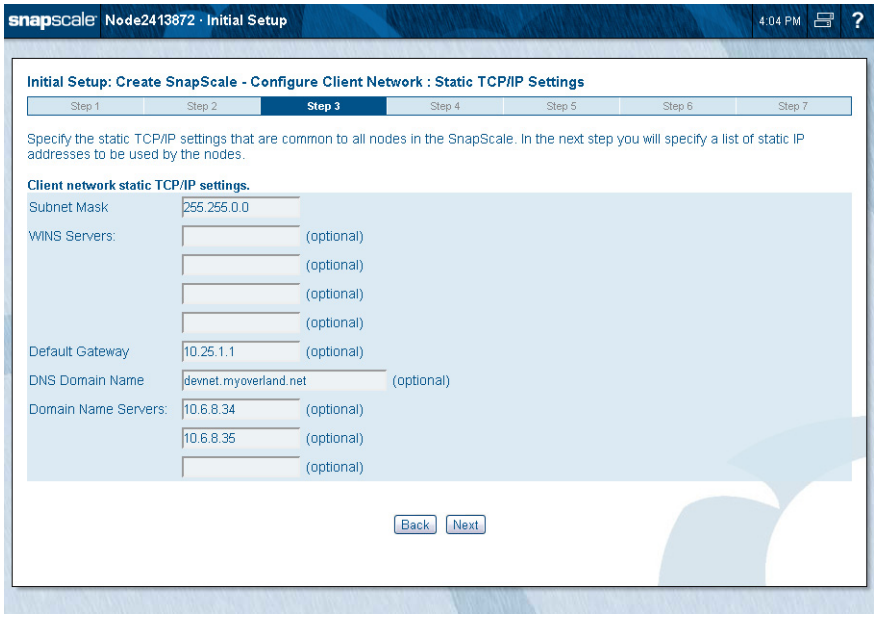
Step 2 – Client Network Configuration Overview

Review the information about setting up your Client network. Click **Next** to continue.



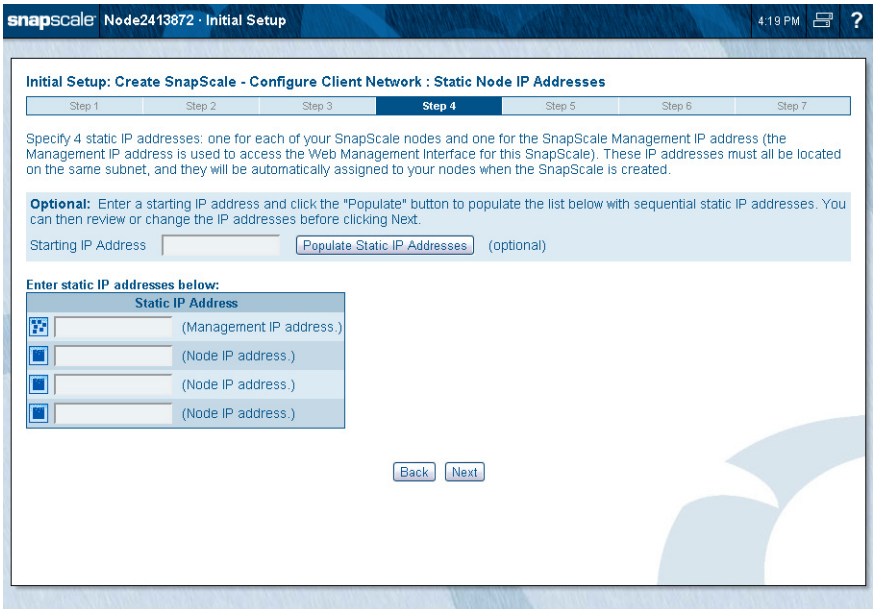
Step 3 – Choose Client Network Static TCP/IP Settings

A SnapScale cluster requires a set of static IP addresses: one for each node, and one for the Management IP. Use this step to specify the static TCP/IP settings that will be common to all nodes in the cluster. Then click **Next** to continue to the next page to set the actual node static IP addresses.



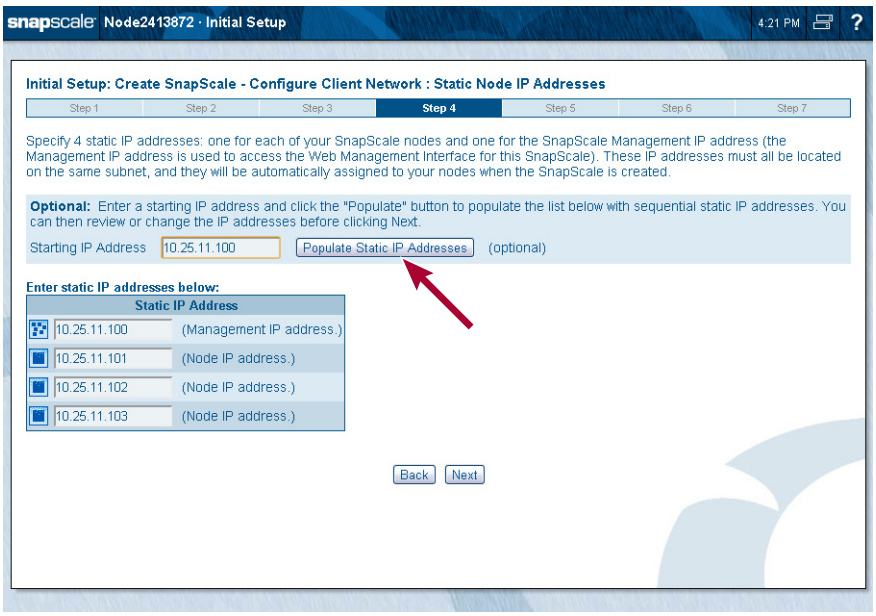
Step 4 – Configure Node Static IP Addresses

Specify the static IP addresses for each of your nodes and one for the SnapScale Management IP address used to access the Web Management Interface for this cluster.



These IP addresses must all be located on the same subnet. They are automatically assigned to your nodes when the SnapScale cluster is created.

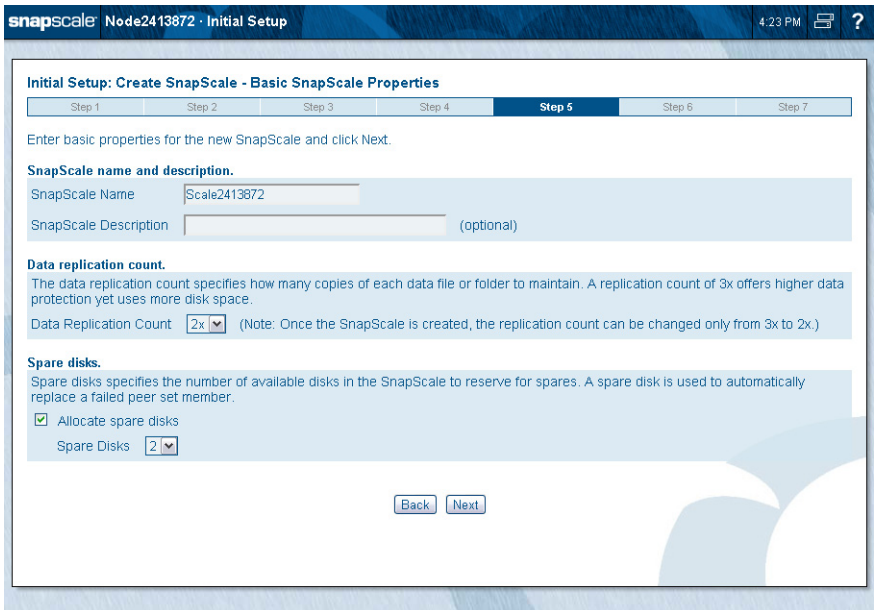
The **Populate Static IP Addresses** button can be used to automatically enter a sequential list of static IP addresses. Just enter an IP address on the subnet and click the **Populate Static IP Addresses** button. The fields below it are automatically populated.



Click **Next** to continue.

Step 5 – Basic SnapScale Properties

Use this step to enter the basic properties for your new SnapScale cluster, then click **Next**.

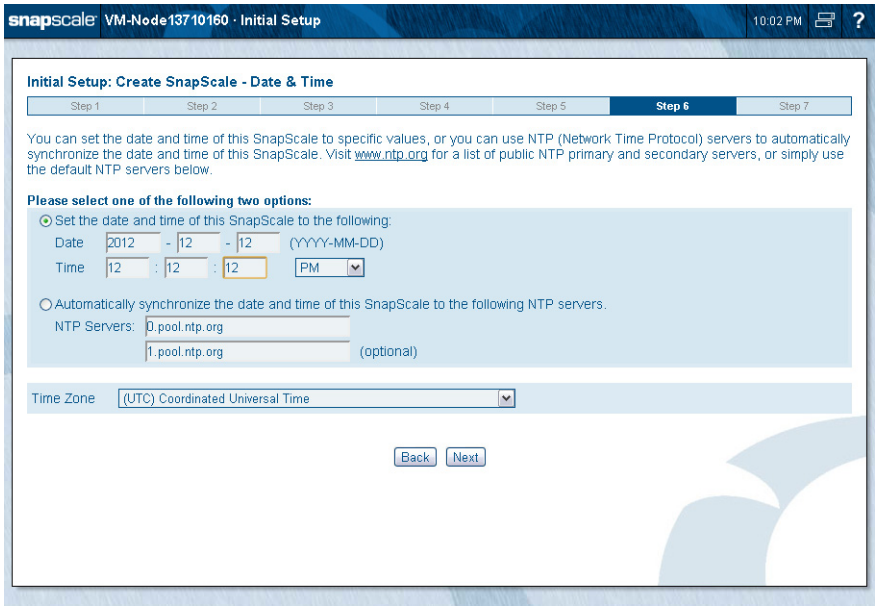


This table lists and describes the basic options:

Option	Description
SnapScale Name	Either accept the default name or enter an alphanumeric name up to 15 characters in length. Network clients use this name with round-robin DNS name resolution to connect to the cluster. The default name is "Scale*nnnnnnn*" (where *nnnnnnn* is the appliance number of the node used to create the cluster).
Description	This optional field provides a place to define the cluster in the overall scheme of your network and better identify the cluster on a LAN.
Data Replication Count	The data replication count establishes the level of data redundancy in the cluster. The setting specifies how many disks are in a peer set and as a result how many copies of each data file or folder to maintain. A count of 3x offers higher data protection but uses more disk space. Once the cluster is created, the count can only be decreased from 3x to 2x. It cannot be increased from 2x to 3x.
Spare Disks	Check the box and select the number of spare disks you want to reserve. A spare disk is used to automatically replace a failed Peer Set member. If there are unused drives remaining after allocating the number of spares requested, they are used for other peer sets. If there is an insufficient number of drives left to create a final peer set, the drives are configured as additional spares.

Step 6 – Set Date and Time

Nodes automatically synchronize time with one another. You can either manually set the date and time to specific values, or you can use NTP (Network Time Protocol) servers to automatically synchronize the date and time. Visit www.ntp.org for a list of public NTP primary and secondary servers, or simply use the default NTP servers below.



If you intend to join the cluster to a Windows domain, configure the cluster using the manual settings to set the date and time. Otherwise, configure the cluster to synchronize with up to two NTP servers.

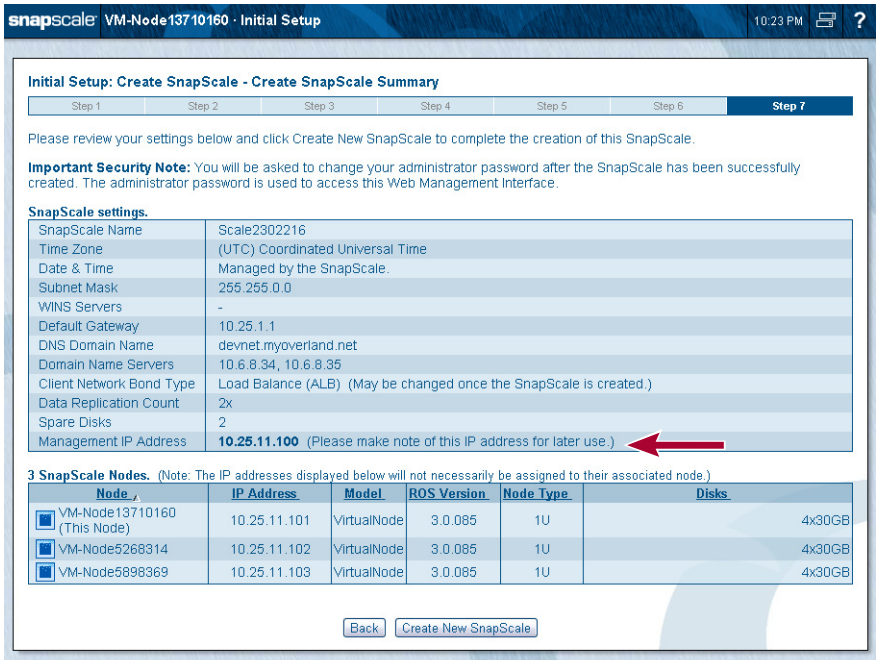
NOTE: NTP cannot be used if you are joining a Windows Active Directory domain.

Default NTP servers automatically populate the server fields. The Time Zone is set automatically to UTC time but can be changed using the drop-down list.

Click **Next** to continue.

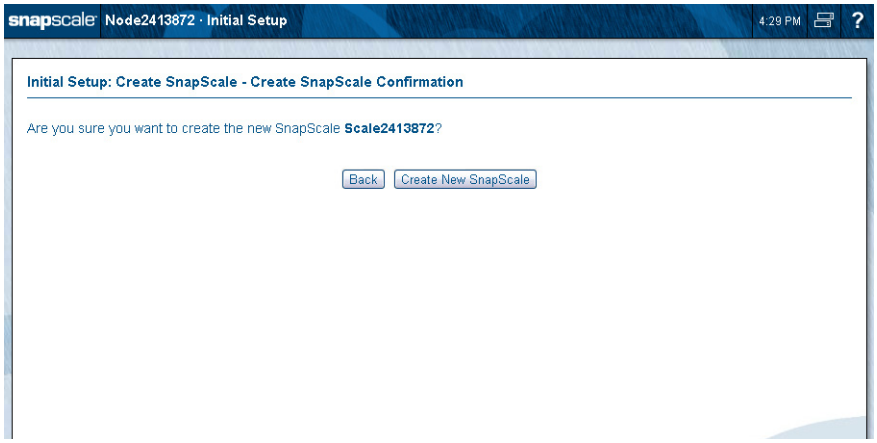
Step 7 – Summary Page Verification & Cluster Creation

At this step, review the current settings and go back if you need to make changes.

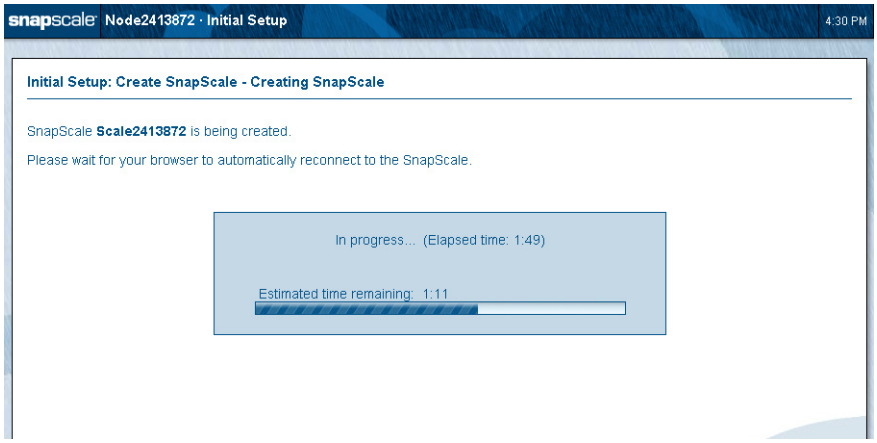


NOTE: Make note of the Management IP address for later use. Also, the Client Network Bond Type can be changed after the cluster is created. See Chapter 3, "TCP/IP Networking."

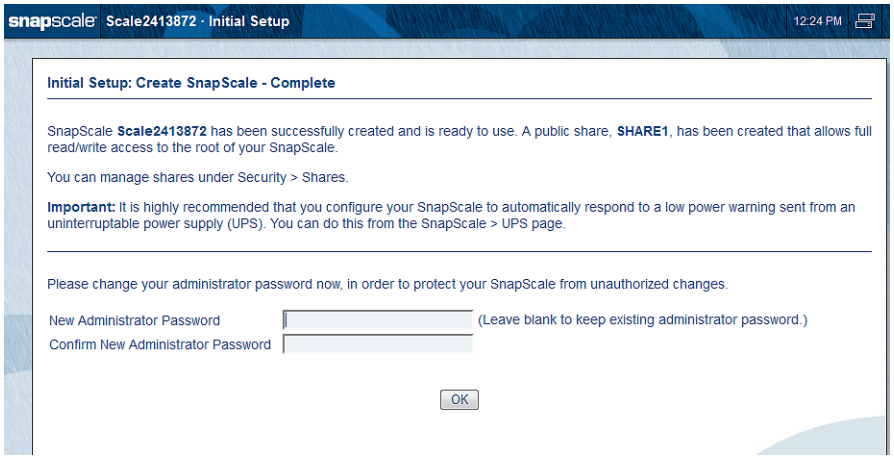
Click **Create New SnapScale** to complete the process. A confirmation screen is shown.



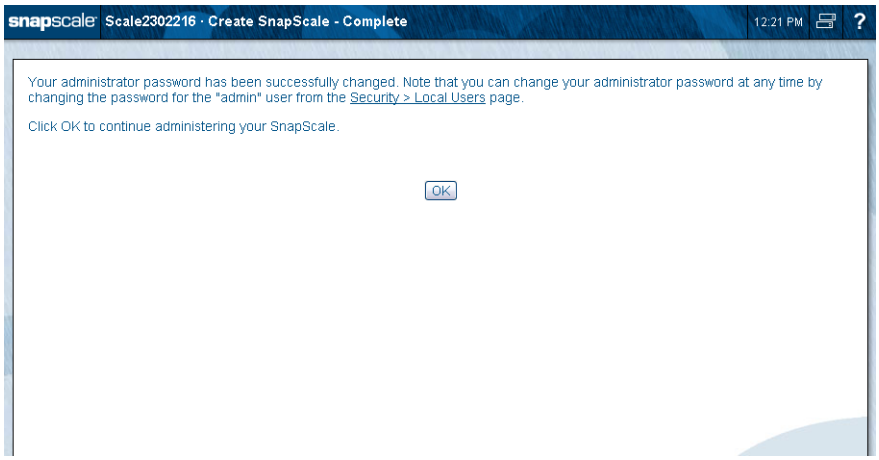
Click **Create New SnapScale** again to create the cluster. A progress bar is displayed as the SnapScale cluster is created.



Once the cluster is created and the system changes the uninitialized node IP addresses from DHCP to the configured static IP address, a completion page is displayed stating that a share was created and suggesting UPS units be enabled. To enhance security, you are asked to change the default administrator password after the cluster has been successfully created:

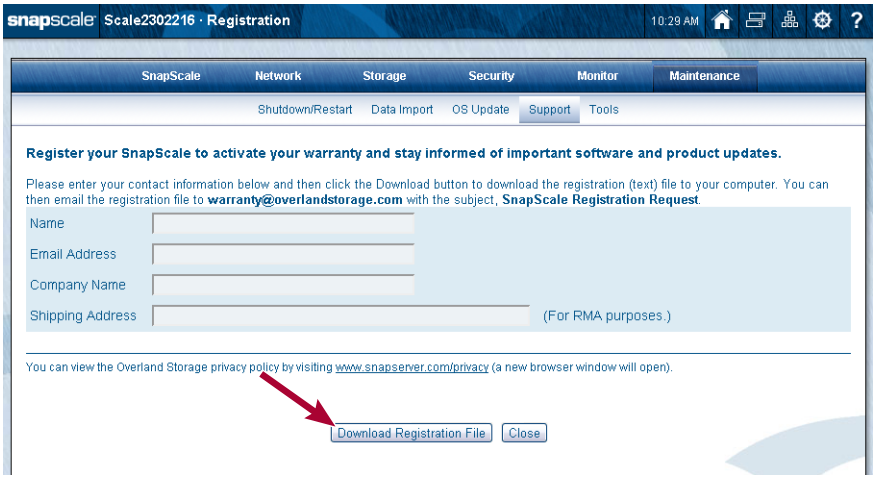


After changing the Administrator's password and clicking **OK**, a success page is shown:



Click **OK** to continue. The Login page is shown. Log in using the new password.

After changing the password and logging back in, the Registration page is displayed to facilitate activating your warranty:



Complete the registration fields and then click **Download Registration File**. Email that file (SnapScaleRegistration.csv) to Overland Storage Service (warranty@overlandstorage.com) with the subject line "SnapScale Registration Request" to initiate your warranty coverage. (See Chapter 7, "Registering Your Cluster.")

Click **Close** to complete the Registration process. You will receive a confirmation email to confirm and complete the registration.

When you close that page, the **Administration** page is displayed:

It is recommended that you configure your DNS in your network so clients can resolve the cluster using round-robin name resolution:

- Add a host record for the cluster management name (<clustername>–mgt) to resolve to the Management IP address.
- Add multiple host records for the cluster name resolving to each of the node IP addresses. The DNS resolves lookups for the cluster name via round-robin.

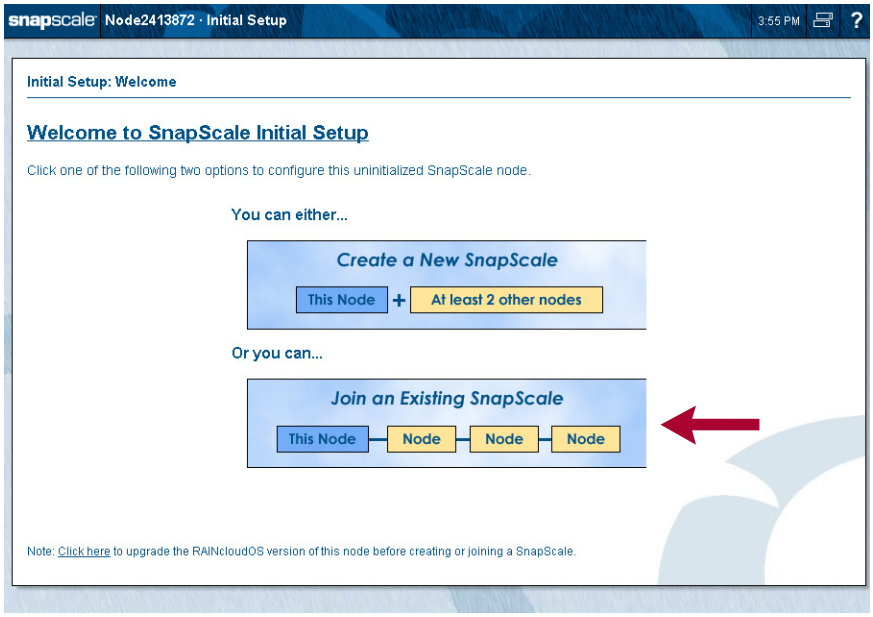
Join an Existing SnapScale Cluster (via Wizard)

IMPORTANT: While the Initial Setup Wizard can be used to add one or more new nodes to an existing cluster, it is recommended that you log into the existing cluster's Web Management Interface and add the nodes using the Add Nodes function (**Storage > Nodes > Add Nodes**). Refer to Chapter 4, "Adding Nodes," for more information.

At any time, one or more new nodes can be added to the cluster to expand the storage pool.

NOTE: To create new peer sets to expand cluster storage, it is recommended that the number of new nodes you add is equal to the Data Replication Count being used (2x or 3x) and they all be added at the same time.

When you log into any of the new, uninitialized nodes, the Initial Setup Wizard launches displaying the Welcome page and its two options. To add this and other nodes to an existing SnapScale cluster, click the **Join an Existing SnapScale** button.



The Initial Setup Wizard then redirects you to the **Add Nodes** page in the Web Management Interface where this node (and all other discovered/new nodes) can be easily added to the cluster. (See Chapter 4, "Adding Nodes," for more information.) You are then directed to select the nodes to add, set the static IP addresses, and confirm the settings.

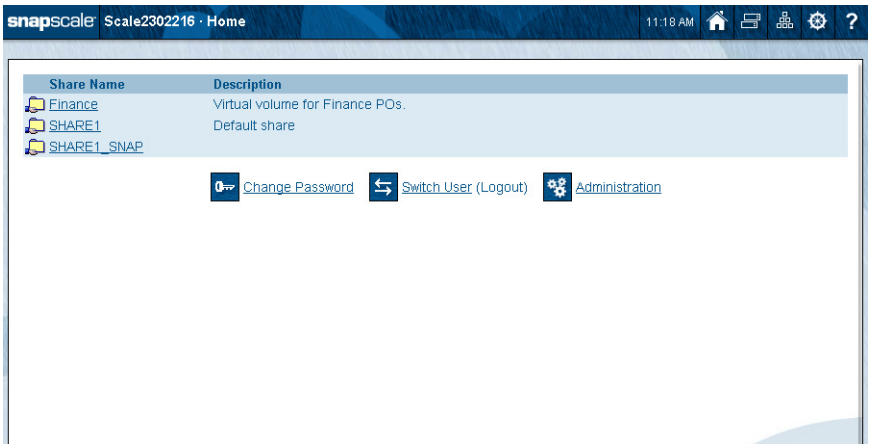
NOTE: If no existing SnapScale cluster is detected, a warning is displayed. Verify that the node is on the same Storage network as the other nodes in the cluster, then click Re-Detect SnapScale.

Web Management Interface

SnapScale nodes use a web-based graphical user interface (GUI), called the Web Management Interface, to administer and monitor the cluster. It supports most common web browsers. JavaScript must be enabled in the browser for it to work.

When connecting to the cluster with a web browser, the Web Home page (see Chapter 8, "Web Home") of the Web Management Interface is displayed. This page shows any shares at the top, the three primary options below the shares list, and has special navigation buttons displayed on the right side of the title bar (see the next table).

NOTE: If you have not gone through the initial setup or authentication is required, you may be prompted to log in when you first access the Web Management Interface.



The **Web Home** page displays the following icons and options:

Icons & Options	Description
Change Password 	Click this icon to access the password change page. Passwords are case sensitive. Use up to 15 alphanumeric characters.
Switch User 	Click this icon to log out and open the login dialog box to log in as a different user.
Administration 	Click this icon to administer the node. If you are not yet logged in, you are prompted to do so.
Navigation Buttons	The following Navigation buttons are present in the upper right on every Web Management Interface page:
	Home – Click this icon to switch between the Web Home page and the Admin Home page. If you have not yet logged in to the Admin Home page, only the Web Home page is available.
	Snap Finder – Click this icon to view a list of all SnapServers, SnapScale clusters, and Uninitialized nodes on your network, and to specify a list of remote servers that can access these servers, clusters, and nodes on other subnets. You can access these servers, clusters, and nodes by clicking the listed name or IP address.
	SnapExtensions – Click this to view the SnapExtensions page, where you can acquire licenses for and configure third-party applications.

Icons & Options	Description
	Site Map – Click this icon to view a Site Map of the available options in the Web Management Interface, where you can navigate directly to all the major utility pages. The current page is shown in orange text.
	Help – Click this icon to access the online help for the UI page you are viewing.
UI Appearance	Click the **Mgmt. Interface Settings** link in the Site Map to choose a background for the Web Management Interface. You can select either a solid-colored background or a textured-graphic background.

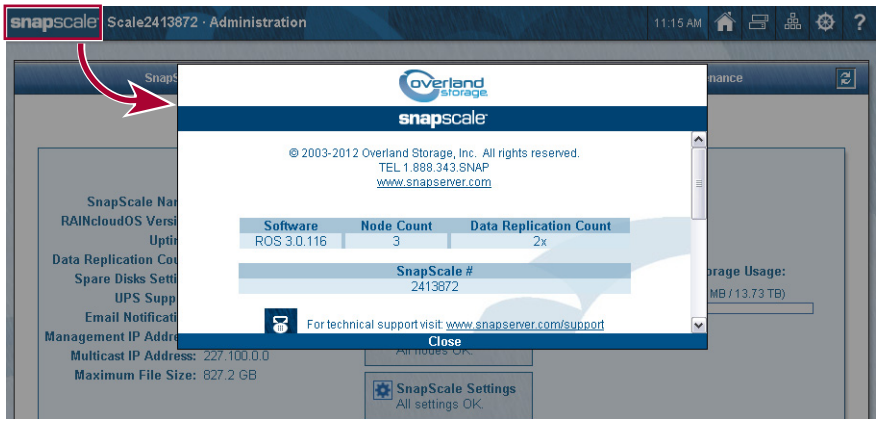
For more information, see "Home Pages – Web/Admin."

When logged in to the Administration page, details about the cluster's health are shown:

The same icons are available at the top of the page plus the SnapExtensions icon ( ) and a refresh icon ( ) for auto-refresh pages located on the tab bar. For more information, see Chapter 8, "Admin Home."

Hardware Information

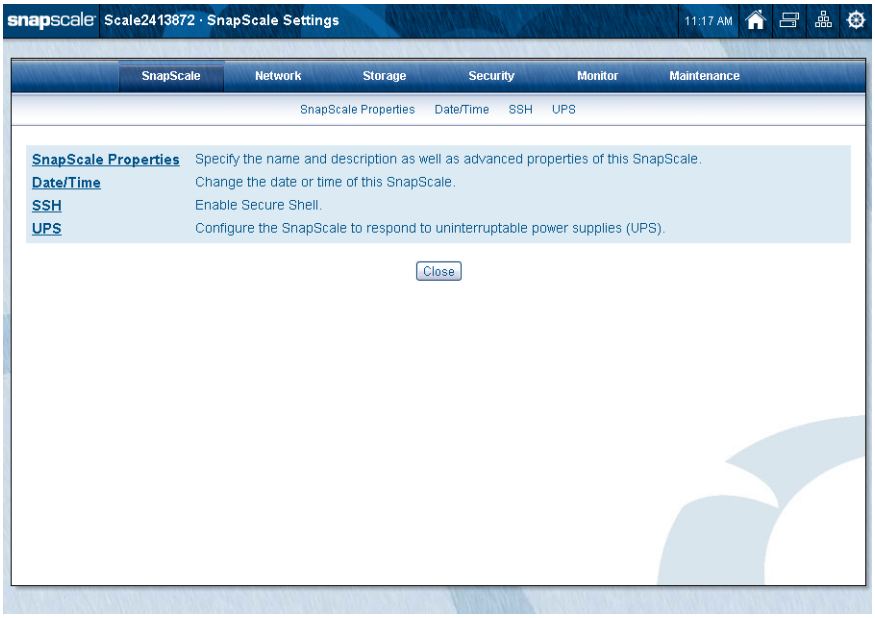
From the Web Management Interface, click the SnapScale logo in the upper left corner to display the pertinent hardware (and software) information and contact links:



Scroll down to view additional contact information. Click outside the box to dismiss.

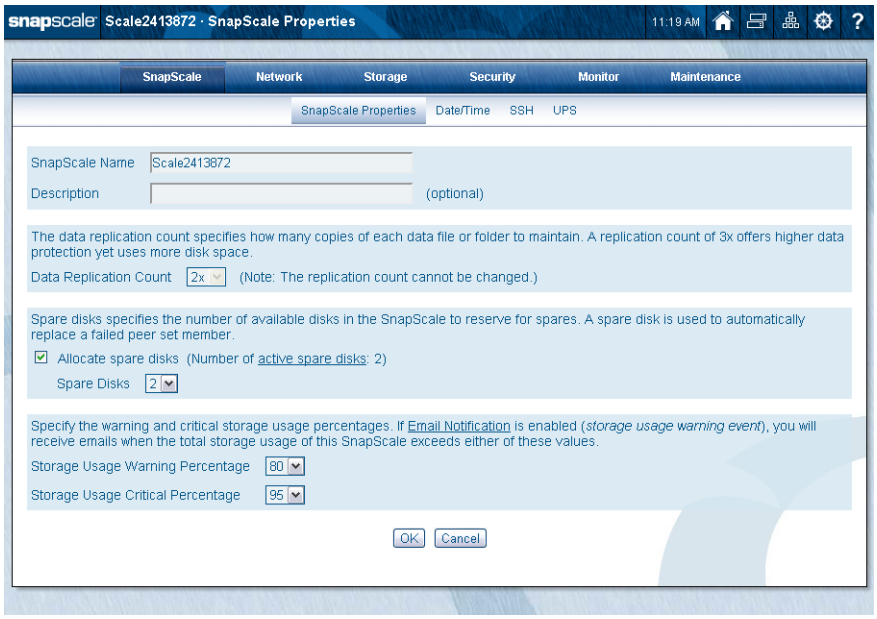
SnapScale Options

The four options for general cluster settings can be found under the SnapScale tab. They can also be accessed using the site map link ( ).



SnapScale Properties

The SnapScale Properties can be set on this page:



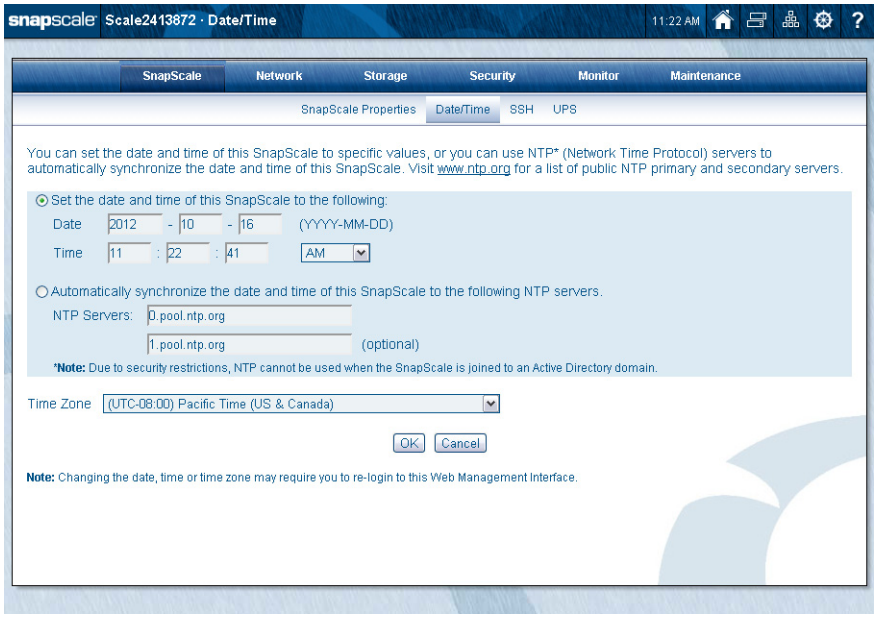
This table details the options on the SnapScale Properties page:

Option	Description
SnapScale Name and Description	Either accept the default cluster name or enter an alphanumeric name up to 15 characters in length. Network clients can use this name along with DNS-based round-robin name resolution to connect to the cluster. The default name is "Scale*nnnnnnn*" (where *nnnnnnn* is the appliance number of the node used to create the cluster).
Description	This optional field provides a place to define the cluster in the overall scheme of your network and better identify the cluster on a LAN.
Data Replication Count	The data replication count establishes the level of data redundancy in the cluster. The setting specifies how many copies of each data file or folder to maintain. A count of 3x offers higher data protection but uses more disk space. Once the cluster is created, the count can only be decreased from 3x to 2x. It cannot be increased from 2x to 3x.
Spare Disks	Check the box and select the number of spare disks you want to reserve. A spare disk is used to automatically replace a failed Peer Set member. If there are unused drives remaining after allocating the number of spares requested, they are used for other peer sets. If there is an insufficient number of drives left to create a final peer set, the drives are configured as additional spares.
Storage Utilization	Use the two drop-down lists to select the percentage of storage used before a warning or critical notice is sent. If not done already, use the link in this section to set up email notification. See "Email Notification" in Chapter 7, "Maintenance."

Date/Time

You can set the cluster date and time manually or have it set automatically via NTP or Windows Active Directory domain membership. Nodes automatically synchronize time with one another.

An ISO 8601 time stamp is applied when recording node activity in the Event Log (Monitor tab), when creating or modifying files, and when scheduling snapshot operations. Use this page to configure date and time settings:



CAUTION: If the current date and time are reset to an earlier date and time, the change does not automatically propagate to any scheduled events you have already set up for snapshot or Snap EDR operations. These operations continue to run based on the previous date and time setting. To synchronize these operations with the new date and time settings, you must reschedule each operation.

Configure Date and Time Settings Manually

1. Click the **Set the date and time** button.
2. Edit date and time settings as described in the following table.
3. From the drop-down list, select the **Time Zone** for the cluster.
4. Click **OK** when finished.

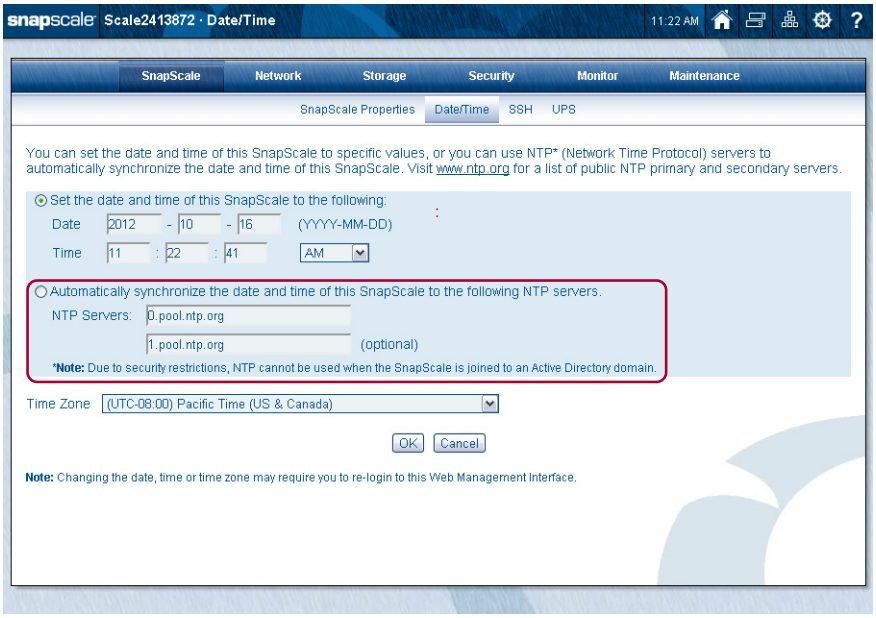
Option	Description
Date	Enter the current date in the format indicated.
Time	Enter the current time in the format indicated.
Time Zone	Select the time zone that you want to use for this node.

Once you join a Windows domain, the settings are automatically adjusted to synchronize with the domain settings.

NOTE: RAINcloudOS automatically adjusts for Daylight Saving Time, depending on your time zone.

Configure Date and Time Settings for Automatic Synchronization

If the cluster is not joined to a Windows Active Directory domain, you can use the automatic synchronization option to configure the cluster to set date and time automatically via Network Time Protocol (NTP).



1. Click the **Automatically Synchronize** button.

   Default NTP servers are displayed. To accept them, skip to Step 2. Otherwise:

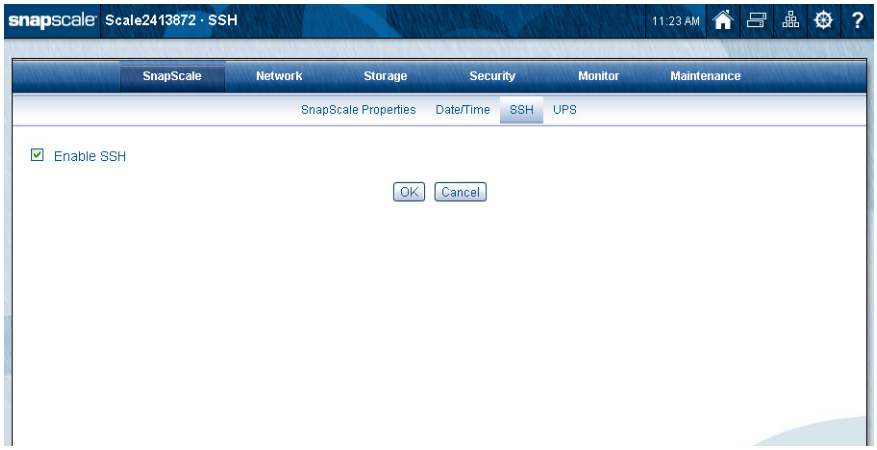
   - Enter the **address** for the primary NTP server.
   - Optionally, enter a **second IP address** for a different NTP server as backup.

2. From the drop-down list, select the **Time Zone** for the cluster.
3. Click **OK** when finished.

   In some cases, this change may require you to log back in to the Web Management Interface.

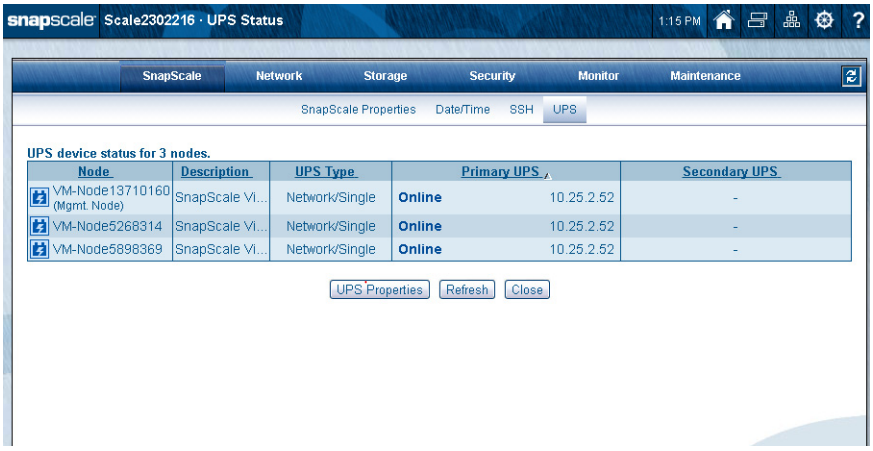
SSH

This page provides the ability to enable/disable Secure Shell (SSH) on the cluster for security purposes. By default, it is enabled.



UPS

SnapScale supports automatic shutdown when receiving a low-power warning from an APC uninterruptible power supply (UPS). Use SnapScale > UPS to manage this feature:



NOTE: If UPS devices have not be configured, the first time you select this option, you are automatically shown the UPS Properties page. See "UPS Properties."

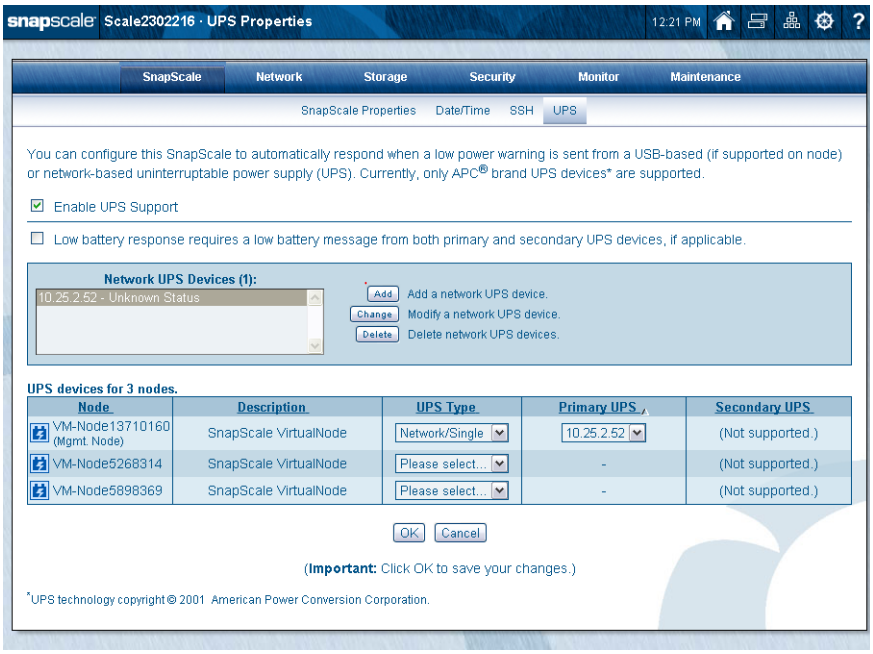
An APC Smart-UPS® series device allows the SnapScale cluster to shut down gracefully in the event of an unexpected power interruption. You can configure the cluster to automatically shut down when a low power warning is sent from one or more APC network-enabled or USB-based UPS devices (some serial-only APC UPS devices are also supported by using the IOGear GUC232A USB to Serial Adapter Cable). To do this, you must enable UPS support on the cluster, as described in this section, to listen to the IP address of one or more APC UPS devices, and you must supply the proper authentication phrase configured on the UPS devices.

NOTE: Select a UPS capable of providing power to a SnapScale node for at least ten minutes. In addition, in order to allow the cluster sufficient time to shut down cleanly, the UPS must be configured to provide power for at least five minutes after entering a low battery condition.

UPS Properties

To manage the network UPS devices, click the **UPS Properties** button:

NOTE: If UPS devices have not been configured, the first time you select that option, you are automatically shown the UPS Properties page.



UPS Properties page options:

Option	Description
Enable UPS Support	Check the Enable UPS Support box to enable support.
Low battery response message	Check the box to initiate a graceful shutdown only when both the primary and secondary UPS devices for a node send a low battery message.
Network UPS Devices (#)	This field shows a list of UPS devices that are used with the cluster. Use the Add, Change, and Delete buttons to manage the list.
UPS Type (Third column in Node table)	Use the drop-down list in the third column of the Node table to select which UPS device is used: • USB – Select this option to use a direct-attached (USB) device. • Network/Single – Use this option to select a network UPS device. • Network/Dual – Use this option to activate the option of a secondary network UPS device.
Primary UPS (Fourth column in Node table)	Selecting the Network/Single option under UPS Type causes a drop-down list to be displayed in this column. Select the primary UPS to associate with the node from the list (which is based on the Network UPS Devices table).
Secondary UPS (Fifth column in Node table)	If supported, selecting the Network/Dual option (under UPS Type) causes a drop-down list to be displayed in this column. Select the secondary UPS to associate with the node from the list (which is based on the Network UPS Devices table).

Procedure to Configure UPS Protection

1. Check **Enable UPS Support**.
2. If desired, check the **low battery message** option.
   This requires both Primary and Secondary UPS devices to have low batteries before the notice is sent to initiate a graceful shutdown.
3. If necessary, **add** network UPS devices.
   See "Add Network UPS Device."
4. Select or change the following from the drop-down lists in the **UPS device table**:
   - UPS Type
   - Primary UPS
   - Secondary UPS
5. Click **OK** to finish.

Add Network UPS Device

SnapScale nodes need to be added to the Network UPS Devices table on the SnapScale > UPS page.

1. Click the **Add** button to the right of the table.
2. At the Add Network UPS Device page, enter:
   - IP Address of the device
   - APC User Name (for authentication)
   - APC Authentication Phrase
3. Click **Add**.

You are returned to the UPS page and the device is shown in the Network UPS Devices table. The table title UPS count is increased by one. Repeat the process for additional devices.

Change Network UPS Device

To change the settings of a network UPS device:

1. Select a **device** in the Network UPS Devices field to change.
2. Click **Change**.
3. Edit any of the **three options** for the device.
4. Click **Change** again.

Any changes you make are applied to all nodes that are currently using this device.

Delete Network UPS Device

To delete a network UPS device:

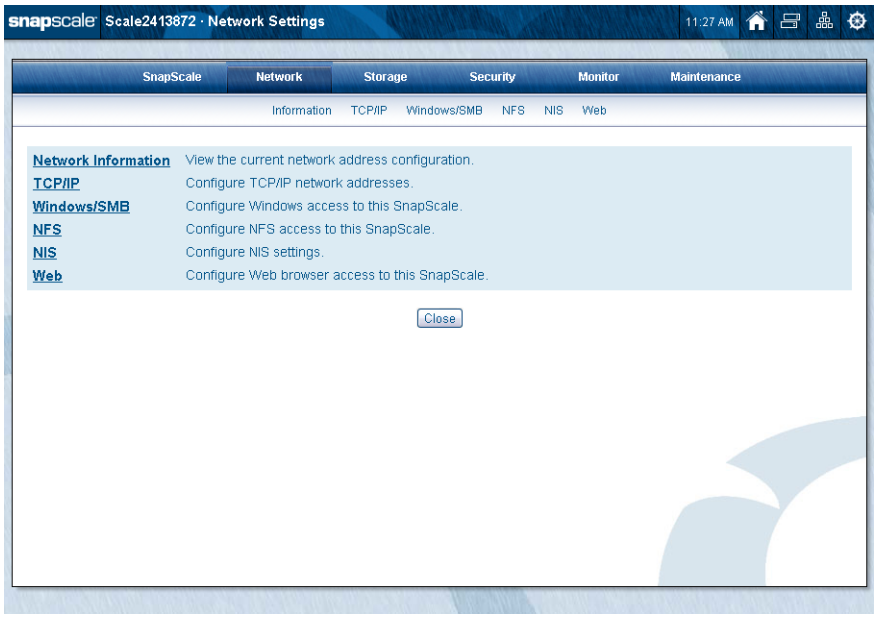
1. If the device is still connected to **any nodes**, deselect the device from the nodes.
2. Highlight the **device** in the Network UPS Devices field.
3. Click **Delete**.

The device is deleted from the list.

Network Access

This chapter addresses the options for configuring TCP/IP addressing, network bonding, and file access protocols. Network bonding options allow you to configure the SnapScale's Client network for load balancing/failover, Switch Trunking, and Link Aggregation (802.3ad). Network file protocols control how network clients can access the cluster. Access to the cluster's storage space is provided via Windows (CIFS/SMB), UNIX (NFS), Mac (SMB), and web (HTTP/HTTPS).

NOTE: Uninitialized nodes are configured to use DHCP until they are added to a cluster when they switch to the static IP addresses used by the cluster.



Topics in Network Access:

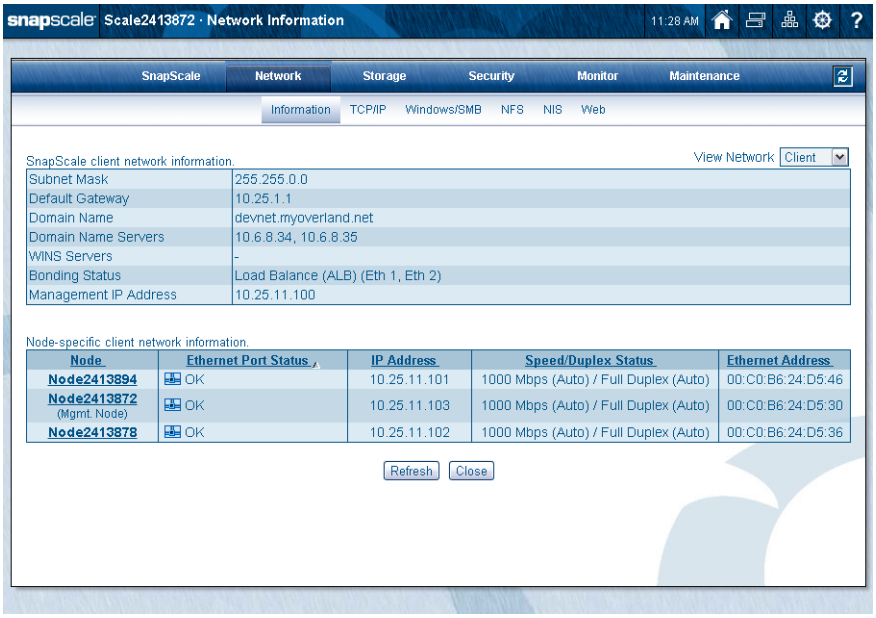
IMPORTANT: The default settings enable access to the SnapScale cluster via all protocols supported by the cluster. As a security measure, disable any protocols not in use. For example, if NFS access to the SnapScale is not needed, disable the protocol in the Web Management Interface under the Network tab.

View Network Information

The **Network > Information** page displays either the SnapScale's Client or Storage network settings, and identifies the node currently serving as the management node. The information is broken into two parts displaying the common and node-specific network information. Use the drop-down menu on the upper right side to select either the Client or Storage network details.

Client Network Information

This page shows the information on the public Client network:



Field definitions are given in the following table:

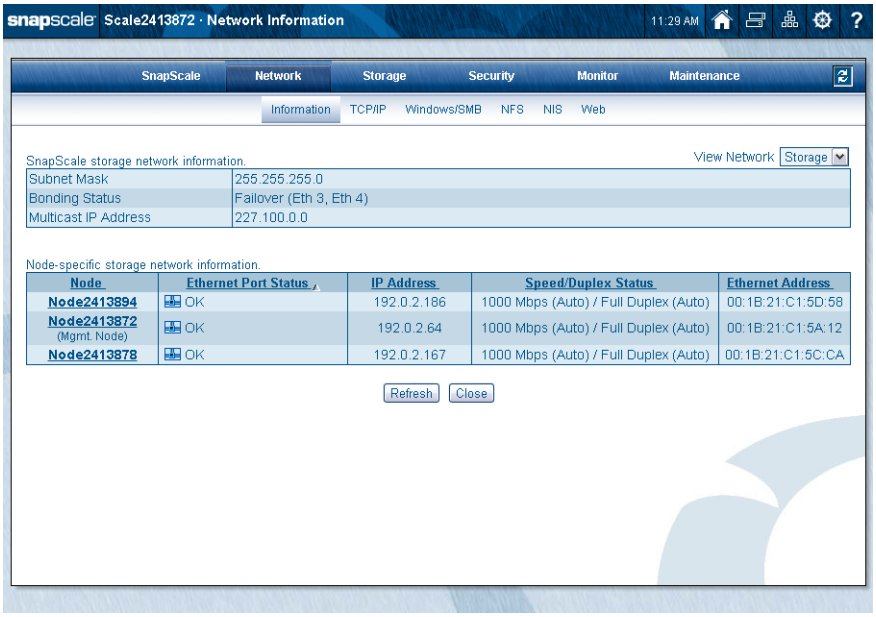
SnapScale Client Network Information	
Subnet Mask	Combines with the IP address to identify the subnet on which the cluster's Client network interfaces are located.
Default Gateway	The network address of the gateway is the hardware or software that bridges the gap between two otherwise unroutable networks. It allows data to be transferred among computers that are on different subnets.

SnapScale Client Network Information	
Domain Name	The ASCII name that identifies the DNS domain name that is added to the cluster name to form the fully-qualified host name of the cluster. Additional space-separated domain names are added to the cluster's domain search suffix list.
Domain Name Servers	The IP address of up to three servers that maintain a mapping of all host names and IP addresses for translating domain names into IP addresses.
WINS Servers	The IP address of up to four Windows Internet Naming Service (WINS) servers which locate network resources in a TCP/IP-based Windows network by automatically configuring and maintaining name and IP address mapping tables.
Bonding Status	Shows Load Balance (ALB), Failover, or Switch Trunking and Link Aggregation (802.3ad). Displays ports assigned to the bond.
Management IP Address	The IP address configured to access the SnapScale cluster through the Web Management Interface.

Node-specific Client Network Information	
Node	The name of the specific node. The node designated as the Management node is so noted.
Ethernet Port Status	• OK – Both ports are connected. • No link – One or both ports are not connected. If one port is not connected, the icon is yellow and the message indicates which port it is. If both ports are not connected, the icon is red and both ports have an error message. • Failed – Port has failed.
IP Address	The unique 32-bit value that identifies the node on a network subnet. This is automatically assigned to each node from the pool of IP addresses configured on the cluster.
Speed/Duplex Status	Speed: 1000 Mbps. Duplex Status: Full-duplex: two-way data flow simultaneously.
Ethernet Address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet port (xx:xx:xx:xx:xx:xx).

Storage Network Information

This page shows the information on the private Storage network:



Field definitions are given in the following table:

SnapScale Storage Network Information	
Subnet Mask	Combines with the IP address to identify the subnet on which the cluster's Storage network interfaces are located.
Bonding Status	Storage network is set to only use Failover. Displays ports assigned to the bond.
Multicast IP Address	Multicast address used for inter-node cluster messaging.

Node-specific Storage Network Information	
Node	The name of the specific node. The node designated as the Management node is so noted.
Ethernet Port Status	• OK – Both ports are connected. • No link – One or both ports are not connected. If one port is not connected, the icon is yellow and the message indicates which port it is. If both ports are not connected, the icon is red and both ports have an error message. • Failed – Port has failed.
IP Address	The unique 32-bit value that identifies the node on a network subnet. This is automatically assigned to each node by the cluster.
Speed/Duplex Status	Speed: 1000 Mbps. Duplex Status: Full-duplex: two-way data flow simultaneously.
Ethernet Address	The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet port (xx:xx:xx:xx:xx:xx).

TCP/IP Networking

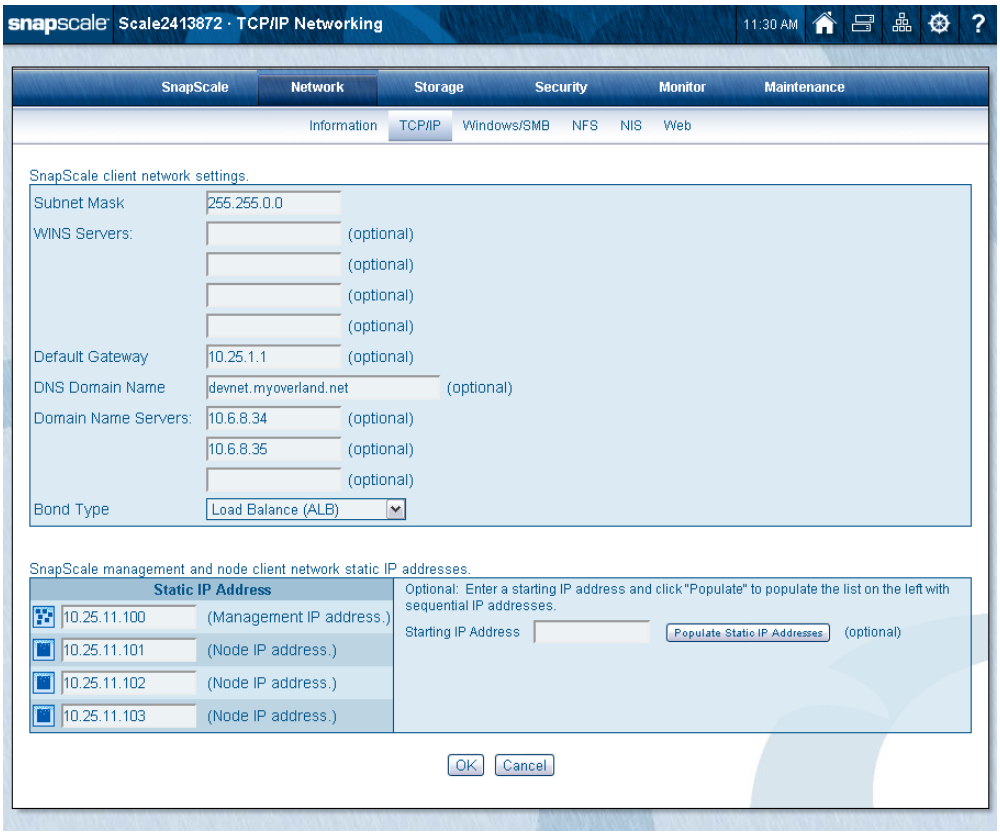
SnapScale nodes ship with either four 1GbE or 10GbE ports at the rear for network connections. The Storage network ports are always bonded using Failover mode. The Client network ports are bonded by default using Load Balance (ALB), and can be changed after the cluster is created to one of the following bonding modes:

- Load Balance (ALB)
- Failover
- Switch Trunking
- Link Aggregation (802.3ad)

See Chapter 1, "SnapScale Client and Storage Networks."

The TCP/IP Networking page provides configuration of the common cluster network settings, the static Management IP address, and the pool of static IP addresses to automatically assign to cluster nodes.

NOTE: If the Client network runs a DHCP server, be sure the static IP addresses assigned to the nodes and management IP are excluded from DHCP assignment.



The following table describes the configuration options found on the TCP/IP page:

Column	Description
Subnet Mask	Combines with the IP address to identify the subnet on which the cluster's Client network interfaces are located.

Column	Description
WINS Servers	The IP address of up to four Windows Internet Naming Service (WINS) servers which locate network resources in a TCP/IP-based Windows network by automatically configuring and maintaining name and IP address mapping tables.
Default Gateway	The network address of the gateway is the hardware or software that bridges the gap between two otherwise unroutable networks. It allows data to be transferred among computers that are on different subnets.
DNS Domain Name	The ASCII name that identifies the DNS domain name that is added to the cluster name to form the fully-qualified host name of the cluster, and also serves as the primary DNS search suffix. Additional space-separated domain names can be specified to extend the domain search suffix list.
Domain Name Servers	The IP address of up to three servers that maintain a mapping of all host names and IP addresses for translating domain names into IP addresses.
Bond Type	Use the drop-down list to select one of the four bonding modes for the Client network interface on all nodes: • Load Balance (ALB) – An intelligent software adaptive agent repeatedly analyzes the traffic flow from the node and distributes the packets based on destination addresses, evenly distributing network traffic for optimal network performance. All ports in the same ALB configuration on a cluster node need to be connected to the same switch. • Failover – This mode uses one Ethernet port (by default, *Ethernet 1* for 1GbE or *Ethernet 3* for 10GbE) as the primary network interface and one port held in reserve as the backup interface. Redundant network interfaces ensure that an active port is available at all times. If the primary port fails due to a hardware or cable problem, the second port assumes its network identity. The ports on a node should be connected to different switches (though this is not required). The Storage network is always configured this way. NOTE: Failover mode provides switch fault tolerance, as long as ports are connected to different switches. • Switch Trunking – This mode groups multiple physical Ethernet links to create one logical interface. Provides high fault tolerance and fast performance between switches, routers, and servers. • Link Aggregation (802.3ad) – This method of combining or aggregating multiple network connections in parallel is used to increase throughput beyond what a single connection could handle. It also provides a level of redundancy in case one of the links fails. It uses Link Aggregation Control Protocol (LACP) to autonegotiate trunk settings.
Static IP Address	This table shows the SnapScale Management IP address and the pool of Client network static IP addresses to be automatically assigned by the cluster to the different nodes. To change or populate the list with a contiguous range of IP addresses, in the area to the right, enter a starting IP address and click **Populate Static IP Addresses**.

Guidelines in TCP/IP Configuration

Consider the following guidelines when connecting a SnapScale cluster to the network.

Configure the DNS for Name Resolution and Round-Robin Load Distribution

To evenly distribute client access loads to the cluster nodes, add a DNS A record for the cluster name for each IP in the node IP address pool. The DNS server then rotates through the node IP addresses in a round-robin basis when serving name resolution requests for the cluster name.

Do not add an A record for the cluster name pointing to the Management IP address. If desired, or if using Snap EDR, add an A record for the cluster name followed by "-MGT" for the Management IP address. For example, if the cluster name is Scale1234567, create an A record for hostname "Scale1234567-MGT."

Make Sure the Switch is Set to Autonegotiate Speed/Duplex Settings

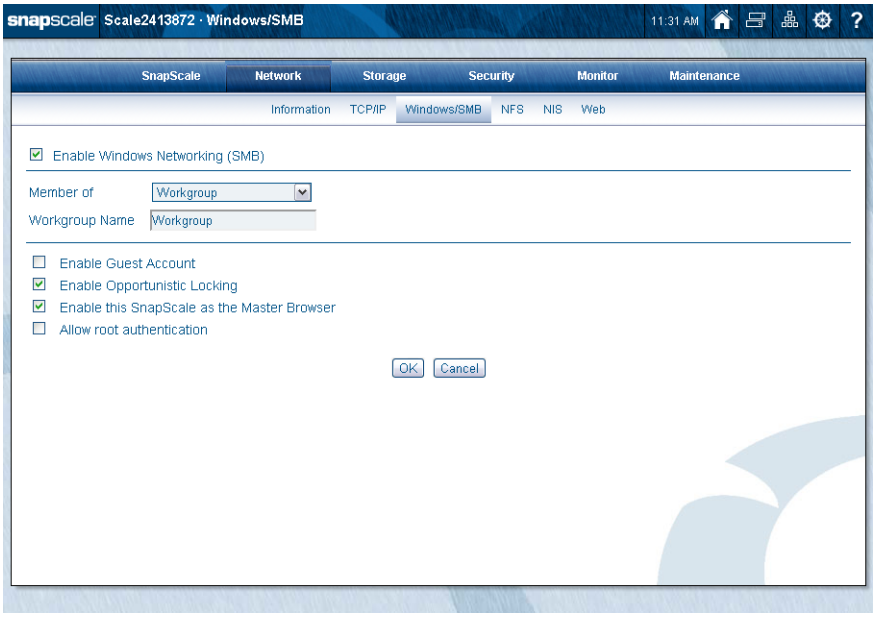
All Ethernet ports on the cluster nodes are set to autonegotiate speed and duplex settings with the Ethernet switch. The switch to which the SnapScale is connected *must* be set to autonegotiate; otherwise, network throughput or connectivity to the node may be seriously impacted.

Configure the Switch for Load Balancing

If you select either Switch Trunking or Link Aggregation network bonding configuration for the Client network bond, be sure the switch is configured correctly for that bonding method **after** configuring the bond on the node. No switch configuration is required for Adaptive Load Balancing (ALB).

Windows/SMB Networking

Windows/SMB and security settings are configured on the **Network > Windows/SMB** page of the Web Management Interface. You can configure the cluster as a member of either a **Workgroup** or an **Active Directory Domain**, as shown below:



If you run Windows networking in domain mode, you must not configure Date/Time to synchronize with an NTP server.

Support for Windows/SMB Networking

The default settings make the SnapScale available to SMB clients in the workgroup named *Workgroup*. Opportunistic locking is enabled, as is participation in master browser elections.

Consider the following when configuring access for your Windows networking clients:

Support for Microsoft Name Resolution Servers

The SnapScale supports NetBIOS, WINS, and DNS name resolution services. However, when you use a domain name server with a Windows Active Directory Service (ADS) server, make sure the forward and reverse name lookup are correctly set up. ADS can use a UNIX BIND server for DNS as well.

ShareName$ Support

RAINcloudOS supports appending the dollar-sign character ($) to the name of a share in order to hide the share from SMB clients accessing the SnapScale.

NOTE: As with Windows servers, shares ending in '$' are not truly hidden, but rather are filtered out by the Windows client. As a result, some clients and protocols can still see these shares.

To completely hide shares from visibility from any protocols, the **Security > Shares** page gives you access to a separate and distinct hidden share option that hides a share from SMB and HTTP/HTTPS clients. However, shares are not hidden from NFS clients, which cannot connect to shares that are not visible. To hide shares from NFS clients, consider disabling NFS access on hidden shares.

For new shares, select **Create Share** and click the **Advanced Share Properties** button to access the Hidden share option. For existing shares, select the share, click **Properties**, and click **Advanced Share Properties** to access the Hidden share option.

Support for Windows Network Authentication

This section summarizes important facts regarding the RAINcloudOS implementation of Windows network authentication.

NOTE: When a SnapScale cluster joins a domain, it does so under its cluster name (Scale*nnnnnnn*). When a domain user is authenticated on a node, the cluster name is used. As such, a user can use any node of the cluster to be authenticated and log on.

Windows Networking Options

Windows environments operate in either workgroup mode, where each SnapScale cluster contains a list of local users it authenticates on its own, or ADS domain mode, where domain controllers centrally authenticate users for all domain members.

Option	Description
Workgroup	In a workgroup environment, users and groups are stored and managed separately on each server or cluster in the workgroup.
Active Directory Service (ADS)	When operating in a Windows ADS domain environment, the SnapScale is a member of the domain and the domain controller is the repository of all account information. Client machines are also members of the domain and users log into the domain through their Windows-based client machines. ADS domains resolve user authentication and group membership through the domain controller. Once joined to a Windows ADS domain, the SnapScale can authenticate SMB users against the domain and can configure share access for domain users. Thus, you must use the domain controller to make modifications to user or group accounts. Changes you make on the domain controller appear automatically on the SnapScale. NOTE: Windows 2000 domain controllers must run SP2 or later.

Kerberos Authentication

Kerberos is a secure method for authenticating a request for a service in a network. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a service from a server or cluster. The user credentials are always encrypted before they are transmitted over the network.

The SnapScale supports the Microsoft Windows implementation of Kerberos. In Windows ADS, the domain controller is also the directory server, the Kerberos Key Distribution Center (KDC), and the origin of group policies that are applied to the domain.

NOTE: Kerberos requires the cluster's time to be closely synchronized to the domain controller's time. This means that (1) the cluster automatically synchronizes its time to the domain controller's and (2) NTP cannot be enabled when joined to an ADS domain.

Interoperability with Active Directory Authentication

The SnapScale supports the Microsoft Windows 2000/2003/2008 family of servers that run in ADS mode. any SnapScale can join Active Directory Service domains as a member server. References to the SnapScale's shares can be added to organizational units (OU) as shared folder objects.

NOTE: Windows 2000 domain controllers must run SP2 or later.

Guest Account Access to the SnapScale

The **Network > Windows/SMB** page in the Web Management Interface contains an option that allows unknown users to access the SnapScale using the guest account.

Connect from a Windows Client

Windows clients can connect to the SnapScale using either the cluster name or any IP address in the node IP address pool. However, if possible, clients should use the cluster name to benefit from round-robin DNS resolution (see "Configure the DNS for Name Resolution and Round-Robin Load Distribution").

To navigate to the cluster using Windows Explorer, use one of these procedures:

- For Microsoft Windows Vista, 2008, and 7 clients, navigate to **Network >** *server_name*.
- For Microsoft Windows XP, 2000, or 2003 clients, navigate to **My Network Places >** *workgroup_name* > *server_name*.

Connect a Mac OS X Client Using SMB

Mac OS X clients can connect using SMB. Specify the cluster name (or an IP address from the node IP address pool) in the Connect to Server window (from **Finder** press **Cmd + K**, or select **Finder > Go > Connect to Server**) as one of the following:

NOTE: If possible, clients should use the cluster name to benefit from round-robin DNS resolution (see "Configure the DNS for Name Resolution and Round-Robin Load Distribution").

- `smb://cluster_name`
- `smb://node_ip_address`

Tip: *To disconnect from the SnapScale cluster, drag its icon into the Trash.*

You can also browse the clusters in the Finder file window, under the Shared tab.

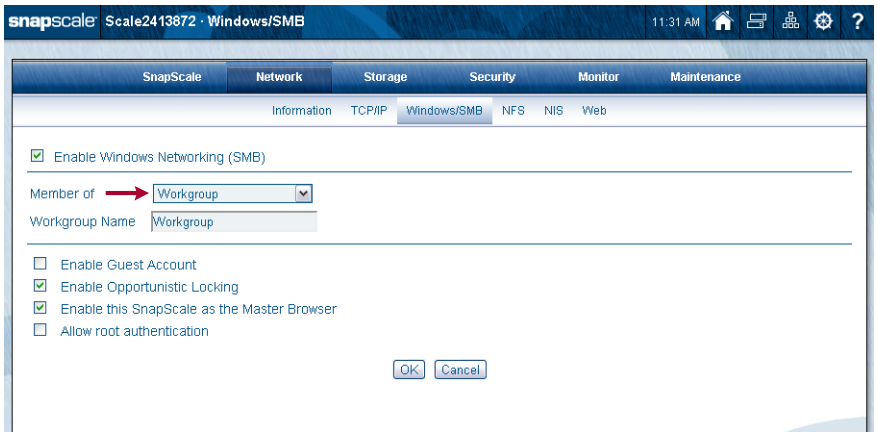
Configure Windows/SMB Networking

Windows SMB and security settings are configured from this page. The cluster can be configured as part of a Workgroup or an Active Directory Domain.

Before performing the configuration procedures provided here, be sure you are familiar with the information provided in "Support for Windows/SMB Networking" and "Support for Windows Network Authentication."

To Join a Workgroup

1. Go to **Network > Windows/SMB**.
2. At the Member list, verify that the default **Workgroup** is selected.



3. Edit the **fields** shown in the following table:

Option	Settings
Enable Windows SMB	Check the **Enable Windows Networking (SMB)** checkbox to enable SMB. Clear the checkbox to disable SMB.
Member Of	Verify that it is set to **Workgroup**. NOTE: For the Active Directory Domain option, see "To Join an Active Directory Domain."
Workgroup Name	The default settings make the SnapScale available in the workgroup named *Workgroup*. Enter the workgroup name to which the cluster belongs.
Enable Guest Account	Check the **Enable Guest Account** checkbox to allow unknown users or users explicitly logging in as "guest" to access the SnapScale using the guest account. Clear the option to disable this feature.
Enable Opportunistic Locking	Enabled by default. Opportunistic locking can help performance if the current user has exclusive access to a file. Clear the checkbox to disable opportunistic locking.
Allow root authentication	Check the **Allow root authentication** checkbox to allow root login to the cluster. NOTE: The root password is synchronized with the cluster's admin password.

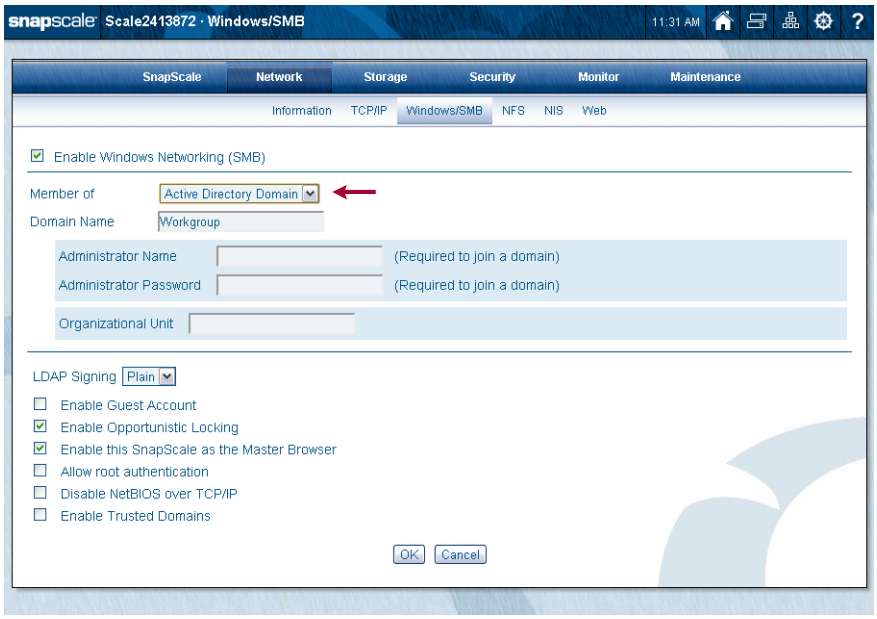
4. Click **OK** to update Windows network settings immediately.

To Join an Active Directory Domain

When the cluster joins a domain, it does so as a single unit under the cluster name, and all nodes operate equally under the cluster name to authenticate against the domain. This provides multipoint access to the domain through each node.

1. Go to **Network > Windows/SMB**.

2. From the drop-down Member list, select **Active Directory Domain** to view the configuration page.



NOTE: You cannot select Active Directory Domain if NTP is enabled.

3. Edit the **fields** shown in the following table:

Option	Description
Enable Windows SMB	Check the **Enable Windows Networking (SMB)** checkbox to enable SMB. Clear the checkbox to disable SMB.
Member Of	Verify it shows *Active Directory Domain.*
Domain Name	The default settings make the SnapScale available in the workgroup named *Workgroup*. Enter the domain name to which the cluster belongs. NOTE: Windows 2000 domain controllers must run SP2 or later.
Administrator Name and Password	If joining a domain, enter the user name and password of a user with domain join privileges (typically an administrative user).
Organizational Unit	To create a machine account at a different location than the default, enter a name in the Organizational Unit field. By default, this field is blank, signaling the domain controller to use a default defined within the controller. NOTE: Sub-organizational units can be specified using Full Distinguished Name LDAP syntax or a simple path ([organizational_unit]/[sub-unit1]/[sub-unit1a])
LDAP Signing	Set ADS domain LDAP signing to Plain (no signing), Sign, or Seal, as appropriate for your domain. Default setting is Plain.
Enable Guest Account	Check the **Enable Guest Account** checkbox to allow unknown users or users explicitly logging in as "guest" to access the SnapScale using the guest account. Clear the option to disable this feature.

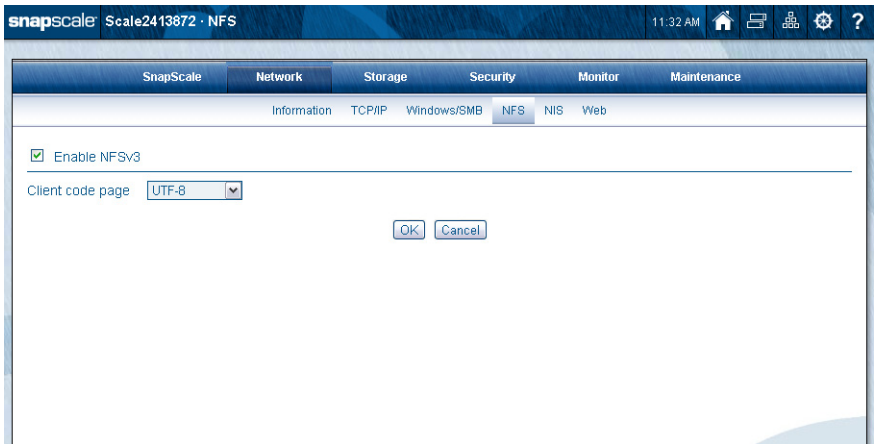
Option	Description
Enable Opportunistic Locking	Enabled by default. Opportunistic locking can help performance if the current user has exclusive access to a file. Clear the checkbox to disable opportunistic locking.
Enable this SnapScale as the Master Browser	Enabled by default. The SnapScale can maintain the master list of all computers belonging to a specific workgroup. (At least one Master Browser must be active per workgroup.) Check the checkbox if you plan to install this cluster in a Windows environment and you want this cluster to be able to serve as the Master Browser for a workgroup. Clear the checkbox to disable this feature.
Allow root authentication	Check the **Allow root authentication** checkbox to allow root login to the cluster. NOTE: The root password is synchronized with the cluster's admin password.
Disable NetBIOS over TCP/IP (Active Dir Domain only)	Some administrators may wish to disable NetBIOS over TCP/IP. Select the checkbox to disable NetBIOS; clear the checkbox to leave NetBIOS enabled. NOTE: If you disable NetBIOS and you are joining a domain, you must enter the domain name as a fully qualified domain name (for example, actdirdomname.companyname.com). A short form such as ActDirDomName does not work.
Enable Trusted Domains (Active Dir Domain only)	SnapScale clusters recognize trust relationships established between the domain to which the SnapScale is joined and other domains in a Windows environment by default. Select the checkbox to toggle this feature. NOTE: SnapScale clusters remember trusted domains. That is, if this feature is disabled and then activated at a later time, the previously downloaded user and group lists, as well as any security permissions assigned to them, is retained.

4. Click **OK** to update Windows network settings immediately.

NFS Access

NFS access to the cluster is configured on the **Network > NFS** page of the Web Management Interface. By default, NFS access is enabled and any NFS client can access the SnapScale via NFSv3 with non-root access.

NOTE: NFSv3 is enabled by default. NFSv2 and NFSv4 are not supported.



NFS client access to shares can be specified by navigating to the **Security > Shares** page and clicking the **NFS Access** link next to the share. You must configure the SnapScale cluster for the code page being used by NFS clients.

Support for NFS

The NFS protocol does not support user-level access control, but rather supports host- and subnet-based access control. On a standard UNIX server, this is configured in an "exports" file. On SnapScale, the exports for each share are configured on the NFS Access page independently of user-based share access for other protocols.

SnapScale supports these versions of the NFS protocol and related services:

Protocol	Version	Source
NFS	3.0	RFC 1094, RFC 1813, RFC 3530
Mount	1.0, 2.0, 3.0	RFC 1094 Appendix A, RFC 1813, RFC 3530
Lockd	1.0, 4.0	RFC 1094, RFC1813, RFC 3530

NFS Share Mounting

A share on a SnapScale is equivalent to an exported filesystem on an NFS server. NFS users can mount SnapScale shares and access content directly, or mount a subdirectory of a share, using the following procedure:

1. To mount an NFS client, enter the following command:

   `mount cluster_name:/share_name  /local_mount`

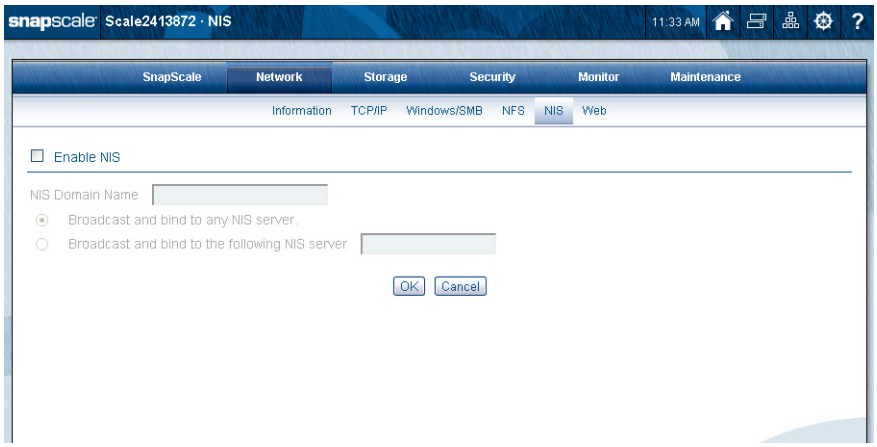
   where **`cluster_name`** is the cluster name (or any address in the node IP address pool), **`share_name`** is the name of the share you want to mount, and **`local_mount`** is the name of the mount target directory.

   NOTE: If possible, clients should use the cluster name to benefit from round-robin DNS resolution (see "Configure the DNS for Name Resolution and Round-Robin Load Distribution"). Syntax can vary depending upon the operating system.

2. Press **Enter** to connect to the specified share on the cluster.

NIS Domain

NIS domains are configured on the **Network > NIS** page of the Web Management Interface.



The SnapScale cluster can join an NIS domain and function as an NIS client. It can then read the users and groups maintained by the NIS domain. Thus, you must use the NIS server to make modifications. Changes you make on the NIS server do not immediately appear on the SnapScale nodes; it may take up to 10 minutes for changes to be replicated.

Guidelines for Configuring NIS

Unless UID/GID assignments are properly handled, NIS users and groups may fail to display properly. For guidelines on integrating compatible SnapScale node UIDs, see "User and Group ID Assignments."

NIS identifies users by UID, not user name, and although it is possible to have duplicate user names, Overland Storage does not support this configuration.

To Join an NIS Domain

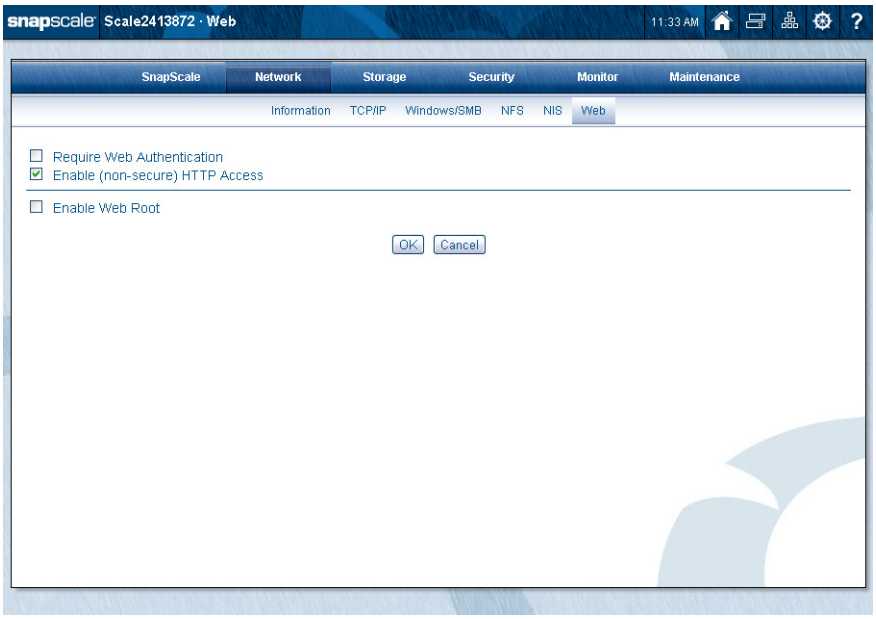
1. Go to **Network > NIS**.
2. Edit the **settings** shown in the following table:

Options	Description
Enable NIS	Check the Enable NIS checkbox to enable NIS, leave the checkbox blank to disable NIS.
NIS Domain Name	Enter the NIS domain name.
NIS Server	To bind to an NIS server, select either: • **Broadcast and Bind to Any NIS server** to bind to any available NIS servers. • **Broadcast and Bind to the following NIS server** enter the NIS server IP address in the field provided.

3. Click **OK** to update the settings immediately.

Web Access

HTTP and HTTPS are used for browser-based access to the cluster via Web View, Web Root, or the Web Management Interface. HTTPS enhances security by encrypting communications between client and cluster, and cannot be disabled. You can, however, disable HTTP access on the **Network > Web** page of the Web Management Interface. Additionally, you can require browser-based clients to authenticate to the cluster.



Configuring HTTP/HTTPS

You can require web authentication, disable HTTP (non-secure) access, and enable the Web Root feature. All HTTP access is made via the root node and the Management IP address.

To Require Web Authentication

Edit the following option and click **OK**.

Option	Description
Require Web Authentication	Check the Require Web Authentication checkbox to require clients to enter a valid user name and password in order to access the cluster via HTTP/HTTPS. Leave the checkbox blank to allow all HTTP/HTTPS clients access to the cluster without authentication. NOTE: This option applies to both Web View and Web Root modes.

To Enable HTTP Access to the SnapScale Cluster

Edit the following option and click **OK**.

Option	Description
Enable (non-secure) HTTP Access	Check the **Enable HTTP Access** checkbox to enable non-secure HTTP access. Leave the checkbox blank to disable access to the cluster via HTTP. NOTE: This option applies to both Web View and Web Root modes.

To Connect via HTTPS or HTTP

1. Enter the **cluster name**, Management IP address, or any IP address from the node IP address pool in a Web browser.

   Web access is case-sensitive. Capitalization must match exactly for a Web user to gain access. To access a specific share directly, Internet users can append the full path to the SnapScale name or URL, as shown in the following examples:

   ```
   https://Node2302216/Share1/my_files
   https://10.10.5.23/Share1/my_files
   ```

2. Press **Enter**.

   The Web View page opens.

Using Web Root to Configure the SnapScale as a Simple Web Server

When you enable the Web Root feature from the **Network > Web** page, you can configure your SnapScale cluster to open automatically to an HTML page of your choice when a user enters the following in the browser field:

`http://[cluster_name]` or `http://[IP address]`

In addition, files and directories underneath the directory you specify as the Web Root can be accessed by reference relative to `http://[cluster_name]` without having to reference a specific share. For example, if the Web Root points to the directory *WebRoot* on share *SHARE1*, the file *SHARE1/WebRoot/photos/slideshow.html* can be accessed from a web browser:

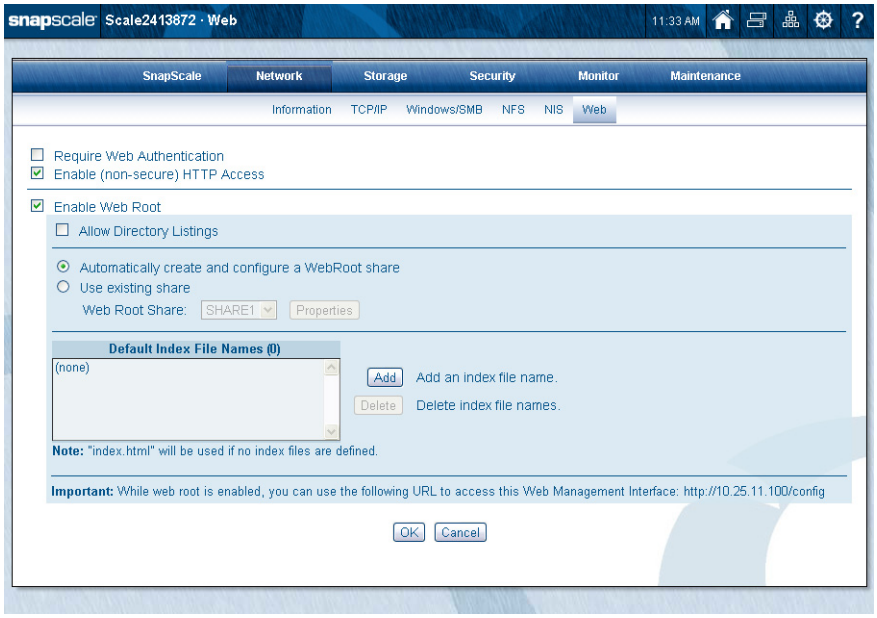
```
http://[cluster_name]/photos/slideshow.html
```

The Web Root can also be configured to support directory browsing independent of Web View (access through shares).

NOTE: SnapScale supports direct read-only web access to files. It is not intended for use as an all-purpose Web Server, as it does not support PERL or Java scripting, animations, streaming video, or anything that would require a special application or service running on the SnapScale cluster.

Configuring Web Root

Check the **Enable Web Root** checkbox to configure the SnapScale to serve the Web Root directory as the top level web access to the SnapScale cluster, and optionally, automatically serve an HTML file inside. When the box is checked, the options described below appear.



1. Complete the following information, then click **OK**.

Option	Description
Allow Directory Listings	If **Allow Directory Listings** is checked and no user-defined index pages are configured or present, the browser opens to a page allowing browsing of all directories underneath the Web Root. NOTE: Checking or unchecking this option only affects directory browsing in Web Root. It does not affect access to Web View directory browsing.

Option	Description
Create and configure a Web Root share	Select one of the following: • **Automatically create and configure a Web Root share**: A share named "WebRoot" is automatically created. By default, the share is hidden from network browsing and has all network access protocols except HTTP/HTTPS enabled (as such, it can be accessed from a browser as the Web Root but can not be accessed via Web View). You can change these settings from the **Security > Shares** page. • **Use existing share**: From the drop-down list of existing shares for selection, select a share and click the **Properties** button to edit the selected share's properties (see **Security > Shares**).
Default Index File Names	Files found underneath the Web Root with names matching those in this list is automatically served to the web browser when present, according to their order in the list. To add a filename, click the **Add** button, enter the name of one or more index HTML files, then click **OK**. The file you entered is shown in the Index Files box. NOTE: If no files are specified, index.html is automatically used if found. To delete a name, highlight it and click **Delete**. At the confirmation page, click **Delete** again.

2. Map a drive to the share you have designated as the Web Root share and upload your HTML files to the root of the directory, making sure the file names of the HTML files are listed in the Index Files box.

Accessing the Web Management Interface when Web Root is Enabled

By default, when you connect to a SnapScale cluster with Web Root enabled, the browser loads the user-defined HTML page or present a directory listing of the Web Root. To access the Web Management Interface (for example, to perform administrative functions or change a password), enter the following in the browser address field:

`http://`*[nodename or ip address]***`/config`**

You are prompted for your User ID and password, then you are placed into the Web Management Interface.

If you need to access the Web View page to browse shares on the server independent of Web Root, enter this in the browser address:

`http://`*[nodename or ip address]***`/sadmin/GetWebHome.event`**

Storage Options

From the Storage default page, you can access and configure the storage options for your SnapScale cluster including nodes and drives.

Topics in Storage Options:

Peer Sets

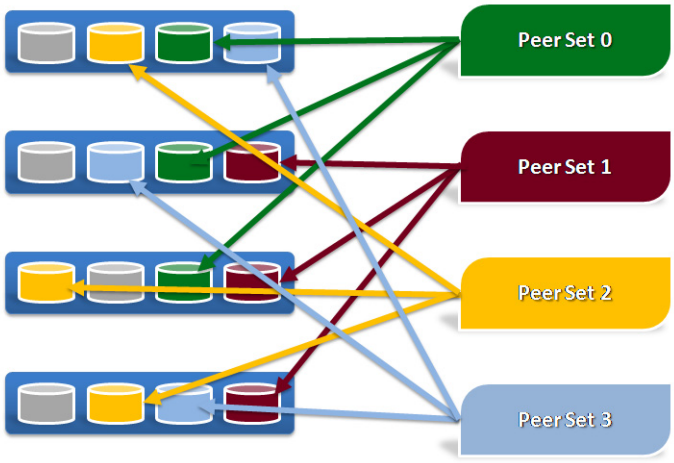
In a cluster, a node is a file server working in tandem with other nodes. The drives on every node are grouped into peer sets or hot spares. Each peer set contains two or three drives, depending on the Data Replication Count, that mirror the same data. To ensure availability, each drive in a peer set resides in a different node.

SnapScale aggregates all the storage on the peer sets in the cluster to form a unified data storage space for network client access. Data access is transparent between the cluster storage space and the peer sets so that users never directly access the peer sets.

When you create a cluster or add new nodes to an existing cluster, SnapScale automatically creates peer sets with the available drives. By distributing peer set members throughout the cluster, the system ensures that content is protected from failure of either individual drives or entire nodes. When they are created, peer sets are assigned a unique peer set ID.

Nodes can be added to expand cluster storage at any time. Based on the configuration settings, the additional drives are either used to create more peer sets or left as hot spares. Nodes can be removed from a cluster for replacement with a new node, and the drives in the replacement node are automatically synchronized with the existing peer sets.

On a four-node cluster configured for 3x replication count, four hot spares, and four drives per node, the peer set formation might look something like this:



Each peer set has members on three different nodes, shown below as peer set 0, 1, 2, and 3. Hot spares are automatically distributed throughout the cluster in order to replace any failed peer set member. When a peer set member fails, a hot spare is assigned from a node on which the peer set does not already have an active member.

The example above uses a 3x Data Replication Count, which means that each peer set contains three members, and as a result all data is replicated three times. The cluster can also be configured for a 2x Data Replication Count, in which case the distribution of two-member peer sets would be different. The system automatically determines which drives are used to form each peer set; you cannot choose them.

NOTE: The Data Replication Count can be decreased from 3x to 2x to increase cluster storage, but cannot be increased from 2x to 3x once the cluster is created.

Individual file size is also important when working with peer sets. While the total free space across the entire cluster might be very large, the maximum size of an individual file is limited to the total amount of free space available on the least-utilized peer set in the cluster, as that is the peer set automatically assigned by the cluster for the next file.

NOTE: Files are not allowed to span across peer sets.

The maximum possible file size is shown on the Admin Home page at the lower left. Refer to "Peer Set Basics" for more details.

Peer Sets and Recovery

Though data on peer sets is served indirectly by the unified cluster storage space, access to files stored on a given peer set is dependent on the health of that peer set. When a drive in a peer set fails, data is served from the remaining peer set member drives. If there is a spare

reserved for the cluster that does not exist on the same node as another active member of the peer set and is not smaller than other members, the peer set can claim the drive and rebuild the data onto that spare without administrator intervention. If a peer set is missing one drive but at least one other drive is available, the peer set continues to be accessible but is in degraded mode.

Peer Set Status	Failure Type	Data Availability
OK	The peer set drives are healthy and connected.	Data is fully available for read and write.
Rebuilding	Spare made available to rebuild the peer set.	Data is fully available for read and write.
Degraded	One drive missing from the peer set	Data is fully available for read and write.
Degraded – Cannot repair; no spares	The peer set cannot be repaired because there are no spare drives.	Data is fully available for read and write.
Degraded – Cannot repair; spares too small	The peer set cannot be repaired because all eligible spares are too small.	Data is fully available for read and write.
Degraded – Cannot repair; spares on same node	The peer set cannot be repaired because the only eligible spares are located on the same node as an active member of the peer set.	Data is fully available for read and write.
Failed	All drives in peer set have failed.	No availability. Contact Overland Support.
Initializing	The peer set is being created or initialized.	Data is not yet available.
inconsistent	The peer set has more members than the data replication count.	Contact Overland Support.

Peer Set Utilization

The system software automatically determines the specific peer set on which to store any given file or directory by using the peer set with the most free space available. Metadata for files and directories is independently distributed among different peer sets using a hash algorithm for optimum performance and protection.

Peer Set Basics

New drives are initially configured automatically as spare drives. Subsequently, if enough spare drives exist on different nodes to construct new peer sets but still satisfy the spare count setting, the SnapScale automatically creates new peer sets and expand cluster storage space.

Drives in a cluster do not all need to have the same capacity, but drives in a given peer set should have the same capacity or space is wasted on the larger drives.

The following points must be observed in regards to drives used in the cluster:

- The drives in a cluster must all be the same type of drive (such as SAS) and the same rotational speed.
- The storage capacity of a peer set is limited to the smallest capacity drive in the peer set.
- While the system reports total free space across the entire cluster, the maximum file size at any given time is dictated by free space on the least-utilized peer set.

In case of peer drive failure, RAINcloudOS continues to serve data reads and writes to that peer set from another member of the peer set as long as the peer set is not offline. If clients are currently using data on the peer set, it continues to operate as-is.

Data Replication Count is an administrator specified, cluster-wide count of the degree of redundancy of data on the cluster. The Data Replication Count can be either 2x or 3x and determines the number of drives (2 or 3) that make up each peer set.

Hot Spares

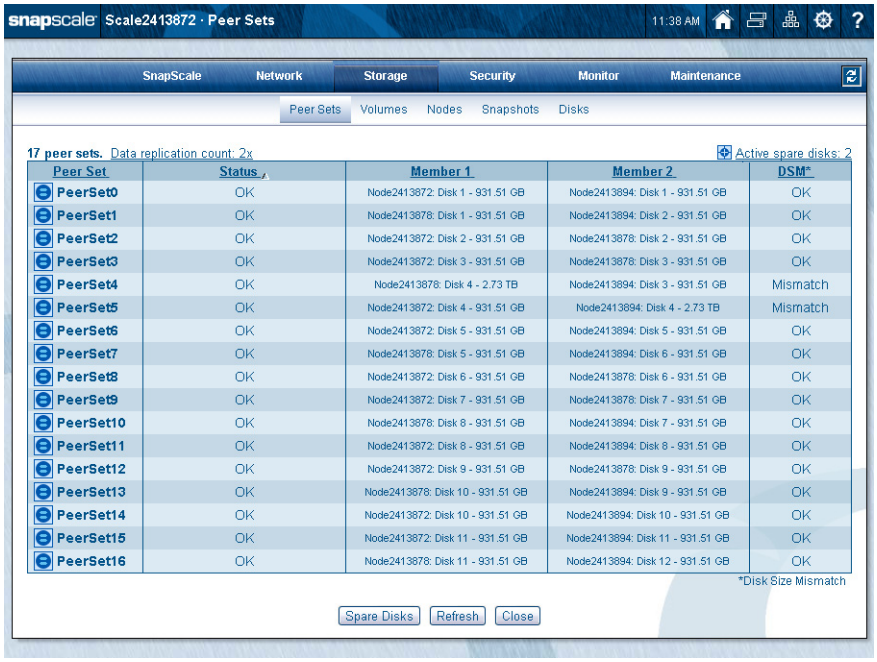
Each node can have a number of hot spares in the event of a drive failure. The total number of hot spares for the cluster is user selectable. A suggested number of hot spares for various node sizes is provided. If a peer set member drive fails, data from a healthy peer set drive on another node is re-synced onto an available spare on any node that doesn't have another active member of that peer set, and the spare then becomes a member of that peer set.

Drives added to nodes as additions or as replacements to failed drives are automatically configured as spares. If enough spares exist across different nodes to satisfy the Data Replication Count and the spare drives count, the cluster automatically creates a new peer set out of available spare drives.

Snapshot Limitations

- All snapshots are deleted when:
  - New peer sets are automatically created when new drives are installed.
  - One or more new nodes are added to a cluster.
  - If a complete peer set fails.
- A Snapshot may be deleted if:
  - Any peer set member drive runs out of snapshot space.
  - A second member of a peer set (containing *unique* snapshot data) fails, even though the main file system data may still be healthy.

Peer Sets Page

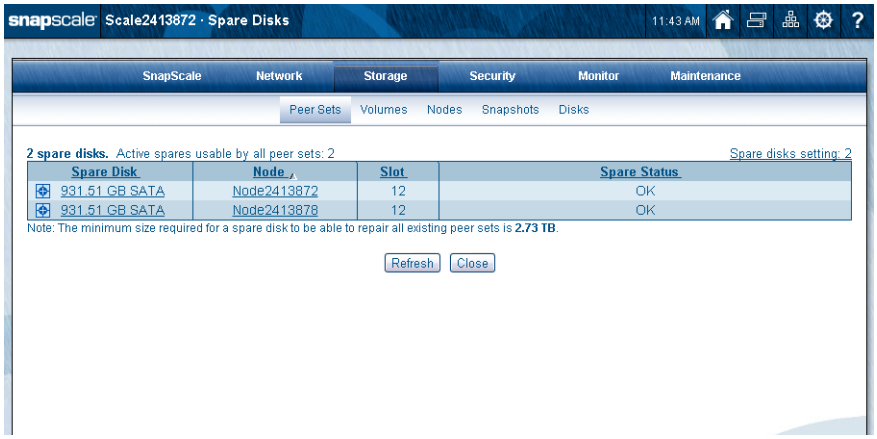


The following table covers the items listed on this page:

Option	Description
# Peer Sets	Displays the number of peer sets configured.
Data Replication Count	Displays the cluster-wide replication count and links to the SnapScale Properties page.
Active Spare Disks	Shows the number of drives allocated as spares. Clicking the link opens the Spare Disks page. This is the same as clicking the **Spare Disks** button.
Peer Set	Lists the peer set.
Status	Shows the current status. Refer to "Peer Sets and Recovery" for complete details.
Member 1	Shows the node, drive/slot number, and the size of the first member of this peer set. Click to view the Disks page and identify the specific disk drive's location.
Member 2	Shows the node, drive/slot number, and the size of the second member of this peer set. Click to view the Disks page and identify the specific disk drive's location.
Member 3 (if shown)	Shows the node, drive/slot number, and the size of the third member of this peer set when the Data Replication Count is set to "3x." Click to view the Disks page and identify the specific disk drive's location.
DSM (Drive Size Mismatch)	Shows either OK or Mismatch. If the member drives are not the exact same size, then capacity is limited to the smallest drive in the peer set, and extra space on larger drives is wasted. Mouseover the word Mismatch to view a tool tip displaying the unutilized capacity of the peer set.
Spare Disks (button)	See Active Spare Disks above.
Refresh (button)	Refreshes the page when clicked.

Spare Disks Page

When you click the **Spare disks setting** link on the upper right above the table on the Peer Sets page, or click the Spare Disks button, the Spare Disks page opens.



The following table covers the items listed on this page:

Option	Description
Spare Disks Setting (link text on upper right)	Displays the number set for spare drives. Clicking the link takes you to the SnapScale Properties page to edit the setting. NOTE: This setting may not equal the number of spare drives currently displayed if there are fewer spare drives available than the setting specifies, or if there is an insufficient number of extra drives to automatically create a new peer set and satisfy the cluster's Data Replication Count.
Spare Disk	Displays drive capacity and type. Click a name in the column to open the **Storage > Disks** page and identify a specific disk drive's location.
Node	Displays the name of the node on which the drive resides. Click a name in the column to open the **Storage > Nodes > Node Properties** page for the specific node.
Slot	Displays the slot number of the listed node where this spare drive is located.
Spare Status	Shows the current status: • OK – Spare drive is healthy and can be used by all peer sets. • Spare too Small – Spare is too small to either repair any existing peer sets or repair *n* existing peer sets. • Failed – Spare drive has failed.
Refresh (button)	Refreshes the page when clicked.

Volumes

Use the **Storage > Volumes** page to manage the volumes that have been created.

From this page, you can:

- Create a new volume.
- Edit or delete the volume (by clicking the name to access the Properties page).

Volume Overview

All the peer sets are unified into a single cluster storage space that can be accessed from any node thus providing multiple access points. One or more volumes can be created to provision the cluster storage:

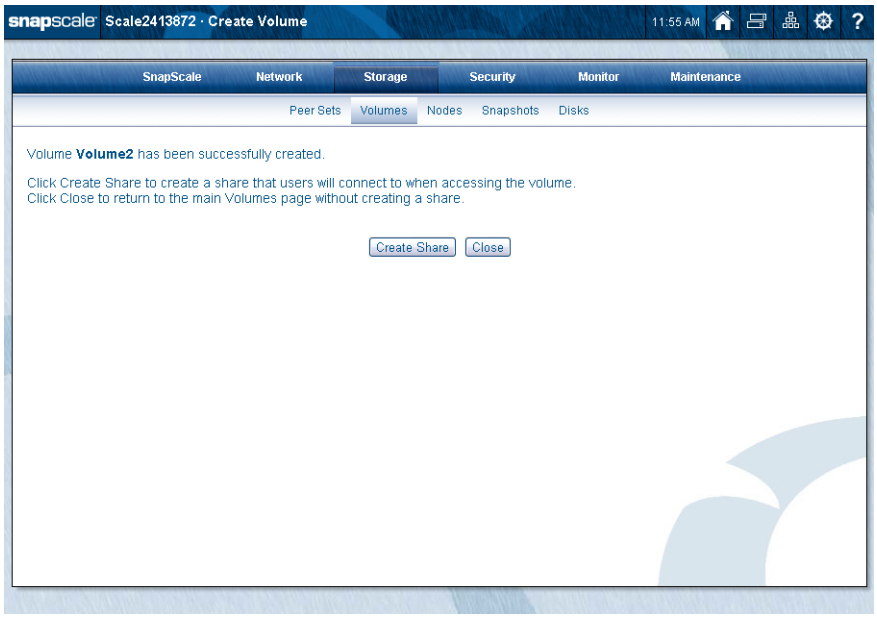
- All volumes share the same cluster storage space and are thinly provisioned to provide better utilization rates of the space.
- Volumes can be configured with a maximum size setting (quota) to prevent one volume from consuming too much shared cluster storage space. See "Creating Volumes."

Creating Volumes

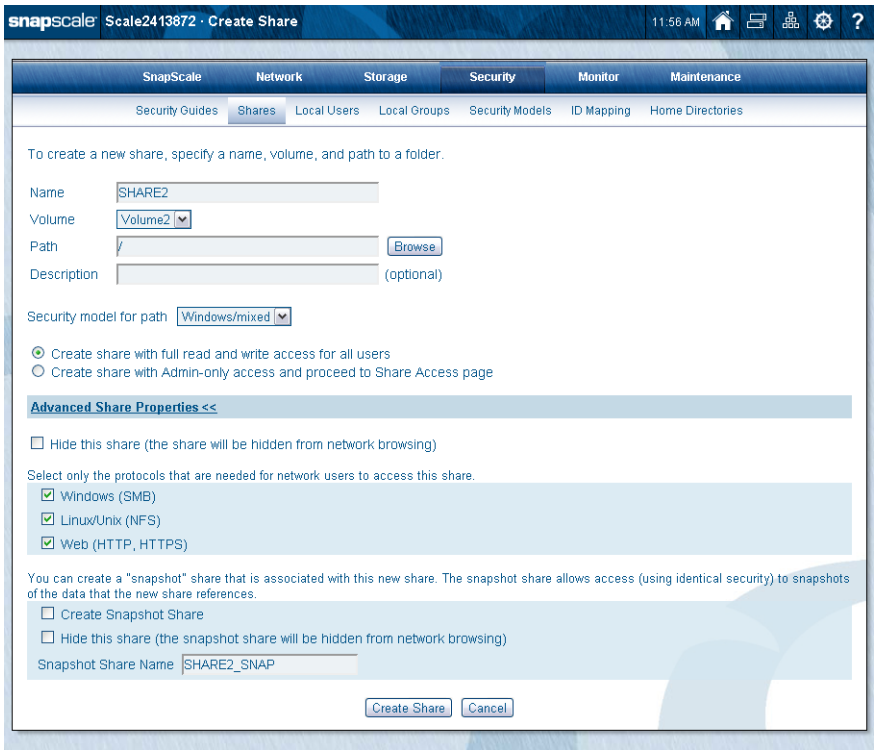
By default, the full cluster storage space is accessible as one large storage space. However, the storage space can be divided into multiple volumes in order to thinly provision space for specific projects, departments, or roles. Volumes can be constrained to use no more than a certain amount of space available in the clustered storage space. This is done using the **Create Volume** page:

1. At **Storage > Volumes**, click the **Create Volume** button.
   - It is recommended to enter a **Volume Name** to easily identify the specific volume.
   - If desired, set the **limit** for this volume to a maximum size.

2. Click the **Create Volume** button again. A confirmation page is shown:



3. At the confirmation screen, click **Create Share** to create a share pointing to this volume (takes you to the **Security > Shares** page).

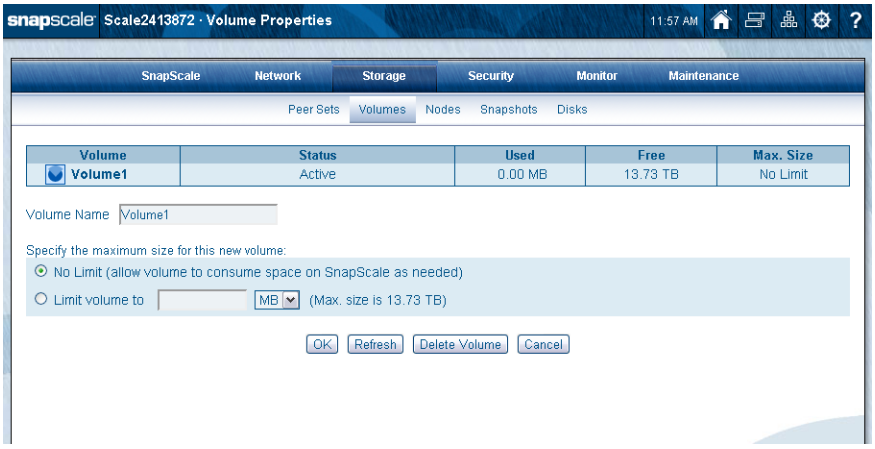


4. Enter the appropriate **data** and select the necessary options, then click **Create Share**. Additional options can be accessed by clicking the **Advanced Share Properties** link at the bottom. See Chapter 5, "Create Shares," for complete details.

5. Click **Close** twice to return to the Admin Home page.

Volume Properties

By clicking a volume's name on the main page, details of that particular volume are shown on the **Volume Properties** page.



From this secondary page, you can:

- Change the volume name.
- Set maximum volume size (specific limit or no limit).
- Delete the entire volume.

Rename a Volume

In the **Volume Name** field, enter a unique volume name of 32 alphanumeric characters and spaces, then click **OK**.

Specify Maximum Volume Size

There are two options controlling the maximum size of a volume:

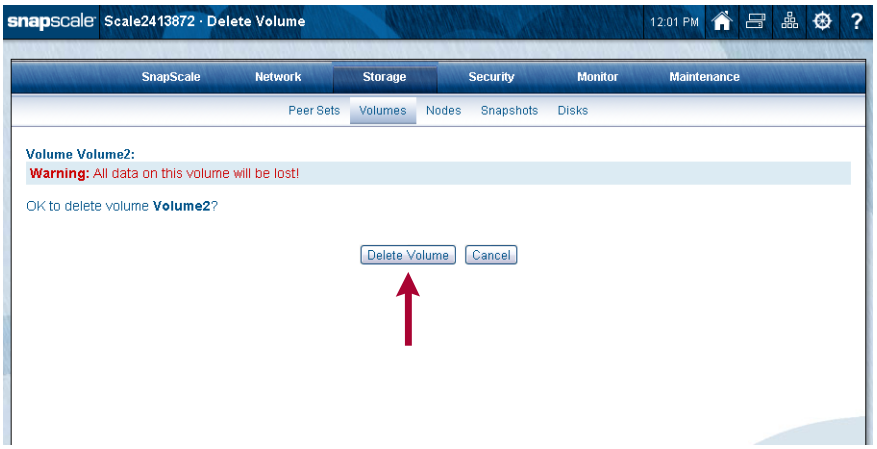
- **No Limit** – This is the recommended option because it allows the volume to consume space as needed.
- **Limit Volume to # MB/GB/TB** – Establish a maximum volume size limit by entering the amount and selecting a unit of measure. The volume then grows in size until it reaches its maximum. If email notification has been enabled, alerts are sent as the maximum is approached. (To enable email notification, see Chapter 7, "Email Notification.")

NOTE: If you reset the maximum size of a volume to less than its current size, the volume is treated as full and no more data can be written to it until the actual space consumed drops below the maximum size again. When done, click OK.

Deleting Volumes

To delete a volume, go to the **Volume Properties** page and click the **Delete Volume** button. At the confirmation page, click the **Delete Volume** button again. You are returned to the Volumes page and the volume is deleted in the background.

CAUTION: Deleting a volume deletes all the shares and data on the volume.



Nodes

Use the **Storage > Nodes** page to manage the nodes that make up the cluster.

From this page, you can:

- Add a new node.
- Edit or delete the node (by clicking the node name to access the Properties page).
- Identify physical nodes via flashing LEDs.

Nodes Overview

Some important points about SnapScale nodes:

- Users can access the cluster storage over any of the configured network protocols by connecting to any of the nodes.
- Because the storage space is unified across the cluster, connecting to any of the nodes provides access to the same data as any other cluster node.
- To balance network client access to the nodes, enter an A record to the DNS pointing to the cluster name for each IP address in the node IP address range. The DNS then uses round-robin name resolution requests for the cluster name among the node IP addresses. Alternatively, manually distribute clients accessing the cluster to different IP addresses in the node IP address range.

- When a node fails, the IP address it uses is automatically reassigned to another node. Clients connected to that IP address are forwarded to the new node, though this may cause a momentary interruption to storage access.
- Files opened by clients connected to any node are recognized by all nodes, and file locks are respected by all nodes.

Node Properties

By clicking a node's name on the main page in the Node column of the table, details of that particular node are shown on a **Node Properties** page.

From this page, you can:

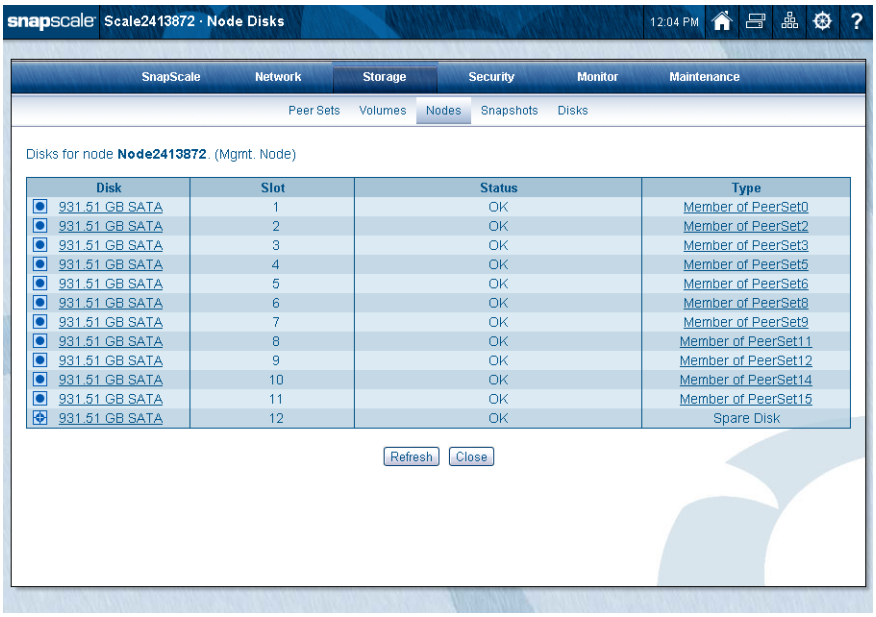
- Flash the node drive LEDs to help identify the node.
- Change the node description.
- View the drives in the node.
- Remove the node from the SnapScale cluster.

Flash the Node LEDs

Click the light-blue box ( ) under the node name to start the LEDs flashing for up to five minutes. Click the box with the red "X" ( ) to stop flashing the LEDs.

Node Drives

To view the drives that are installed in the node, click the **View Disks** button.



When you click a Disk name, the **Storage > Disks** page is displayed indicating the physical location of the disk drive. See "Disks" for more information.

Clicking the member name in the Type column takes you to **Storage > Peer Sets**. See "Peer Sets Page" for more information.

When done, click **Close** to return to the Properties page.

Adding Nodes

A SnapScale cluster can also be expanded by adding more nodes. Expansion kits are available that consist of either two or three additional nodes and all the necessary cables. Documentation is included with each node that details how to install, cable, and power up the new node.

Once installed in a rack, clicking the **Add Node** button on the Nodes page starts a wizard to add one or more nodes to the cluster to expand the storage space. By default, all eligible nodes are pre-selected.

IMPORTANT: In order to expand storage by adding nodes, the cluster must be able to create peer sets with each member on different nodes. As a result, to increase storage, the number of new nodes you add must be equal or greater to the Data Replication Count being used (2x or 3x) to efficiently expand cluster storage space.

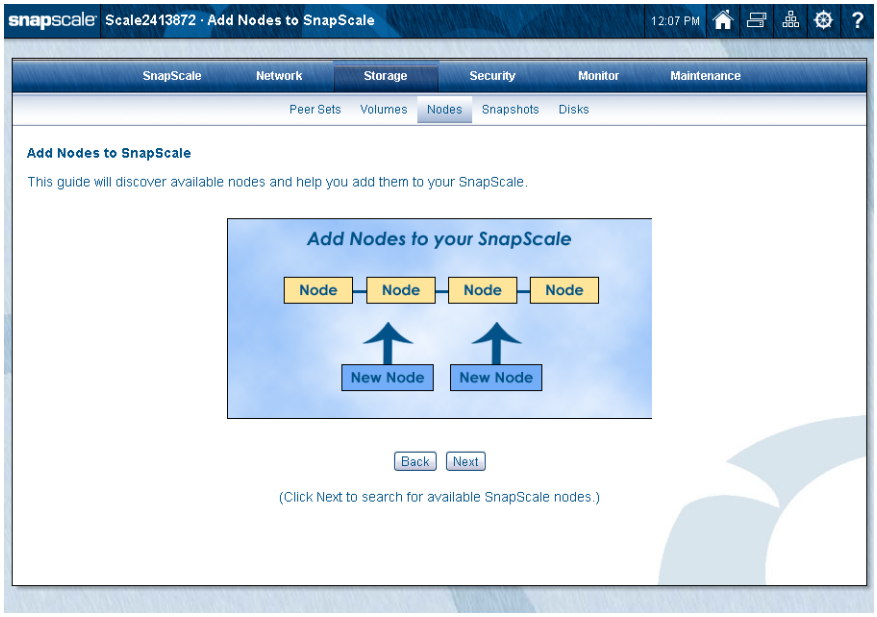
When adding nodes, all the following must be taken into consideration:

- The nodes must all be running the same version of RAINcloudOS (ROS). See Chapter 7, "OS Update."
- All the nodes, those already part of the cluster and those being added, must be attached to the same Client subnet.
- No expansion units can be attached to a node.
- All four ports on the node must be available to create the proper bonding.

- Drives must be contiguously installed with no empty slots between drives (going left to right, top to bottom).

Follow these steps using the wizard to add your nodes:

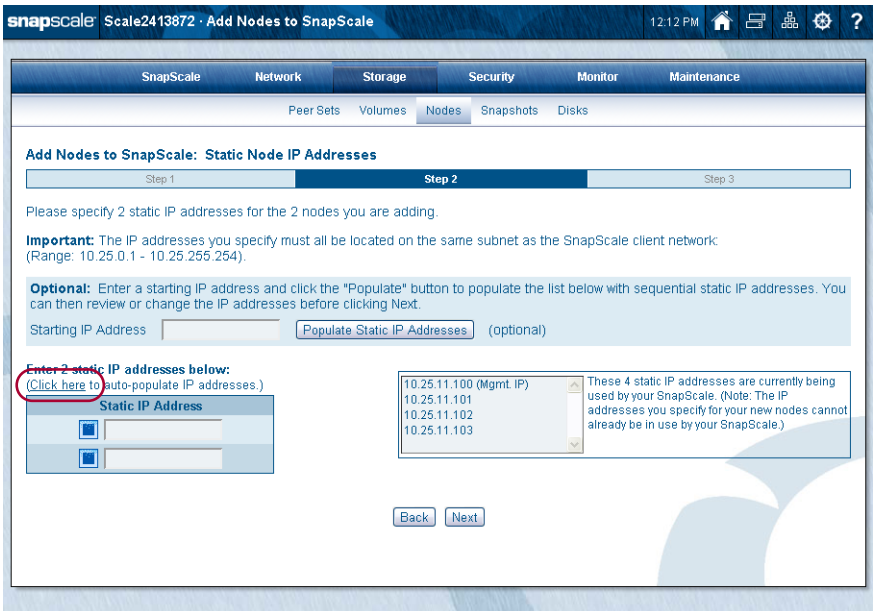
1. Click **Add Nodes**.



2. Click **Next** to display node choices:

3. At Wizard Step 1, check the **nodes** you want to add to the cluster, and click **Next**.

   By default, all eligible nodes are pre-selected. It is recommended to accept all the nodes to ensure the optimum configuration.

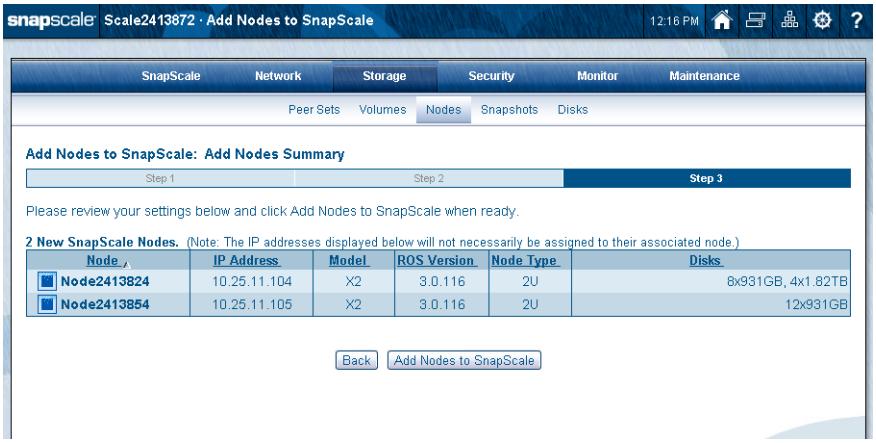


4. At Wizard Step 2, enter the **static IP addresses** for the nodes, and click **Next**.

   NOTE: When more new nodes are being added to the cluster than there are unused IP addresses in the node address pool, more IP addresses must be added to the pool.

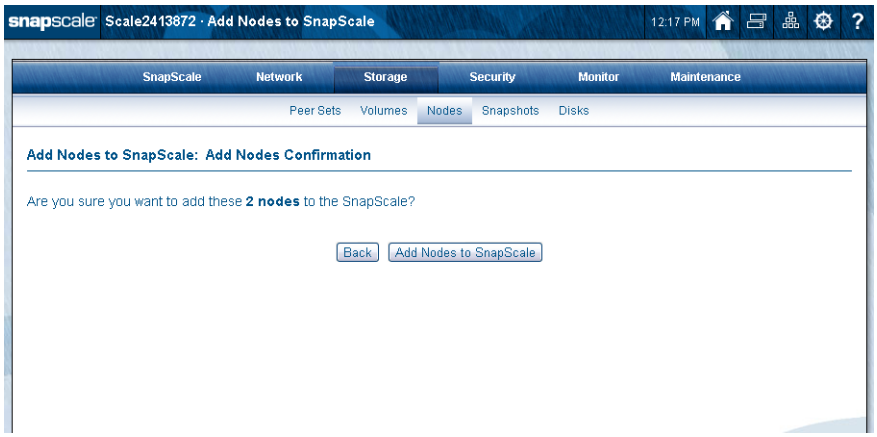
   It is recommended that you click the **Click here** option to automatically add IP addresses based on the addresses being currently used.

   Also, you can enter a starting address in the Populate field based on the static IP addresses (in the list on the right) currently being used by your SnapScale cluster, and then click the **Populate Static IP Addresses** button.



5. At Wizard Step 3, verify the data and click **Add Nodes to SnapScale**.

   The confirmation screen is shown:



6. At the confirmation screen, click **Add Nodes to SnapScale** again.

The new nodes are added to the cluster and the peer sets are built. This process takes several minutes.

Removing Nodes

To remove a node from a SnapScale cluster, go to the **Node Properties** page and click the **Remove Node from SnapScale** button. At the confirmation page, click the **Remove Node from SnapScale** button again.

IMPORTANT: Removing a node may result in one or more peer sets becoming degraded. These degraded peer sets may not be automatically repaired if there are not enough eligible spare drives on other nodes. Removing this node may also result in your SnapScale operating with less than the minimum requirement of 3 nodes.

NOTE: If removing the node would destroy one or more peer sets, an error message is returned and the node is not removed.

The node itself is no longer associated with the cluster and becomes an Uninitialized node that can be added to another cluster.

Node Identification

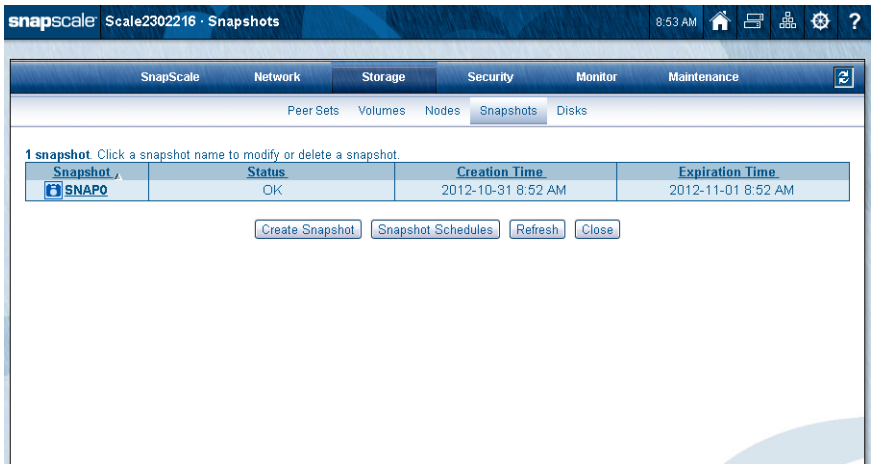
This page provides a convenient place to check the nodes and optionally change their descriptions for easier identification in the Web Management Interface. Click a light-blue box ( ) next to the node name to start the node's LEDs flashing for up to five minutes. Click the box with the red "X" ( ) to stop flashing the LEDs or click the link next to the same icon below the nodes table to stop all node LEDs flashing.

Snapshots

A *snapshot* is a consistent, stable, point-in-time image of the cluster storage space that can be backed up independent of activity on the cluster storage. Snapshots can also satisfy short-term backup situations such as recovering a file deleted in error without resorting to tape. Perhaps more importantly, snapshots can be incorporated as a central component of your backup strategy to ensure that all data in every backup operation is internally consistent and that no data is overlooked or skipped.

NOTE: To preserve your cluster configuration and protect your data from loss or corruption, it is critical to schedule backups and snapshots.

Navigate to **Storage > Snapshots** in the browser-based Web Management Interface to create or schedule snapshots:



Snapshots Overview

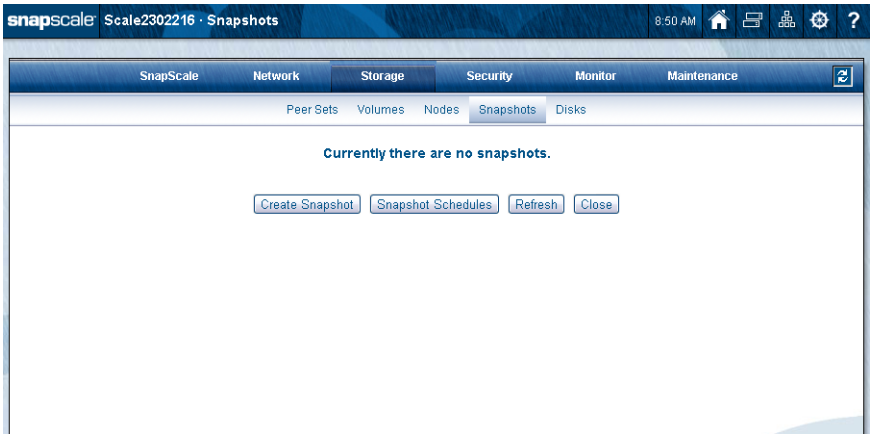
When working with snapshots, consider the following caveats:

- It is recommended that snapshots be taken when the system is idle or under low data traffic to minimize conflicts.
- Snapshots for the cluster storage space use snapshot space reserved on each peer set member drive.
- The snapshot space is fixed to 10% of the cluster storage space and cannot be changed.
- Snapshot space reserved from each peer set member drive is not necessarily identical to snapshot space of other drives in the same peer set. (This is most likely to occur if two or more drives in the same peer set have recently failed, even if they've been replaced with spares.) As a result, failure of a drive with unique snapshot data may cause one or more snapshots to be automatically deleted.
- Addition of a peer set to the cluster (including automatic peer set creation using new drives inserted into nodes or the addition of new nodes to the cluster) deletes all existing snapshots.
- Failure of a peer set deletes all snapshots.

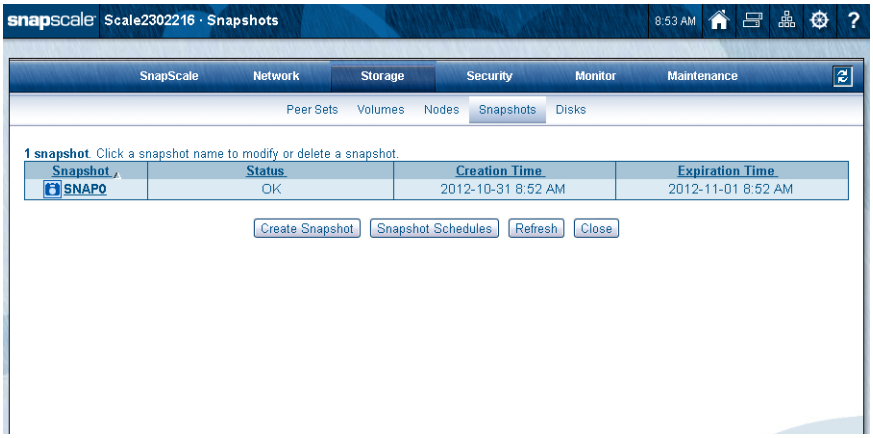
Creating Snapshots

Creating a snapshot involves naming, scheduling, and setting the duration of the snapshot. For regular data backup purposes, create a recurring snapshot. A recurring snapshot schedule works like a log file rotation, where a certain number of recent snapshots are automatically generated and retained as long as possible, after which the oldest snapshot is discarded. You can also create individual, one-time-only snapshots as needed.

If no snapshots are currently configured, you only see an empty page:



Once a snapshot is created, the page is populated with options for managing the snapshots:



These options are available in the Snapshots section of the Web Management Interface:

Action	Procedure
Create a New Snapshot	Click **Create Snapshot**. The process involves first defining snapshot parameters, and then scheduling when and how often to run the snapshot. Do not take more snapshots than your system can store, or more than 250 snapshots. Under normal circumstances, nine or ten snapshots are sufficient to safely back up any system.
Edit a Snapshot Schedule	Click the **Snapshot Schedules** button, and then click the snapshot name. You can modify all snapshot parameters.
Edit and Delete	Click the snapshot's name to open the Snapshot Properties page. You can edit the snapshot's name and duration, or delete the snapshot.

Clicking the **Refresh** button updates the page. This is helpful when waiting for a snapshot to complete.

When single snapshots are originally created or while recurring snapshots are active, the Refresh icon ( ) is displayed on the right of the tab bar. It indicates that the snapshot data in the table is being refreshed every 5 minutes and can be clicked to manually refresh the data.

Clicking the **Close** button returns you to the **Storage** home page.

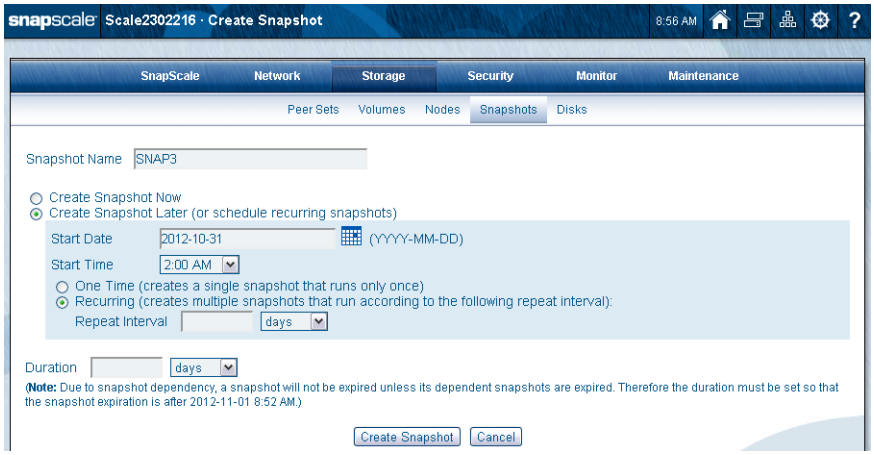
NOTE: The presence of one or more snapshots on a cluster can impact write performance. Additional snapshots do not have additional impact; in other words, the write performance impact of one snapshot on a cluster is the same as the impact of 100 snapshots.

Snapshots and Backup Optimization

When you back up a live volume directly, files that reference other files in the system may become out-of sync in relation to each other. The more data you have to back up, the more time is required for the backup operation, and the more likely these events are to occur. By backing up the snapshot rather than the volume itself, you greatly reduce the risk of archiving inconsistent data.

To Create a Snapshot

Follow these steps to create a snapshot:



1. Go to **Storage > Snapshots**, and click **Create Snapshot**.
2. Enter or select the **options** for the snapshot:
   a. Type in the **Snapshot Name** (20 character maximum).
   b. Specify **when** to create the snapshot.
      - Click **Create Snapshot Now** to run the snapshot immediately.
      - Click **Create Snapshot Later** to schedule the snapshot for a later time.

      When you select the **Create Snapshot Later** button, a new input section appears below the option. Enter the Start Date and Start Time. Select either to create the snapshot only once (**One Time**) or to have it recurring periodically (**Recurring**) using an interval in hours, days, weeks, or months.
   c. Specify the **duration** of the snapshot.

      NOTE: In the Duration field, specify how long the snapshot is to be active in hours, days, weeks, or months. The SnapScale automatically deletes the snapshot after this period expires, as long as no older unexpired snapshots exist on which it depends. If any such snapshot exists, its termination date is displayed at the bottom of the page. You must set the duration to a date and time after the displayed date.

3. Create the snapshot by clicking **Create Snapshot**.

   If you elected to run the snapshot immediately, it appears in the Current Snapshots table. If you scheduled the snapshot to run at a later time, it appears in the Scheduled Snapshots table.

Accessing Snapshots

After snapshots are created, they can be accessed via a snapshot share. Just as a share provides access to a portion of a live volume, a snapshot share provides access to the same portion of the filesystem on all current snapshots of the volume. The snapshot share's path into snapshots mimics the original share's path into the live volume. The snapshot share is created in the **Shares** section under the **Security** tab. See Chapter 5, "Shares," for details.

Scheduling Snapshots

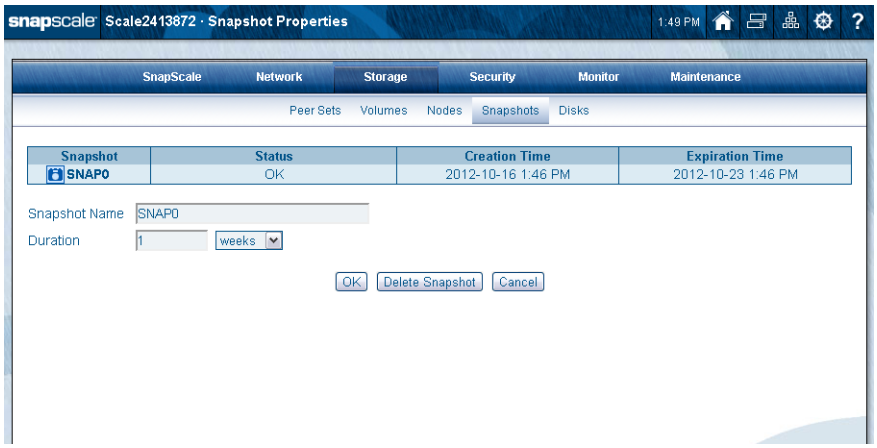
To view when snapshots are currently scheduled to occur, click **Snapshot Schedules**:

The Snapshot Schedule page shows a list of scheduled snapshots pending. **Repeat Interval** and **Next Snapshot Time** shows the details of when snapshots are scheduled to be taken.

Snapshots should ideally be taken when your system is idle. It is recommended that snapshots be taken before a backup is performed. For example, if your backup is scheduled at 4 a.m., schedule the snapshot to be taken at 2 a.m., thereby avoiding system activity and ensuring the snapshot is backed up.

Snapshot Properties

From the **Snapshot** primary page table, you can click a snapshot name to access the **Snapshot Properties** page. There you can edit the name and duration, or delete the snapshot:



Edit a Snapshot

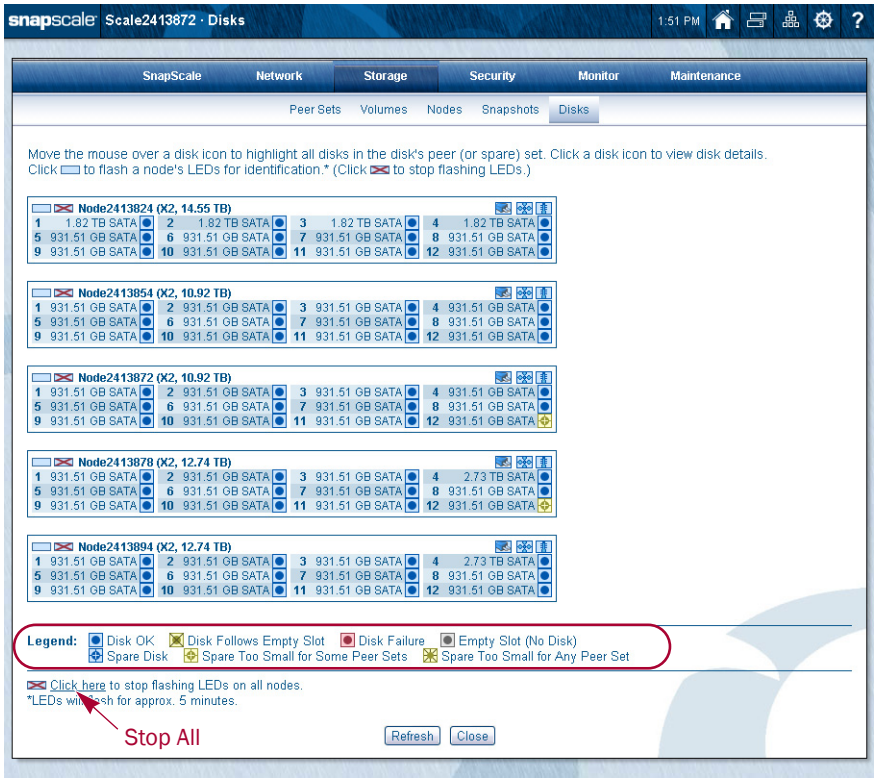
You can edit the name and duration by changing the data in the detail fields, and clicking **OK**.

Delete a Snapshot

Click the **Delete Snapshot** button and then click it again on the confirmation page. The snapshot is deleted.

Disks

The Disks page is a graphic representation of the peer sets and disk drive status on your cluster. The legend on the **Storage > Disks** page explains the meaning of each icon.



- Click a drive icon ( ) to view drive details.
- Hover over a drive icon ( ) to view the other members of the peer set.
- Hover over a spare drive icon ( ) to view other spare drives.
- Click a unit's LED icon ( ) to flash the unit's status and drive status LEDs for identification. The LEDs flash amber. Click the LED stop icon ( ) to stop the unit's LEDs from flashing.

  NOTE: The LEDs continue to flash for five minutes unless stopped. To stop flashing LEDs for all units, click the link next to the stop icon located below the Legend list.

Replacing Drives

Should a drive fail (solid red LED), it can be replaced (hot-swapped) without shutting down the SnapScale node. If a spare is available on a node that doesn't already have an active member of the failed drive's peer set, the spare automatically replaces the failed drive and the new drive being installed automatically becomes a spare. If no spares are available, the new drive automatically becomes a member of the failed drive's peer set.

A failed drive can be removed and replaced anytime if two or more peer set member drives are active in the same peer set. When adding multiple drives to create new peer sets, add one drive at a time to avoid timing issues.

NOTE: Hot-removed drives cannot be added directly back into a peer set. When any drive is removed, it is removed from the peer set. The peer set then becomes degraded and attempts to incorporate an available spare on the node. If the drive is reinserted, it's reconfigured as a spare. If no spare was available when it was removed, SnapScale then incorporates it back into the peer set.

If there are no errors, after the new drive is incorporated, any alert LEDs are turned off and system statuses are updated.

Adding Drives

CAUTION: Adding new drives to a SnapScale cluster automatically creates new peer sets and expands cluster storage. It also deletes all existing snapshots.

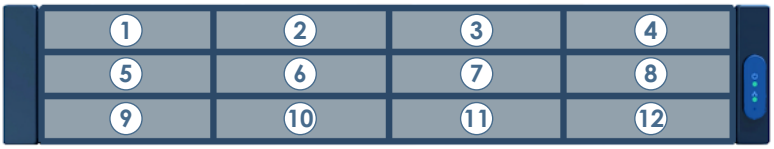
If empty slots are available on a node, you can add Overland-approved drives to either expand cluster storage space or add hot spares. When adding drives to expand storage space, distribute the new drives evenly across all the cluster nodes. Insert them one at a time, cycling through the nodes.

As the drives are added, the SnapScale first checks to see if it can create a peer set using spares on the other nodes. It then checks as each drive is added to see if it has enough drives on different nodes to form a new peer set.

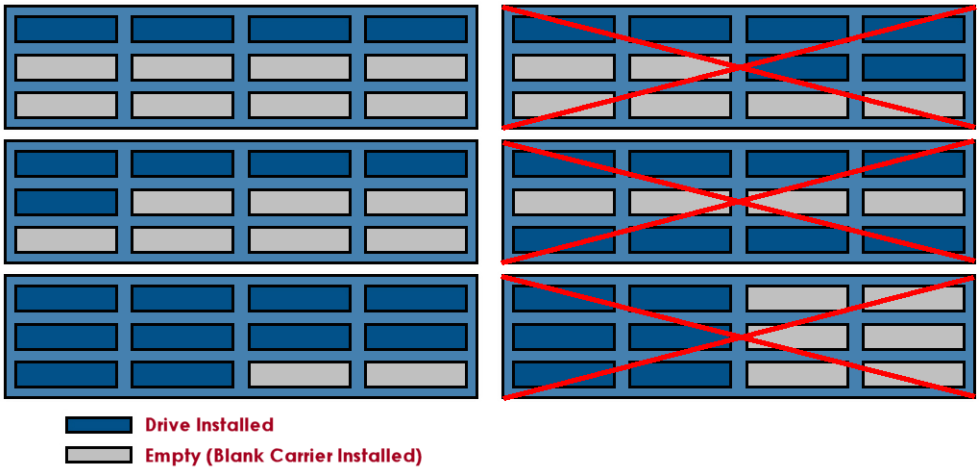
For example, when adding a four-pack of new drives to a three-node cluster with a 3x Data Replication Count (DRC) with no spares, add the first drive to node one, the next to node two, then node three, and finally the last drive to node one. When done, you will have one new peer set and one new spare.

Drives can be added without shutting down the node. However, different types of drives (for example, SAS and SATA drives) or different rotational speeds cannot be combined in the same cluster.

IMPORTANT: The drives must be installed contiguously from left to right starting with the top row, and moving downward. If an empty slot exists between drives, all the newly added drives that follow that slot are labeled as "Disk Follows Empty Slot" in the Web Management Interface and are not incorporated into the cluster.



The following diagram shows different ways to install the drives with the incorrect ways crossed out:



The drives are automatically incorporated to expand cluster storage space. If there are sufficient spare drives on other nodes, the drives are used to create new peer sets. Otherwise, they are automatically configured as spare drives.

In order to properly create peer sets with each member on different nodes, if you have the Data Replication Count set at 2x, you must add drives in groups of two, each to different nodes; for a 3x count, add in groups of three, each to different nodes.

When adding new drives, consider the following:

- Drives added to any cluster node are initially configured automatically as hot spares.
- When more drives are added to the cluster, the cluster will automatically create new peer sets and expand cluster storage if all the following conditions are met:
  - There are more drives than are required by the cluster's Spare Disks count.
  - There are enough extra drives being added to satisfy the Data Replication Count.
  - The newly installed drives or existing spares are distributed evenly across different cluster nodes.
- If there is a degraded peer set on the cluster when adding a new drive and there are no existing spares, the drive will automatically be incorporated into the peer set as long as it is not on one of the nodes containing another active member of the peer set.
- When replacing a failed drive, the new drive must be installed in the same slot as the old one to prevent the introduction of an empty slot between drives.
- When adding a drive that replaces a failed drive in a peer set, the **Peer Sets** page will display that peer set as rebuilding the new drive into the peer set. Similarly, if the conditions are met for the creation of new peer sets, the **Peer Sets** page will display that new peer sets are being created.

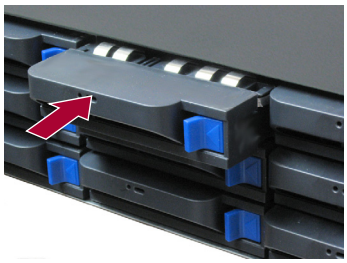
Drive Installation

NOTE: Do not remove the disk drives from their carriers. Doing so voids the drive warranty.

Install the drives into the next available slots (left to right, then down):

1. Remove the **blank drive carriers** from the slots that will be used for the new drives (leaving the remaining blank carriers in place).

2. Positioning a **drive carrier** in front of the appropriate **bay**, slide it in until the **latch** clicks, locking the assembly in the bay.



3. Repeat Step 2 for **each** remaining drive carrier being installed.

IMPORTANT: To maintain proper airflow and cooling, a drive carrier or a blank carrier must be installed in *every* slot. No empty slots are allowed.

Security Options

This section covers Security options for users, groups, shares, and file access.

Topics in Security Options

Overview

Authentication validates a user's identity by requiring the user to provide a registered login name (User ID) and corresponding password. SnapScale clusters have predefined local users and groups that allow administrative (admin) and guest user access to the cluster via all protocols. Those options are found on the Security tab:

Administrators may choose to join the SnapScale cluster to a Windows Active Directory domain, and CIFS/SMB clients can then authenticate to the cluster using their domain credentials. To accommodate NFS clients, the SnapScale cluster can also join an NIS domain, and can look up user IDs (UIDs) and group IDs (GIDs) maintained by the domain. See "User and Group ID Assignments."

The SnapScale default security configuration provides one share to a default volume that can consume the entire cluster storage space. All network protocols for the share are enabled, and all users are granted read-write permission to the share via the guest account. By default, the **guest** user is disabled in SMB but enabled for HTTP.

Network clients can initially access the cluster using the guest account (where enabled), but if you require a higher degree of control over individual access to the filesystem for these clients, you must create local accounts (or use Windows Active Directory security for CIFS/SMB clients).

Local users or groups are created using the **Security > Local Users** and **Security > Local Groups** pages in the Web Management Interface. Local users are also used for administrative access to the cluster through the cluster's Web Management Interface or SSM.

A local user or group is one that is defined locally on a SnapScale cluster using the Web Management Interface. The default users and groups listed below cannot be modified or deleted.

- **admin** – The local user admin account is used to log into the Web Management Interface. The default password for the admin account is also *admin*.
- **guest** – The local user guest account requires no password.
- **admingrp** – The Admin group account includes the default admin user account. Any local user accounts created with admin rights are also automatically added to this group.

Guidelines for Local Authentication

These password authentication guidelines are for both users and groups.

Duplicating Client Login Credentials for Local Users and Groups. To simplify user access for Windows Workgroup, duplicate their local client logon credentials on the SnapScale cluster by creating local accounts on the cluster that match those used to log on to client workstations. This strategy allows users to bypass the login procedure when accessing the cluster.

CAUTION: This strategy applies only to local users. Do not use duplicate domain user credentials if joined to an Active Directory domain.

Default Local Users and Groups. Default users and groups *admin*, *guest*, and *admingrp* appear on the list of users or groups on the User or Group Management pages, but they cannot be deleted or modified (although the admin password can be changed).

Changing Local UIDs or GIDs. The SnapScale cluster automatically assigns and manages UIDs and GIDs. Because you may need to assign a specific ID to a local user or group in order to match your existing UID/GID assignments, the cluster makes these fields editable.

Password Policies. To provide additional authentication security, set password character requirements, password expiration dates, and lockout rules for local users.

Local users can also be individually exempted from password expiration and character requirement policies. The built-in *admin* user is exempt from all password policies.

Local Account Management Tools. The following tools are available for creating, modifying, and editing local user and group accounts:

Function	Navigation Path
Local User Management	Navigate to the **Security > Local Users** page, from which you can create, view, edit, and delete local users. You can also set user password policy, including password character requirements, maximum number of allowed logon failures, and password expiration settings.
Local Group Management	Navigate to the **Security > Local Groups** page, from which you can create, view, edit, and delete local groups.

User and Group ID Assignments

A SnapScale cluster uses the POSIX standard to assign UIDs or GIDs, in which each user and group must have a unique ID. This requirement applies to all users and groups on the cluster, including NIS, Windows domain, and local users plus NIS groups.

If you join the cluster to a Windows or NIS domain, IDs are assigned using available IDs only. Consider the following when creating users and groups:

- UIDs and GIDs from 0 to 100 are unavailable for use. If you try to assign a UID or GID that is less than 101 (or in use by NIS or the Windows domain), you will get an error message.
- When the cluster automatically generates UIDs or GIDs for imported Windows domain users or groups, UIDs or GIDs that are already in use by local and NIS users are skipped.
- When NIS domain users and groups are imported, the cluster discards any UIDs that are less than 101 or are in conflict with UIDs already in use by local or Windows domain users and groups.

The **`nfsnobody`** and **`nobody`** user IDs (UID 65534 and 65535, respectively) and GIDs are reserved. They are not mappable to other IDs, nor is another ID mappable to **`nfsnobody`** or **`nobody`**.

Security Guides

Security Guides are special wizards to guide you through:

- Setting up Windows Active Directory security.
- Giving users or groups share-level access to an entire volume.
- Giving users or groups share-level access to a folder on a volume.

Windows Active Directory Security Guide

The Windows Active Directory Security Guide wizard guides you through the setup of Windows Active Directory on your cluster.

NOTE: You cannot join an Active Directory domain if NTP is enabled. If you see such a message, click the NTP link to change your settings.

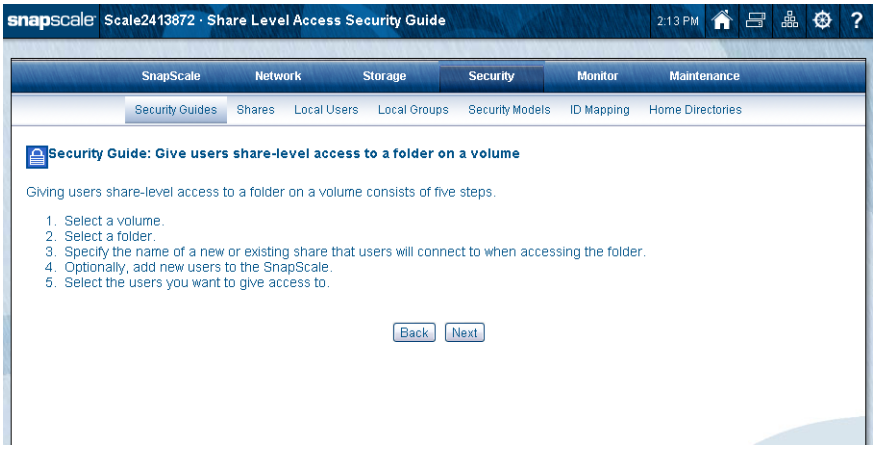
When the cluster joins a domain, it does so as a single unit under the cluster name, and all nodes operate equally under the cluster name to authenticate against the domain. This provides multipoint domain-authenticated access to the cluster through each node.

Entire Volume Security Guide

This Share Level Access Security Guide wizard guides you through the four steps it takes to give share-level access to an entire volume.

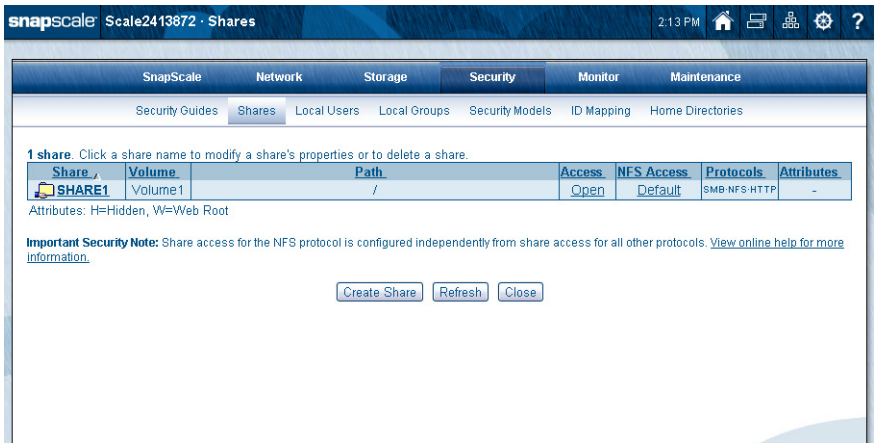
Folder on Volume Security Guide

This Share Level Access Security Guide wizard guides you through the five steps it takes to give share-level access to a folder on a volume.



Shares

SnapScale provides full integration with existing Windows Active Directory domain or UNIX NIS user and group databases. At the share level, administrators can assign read-write or read-only share access to individual Windows (and local) users and groups. Administrators can also edit the NFS exports file to control how shares are exported to NFS client machines.

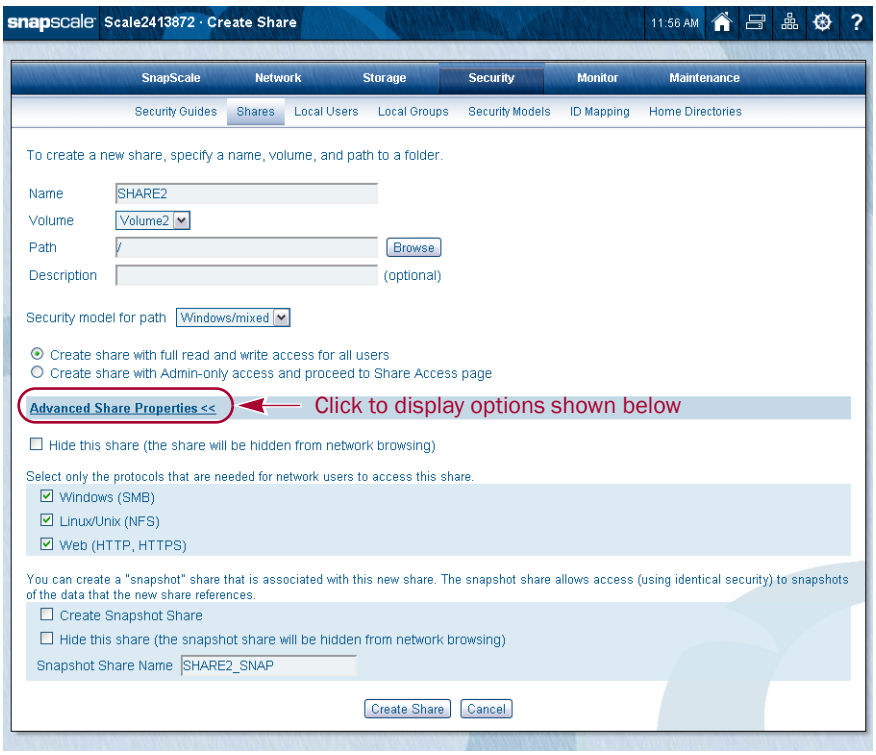


Share Security Overview

SnapScale supports file access in Windows and UNIX networks. New shares are created by default with full read-write access to all users, subject to the filesystem permissions on the share target directory. The first step to securing a cluster is to specify access at the individual share level. Administrators can assign read-write or read-only share access to individual Windows (and local) users and groups.

Create Shares

To create a new share, you need, at a minimum, to specify the share name, volume, and folder path. Click **Create Share** on the default Shares page to start the process.



By clicking the Advanced Share Properties link, additional options are displayed. Use these options to hide the share from network browsing, select the protocols supported, and create a snapshot share associated with this share.

Creating a Share

Creating a share includes selecting the volume, security model, and directory path for the share and then defining share attributes and network access protocols.

1. Accept the default **share name** or enter a new one.

   To ensure compatibility with all protocols, share names are limited to 27 alphanumeric characters (including spaces).

2. Choose the **volume** you need from the drop-down menu.

3. Select from the following **path options**:

   - **To create a share to the entire volume** – The current Path field defaults to the root path of the volume. Simply leave it blank if this is the desired configuration.
   - **To create a share to a folder on the volume** – Browse to the folder to which you want to point the share, click the folder name, and click **OK**.

   NOTE: If you want to create a new folder inside any other folder, type the folder name into New Folder Name and click Create Folder.

4. If desired, enter a **description** to clarify the purpose of the share.

5. Choose a **security model for path** by selecting either **`Windows/Mixed`** or **`UNIX`** from the drop-down list.

   The option defaults to the current security model at the specified path. If changed to a different security model, the change will propagate to all files and subdirectories underneath. For more information, see "Security Models."

6. Choose the user-based **Share Access** option desired.

   Choose either **Create share with full read and write access for all users**, or **Create share with Admin-only access and proceed to Share Access page** to configure the share access. For more information, see "Share Access Behaviors."

   NOTE: If selecting Create share with Admin-only access and if the share has NFS enabled, be sure to configure the NFS Access settings afterward.

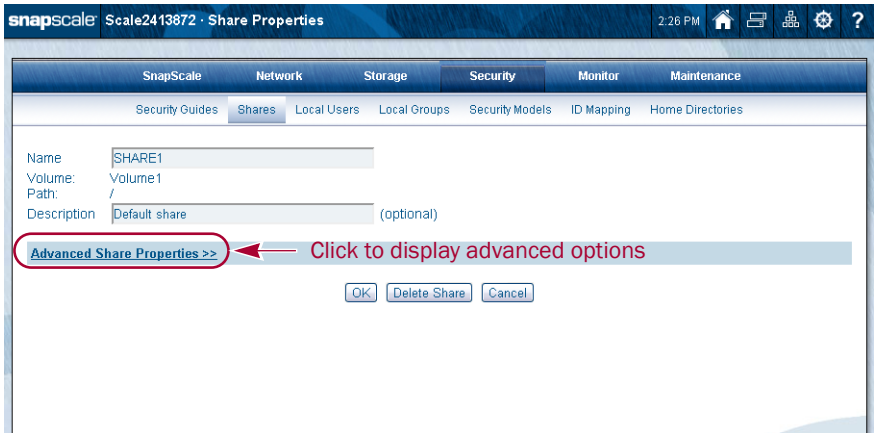
7. To further configure the share, click **Advanced Share Properties**, and enter any of the following:

Option	Description
Hide this Share	Select this option if you want the share to be hidden from network browsing using SMB and HTTP/HTTPS protocols (but not NFS).
Protocols	Select the access protocols for the share: Windows (SMB), Linux/UNIX (NFS), or Web (HTTP/HTTPS).
Snapshot Share	To create a snapshot share, select the Create Snapshot Share checkbox. Optionally, do either of the following: • To hide the snapshot share from the SMB and HTTP protocols, select the Hide Snapshot Share checkbox. • If you do not want to accept the default name provided, enter a unique name for the Snapshot Share Name field. Use up to 27 alphanumeric characters (including hyphens and spaces).

8. Click **Create Share** to complete the process.

Edit Share Properties

Once a share has been created, you can change its name, description and the advanced properties. To edit the properties, go to **Security > Shares > Share Properties** (displayed by clicking the share name in the table).



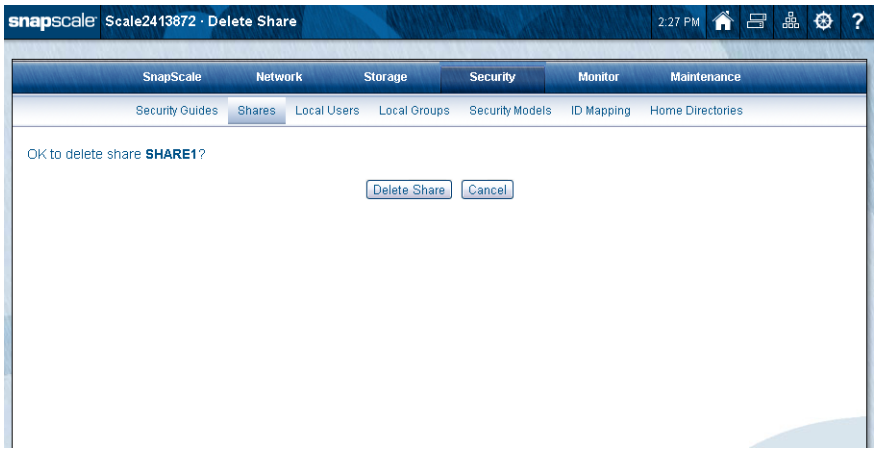
NOTE: You cannot change the volume (or path). If you need to change the volume, you must delete the share and create a new one on the other volume.

Option	Description
Name	Accept the default share name or enter a new one. If you change the default, observe the following guidelines: • Make sure the share name is unique on this cluster. • To ensure compatibility with all protocols, share names are limited to 27 alphanumeric characters (including hyphens and spaces).
Description	If desired, enter a description of the share. This is an opportunity to clarify the purpose of the share.
Hide this share	Select this option if you want the share to be hidden from network browsing using SMB and HTTP/HTTPS (but not NFS) protocols.
Protocols	Select the access protocols for the share: Windows (SMB), Linux/UNIX (NFS), or Web (HTTP/HTTPS).
Snapshot Share	The option that displays depends on whether a snapshot share currently exists. To create a snapshot share, select the Create Snapshot Share checkbox. Optionally, do either of the following: • To hide the snapshot share from the SMB and HTTP protocols (but not NFS), select the Hide Snapshot Share checkbox. • If you do not want to accept the default name provided, enter a unique name for the Snapshot Share Name field. Use up to 27 alphanumeric characters (including hyphens and spaces). To remove a snapshot share, do the following: • Select the Remove Snapshot Share checkbox.

Delete Shares

To delete a share, go to **Security > Shares > Share Properties** (displayed by clicking the share name in the table).

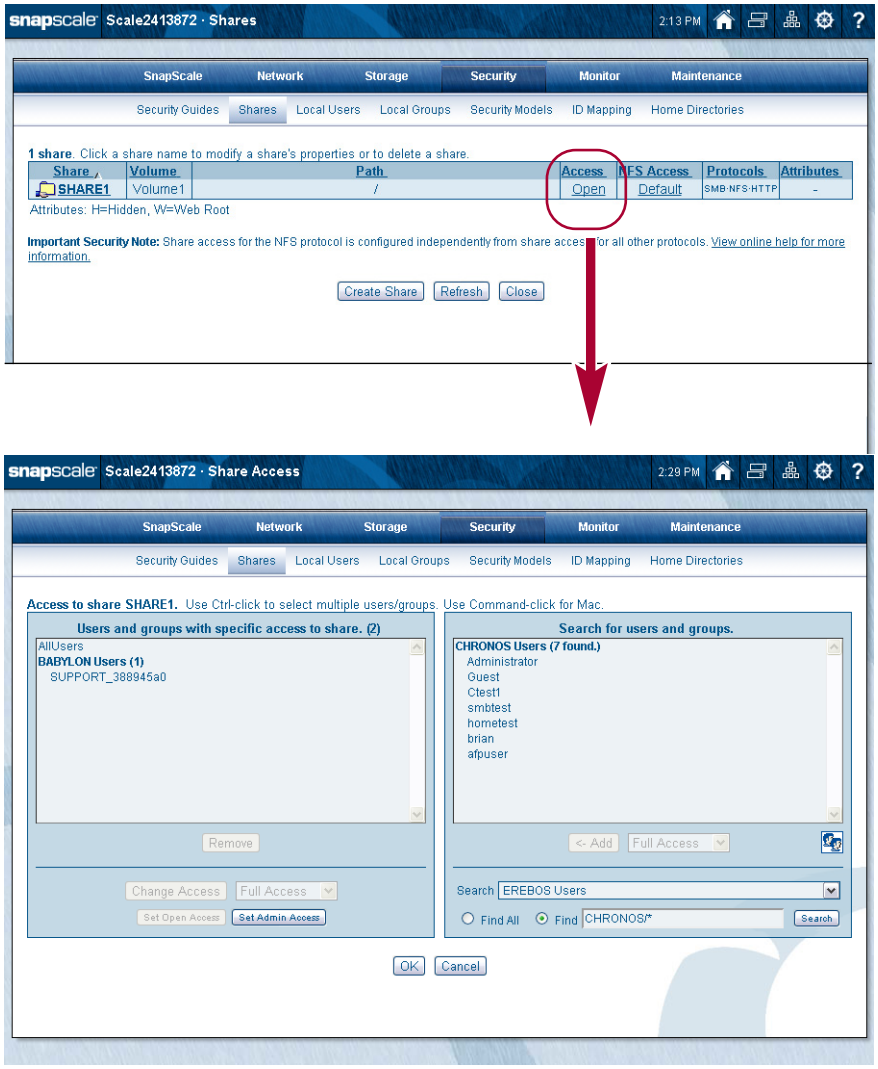
1. At the Delete Share page, click **Delete Share**.
2. At the confirmation page, click the **Delete Share** button again.



Configuring Share Access

In **Security > Shares**, in the **Access** column, click the link next to the share you want to configure. The Share Access page displays. You can set access levels for the share, as well as grant or deny access to specific users and groups.

NOTE: To add a new user to a share, you must first create the user, then add that user to the share. Please see "Local Users" for information on creating new users.



Share Access Behaviors

Administrators tasked with devising security policies for SnapScale clusters will find the following share access behaviors informative:

- **Share access defaults to full control** – The default permission granted to users and groups when they are granted access to the share is full control. You may restrict selected users and groups to read-only access.
- **User-based share access permissions are cumulative** – An SMB or HTTP user's effective permissions for a resource are the sum of the permissions that you assign to the individual user account and to all of the groups to which the user belongs in the Share Access page. For example, if a user has read-only permission to the share, but is also a member of a group that has been given full-access permission to the share, the user gets full access to the share.
- **NFS access permissions are not cumulative** – An NFS user's access level is based on the permission in the NFS access list that most specifically applies. For example, if a user connects to a share over NFS from IP address 192.168.0.1, and the NFS access for the share gives read-write access to "*****" (All NFS clients) and read-only access to 192.168.0.1, the user will get read-only access.

- **Interaction between share-level and file-level access permissions** – When both share-level and file-level permissions apply to a user action, the more restrictive of the two applies. Consider the following examples:

  Example A: More restrictive file-level access is given precedence over more permissive share-level access.

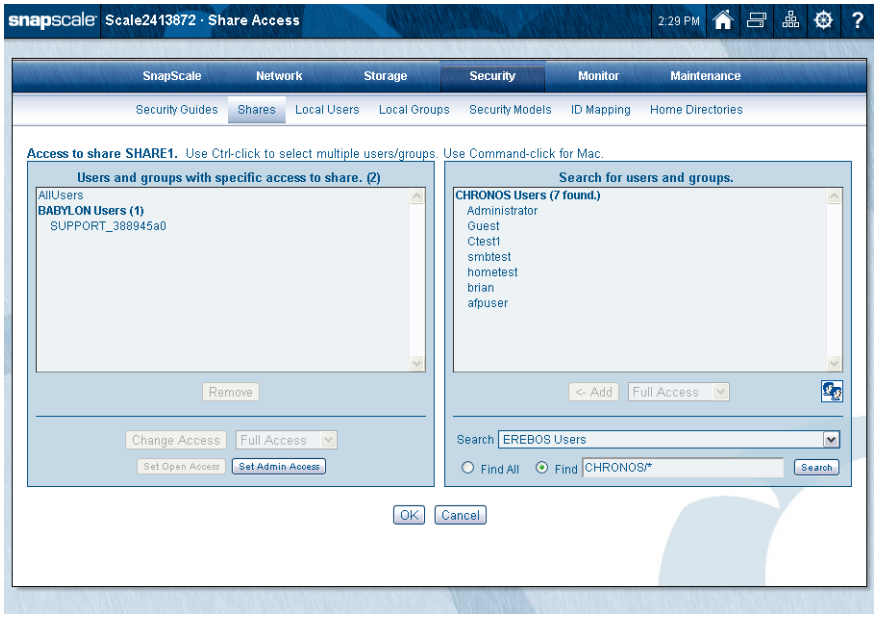
Share Level	File Level	Result
Full control	Read-only to File A	Full control over all directories and files in SHARE1 *except* where a more restrictive file-level permission applies. The user has read-only access to File A.

  Example B: More restrictive share-level access is given precedence over more permissive file-level access.

Share Level	File Level	Result
Read-only	Full control to File B	Read-only access to all directories and files in SHARE1, *including* where a less restrictive file-level permission applies. The user has read-only access to File B.

Setting User-based Share Access Permissions

Share permissions for Windows and HTTP users are configured from **Security > Shares** by clicking the link in the **Access** column of the share you want to configure. Share permissions for NFS are configured and enforced independently. See "NFS Access for Shares" for more information.



User-based share access permissions apply to users connecting over SMB or HTTP. Users and groups with assigned share access permissions appear in the list on the left (*Users and groups with specific access to share*). To search for those without assigned access, use the box on the right (*Search for users and groups*).

The default permission granted to users and groups when they are granted access to the share is Full access. You may restrict selected users and groups to Read-only access.

Share-Level Access Permissions	
Full access	Users can read, write, modify, create, or delete files and folders within the share.
Read-only	Users can navigate the share directory structure and view files.

1. Display the **Share Access** page (**Security > Shares > access_link**).
2. To **add** share access permissions for a user or group:
   a. At the bottom, using the drop-down list, select the **domain** or **local user/group list** to search.

   NOTE: For domains that require authentication (showing an "(A)" after the name), after selecting the domain name, enter the User Name and Password for that domain. The user name and password can be for any user in the domain and are used to retrieve basic information (like the user & group lists) from the domain.

   b. Enter the **search string** (or select Find All).

   When entering a search string:

   - Returned results will include all users and groups whose name **begins** with the string entered in the Search field.
   - The search results returned may be limited. Fine tune your search by using a more specific string to return the names desired.
   - On the rare occasion you need to search for a domain that is not listed ("remote domain"), select a domain from the Search drop-down list through which to search, then enter in the Find box the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, **`remote_domain\user_name`**).

   c. Click **Search** to display any matches.

   After you click Search, another authentication prompt may be presented to authenticate with the remote domain.

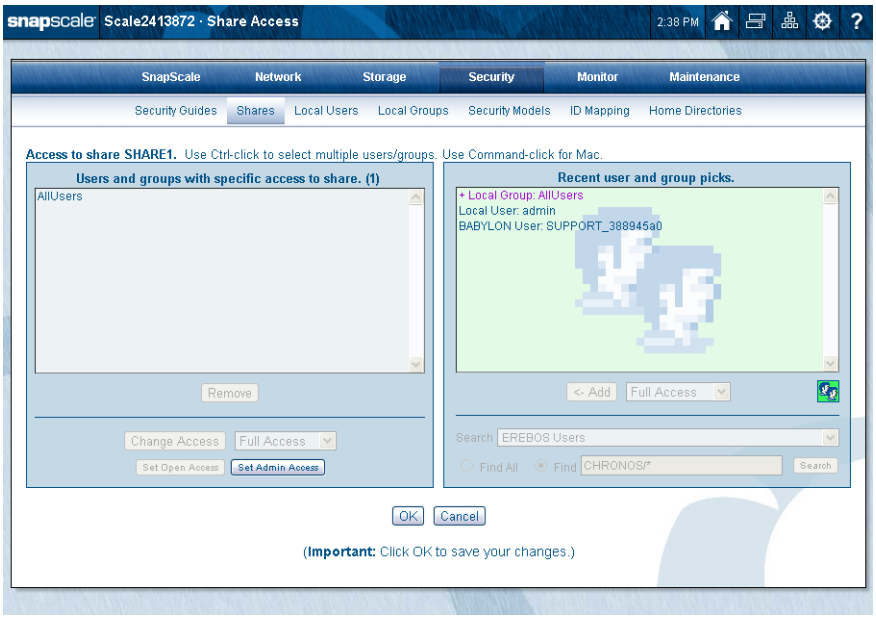
   d. Select one or more **names** in the list.

   Users that already have access are shown in purple font with a plus sign (+) in front of their name.

   e. Choose either **Full Access** or **Read Only** from the drop-down list.

   f. Click **Add**.

   NOTE: To display recent user or group picks, click the faces () icon. A list with a green background is displayed. Click the now green icon to return to the normal search box.



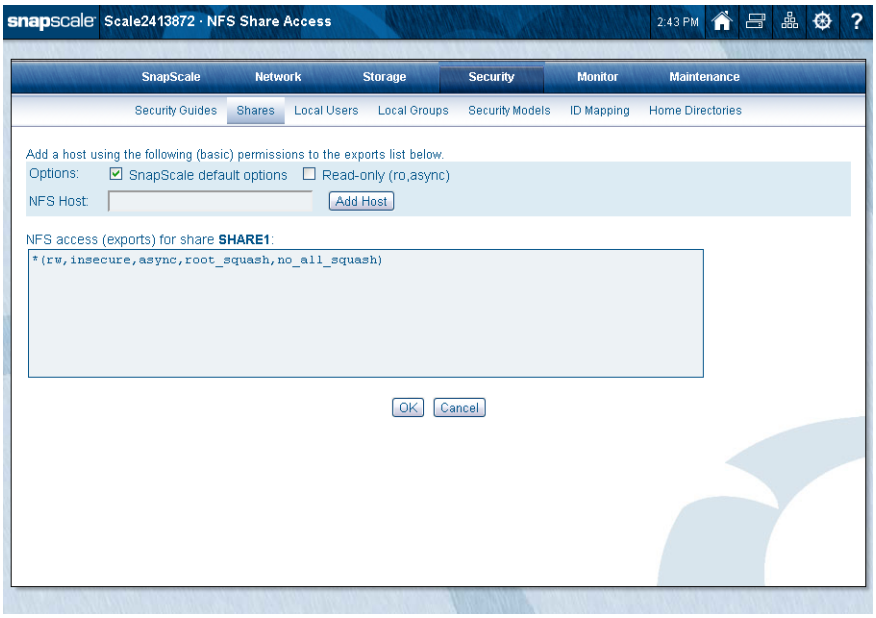
3. To **remove** share access permissions for a user or group:
   a. Select one or more **users or groups** in the left box.
   b. Click **Remove**.
4. To change **access permissions** for a user or group, select one or more users or groups in the left box, then select either **Full Access** or **Read Only** from the drop-down list, and click the **Change Access** button.
5. To quickly specify either Open or Admin-only **access** for the entire share, click either the **Set Open Access** or **Set Admin Access** button.
6. Click **OK** to save share permissions.

NFS Access for Shares

NOTE: Multiple shares pointing to the same target directory must have the same NFS access settings. The Web Management Interface applies the same NFS access for all shares pointing to the same directory.

Click the link in the **NFS Access** column next to the share you want to configure. The NFS Share Access page is displayed. You can configure NFS access to the share using standard Linux "exports" file syntax.

On the Shares page, click the name of the access type listed in the NFS Access column to open the NFS Share Access page.



The NFS Access text box is a window into the client access entries in the cluster's *exports* file. This file serves as the access control list for filesystems that may be exported to NFS clients. You can use the Add Host controls as described below to assist in making entries to the file, or you can directly edit the text box. After all entries are made, click **OK** to return to the **Security > Shares** page.

NOTE: The syntax used in this file is equivalent to standard Linux exports file syntax. If the cluster detects any errors in syntax, a warning message appears. You can choose to correct or ignore the error warning.

The Exports File Default Options. The default entry provides read-write access to all NFS clients.

```
*(rw,insecure,async,root_squash,no_all_squash)
```

The entry options are explained in the following table:

Entry Code	Meaning
Asterisk	All NFS clients
ro	The directory is shared read only (ro).
rw	The client machine will have read and write (rw) access to the directory.
insecure	Turns off the options that require requests to originate on an Internet port less than IPPORT_RESERVED (1024).
root_squash	Forces users connected as root to interact as the "nobody" user (UID 65534). This is the RAINcloudOS default.

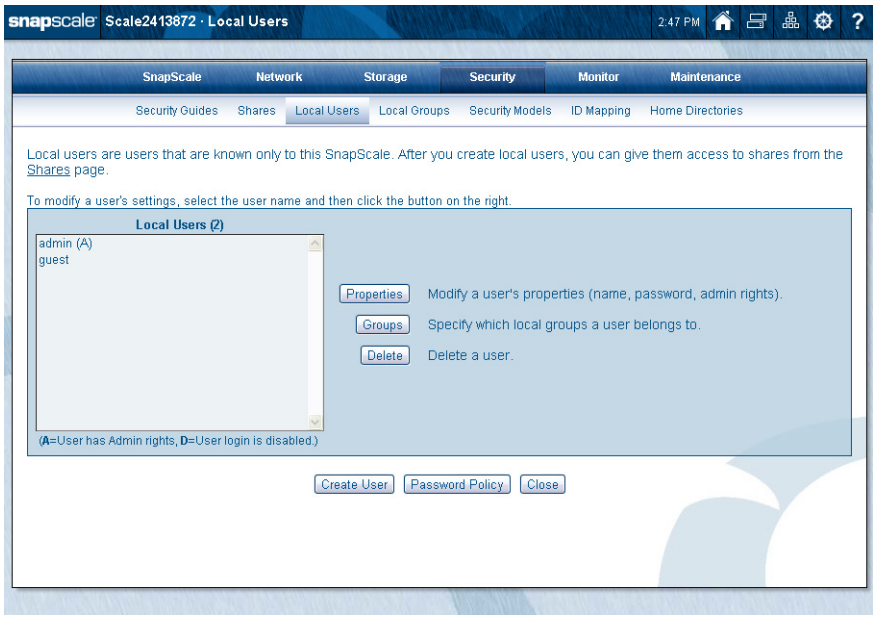
Entry Code	Meaning
no_root_squash	no_root_squash means that if root is logged in on your client machine, it will have root privileges over the exported filesystem. By default, any file request made by user root on the client machine is treated as if it is made by user nobody on the cluster. (Exactly which UID the request is mapped to depends on the UID of user nobody on the cluster, not the client.) If no_root_squash is selected, then root on the client machine will have the same level of access to the files on the system as root on the cluster. This can have serious security implications, although it may be necessary if you want to perform any administrative work on the client machine that involves the exported directories. You should not specify this option without a good reason.
async	Tells a client machine that a file write is complete – that is, has been written to stable storage – when NFS has finished handing the write over to the filesystem.
no_all_squash	Allows non-root users to access the nfs export with their own privileges.

Using the Add Host Controls. Follow these steps:

1. Select **one** of the following options:
   - **SnapScale Default Options** – Inserts the default options as described above
   - **Read Only** – Inserts the read only option only
   - **Both** – Inserts default options, but substitutes read only for read/write
2. Do **one** of the following in the NFS host text box:
   - **To apply the options to all NFS hosts** – Leave this field blank
   - **To apply the options to specific hosts** – Enter one or more IP addresses.
3. Click **Add Host**.

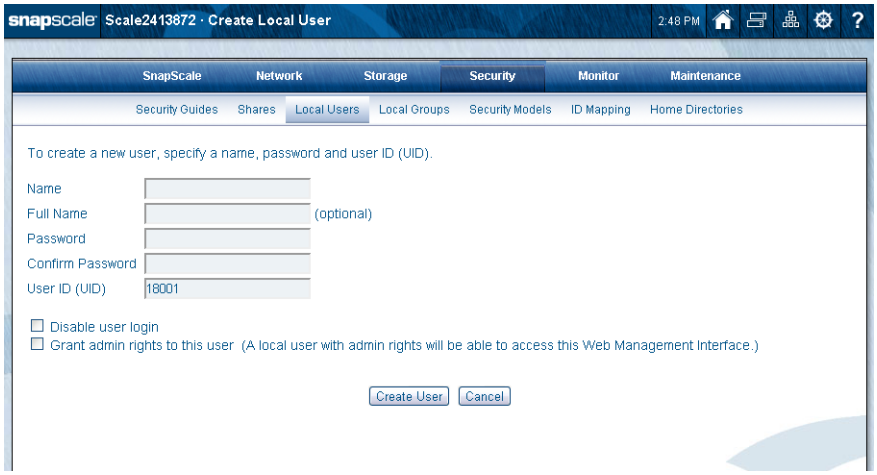
Local Users

The Local Users page (**Security > Local Users**) provides all the options to manage local users. Local users are users that are known only to the cluster being accessed. Each SnapScale cluster comes with two predefined users: admin and guest. The admin user has full Administrator rights. Go to **Security > Local Users** to view settings or make changes.



Create a User

Click the **Create** button to create a new user on this cluster. Enter the user data, select any special options, and click the **Create User** button again.



To Create a Local User

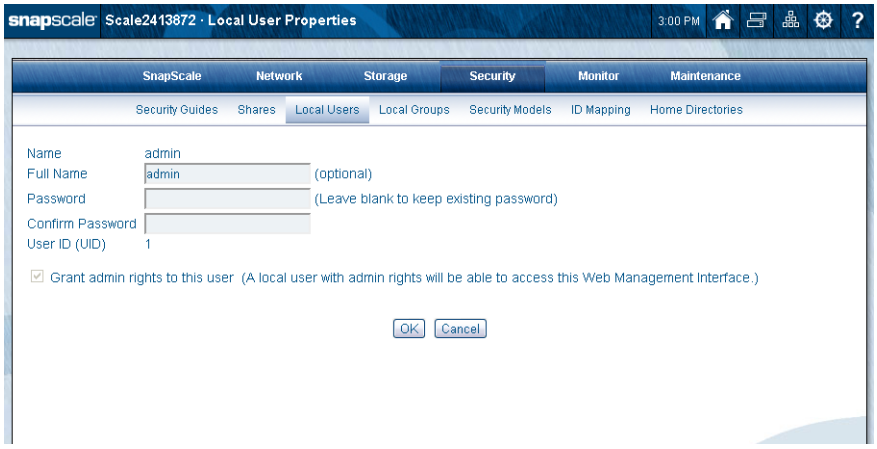
1. On the **Local Users** page, click **Create**.
2. On the **Create Local User** page that opens, enter the requested **information**:

Option	Description
Name	Use up to 31 alphanumeric characters and the underscore.
Full Name	Use up to 49 alphanumeric characters (includes spaces). Input in this field is optional.
Password	Passwords are case-sensitive. Use up to 15 alphanumeric characters without spaces.
Password Verify	Type the chosen password again for verification.
User ID (UID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see "User and Group ID Assignments."
Disable User Login	Select this checkbox to disable the user login. The user's information will remain in the system, but login rights are denied. The user login can be enabled by deselecting the checkbox. This checkbox can also be used to enable a user locked out by the *Disable login after n attempts* password policy.
Exempt from Password Expiration and Character Requirements	This checkbox is only visible if Password Policy is enabled. Select this checkbox to exempt this user from password expiration and character requirement policies.
Grant Admin Rights To This User	Select this checkbox to allow the user access to the Web Management Interface and SSH (for access to the CLI and backup agent installation.

3. Click **Create User** again to create the user account.

Edit User Properties

Use the **Properties** button to open the Local User Properties page to make changes.



To Edit Local User Properties

1. On the **Security > Local Users** page, select the user you want to edit and click **Properties**.
2. On the Local User Properties page that opens, enter or change the following **information**:

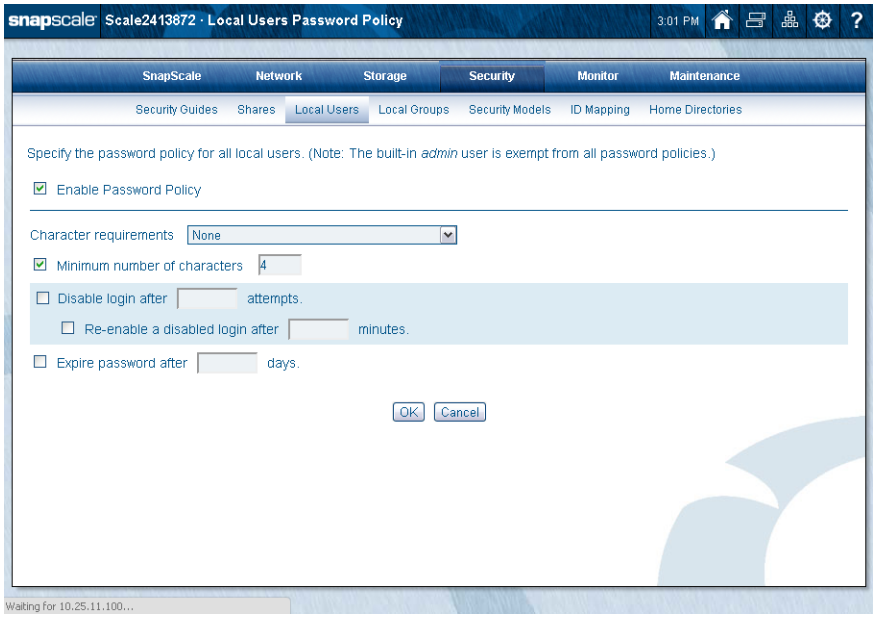
Option	Description
Name	Cannot be modified.
Full Name	Use up to 49 alphanumeric characters (includes spaces). Input in this field is optional.
Password	Passwords are case-sensitive. Use up to 15 alphanumeric characters. Leave this field blank to keep the existing password.
Password Verify	Type the chosen password again for verification. Leave this field blank to keep the existing password.
User ID (UID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see "User and Group ID Assignments." NOTE: Changing a user's UID may alter filesystem access permissions that apply to that UID. In addition, any existing permissions for a UID previously assigned to a user that are changed to a different UID may become active if another user is created with the same UID. Carefully consider security configuration on existing files and directories before changing the UID of a user.
Disable User Login	Select this checkbox to disable the user login. The user's information will remain in the system, but login rights are denied. The user login can be re-enabled by deselecting the checkbox. This checkbox can also be used to enable a user locked out by the *Disable login after n attempts* password policy.
Exempt from Password Expiration and Character Requirements	NOTE: This checkbox is only visible if Password Policy is enabled. Select this checkbox to exempt this user from password expiration and character requirement policies.
Grant Admin Rights To This User	Select this checkbox to allow the user access to the Web Management Interface and SSH (for access to the CLI and backup agent installation).

3. Click **OK**.

User Password Policies

NOTE: Local users can be individually exempted from password expiration and character requirements. This may be necessary for some special users, such as users configured to perform backups. See "To Create a Local User" for procedures to set password policy for local users. Also, the built-in *admin* user is automatically exempt from all password policies.

Click the **Password Policy** button to make changes to all the local user password settings.



To Set Password Policy for Local Users

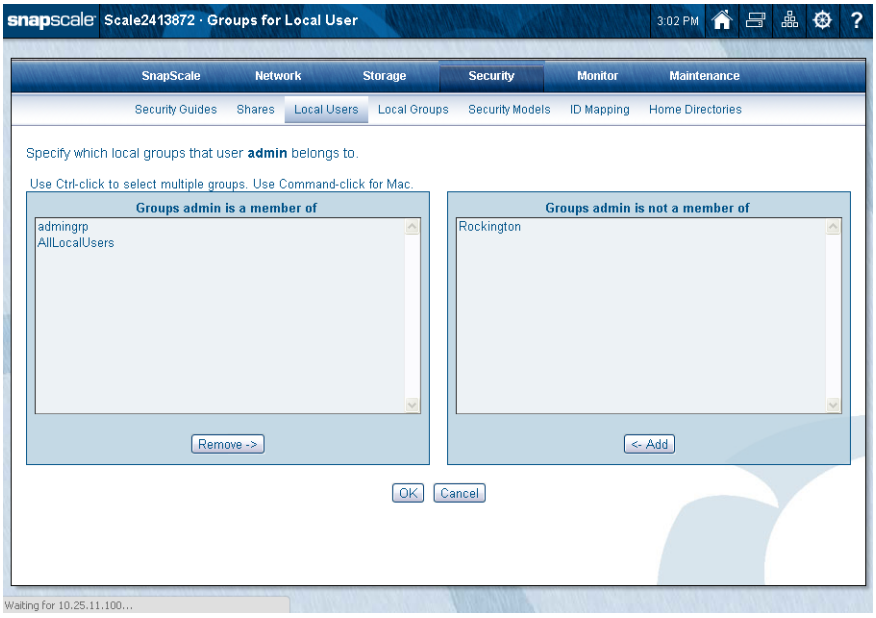
1. On the **Security > Local Users** page, click the **Password Policy** button.
2. On the Local Users Password Policy page, check the **Enable Password Policy** box.
3. Enter the following **information**:

Option	Description
Character Requirements	Select the alpha/numeric/special character requirements for the password from the drop-down list.
Minimum Number of Characters	Check the checkbox to enable the policy, then enter the minimum number of characters required for the password.
Disable Login After *n* Attempts	Check the checkbox to enable the policy, then enter the number of times a user can fail to login before the system locks the user out. This applies to failed logins when connecting to any node in the cluster. NOTE: To unlock a user, clear the Disable User Login checkbox for the user in the Local Users page.
Re-enable a Disabled Login After *n* Minutes	If you have defined a limit to the number of times a user can fail to log in, you can also check this checkbox and enter a time period after which the system will allow the user to log in again. NOTE: This saves the administrator from having to manually re-enable the user.
Expire Password After *n* Days	Check the checkbox to enable the policy, then enter the number of days before the password must be changed. NOTE: Local users with expired passwords can change their passwords at: http://<clustername>/changepassword.

4. Click **OK** to save the settings and return to the Local Users page.

Assign User to Group

Use the Groups for Local User page (**Security > Local Users > Groups**) to make changes to a local group membership.



To Add or Remove Users from Groups

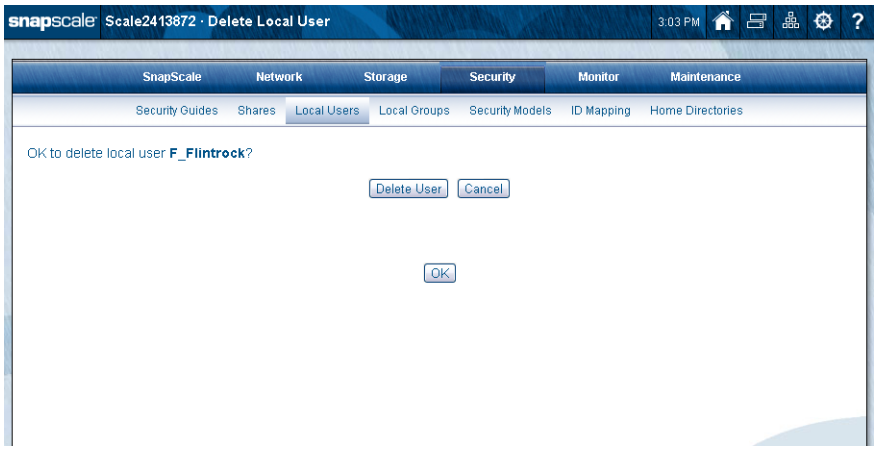
1. On the **Groups for Local User** page, select a **user**.
2. Click **Groups**.
   The group settings for the selected user are shown.
3. To add the user to a group, select the group from the right-side list and click **Add**.
4. To delete the user from a group, select the group from the left-side group and click **Remove**.
5. Click **OK** to save your changes and return to the Local Users page.

Delete Local User

On the Local Users page, use the following process to remove a user.

To Delete a Local User

1. On the **Security > Local Users** page, select the user to be deleted.
2. Click **Delete**.
   The confirmation page is displayed.
3. Click **Delete User** to delete the selected user (or click **Cancel**).

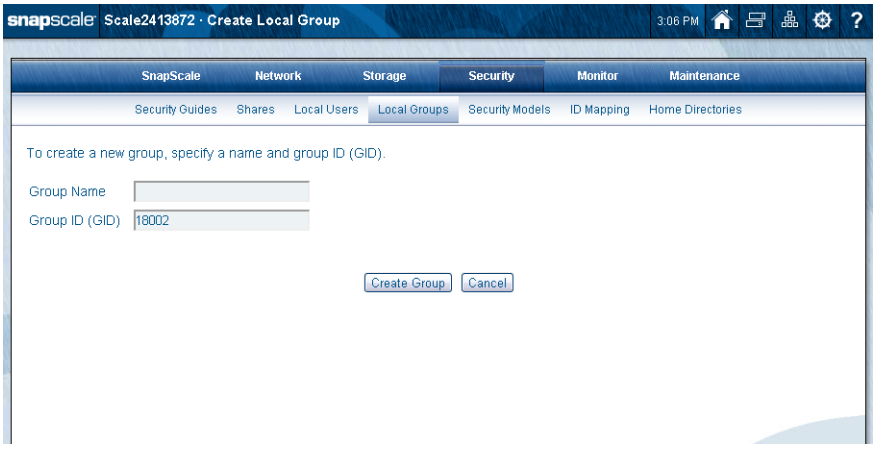


Local Groups

The Local Groups page (**Security > Local Groups**) provides all the options to manage local groups. Local groups are groups of local users that are known only to the cluster being accessed. Each SnapScale cluster comes with one predefined group: admingrp.

Create New Group

Click the **Create** button to create a new group on this cluster. Enter the group name, accept or change the Group ID (GID), and click the **Create Group** button.



To Create a New Local Group

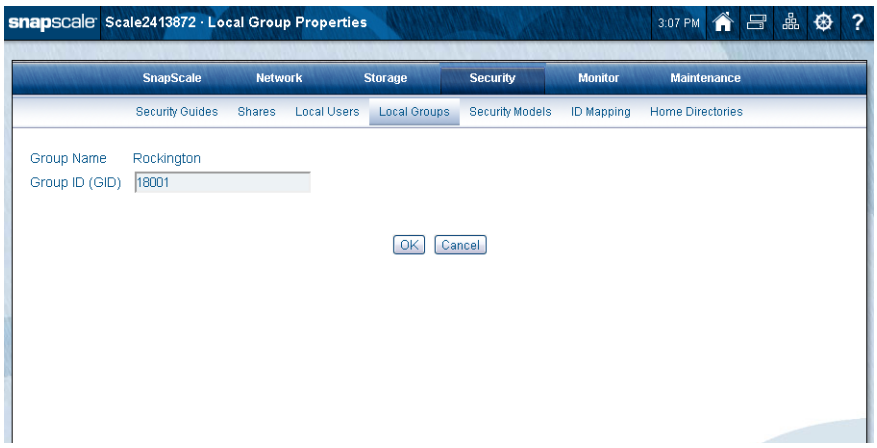
1. On the **Local Groups** page, click **Create**.
2. On the **Create Local Group** page that opens, enter the following information:

Option	Description
Group Name	Use up to 31 alphanumeric characters and the underscore.
Group ID (GID)	Displays the user identification number assigned to this user. Alter as necessary. For information on available UID ranges, see "User and Group ID Assignments."

3. Click **Create Group** when finished. The Users for Local Group page is displayed, allowing you to add users to your new group.
4. Click **Close** when you are finished with local groups.

Edit Group Properties

Use the **Properties** button to open the Local Group Properties page to make changes to the options there.



To Edit Local Group Properties

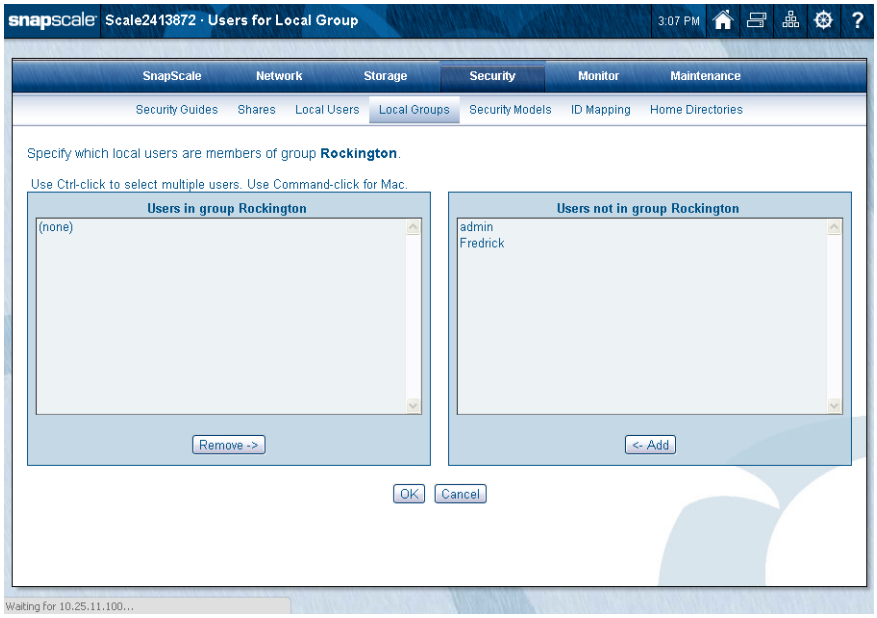
1. On the **Security > Local Groups** page, select the group you want to edit and click **Properties**.
2. On the page that opens, you can change the GID. For information on available UID ranges, see "User and Group ID Assignments."

   NOTE: Changing a group's GID may alter filesystem access permissions that apply to that GID. In addition, any existing permissions for a GID previously assigned to a group that are changed to a different GID may become active if another group is created with the same GID. Carefully consider security configuration on existing files and directories before changing the GID of a group.

3. Click **OK**.

Specify Users in Group

Use the Users for Local Group page (**Security > Local Groups > Users**) to make changes to a local group membership.



To Add or Remove Group Users

1. After creating a new group, or when editing an existing group, add and remove users by selecting the desired group and clicking **Users**.
2. Add users by selecting the user and clicking **Add**.
3. Delete users by selecting the user and clicking **Remove**.
4. Click **OK** when finished.

Delete Group

1. On the **Local Groups** page, select the group to be deleted and click **Delete**.
   The confirmation page is displayed.
2. Click **Yes** to delete the selected group, or click **No** to cancel the deletion.

Security Models

There are two file-level security models that can be used by a SnapScale cluster: Windows/Mixed and UNIX. The security model can only be configured on the volumes.

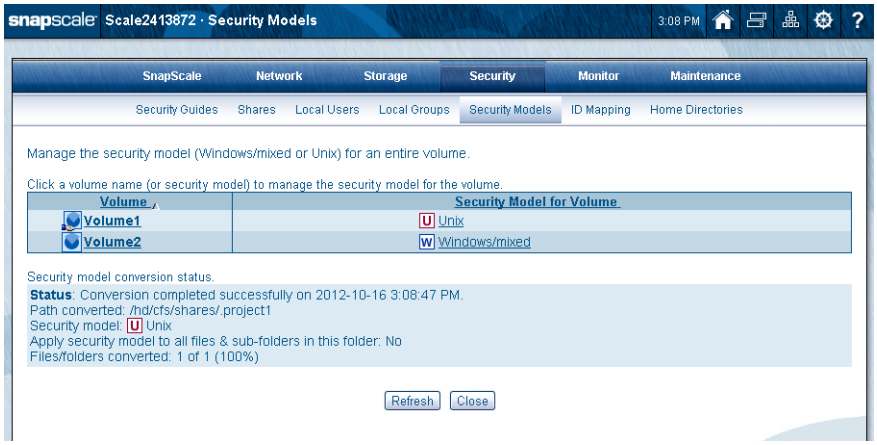
The security model determines the rules regarding which security personality that is present on files and folders created by the various protocols and clients, and whether the personality of files and folders can be changed by changing permissions.

Folders created in a volume default to the security model of that volume. The folder's security model may differ from the personality of the folders (for example, folders with a Windows/Mixed security may have a UNIX personality).

For more information about security models, see Appendix B, "Security and Access."

Managing Volume Security Models

1. Select **Security > Security Models**.

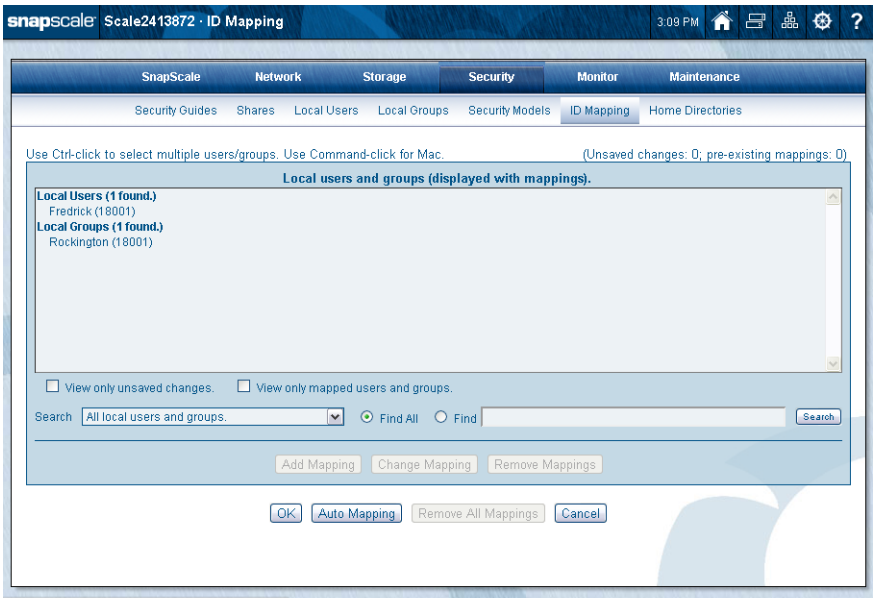


2. Click the **security model name** (Windows/Mixed or UNIX).
3. From the drop-down list, select the **security model type** desired, and click **OK**.
4. At the confirmation message, click **Apply Security Model**.

   If there are files and directories under the volume, you are prompted whether you want to recursively apply the change. When done, the main page displays a conversion status.

ID Mapping

ID mapping allows users and groups that exist on Windows domains to share user IDs with local or NIS users and groups. This results in the same permissions and quota consumption applying to both the Windows domain user and the local or NIS user.



Example: John Smith is a local user on a SnapScale cluster, as well as having a user ID on a Windows domain. John's quota for the cluster has been set to 200 MB. The administrator of the cluster maps the Windows domain user's UID for John Smith to the local UID for John Smith, giving both users access to John's 200 MB.

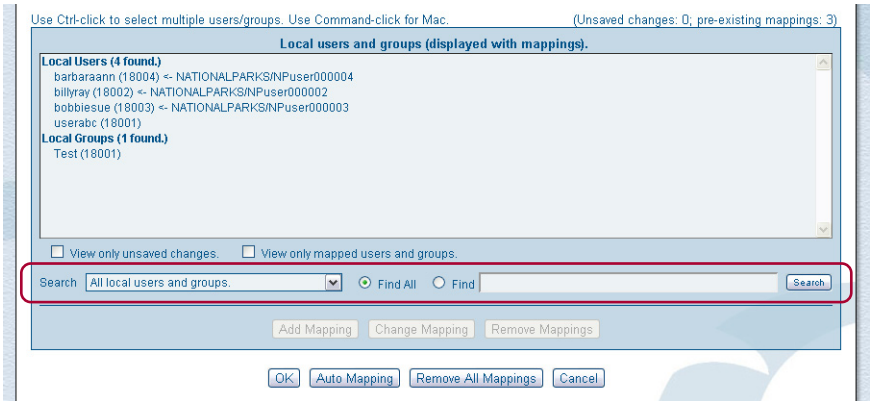
Select a local or NIS user or group from the displayed list on the default page. You can then click **Add Mapping** to map the user's UID or group's GID to that of a Windows domain user or group. **Change Mapping** is used to change existing mappings. **Remove Mappings** removes one or more mappings while **Remove All Mappings** removes all mappings that had been previously established.

To simplify the discovery of a desired user or group to manage their ID mapping search options are presented at the bottom of the selection pages. On the search results page, you can narrow the list by using the following options:

- Check **View only unsaved changes** to display only mapping changes that have not yet been applied.
- Check **View only mapped users and groups** to display only local or NIS users and groups that have been mapped to a Windows domain user or group.

Add Mapping

1. If the desired user or group to be mapped to does not appear in the default page list, use the **search option** to locate them.



a. At the bottom of the list, using the Search drop-down list, select the **local or NIS user or group list** to search.

b. Enter the **search string** (or select Find All).

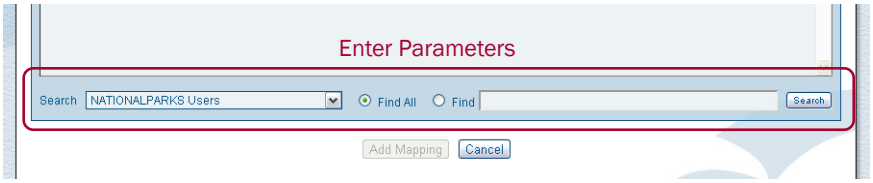
Enter the exact **name** (or a string with a wildcard "*" before or after).

c. Click **Search** to display any matches.

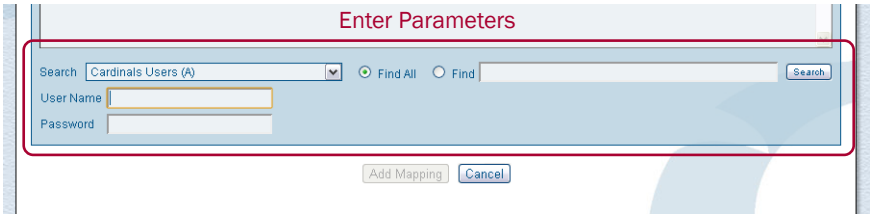
2. Select a user or group from the results list, and click **Add Mapping**.

3. At the Add Mapping page, select the Windows domain **user or group** list, and click **Search**.

- To search for a specific user or group, use either Find All or a Find search string (wildcard "*" before or after allowed).

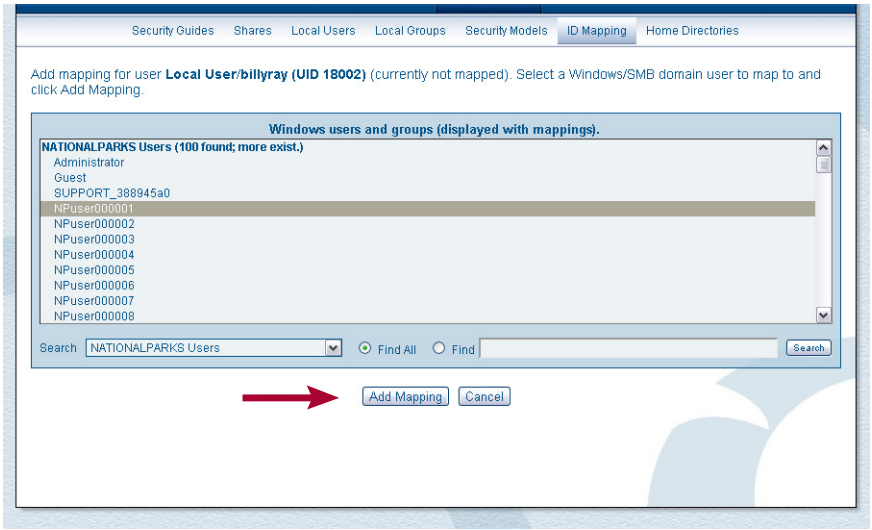


- For domains that REQUIRE authentication (showing an "(A)" after the name), select the domain name, enter the User Name and Password for that domain, and use either Find All or a search string (use the beginning of the user/group name).

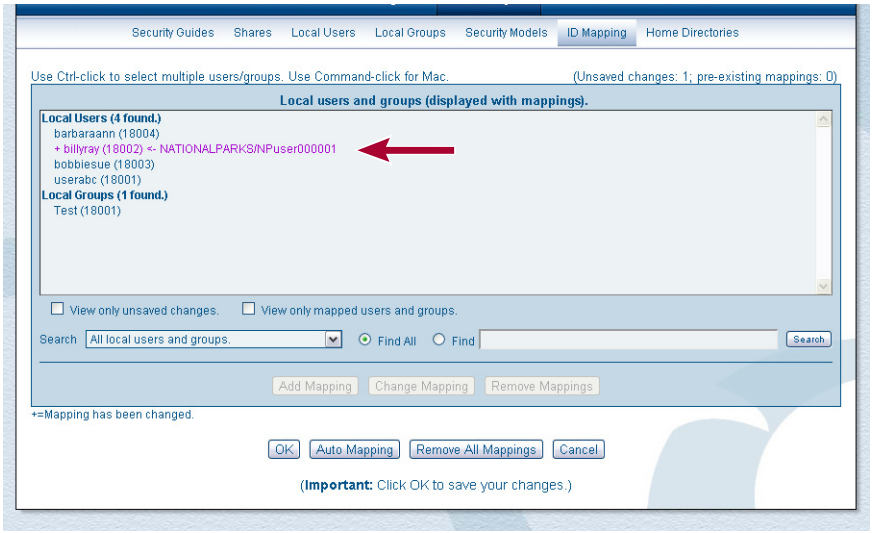


- On the rare occasion you need to search for a Windows domain that's not listed ("remote domain"), select a Windows domain from the Search drop-down list through which to search, then enter in the Find box the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, **`remote_domain\user_name`**). After you click Search, another authentication prompt may be presented to authenticate with the remote domain.

4. From the search results, select the Windows domain user you want to map the local or NIS user to, and click **Add Mapping**.



The mapping result is shown on the default page.



Check **View only unsaved changes** to display only changes that have not yet been applied. Check **View only mapped users and groups** to display only local or NIS users or groups that have been mapped to a Windows domain user or group.

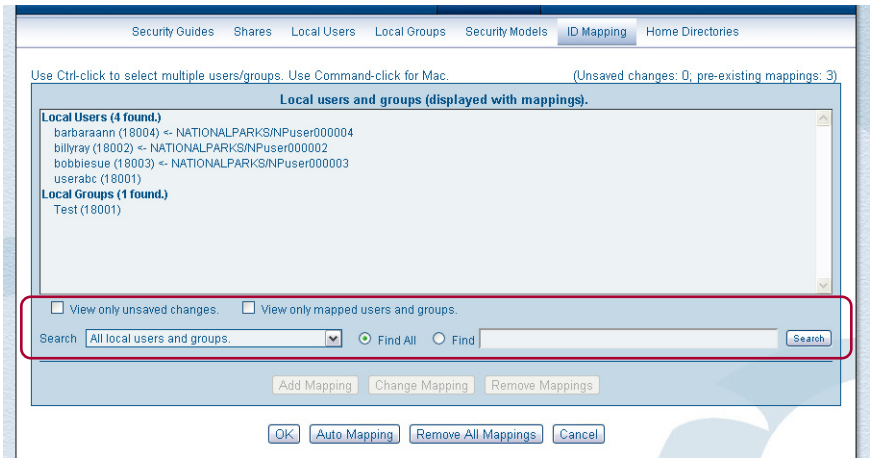
5. Repeat Steps 1–4 to add any other mappings.
6. Save your **changes**:
   a. Click **OK** to save changes (or Cancel to reset).
   b. At the confirmation page, click **Save Changes**.
   c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.
      See "Filesystem Updates" for more details.

IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Change Mapping

To re-map a mapped local or NIS user or group to a different Windows domain user or group:

1. If the desired user or group to be changed does not appear in the default page list, use the **search option** to locate them.



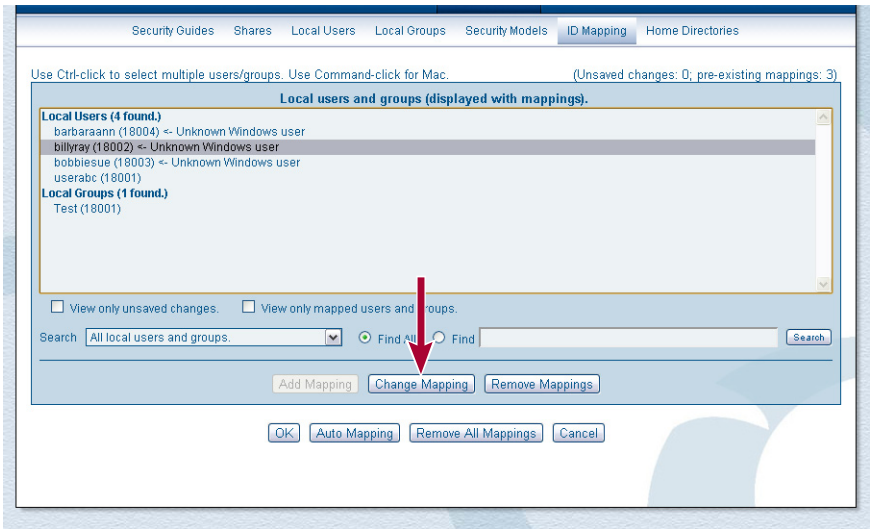
   a. At the bottom of the list, using the Search drop-down list, select the **local or NIS user or group list** to search.

   b. Enter the **search string** (or select Find All).

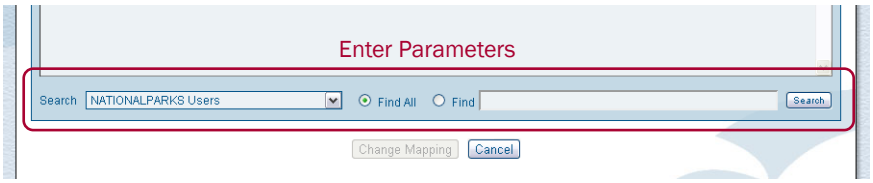
      Enter the exact **name** (or a string that uses the beginning characters of the user/group name).

   c. Click **Search** to display any matches.

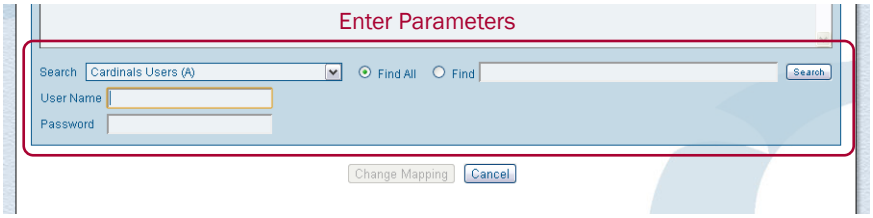
2. Select a mapped user or group to be changed, and click **Change Mapping**.



3. At the Change Mapping page, select the Windows domain **user or group** list, and click **Search**.
   - To search for a specific user or group, use either Find All or a Find search string (wildcard "*" before or after allowed).

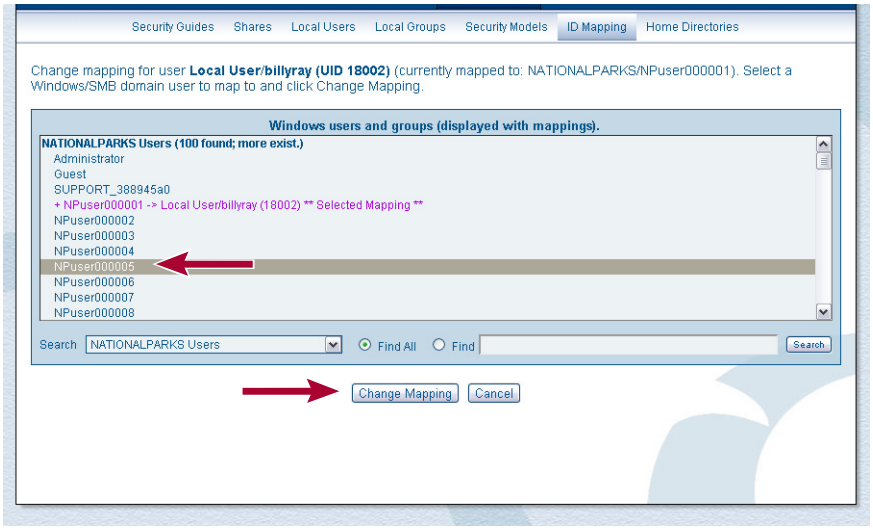


   - For domains that REQUIRE authentication (showing an "(A)" after the name), select the domain name, enter the User Name and Password for that domain, and use either Find All or a search string (use the beginning of the user/group name).



   - On the rare occasion you need to search for a Windows domain that's not listed ("remote domain"), select a Windows domain from the Search drop-down list through which to search, then enter in the Find box the name of the remote domain, followed by a slash (/) or backslash (\) and the user name for which you are searching (for example, **`remote_domain\user_name`**). After you click Search, another authentication prompt may be presented to authenticate with the remote domain.

4. From the search results, select a Windows/SMB domain user to map to and click **Change Mapping**.



5. Repeat Steps 1–4 until all **changes** are made.
6. Save your **changes**:
   a. Click **OK** to save changes (or Cancel to reset).
   b. At the confirmation page, click **Save Changes**.

c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

See "Filesystem Updates" for more details.

IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

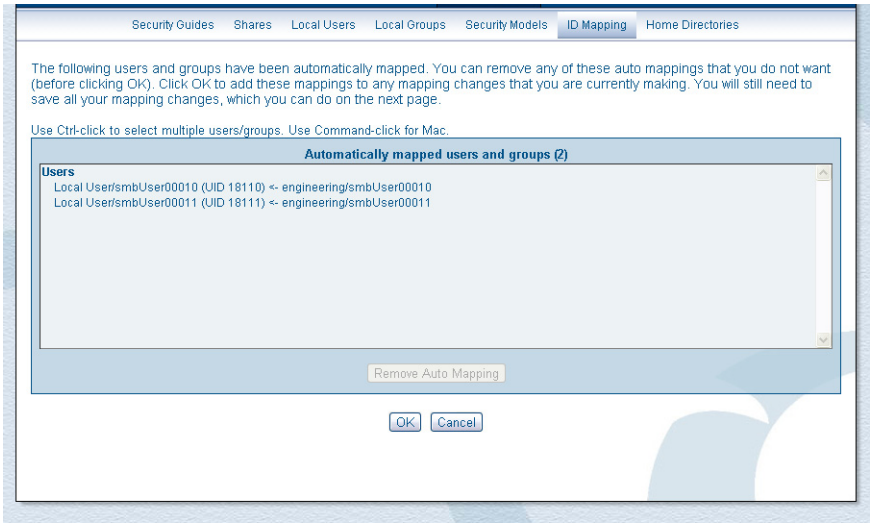
Auto Mapping

1. Click **Auto Mapping** to generate a list of Windows domain users/groups that have the same name as your Local or NIS users and groups:

   Domain, local, and NIS user/group lists are compared. The matches are automatically queued. Users and groups already mapped are not affected

2. At the Auto Mapping confirmation page, click **View Auto Mappings** to continue.

   A page is displayed summarizing your changes.



3. Save your **changes**:

   a. Click **OK** to save changes (or Cancel to reset).

   b. At the confirmation page, click **Save Changes**.

   c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

   See "Filesystem Updates" for more details.

IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove Mappings

User mappings can be removed individually or all at once. Once removed, they can not be restored but must be added back using "Add Mapping." You also have the option to update the filesystem after removing the ID mappings.

Remove a Mapping

1. At the default page, select one or more users/groups you wish to unmap and click **Remove Mappings**.

   Check **View only mapped users and groups** to display only local or NIS users or groups that have been mapped to make it easier to find ones to remove.

2. At the Remove Mappings page, verify the users/groups on the list, and click **Remove Mappings**.

   The mappings are removed and the default page is displayed.

3. Repeat Steps 1–2 until all **changes** are made.
4. Save your **changes**:
   a. Click **OK** to save changes (or Cancel to reset).
   b. At the confirmation page, click **Save Changes**.
   c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.

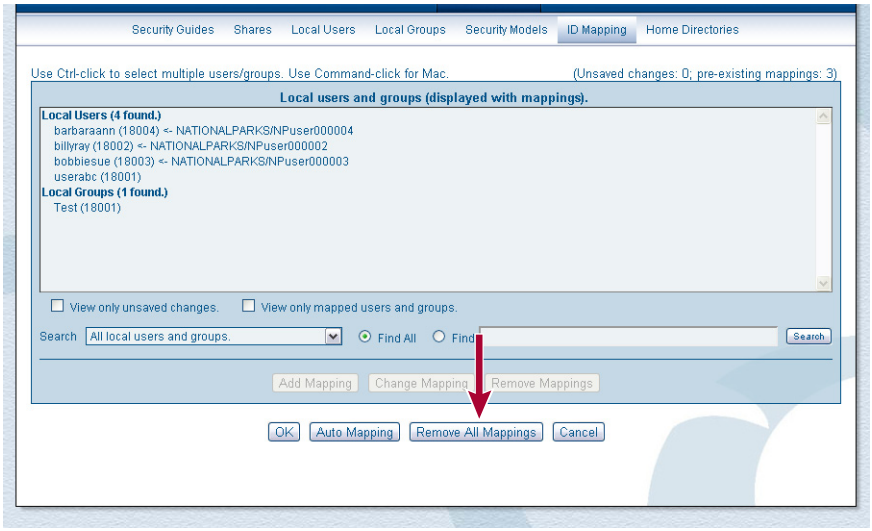
      See "Filesystem Updates" for more details.

> IMPORTANT: Updating may take some time, depending upon how many files and folders are on your cluster storage. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove All Mappings

The **Remove All Mappings** button allows you to remove all ID mappings on the cluster. Click this only if you want to remove all ID mappings. If there are no mappings, the button is grayed out.

1. At the default page, click the **Remove All Mappings** button.



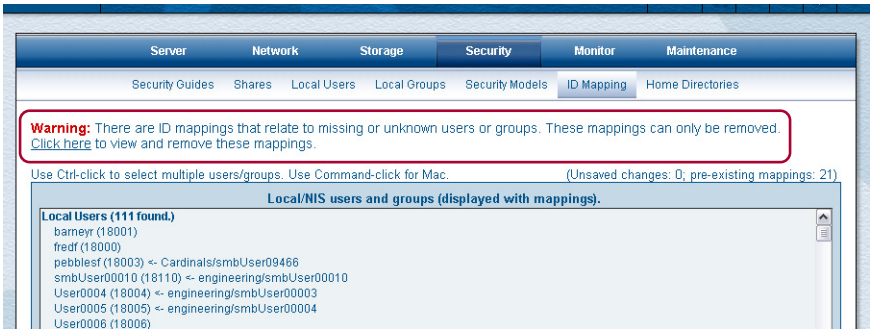
Check **View only unsaved changes** to display only mapping changes that have not yet been applied. Check **View only mapped users and groups** to display only local or NIS users/groups that have been mapped to a Windows domain user or group.

2. A confirmation page appears. Click **Remove All Mappings**.
3. Save your **changes**:
   a. Click **OK** to save changes (or Cancel to reset).
   b. At the confirmation page, click **Save Changes**.
   c. At the filesystem update option page, choose either **Update Filesystem** or **Do Not Update Filesystem**.
   See "Filesystem Updates" for more details.

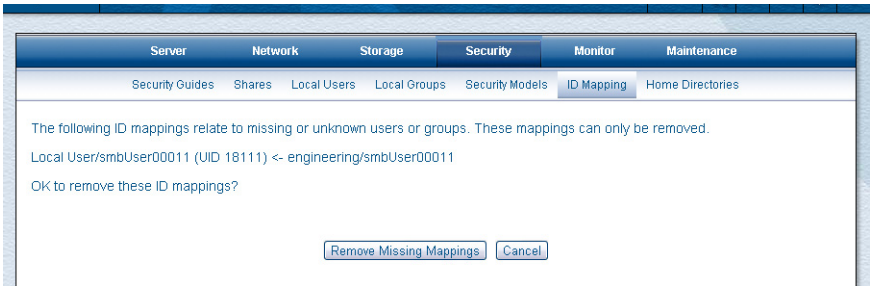
IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Remove Missing ID Mappings

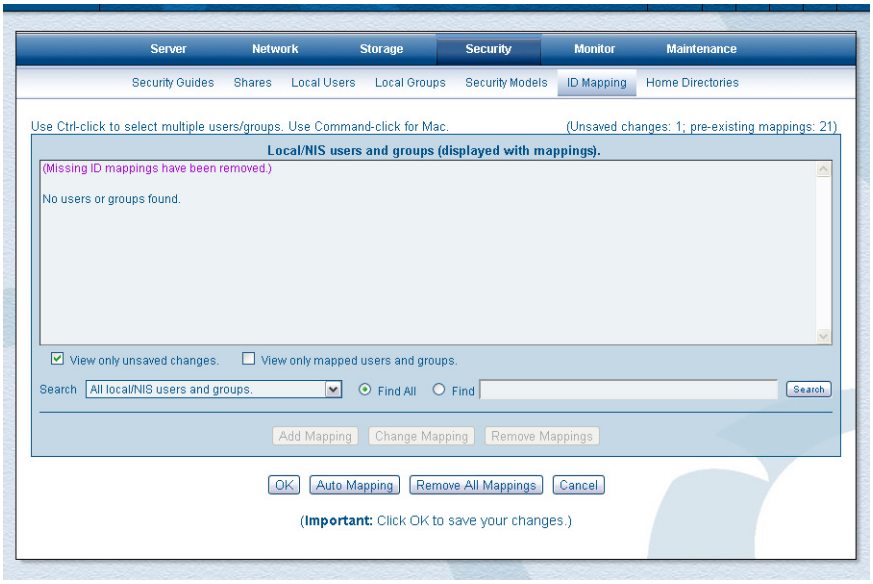
If the cluster has mappings for users or groups that no longer exist, the following warning message may be displayed at the top of the main ID Mappings page:



1. Click the **Click here** link in the warning message to display the following page:



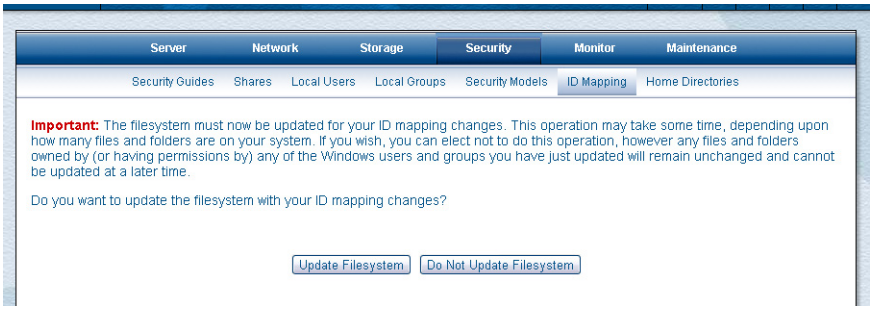
2. Click **Remove Missing Mappings** to clear them from the system. A confirmation is shown on the ID Mapping main page.



3. Click **OK** to save changes.

Filesystem Updates

After making any changes to ID mappings, you are presented with a filesystem update option page, where you can choose either **Update Filesystem** or **Do Not Update Filesystem** options.



If you choose Update Filesystem, UID and GID ownership on files and SIDs in ACLs are updated to reflect the ID mapping operation.

IMPORTANT: Updating may take some time, depending upon how many files and folders are on your system. If you elect not to do this operation, any files and folders owned by (or having permissions by) any of the Windows users and groups you have just updated will remain unchanged and cannot be updated at a later time.

Home Directories

To enable Home Directories, go to Security > Home Directories and check Enable Home Directories. Choose the volume, path, and protocols you want.

The Home Directories feature creates a private directory for every local or Windows domain user that accesses the system. When enabling Home Directories (from the Security > Home Directories page), the administrator creates or selects a directory to serve as the home directory root. When a user logs in to the cluster for the first time after the administrator has enabled Home Directories, a new directory named after the user is automatically created inside the home directory root, and is configured to be accessible only to the specific user and the administrator.

Depending on the protocol, home directories are accessed by users either via a user-specific share, or via a common share pointing to the home directory root.

Home directories are supported for SMB, NFS, and HTTP/HTTPS. They are accessed by clients in the following manner:

- For SMB and HTTP/HTTPS, users are presented with a virtual share named after the user name. The virtual share is visible and accessible only to the user. Users are not limited only to their virtual shares; all other shares on the cluster continue to be accessible in the usual fashion.
- For NFS, the home directory is exported. When a user mounts the home directory root, all home directories are visible inside the root, but the user's home directory is accessible only by the user and the administrator.

NOTE: If desired, UNIX clients can be configured to use a Snap Home Directory as the local user's system home directory. Configure the client to mount the home directory root for all users, and then configure each user account on the client to use the user-specific directory on the SnapScale as the user's home directory.

If ID Mapping is enabled, domain users and local users mapped to the same user are directed to the domain user's home directory. In some cases, data in the local user's home directory is copied to the domain user's home directory:

- If a local user home directory accumulates files before the local and domain users are mapped, and if the domain user's home directory is empty, the local user's files are copied to the domain user's home directory the first time the local user connects after the users are mapped.
- If both the local and domain user home directories accumulate files before the local and domain users are mapped, the files in the local user's home directory are not copied to the domain user's home directory.

Configure Home Directories

Complete the following fields and click OK.

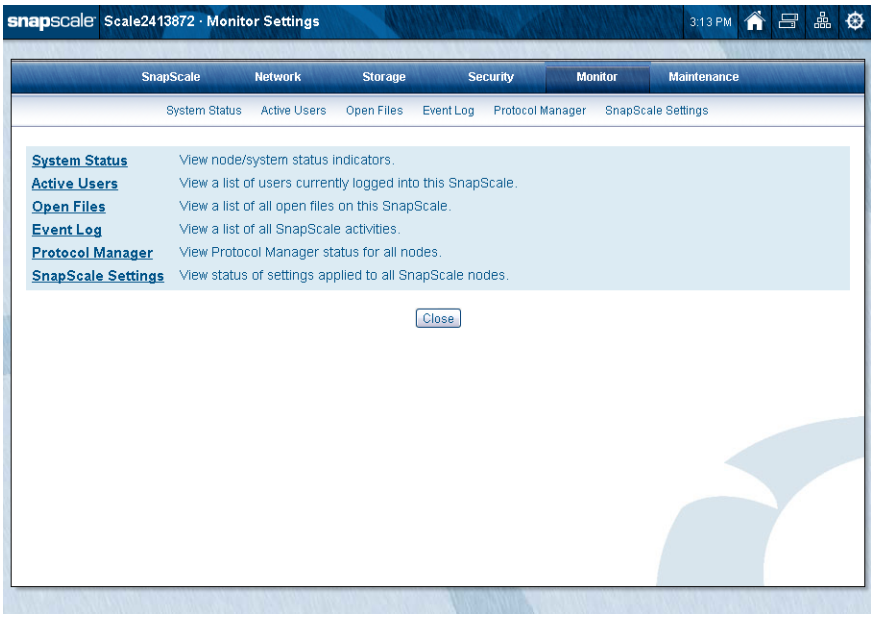
Field	Description
Enable Home Directories	Check to enable Home Directories for local users. Remove the check to disable.
Volume	Select the volume where the Home Directories will be located. NOTE: Be sure the volume you select has enough disk space. Once Home Directories are placed, they cannot be moved.
Path	Provide the path to the Home Directories or click Browse to create a new folder. The default path is **`/home_dir/`**.
Protocols	Check each of the protocols where Home Directories will be enabled.

NOTE: Do not put Home Directories on a volume that might be deleted. If you delete the volume, you will also delete the Home Directories.

Chapter 6

System Monitoring

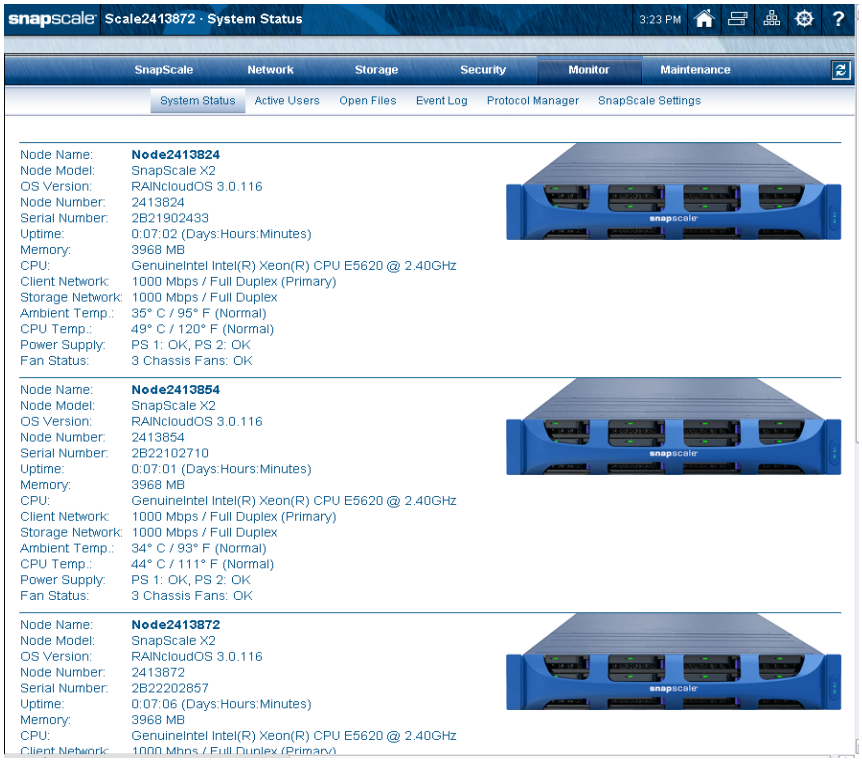
This chapter addresses the options for monitoring the SnapScale cluster. Here you can view the system status and other activities.



Topics in System Monitoring:

System Status

Use the System Status page (**Monitor > System Status**) to assess the hardware status of the cluster member nodes.



SnapScale Status

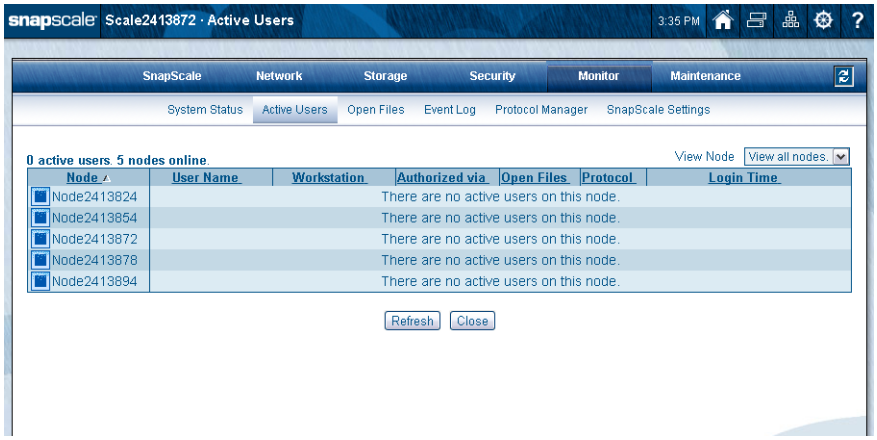
The following status fields are displayed for each node that is part of the SnapScale cluster. Any critical messages are displayed in **red**.

Field	Description
Node Name	Name of the node: Node*nnnnnnn* (where *nnnnnnn* is your node number). Example: Node2302216.
Node Model	Node hardware model.
OS Version	The version of RAINcloudOS currently loaded on the node.
Node Number	Number derived from the MAC address of *Ethernet 1* port that is used as part of the node name.
Serial Number	Unique number assigned to the node.
Uptime	The amount of time the node has been up (since the last reboot) in "days:hours:minutes" format.
Memory	Amount of system RAM.
CPU	The type of central processing unit for the node's first CPU.
Client Network	Details on the node's client Ethernet connections.
Storage Network	Details on the node's storage Ethernet connections.
Ambient Temp.	The temperature of the space inside the chassis.

Field	Description
CPU Temp.	Current CPU temperature.
Power Supply	The status of power supply modules
Fan Status	The status of fan modules.

Active Users

Use this page to view read-only details on the active users logged on to each of the nodes on the cluster.

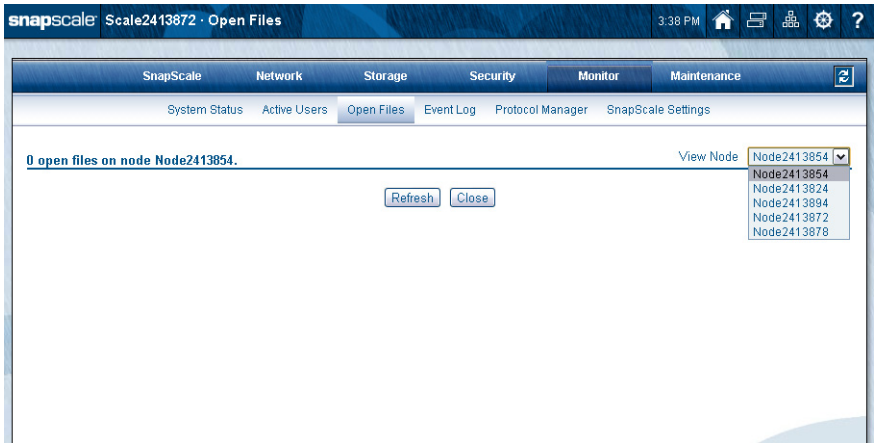


Information available on this page includes user names of all active users, their workstation names, authorization, the number of open files they have on the node, the protocol, and when they logged on. Columns can be sorted in ascending or descending order by clicking the column head.

NOTE: Active users are not displayed for HTTP or NFS.

Open Files

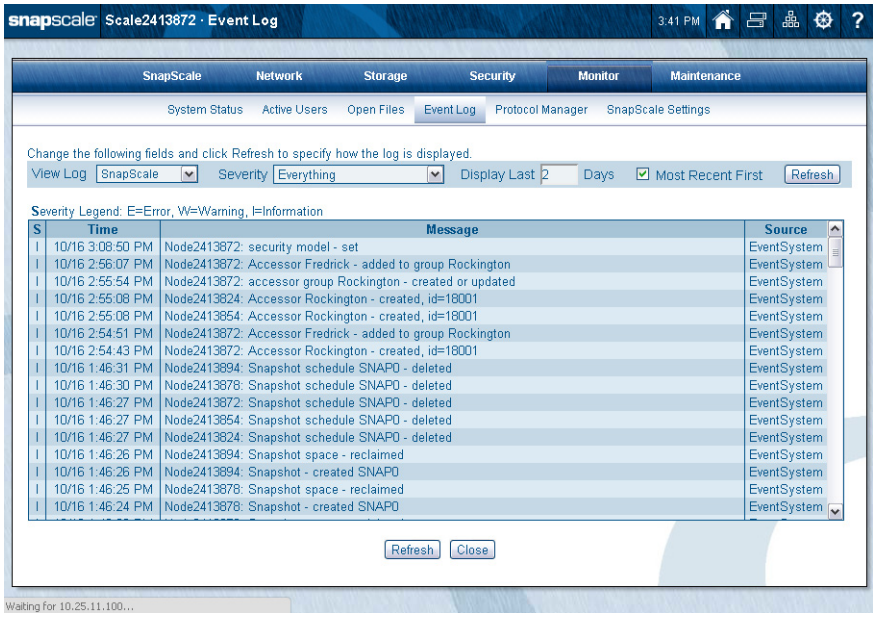
Use this page to view read-only details on the open files on a specific node.



Use the drop-down list on the right to choose a different node to view.

Event Log

Use the **Event Log** page to view a log of operations performed on the cluster.



Entries are color coded according to severity as described in the following table:

Background Color	Entry Type
Red	Error (E)
Yellow	Warning (W)
(no color)	Informational or Unclassified (I)

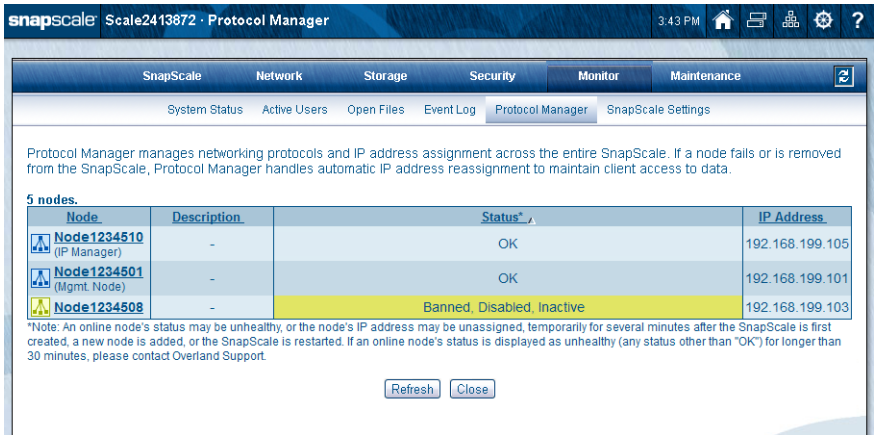
Filter the Log

Edit the following fields as appropriate, then click **Refresh**.

Option	Description
View Log	Select to view either the SnapScale cluster-wide or node-specific logs. The SnapScale option shows general cluster-related log messages while the node-specific options show log messages specific to the selected node.
Severity	Select the type of alerts and information you want to view.
Display Last *n* Days	Enter the number of days' worth of entries you want to view.
Most Recent First	Check this box to start the list with the most recent entry; deselect to start the list with the oldest entry.

Protocol Manager

Protocol Manager manages networking protocols and IP address assignment across the entire SnapScale. If a node fails or is removed from the SnapScale, Protocol Manager handles automatic IP address reassignment to maintain client access to data.



The following table addresses the possible status:

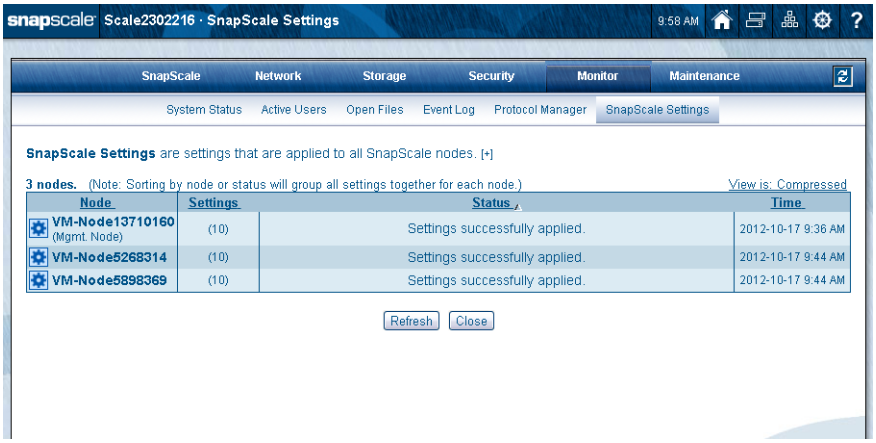
Status	Description
OK	This node is fully functional.
Disconnected	This node could not be connected through the Storage network and is currently not participating in the cluster. If there is a public IP address associated with this node it should have been taken over by a different node. No services are running on this node.
Banned	This node failed too many recovery attempts and has been banned from participating in the cluster temporarily. Any public IP addresses have been taken over by other nodes.
Disabled	This node has been administratively disabled. This node is still functional and participates in the cluster but its IP addresses have been taken over by a different node and no services are currently being hosted.
Unhealthy	A service provided by this node is malfunctioning. The node itself is operational and participates in the cluster, however its public IP addresses have been taken over by a different node and no services are currently being hosted.
Stopped	A node that is stopped does not host any public IP addresses, and does not participate in the cluster.
PartiallyOnline	A node that is partially online participates in the cluster like a node that is OK. Some interfaces which serve public IP addresses are down, but at least one interface is up.

SnapScale Settings

When cluster settings are configured in the Web Management Interface, success or failure of the operation is determined by the attempt to perform it on the Management node. If successful, the same configuration operation is pushed to all member nodes in the background.

The SnapScale Settings page displays a list of settings that have been applied to the nodes in the cluster and the status of each setting. When you make changes to your SnapScale via the Web Management Interface, the settings are applied to the Management node first to determine success or failure of the configuration, then the settings are applied to the other nodes in the background. When a SnapScale setting has not been applied yet, its status is displayed as **Pending**. When a SnapScale setting fails to be applied, its status is displayed in detail and the failed settings are automatically re-applied until they are successful.

The initial view is compressed to show all nodes and a count of the settings:



Click the upper right text that says "View is: Compressed" to expand the view:

Node	Settings	Status	Time
VM-Node13710160 (Mgmt. Node)	Security Model	Settings successfully applied.	2012-09-20 11:57 AM
	Users & Groups	Settings successfully applied.	2012-10-15 6:37 PM
	Volumes	Settings successfully applied.	2012-09-19 9:03 AM
	Shares	Settings successfully applied.	2012-09-20 1:20 PM
	Share Access	Settings successfully applied.	2012-09-19 9:19 AM
	Server	Settings successfully applied.	2012-09-18 1:34 PM
	NFS Exports	Settings successfully applied.	2012-09-19 9:19 AM
	Email	Settings successfully applied.	2012-09-17 5:13 PM
	NTP	Settings successfully applied.	2012-09-20 2:31 PM
	Profiles	Settings successfully applied.	2012-10-17 9:36 AM
VM-Node5268314	Security Model	Settings successfully applied.	2012-09-20 11:57 AM
	Users & Groups	Settings successfully applied.	2012-10-17 9:44 AM
	Volumes	Settings successfully applied.	2012-09-19 9:03 AM
	Shares	Settings successfully applied.	2012-09-20 1:20 PM
	Share Access	Settings successfully applied.	2012-09-19 9:19 AM
	NFS Exports	Settings successfully applied.	2012-09-19 9:19 AM
	Server	Settings successfully applied.	2012-09-18 1:34 PM
	Email	Settings successfully applied.	2012-09-17 5:13 PM
	NTP	Settings successfully applied.	2012-09-20 2:30 PM
	Profiles	Settings successfully applied.	2012-10-17 9:36 AM
VM-Node5898369	Security Model	Settings successfully applied.	2012-09-20 11:57 AM
	Users & Groups	Settings successfully applied.	2012-10-17 9:44 AM
	Volumes	Settings successfully applied.	2012-09-19 9:03 AM
	Shares	Settings successfully applied.	2012-09-20 1:20 PM
	Share Access	Settings successfully applied.	2012-09-19 9:19 AM
	Server	Settings successfully applied.	2012-09-18 1:34 PM
	NFS Exports	Settings successfully applied.	2012-09-19 9:19 AM
	Email	Settings successfully applied.	2012-09-17 5:14 PM
	NTP	Settings successfully applied.	2012-09-20 2:31 PM
	Profiles	Settings successfully applied.	2012-10-17 2:36 AM

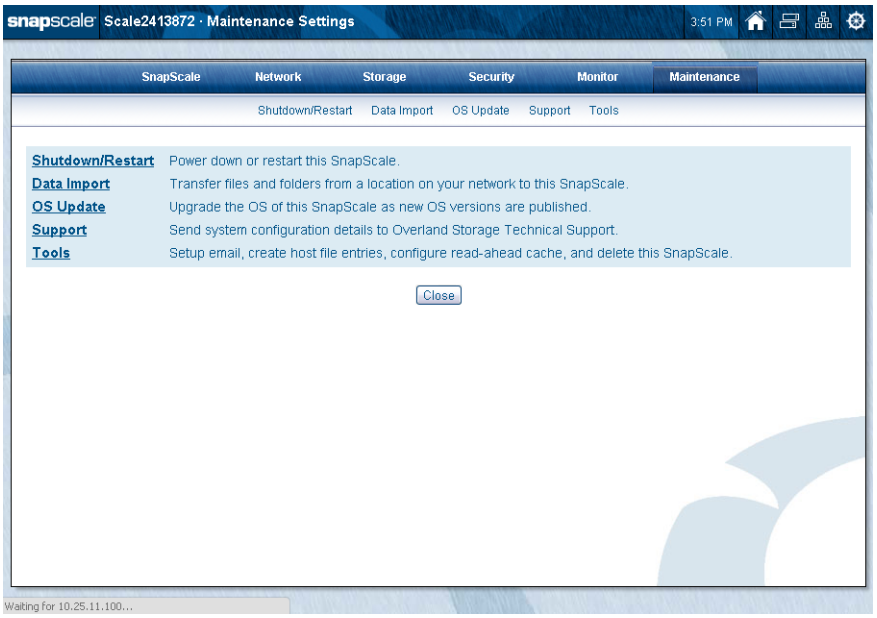
In expanded mode, detailed information on each node is available:

- Each line reports the setting category, status, and date/time the setting was applied.
- If an operation is still in progress on a node, the Status will be set to **Pending** with a yellow background.
- If an operation failed on a node, the Status will have an error message and a red background.
- Column headers can be clicked to sort by Node, Settings, Status, or Time.
- When sorting by Status or Node, settings are grouped by node.

Click the "View is: Expanded" text to revert back to the compressed view. The displayed view from that point on will be the last view selected. Clicking the column heading resorts the table on that function.

Maintenance

Clicking the **Maintenance** tab on the Web Management Interface displays options used to maintain this SnapScale cluster.

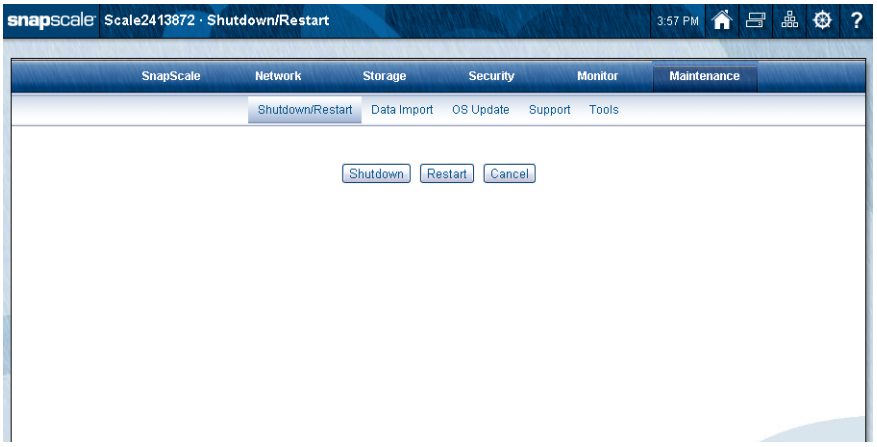


Topics in Web Management Interface

- Shutdown and Restart
- Data Import
- OS Update
- Support
- Maintenance Tools
  - Email Notification
  - Host File Editor
  - Read-Ahead Cache
  - Delete SnapScale Cluster

Shutdown and Restart

Use the **Shutdown/Restart** page to reboot or shut down the cluster.



Click one of the following buttons:

- **Shutdown** – Shuts down and powers off all nodes in the cluster.
- **Restart** – Reboots the cluster via a controlled shutdown and restart.

Manually Powering Nodes On and Off

CAUTION: To prevent possible data corruption or loss, it is NOT recommended to directly power down any nodes that are part of a SnapScale cluster. When powering down a cluster, always use the **Shutdown** button that can be found under **Maintenance > Shutdown/Restart** in the Web Management Interface.

Use the power button on the front to power ON and power OFF a node:

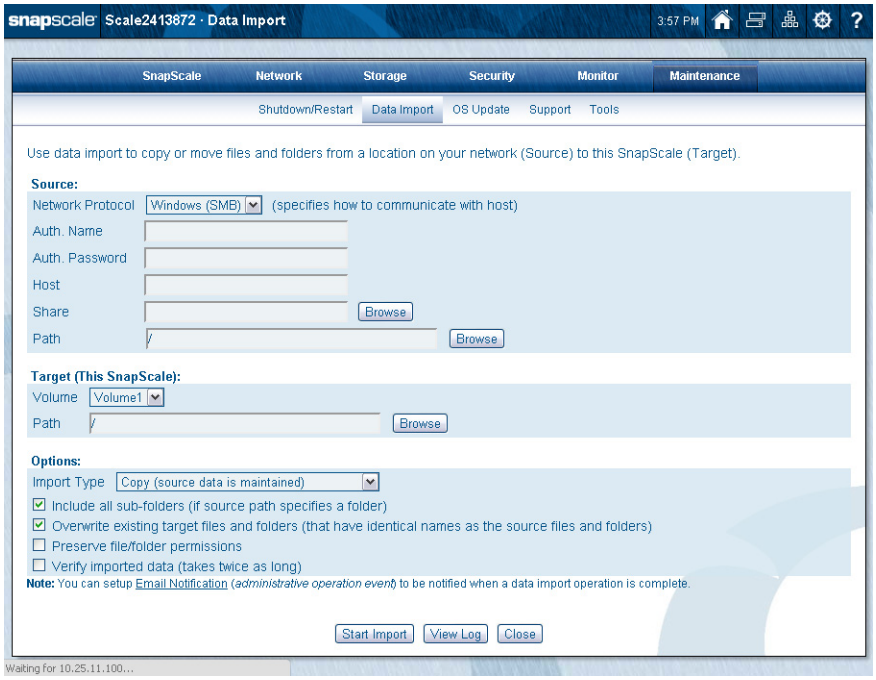
- To turn the node ON, press the power button on the front of the node.

  The node takes a few minutes to initialize. A green system/status LED indicates when the system is up and running.
- To turn the node OFF, press and release the power button to begin the shutdown process. Do not depress this button for more than four seconds.

NOTE: All SnapScale nodes have a persistent power state. When a physical loss of power occurs, the node returns to the same operation being performed when the power went out. Therefore, if the node is powered down prior to a power loss, it will remain powered down when the power is restored, and if it was powered on prior to a power loss, it will power back on when power is restored.

Data Import

Use the **Data Import** page to import (migrate) data from another SnapScale cluster or other computer that supports CIFS or NFS (v2 or v3) to this cluster. To access the Data Import utility, navigate to **Maintenance > Data Import**.



If an error is encountered during the import (for example, a file or folder is locked and cannot be imported), the utility records the error in a log, and continues the operation. When the import is completed, the administrator can view the log of import errors. Once the errors have been corrected, the administrator can return to the main page, and recreate the import. With the exception of the password, all fields are still be populated with the specifications of the last job.

The following data import options can be specified:

- Import type: copy or move data
- Include subfolders
- Overwrite existing files
- Preserve the original permissions settings

  NOTE: If you elect to preserve original permissions settings, review "Preserving Permissions".

- Verify imported data

  NOTE: If you elect to verify imported data, all data is read twice, once for import and once for comparison to the copied data. This could be a lengthy process.

Setting Up a Data Import Job

Before setting up a data import job, be sure to specify a user identity for the operation that has full access to all files on the source, regardless of permissions set:

- For Windows import, specify an administrator or member of the Windows server/domain administrators group.

- For NFSv2/3 import, consider using the user root, and configuring the NFS export on the source to **`no_root_squash`** for the IP Address of the node for the duration of the import.

NOTE: Only one import job can run at a time.

To create a data import job, perform the following procedure:

1. On the **Data Import** page, complete the required **information** for both the source and target.

Option	Description
Source:	
Network Protocol	Protocol that the node uses to connect to the source server. Use the drop-down list to select: • **Windows (SMB)** – Uses SMB for Windows with the source data on a Windows root directory. Default option. NOTE: If you are importing via SMB, SMB must also be enabled on the target node (enable at Network > Windows/SMB). • **NFS** – NFSv2/3 for UNIX/Linux-based servers or RAINcloudOS nodes with source data on a UNIX root directory.
Auth. Name & Auth.Password / User Name	• For the Windows (SMB) network protocol, enter both the **Auth. Name** and **Auth. Password** (Windows user name and password to log in to the server over SMB). • For the NFS network protocol, enter the **User Name** (node local user name or NIS user, representing the UID used to perform the operation over NFS).
Host	Enter the name or IP address of the source computer you are importing data from.
Share/Export	Specify the share (Windows) or export (NFS) on the source server containing the data you want to import. NOTE: Wildcards are not supported when specifying the source share to import.
Path	Enter the path to the file or folder you want to import. If you are importing the entire share, you can leave the Path field blank. NOTE: Wildcards are not supported when specifying the path to import.
Target (The SnapScale):	
Volume	Specify the cluster volume where you want the data imported.
Path	Specify the path to the directory where you want the data imported.
Options:	
Import Type	Options for the import data are to **Copy** (source data is maintained) or **Move** (source data is removed during copy). If **Verify imported data** is enabled, the Move option removes the original data after the verification is complete. The default is Copy. NOTE: If you select to Move rather than Copy data, it is strongly recommended that you also select the Verify imported data option.

Option	Description
Include All Sub-folders	If the folder you select for import contains subfolders, selecting this option imports all files and folders underneath this folder (checked by default). If disabled, *only* the files in this folder are imported.
Overwrite Existing Target Files & Folders	If any files/folders on the target have identical names with files/folders on the source, checking this option overwrites those files/folders during import (checked by default.)
Preserve File/Folder Permissions	Selecting this option retains the source permissions when the files/folders are imported to the target (unchecked by default). NOTE: Before selecting this option, review Preserving Permissions.
Verify Imported Data	Selecting this option causes all source data to be read twice, once to write to the target and once to perform a binary comparison with the data written (unchecked by default). If enabled, and if the Import Type is **Move**, files on the source are only removed after verification. Otherwise, files are removed during the process of copying them to the target. If you select to move files rather than copy them, it is strongly recommended that you enable the **Verify imported data** option. If a file mismatch occurs during verification, the target file is moved to a *data_import_verify_failures* directory on the root of the same volume. Check the failed file to determine the problem, then run the import again with **Overwrite Existing Target Files & Folders** deselected (so you do not re-copy files that have already been copied and verified). NOTE: Depending upon how much data is being imported, verifying imported data can be a lengthy process.
Email Notification	Clicking the email notification link takes you to the Email Notification page (for more information, see "Email Notification"). Fill in notification information and check the box next to **Administrative Operation Event** in order to receive an email when the import operation is complete.

2. Once you have completed the import information, click the **Start Import** button to begin the import. You can see the progress of the import, the estimated time until completion, and the Import log on the secondary **Data Import** page.
3. When the import is complete, click the **View Log** button to see details of all errors. Click the **Data Import Error Log** link to download the entire log.

Stopping an Import Job

To stop the import at any time, click the **Stop Import** button on the **Data Import** secondary page. If a file was in the process of being copied, the partially-copied file on the target is removed.

Recreating an Import Job

The Data Import log records all errors that occurred during import. You can import just the files and folders that were not imported during the original job due to an error condition (for example, the file was locked).

1. Review the Data Import **errors log** and correct all error conditions (such as unlock a file).

2. Reopen the **Data Import** page. All fields (except the password) from the last import will still be visible on the page.

   By default, all files will be re-imported. If you want only to import those files that failed to import the first time, you can disable the **Overwrite existing target files** option. However, make sure that all problematic files from the first import are deleted from the target so they can be re-imported.

   NOTE: If an import failed, it is strongly recommended that you enable the Verify imported data option for the re-importation.

3. Enter your password and click **Start Import** to run the import again.

Preserving Permissions

The types of permissions retained will differ, depending on which import scenario is applied.

Importing from a Windows Security Model to a Windows Personality Directory

If you are importing from a Windows server (or other type of server that follows the Windows security model) to a Windows personality directory, permissions are retained exactly as they exist on the source. However, as is the case when moving files with permissions between Windows servers, permissions for users who are unknown on the target are retained but not enforced. This includes permissions for:

- Local users on the source machine.
- Domain users for domains unknown to the cluster (for example, trusted domains, if the cluster is not configured to support trusted domains).
- Certain built-in Windows users and groups.

Importing from a UNIX Security Model to a UNIX Personality directory

If you are importing from a UNIX server to a UNIX personality directory, UNIX permissions for UIDs/GIDs are copied exactly from source to target; thus, identities of the users and groups are best retained if the SnapScale cluster belongs to the same NIS domain as the UNIX server.

Importing Between Conflicting Security Models

When importing from a UNIX source to a Windows security model target, UNIX permissions are retained and the security personality on the resulting files and directories will be UNIX.

However, when importing from a Windows source to a UNIX security model target, permissions cannot be retained (since UNIX root directories are required to be UNIX personality throughout). Files and directories will inherit the UNIX personality and will have a set of default UNIX permissions.

Importing from a SnapServer or SnapScale Cluster

When importing from a SnapServer or another SnapScale cluster, it is recommended that you maintain the same security model on the target that you have on the source.

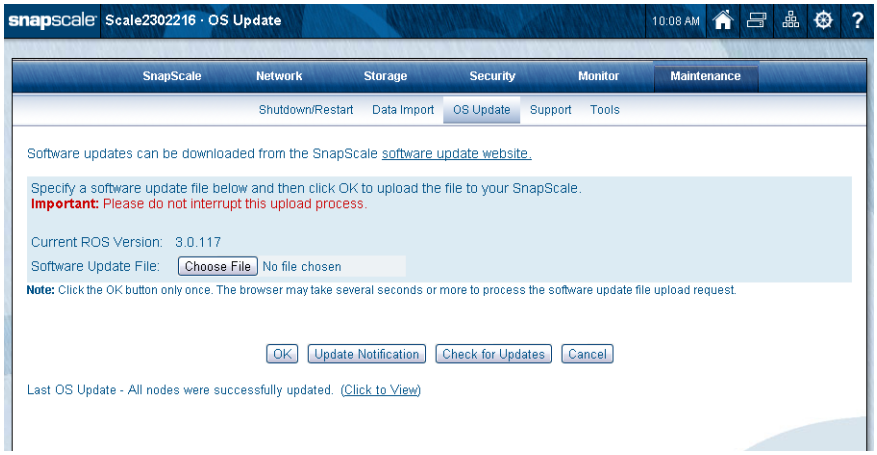
- If your source uses a Windows security model and has permissions assigned to Windows domain users, use a Windows (SMB) connection for import. Windows permissions are retained exactly as they are on the source, with the same enforcement limitations for unknown users as for importing from Windows servers (see Importing from a Windows Security Model to a Windows Personality Directory).

- If your source server or cluster uses a UNIX security model and has permissions assigned to local or NIS users, use an NFS connection for import.

  NOTE: Local users who have UNIX permissions on the source are not created on the target with the same UIDs.

OS Update

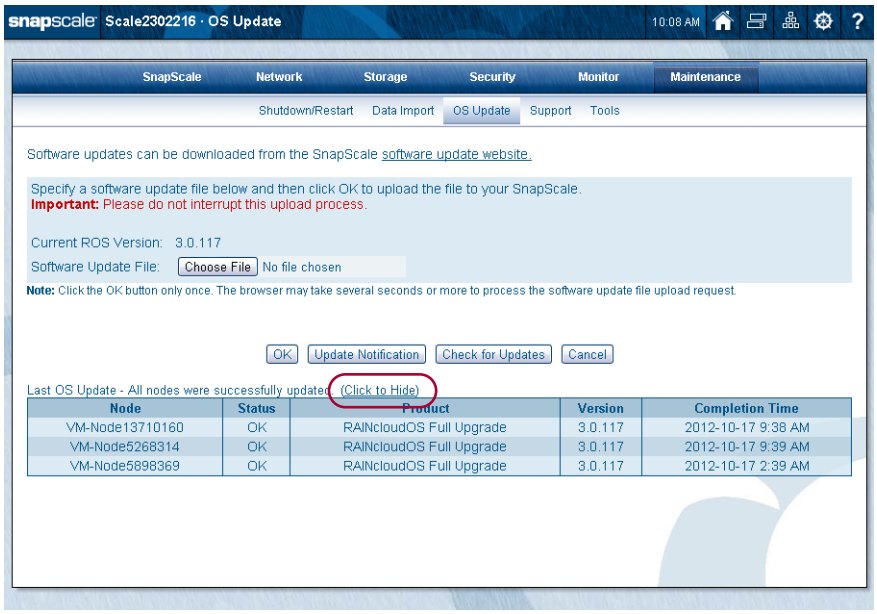
Use this page to install updates to RAINcloudOS and other installed software, and to configure RAINcloudOS to automatically check for updates to RAINcloudOS and Snap EDR.



Information about the last RAINcloudOS update is listed at the bottom of the page, and may include the status of the update, product and version, and the completion time.

CAUTION: Do not interrupt the update process. You may severely damage the cluster's ability to run if you interrupt a software update operation.

To view the last OS updates for each of the nodes, click the link under the buttons to show (or hide) the table:



Update the RAINcloudOS Software

1. Click the **Check for Updates** button. If an update is available, follow the instructions on the page to download it.

   NOTE: If the cluster does not have access to the Internet, download the latest RAINcloudOS image (.gsu) or other software package from the Overland Storage website.

2. On the **OS Update** page, click **Browse**, locate the downloaded file, and select it.
3. Click **OK** to start the update (or **Cancel** to stop).

   The software package is uploaded and then prompts you to reboot the cluster to perform the upgrade.

Note the following caveats:

- If upload fails on one or more nodes, the upgrade will abort with an error and list the nodes that had problems.
- After an upgrade and reboot, the OS Update page shows the status of the last update performed (success/failure) for each node.
- Snap EDR cannot be installed using the OS update page.

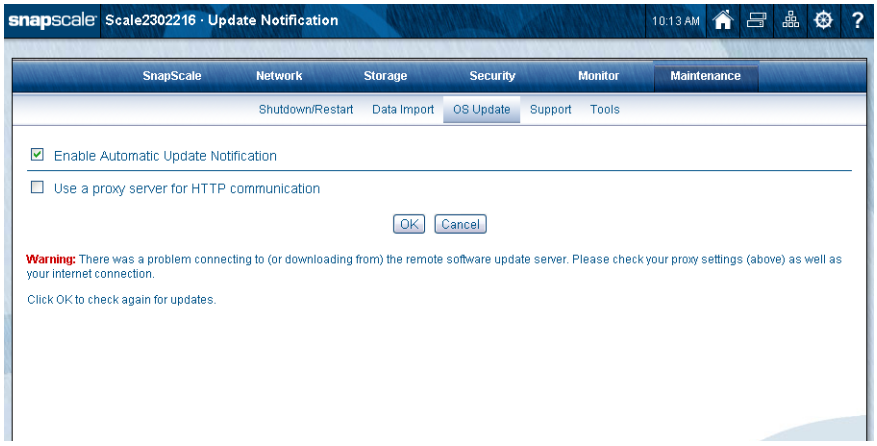
Software Update Notification

You can configure RAINcloudOS to display an alert when RAINcloudOS or Snap EDR updates are available for the cluster. When enabled, Update Notification checks weekly for RAINcloudOS or EDR updates that are applicable to the cluster. If updates are available, a banner alert is displayed just below the menu bar on all Web Management Interface pages.

NOTE: You can choose to hide the banner by clicking the *Remind me later* or *Hide this message* link on the banner. If *Remind me later*, the Web Management Interface displays the banner after the next check for updates; if *Hide this message*, the banner is hidden for the update in question until a later version is released.

Configuring Update Notification

1. Click the **Update Notification** button to display the options:



2. Check the **Enable Automatic Update Notification** option box.
3. If your environment requires using a proxy server for external web-based communication, check the **Use a proxy server for HTTP communication** check box and complete the Proxy Host and Proxy Port fields.

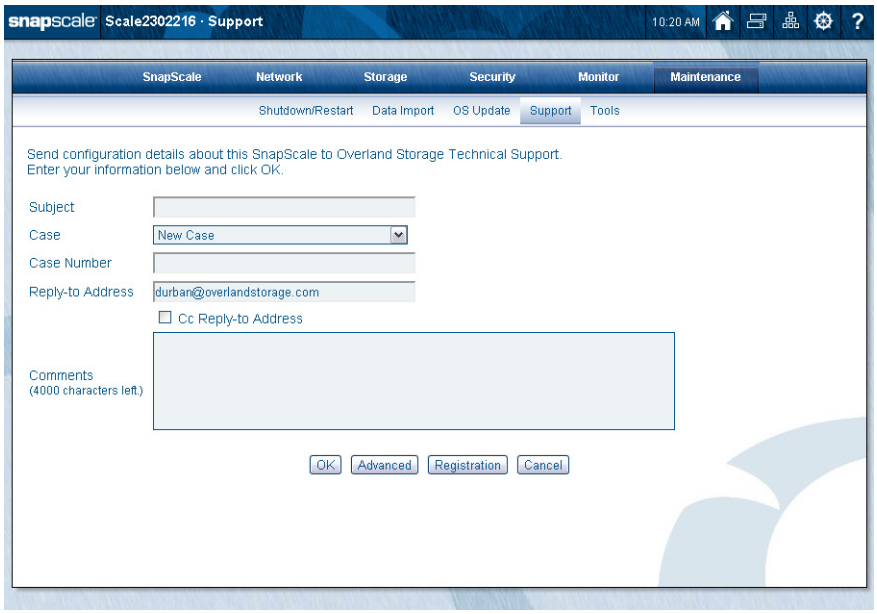
4. Click **OK**.

Manually Checking for Updates

Click the **Check for Updates** button to force the cluster to immediately search for applicable updates. If an update is available, it is displayed with information about it and a link to download the software.

Support

The **Support** page provides an easy way to contact Overland Technical Support.



Phone Home Support

Once email notification has been configured, Phone Home Support becomes available for registered SnapScale clusters. Phone Home Support optionally uploads and emails system logs and files that contain information useful for troubleshooting purposes to Overland Storage technical support. You can use the **Maintenance > Support** page to open a new case with technical support; or, in the course of working to resolve an issue, a technical support representative may ask you to fill out and submit this page. If a case is already in progress, you will need to enter the case number provided by the technical support representative.

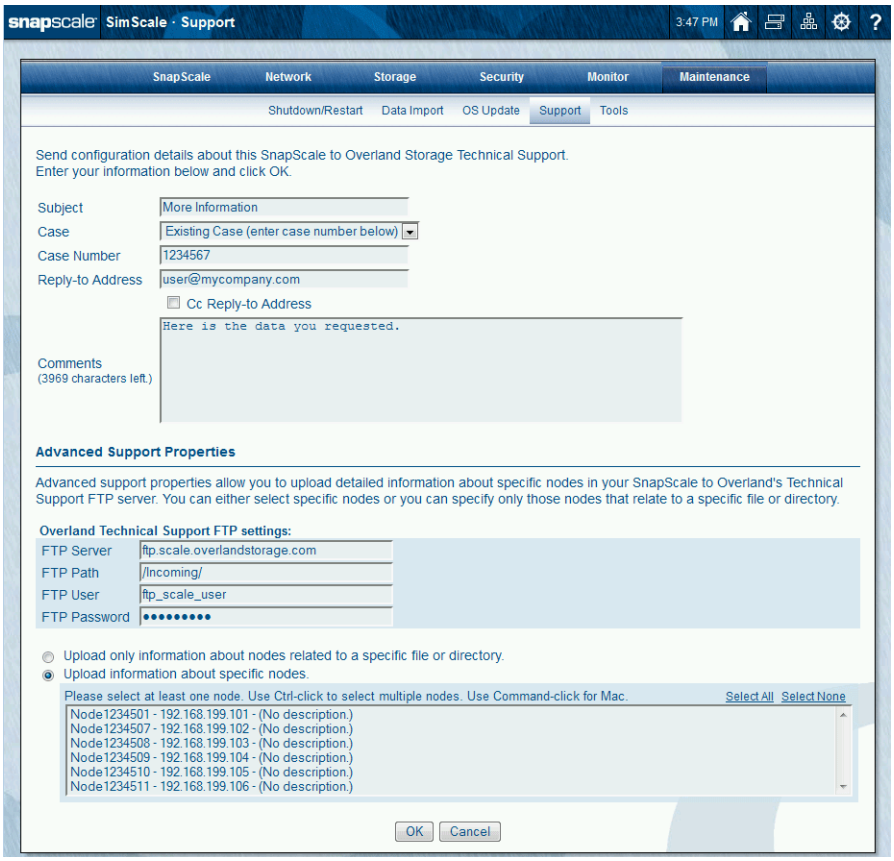
NOTE: Phone Home Support interacts with two fields on the Maintenance > Tools > Email Notification page: (1) To use Phone Home Support, you must enter a valid SMTP server IP address on the Email Notification page; and (2) the first email address listed in the Recipients field populates the Reply-to Address field on the Support page.

Complete the following fields as appropriate, then click **OK**:

Text Field	Description
Subject	(Required) Enter a concise description that identifies the issue.
Case	(Required) Select *New Case* if you are emailing technical support for the first time. Select *Existing Case* if you have previously contacted technical support concerning the issue.
Case Number	If you selected *Existing Case* above, enter the case number provided by technical support.
Reply-to Address	(Required) This field defaults to the first email address entered as a recipient on the **Maintenance > Tools > Email Notification** page. If necessary, enter at least one email address that will serve as the contact email address for this issue. To receive a copy of the email and system information attachment, check the *Cc Reply-to Address* box.
Comments	(Required) Enter additional information that will assist in the resolution of the problem.

Advanced Help

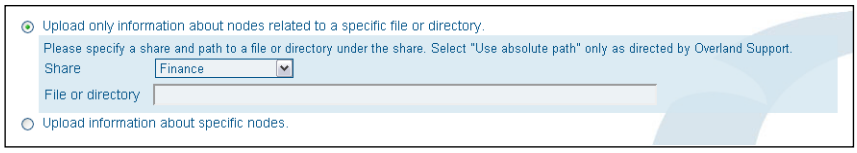
If you have an open case and have entered the Case Number, clicking the **Advanced** button opens additional options for the phone home feature. These options provide the ability to upload specific log files via FTP, which is sometimes necessary for the large logs the cluster can generate, and tech support may direct a user to use this for a particular case.



Options include:

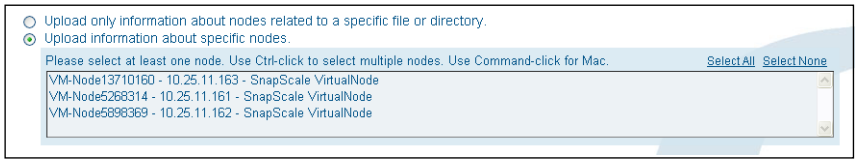
- **FTP Server** – Name of the server to upload to.
- **FTP Path** – FTP server path used to upload to.
- **FTP User** – Name of the user to log in to the FTP server as.
- **FTP Password** – User's password.
- Click an **upload option**:
  - **Upload only information about nodes related to a specific file or directory**

    Use the **Share** drop-down list to select the share and **File or Directory** path field to enter the path to a file or directory to gather logs. Only select **(Use absolute path.)** from the drop-down list when directed by Overland Support.



  - **Upload information about specific nodes**

    Select one or more nodes to upload logs from them. Use the **Select All** and **Select None** options on the right as needed.



Registering Your Cluster

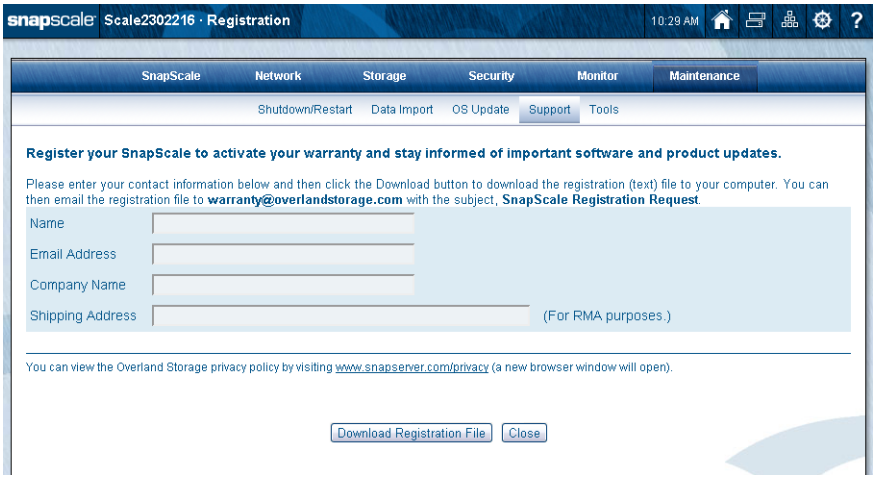
When you first start a cluster, a Registration Reminder page appears. Registering your cluster activates your warranty and allows you to create and track service requests. Registration also provides access to RAINcloudOS upgrades, third-party software, and exclusive promotional offers.

NOTE: Warranty information is available at http://docs.overlandstorage.com/support.

To Register Your Cluster

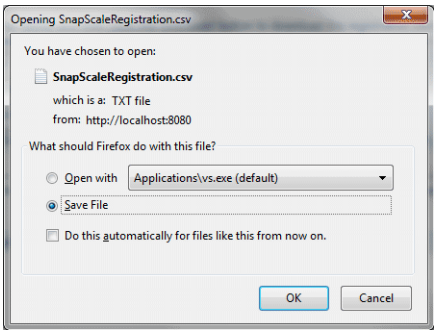
NOTE: To use this feature, access to the Internet is required.

Go to **Maintenance > Support** and click **Registration** to view the registration page:



Use this page to easily register your cluster:

1. Enter the **four required items** in the appropriate fields.
2. Click **Download Registration File**.
   The information, including all the node data, is incorporated into a CSV file.
3. At the dialog box, select **Save File**.



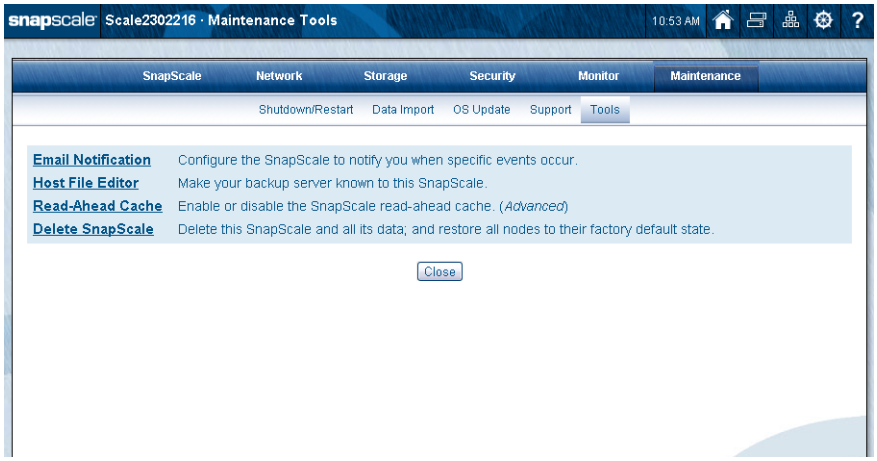
   This saves the registration file to your local computer.
4. Email the downloaded registration file to **warranty@overlandstorage.com**.
   Use the subject line "SnapScale Registration Request" for the email.

The same page is also used to update your registration information. For example, when you add new nodes to your cluster, they need to be added to the cluster registration so that they are also covered.

Once you have registered, you will receive a confirmation email to complete the registration.

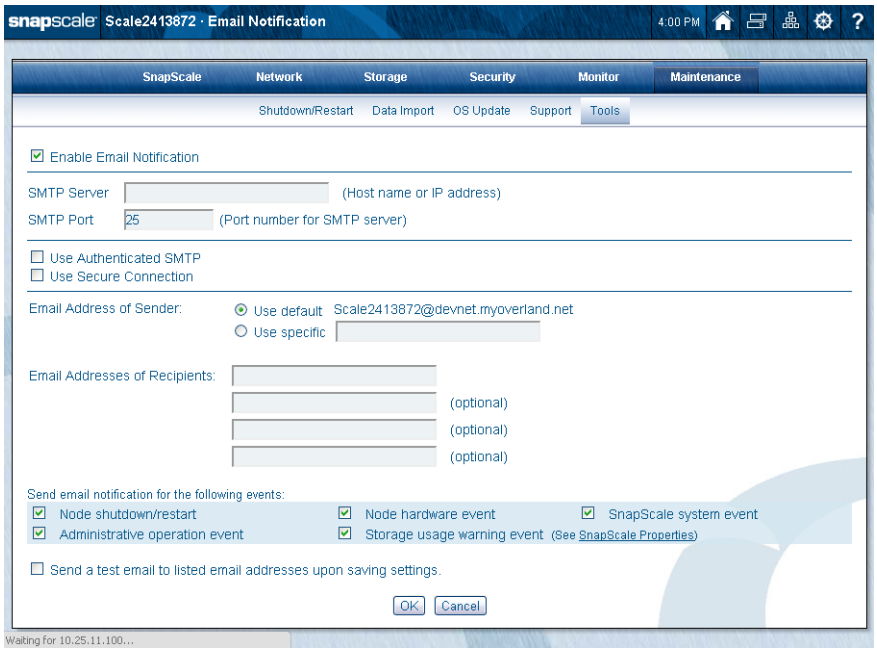
Maintenance Tools

The tools under the (Maintenance) Tools subheading provide general-purpose maintenance options and features.



Email Notification

To configure the cluster to send email alerts in response to system events, navigate to the **Maintenance > Tools > Email Notification** page.



To set up email alerts, you need: (1) the SMTP server's IP address; and (2) the email address of each recipient to receive an alert.

Configuring Email Notification

Edit settings as described in the following table, and then click **OK**.

Option	Description
Enable Email Notification	To enable email notification, check the Enable Email Notification check box.
SMTP Server	Enter a valid SMTP server IP address or host name.
SMTP Port	Enter a port number for the SMTP server or accept the default.
Use Authenticated SMTP	Check this box to authenticate when an email is sent to the SMTP server by the cluster. Provide an authentication User Name and Password in the fields that appear when the feature is enabled.
Use Secure Connection	Check this box to encrypt emails from the cluster. STARTTLS and TLS/SSL encryption protocols are supported.
Email Address of Sender:	Choose: • The default address (*clustername@domain*) where *domain* is the DNS domain name (or the management IP address (*clustername@ipaddress*) if no DNS domain name is configured. • Specify a specific sender.
Recipients	Enter one or more email addresses to receive the notifications. One address is required. Three additional email addresses can be added.
Send Email Notification Events	Check the boxes next to the events you wish to be notified about: • Node shutdown/restart – A node shuts down or reboots due to an automatic or manual process. • Node hardware event – The internal temperature for a node exceeds its maximum operating temperature or other hardware problems. • SnapScale system (cluster) event – A change or error occurs that impacts the entire cluster. • Administrative operation event – A Data Import operation has finished or experienced an error. • Storage usage warning event – Storage space usage on a volume reaches either the maximum utilization or the critical utilization setting. See "SnapScale Properties."
Send a Test Email	To verify your settings, check **Send a test email**, then click OK.

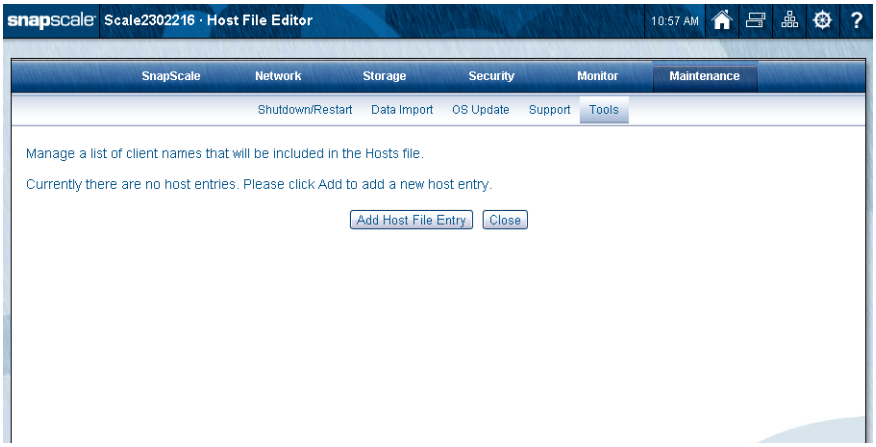
If Send a Test Email is checked, when you save your changes, the following email is sent to all configured email recipients:

```
Cluster Name: Scalennnnnnn
Node Name: Nodennnnnnn
IP Address:
Severity: Testing
Node Number: nnnnnnn

This is a test message.
```

Host File Editor

Use this page to identify external hosts in the SnapScale cluster's hosts file. This page allows you to supply a hostname-to-IP address mapping that persists across system reboots.



Click **Add Host File Entry**, complete the fields as described on the following table, and then click **Add Host File Entry** again.

Use this table to complete the options shown:

Option	Description
IP Address	The IP address of the external host.
Host Name	Enter the fully qualified hostname for the external host, using the format: *myserver.mydomain.com*. NOTE: Some applications may require that you enter either one or both of these fields. See the OEM documentation to determine requirements.
Alias (optional)	Enter an optional abbreviated address for the external host, using the format: *myserver*. NOTE: Some applications may require that you enter either one or both of these fields. See the OEM documentation to determine requirements.

Read-Ahead Cache

Read-ahead cache is a predictive function used to accelerate reads of sequential data (large files) from the cluster storage. By predicting what the user will want to read next based on the data previously accessed, the information is moved into the system memory cache ahead of the user's subsequent request allowing for faster fetching than direct from storage.

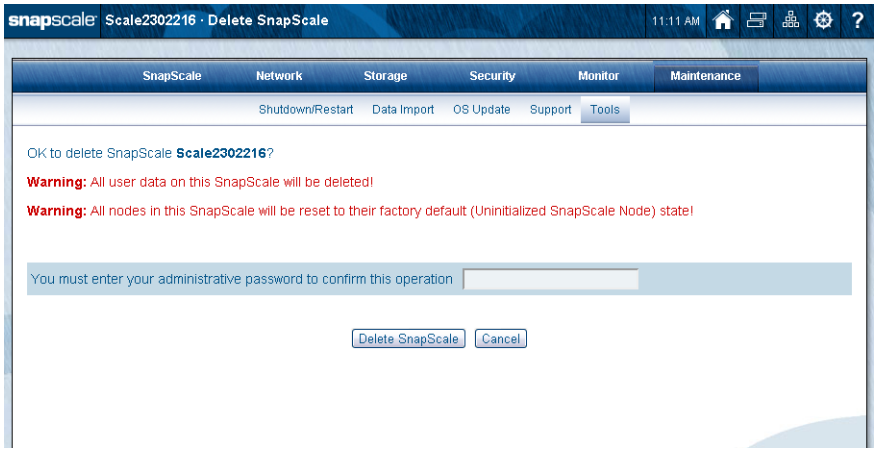
By default, read-ahead cache is disabled freeing up memory. Enabling the feature may impact disk read performance.

Delete SnapScale Cluster

This page is used to delete a SnapScale cluster and all its data.

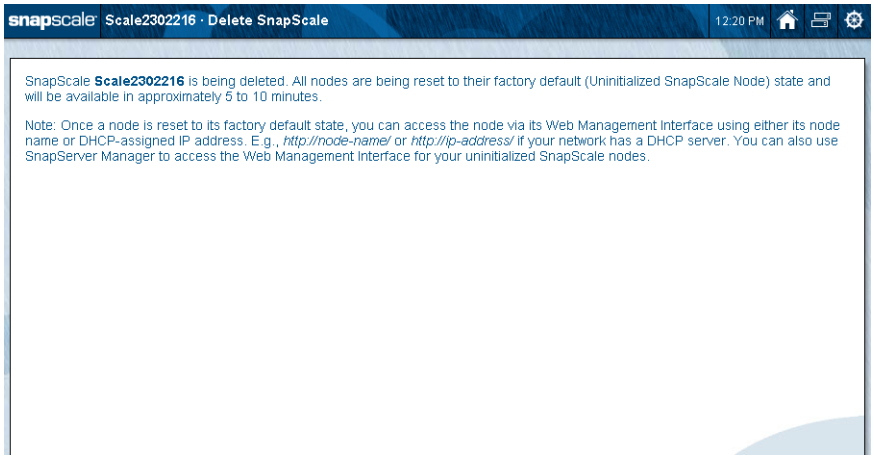
CAUTION: All data on all the nodes will be lost and all the nodes will be reset to their original factory default settings.

When you click **Delete SnapScale**, a confirmation page is shown:



Click **Delete SnapScale** again to start the process.

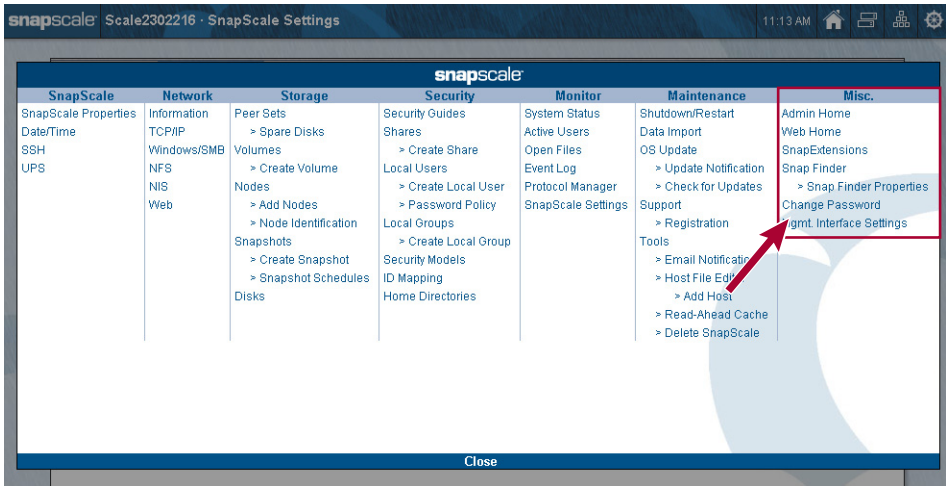
Once you confirm the deletion, the nodes reboot, automatically perform a fresh install, and then boot again into Uninitialized mode. During the deletion, the following information page is shown:



Misc. Options

The RAINcloudOS site map provides links to all the web pages that make up the Web Management Interface. It also provides, in the last column, special links to higher level options and processes which is the focus of this chapter.

With the exception of Mgmt. Interface Settings, these options are also directly navigable from the various menus in the Web Management Interface. Also the Home, Snap Finder, SnapExtensions, Site Map, and Help options are accessible from any page by clicking their respective icon in the top right corner of the screen (see the table in "Web Management Interface").



Topics in Misc. Options

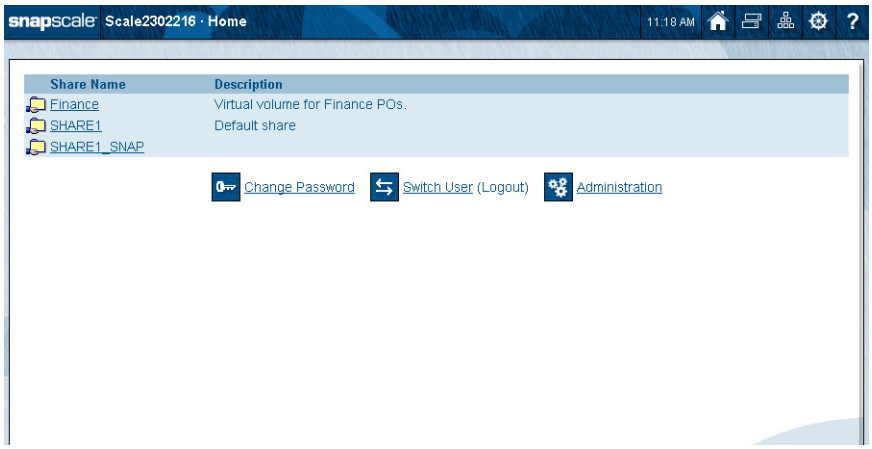
- Home Pages – Web/Admin
- SnapExtensions
- Snap Finder
- Change Password
- Mgmt. Interface Settings

Home Pages – Web/Admin

When you first log in to the Web Management Interface, the Web Home page is displayed. Once logged in, you can switch between the Web Home page and the Admin Home page using the Home ( ) icon.

Web Home

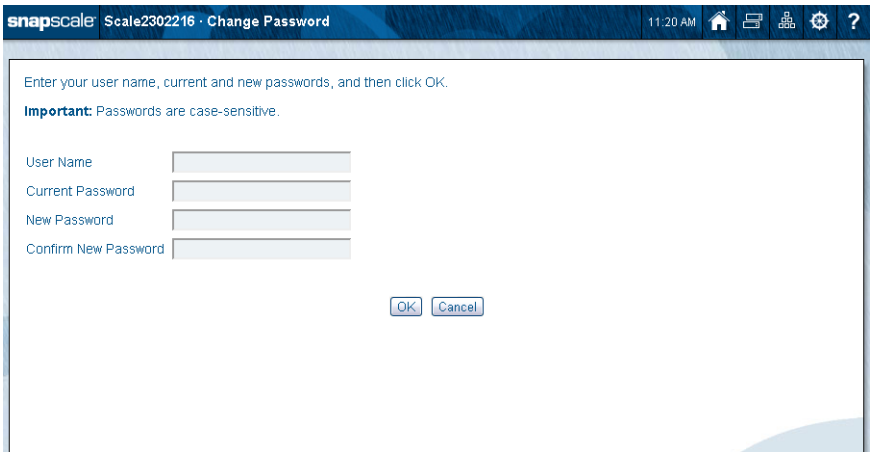
The Web Home page shows a list of all the shares on the SnapScale cluster.



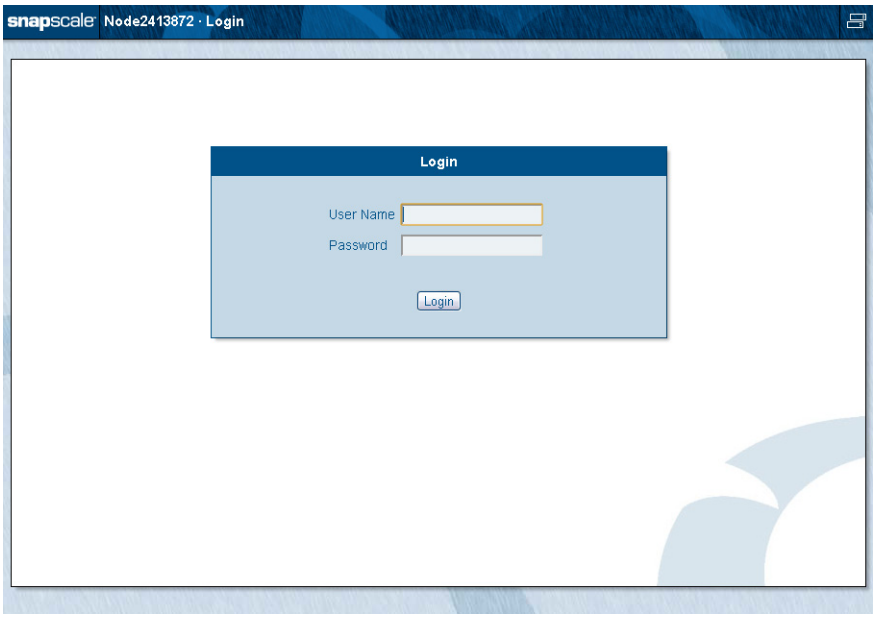
For users with admin rights, a key icon ( ) appears next to the file/folder in the share. Clicking this icon displays a popup box with security information about the file/folder.

This page also provides three key administrative function links:

- **Change Password** ( ) – Takes you to the **Change Password** page where you can change your administration password, or local users can change their password. Enter your **User Name** and **Current Password** for access. See "Change Password."



- **Switch User (Logout)** ( ) – Automatically logs out the current user and displays the **Login** page for the new user to gain access to the SnapScale cluster.



- **Administration** – Displays the Admin Home page (see "Admin Home"). You are prompted to log in if you have not already done so.

If any of the following conditions are present, you may not be able to access the Home page:

- **Require Web Authentication** is enabled (via **Network > Web > Require Web Authentication**) and you do not have a valid user name and password on the cluster.
- The cluster or node has not completed the **Initial Setup Wizard** (if this is the case, you will not be able to access the Administration page of the Web Management Interface either).
- **Web Root** is enabled (via **Network > Web > Enable Web Root**).

Admin Home

The Admin Home page is accessible by clicking either the Admin Home link in the Site Map or the Administration ( ) or Home ( ) icons on the Web Home page. It provides a high-level view of the SnapScale status, links to key items such as peer sets, and a link to find out what's new in RAINcloudOS. The tabs at the top provide access to the various functions and features of the RAINcloudOS.

This table details the information on the Admin Home page:

Option	Description
SnapScale Name	Shows the name used to identify the cluster. The default name is "Scale*nnnnnnn*" (where *nnnnnnn* is the appliance number of the node used to create the cluster).
RAINcloudOS Version	Lists the version of the RAINcloudOS running on all the nodes.
Uptime	Displays the length of time the cluster has been up and running since the last reboot.
Data Replication Count	Shows the data replication count establishing the level of data redundancy in the cluster (either 2x or 3x).
Spare Disks Setting	Displays the number of spare disks requested by user to automatically replace a failed Peer Set member.
UPS Support	Displays whether UPS support is enabled.
Email Notification	Displays whether Email Notification is currently enabled.
Management IP Address	Lists the IP address that is used to access the cluster through the Web Management Interface.
Multicast IP Address	Shows the multicast address used for inter-node messaging on the Storage network.
Maximum File Size	Displays the maximum size of a file that can be saved on the cluster at any given time based on the free space found on the least-utilized peer set.

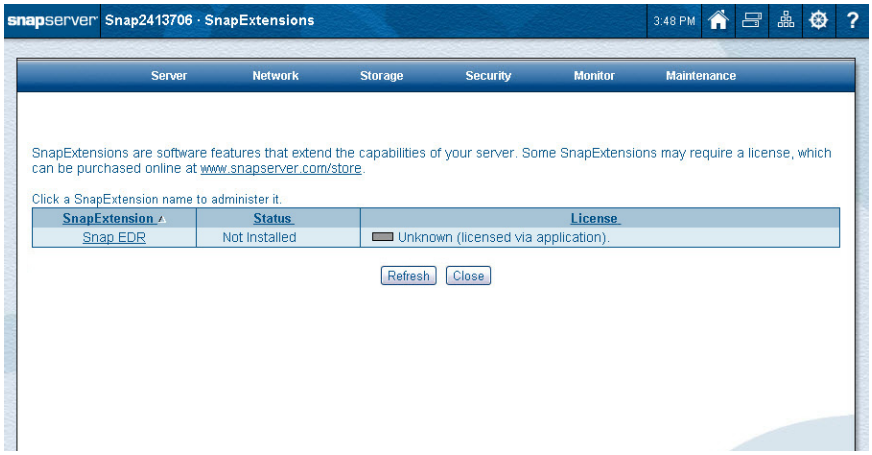
Option	Description
Peer Sets	Shows the total number of peer sets on the cluster and their status.
Nodes	Shows the number of nodes that make up the cluster and their status.
Active Spare Disks	Displays the total number of available hot spares and their status.
SnapScale Settings	Provides the current status of the cluster.
UPS Status	Displays UPS status for all nodes. This option is only displayed if UPS support is enabled.
Total Storage Usage	Displays a bar chart, percentage, and actual amount of cluster storage space used compared to total storage space available (**Actual**/**Total**).

The **Refresh** button at the bottom or the Refresh icon ( ) on the right corner of the tab bar can be clicked to manually refresh the information.

From the Administration page, clicking takes you to the Web Home page.

SnapExtensions

The SnapExtensions icon ( ) opens the SnapExtensions page. This page is used to manage the SnapExtensions installed on your cluster.



If any SnapExtensions are installed, you can click the SnapExtension name in the table to display the management page for that extension.

Snap EDR

At the Snap EDR (Snap Enterprise Data Replicator) configuration page, you can install Snap EDR, configure it as either the Management Console or the Agent of another Management Console, or launch the Snap EDR Management Console interface. If configuring it as an Agent, enter the server name or cluster management name (<clustername>–mgt) of the Management Console.

Refer to Appendix A, "Configuring Snap EDR for RAINcloudOS,"for details on installing and configuring Snap EDR.

NOTE: All other agents and management consoles must be able to resolve this cluster by the cluster management name (<clustername>–mgt) to the Management IP. This is typically done by a host record in the DNS.

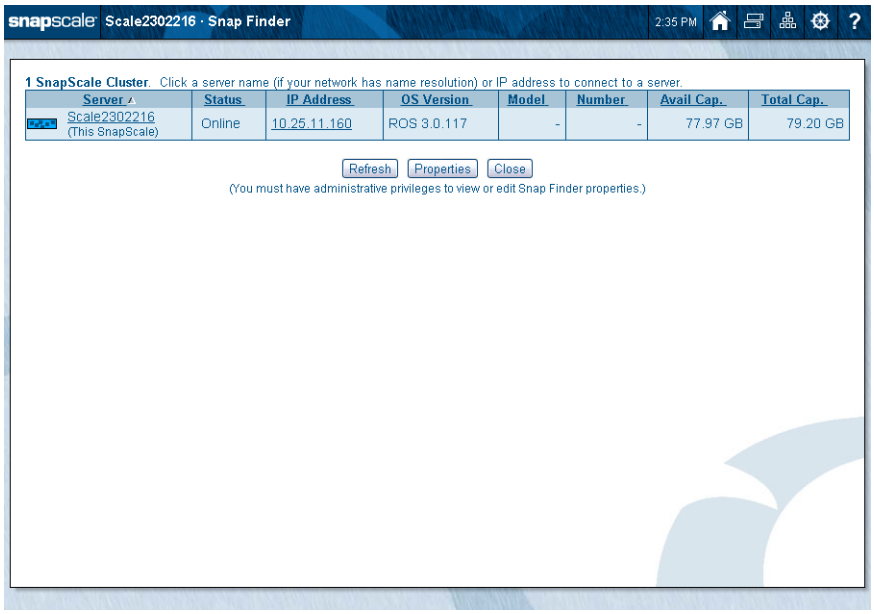
After Snap EDR finishes its configuration, the Management Console screen is shown.

For information on using Snap EDR, see Appendix A, "Snap EDR Usage."

Snap Finder

Snap Finder ( ) is a powerful tool that lists all the SnapScale clusters, Uninitialized nodes, and SnapServer appliances on your network (and on a remote network segment if so configured), and shows the current status of each. Click the unit name (if you have name resolution) or IP address of a cluster, node, or server to access it through the Web Management Interface.

NOTE: You can sort the columns (ascending or descending order) by clicking the column heading.



The following table details the columns in the table:

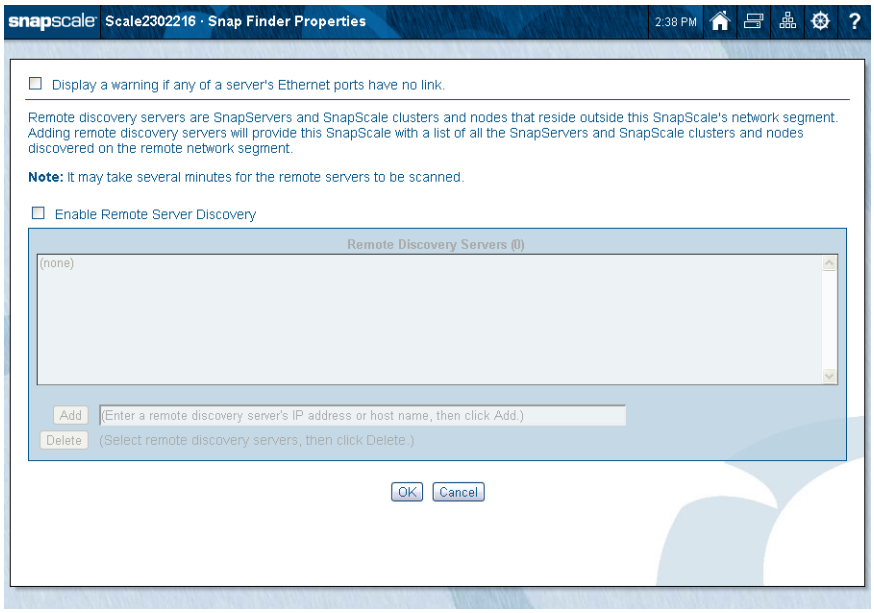
Identification	Description
Server	Name of the SnapScale cluster, Uninitialized node, or SnapServer appliance. The default cluster name is Scale*nnnnnnn*, where *nnnnnnn* is the number of the node originally used to create the cluster. For example, "Scale2302216."
Status	• The status of the SnapServer or Uninitialized node (for example, **OK** or **Fan Failure**). • The status of a SnapScale cluster is always **Online**.
IP Address	The IP address of the SnapServer, Uninitialized node, or the Management IP address of the SnapScale cluster.

Identification	Description
OS Version	The OS version currently installed on the SnapServer, Uninitialized node, or SnapScale cluster.
Model	The hardware model number of the SnapServer or Uninitialized node. This field is not applicable to a SnapScale cluster.
Number	The Server or Node Number derived from the MAC address of the primary Ethernet port, used as part of the default name. This field is not applicable to a SnapScale cluster.
Avail Cap	The available capacity on the cluster or SnapServer. This field is not applicable to an Uninitialized node.
Total Cap	The total capacity on the cluster or SnapServer. This field is not applicable to an Uninitialized node.

To enable remote discovery of clusters, nodes, or servers on a different subnet or to display a warning icon for SnapServers or Uninitialized nodes with an enabled Ethernet port that has no link, click the **Properties** button to open the **Snap Finder Properties** page.

Snap Finder Properties

Anyone with administrative privileges can view or edit the Snap Finder properties. Click the **Properties** button to access the **Snap Finder Properties** page.



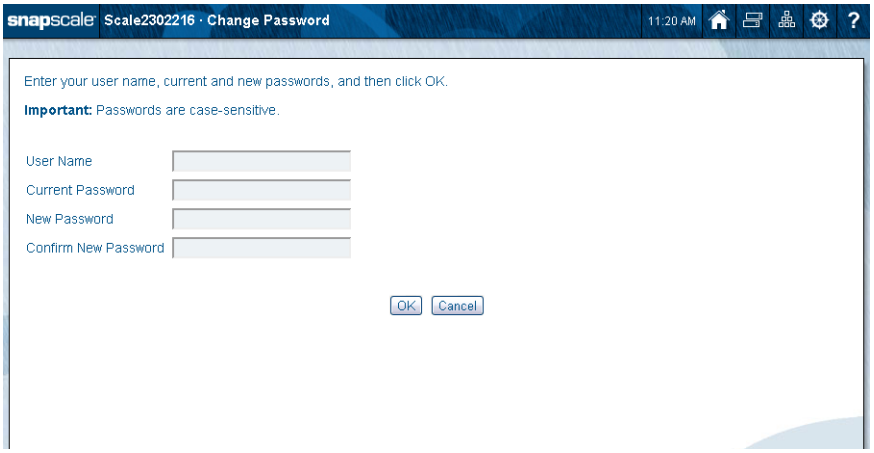
From this screen you can select to display a warning icon for Uninitialized nodes or SnapServers with an enabled Ethernet port that has no link and enable remote discovery of units on a different subnet. Complete the following fields and then click **OK** to return to the Snap Finder screen:

Option	Description
Display warning if any of a server's Ethernet ports have no link	Check to display a warning icon in the Status column for any nodes or SnapServers that have an enabled Ethernet port with no link. By default, this box is unchecked.

Option	Description
Enable Remote Server Discovery	Check to enable remote discovery of clusters, nodes, or SnapServers on a different subnet.
Add Server	Enter the host name or IP Address of a cluster, node, or server in the field to the right of the **Add** button, and click **Add** to incorporate it into the list of Remote Discovery Servers. Remote Discovery Servers send information about themselves as well as all other servers they've discovered on the remote network.
Delete Server	Select a cluster, node, or server, in the Remote Discovery Servers field and click **Delete**. When asked to confirm the deletion, click **Delete** again.

Change Password

To enhance the security of your SnapScale cluster, it is recommended that users change their passwords regularly. This is done using the **Change Password** page.

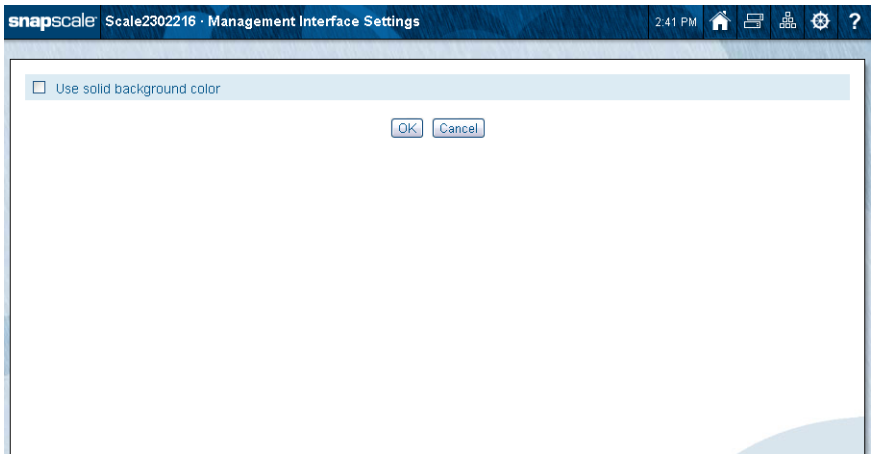


Changing Your Password

1. On the **Home** page, click the **Change Password** link ( ).
2. At the **Change Password** page, enter your **User Name** and **Current Password**.
3. Enter and confirm your **new password**.
   Passwords are case-sensitive. Use up to 15 alphanumeric characters without spaces.
4. Click **OK**.
5. At the confirmation page, click **OK** again.
   You are returned to the Web Home page.

Mgmt. Interface Settings

The Web Management Interface default background is light blue with the stylized "O" symbol. This can be changed to a solid blue background on the Web Management Interface Settings page by clicking the Site Map icon ( ), then **Mgmt. Interface Settings**, then **Use solid background color**.



Appendix A

Backup Solutions

This appendix provides a brief description of the supported backup solutions and, where applicable, gives instructions on how to install the solutions on the SnapScale cluster.

Topics in Backup Solutions:

Backup and Replication Solutions Table

RAINcloudOS supports several backup methods, including third-party off-the-shelf backup applications and applications that have been customized and integrated with RAINcloudOS on the SnapScale cluster.

RAINcloudOS	Backup and Replication Solutions		
	Snap EDR	CA BrightStor	Symantec Backup Exec
Snap to Backup Server via network protocol		X	X
Data and Security Meta Data Backup and Replication	X		

Snap Enterprise Data Replicator

Snap EDR provides server-to-server synchronization by moving, copying, or replicating the contents of a share from one cluster or server to another share on one or more different clusters or servers. It comes preinstalled on SnapScale clusters and activates a 45-day free trial if configured as a Management Console.

Snap EDR consists of a Management Console and a collection of Agents. The Management Console is installed on a central system. It coordinates and logs the following data transfer activities carried out by the distributed Agents:

- Replicates files between any two systems including SnapServers, SnapScale clusters, and Windows, Linux, and Mac Agents.
- Transfers files from one source host to one or more target hosts

- Transfers files from multiple hosts to a single target host, and stores the files on a local disk or locally attached storage device.
- Backs up data from remote hosts to a central host with locally-attached storage.
- Restores data from a central storage location to the remote hosts from which the data was originally retrieved.

See Chapter 8, "Snap EDR."

Snap EDR Usage

The Snap Enterprise Data Replicator software distribution comes preinstalled on the cluster, and must first be installed in SnapExtensions and then configured before it's available for use. It operates under the cluster management name (in the style of <*clustername*>–mgt) and the management IP address.

All other Snap EDR installations (including another machine running as the Management Console that the cluster registers to, other Agents that register to a Snap EDR Management Console running on the cluster, or other Agents replicating to/from the cluster) need to be able to resolve the cluster's management name to the cluster management IP in order to interoperate properly with the cluster. This can be accomplished via a DNS host record or local hosts file entries.

When installing EDR to the cluster for the first time, it installs to all nodes and runs on whichever node currently serves as the management node.

When adding a node to an existing cluster with Snap EDR installed, it is automatically installed on that node.

Configuring Snap EDR for RAINcloudOS

To configure the cluster as a Snap EDR Management Console or an Agent:

1. Click the **SnapExtensions icon** located in the upper right corner of the Web Management Interface.
2. If necessary, install the **software package**:
   a. Run the **installation routine** from SnapExtensions.
      SnapExtensions displays a Snap EDR link and the status **Not Installed**.
   b. Click the **Snap EDR link** and confirm the installation.
      Wait for the installation to complete. The SnapExtensions page then displays the Snap EDR Configuration link.
3. Click the **link** to launch the Management Console/Agent configuration page.
4. Select either the **Configure as the Management Console** or **Configure as the Agent** button.

   NOTE: If you are configuring the cluster as an Agent, you must provide the server name (for a SnapServer) or cluster management name of the Management Console (for a SnapScale). The cluster must be able to resolve the name to the correct IP address.

5. Once the cluster is configured, select the following options from the page that appears:

Option	Description
Click here to configure jobs	Opens the Management Console where jobs can be scheduled.

Option	Description
Stop Service	Stops all services.
Restart Service	Restarts all services. CAUTION: Use only if you have encountered a problem, and customer support advises you to restart the service. Any jobs currently running will stop and will not resume when you restart the service.

Scheduling Jobs in Snap EDR

To schedule jobs, click the **Snap EDR** link in the Site Map (under **Misc.**).

For complete information on scheduling jobs in Snap EDR, see the *Snap EDR Administrator's Guide*.

Appendix B

Security and Access

This appendix provides additional information and configuration options about accessing shares and files on the SnapScale cluster.

File and directory security can be configured using either Windows NTFS-style security or classic Unix-style security. The type of security present on a file or directory is its "security personality" (see "File-level Security"). The default security model on newly-created volumes is always Windows/Mixed. It can be changed to a Unix security model if necessary.

RAINcloudOS on the SnapScale supports share-level as well as file- and directory-level permissions for all local and Windows domain users and groups (see "Windows ACLs").

Topics in Shares and File Access:

Security Model Rules

Files and directories are stored on the cluster on volumes with a configured "security model." The security model on the volume governs the permitted security personalities, the default personalities, and the ability to change personalities on child files and directories.

Windows/Mixed Security Model:

- Files and directories created by SMB clients have the Windows security personality. Permissions will either be inherited according to the ACL of the parent directory (if Windows) or will receive a default ACL that grants the user full access only (if the parent is UNIX or has no inheritable permissions).
- Files and directories created by non-SMB clients will have the UNIX personality. UNIX permissions will be as set by the client (per the user's local umask on the client).
- The security personality of a file or directory can be changed by any user with sufficient rights to change permissions or ownership. If a client of one security personality changes permissions or ownership of a file or directory of a different personality, the personality will change to match the personality of the client protocol (for example, if an NFS client changes UNIX permissions on a Windows file, the file will change to the UNIX personality).

UNIX Security Model:

- Files and directories created by non-SMB clients will have the UNIX personality. UNIX permissions will be as set by the client (per the user's local umask on the client).
- Files and directories created by SMB clients will have the UNIX personality. UNIX permissions are set to a default.

- The personality of files and directories cannot be changed on a UNIX security model. All files and directories always have the UNIX personality.

Security Model Management

A single security model can be set on a storage volume at the root level but different security models cannot be set on the directories immediately underneath the volume as the directories inherit the model from the top-level. Changes to a security model for the volume can optionally be propagated with the corresponding personality and default permission to all files and directories underneath.

When changing the security model:

- If changing from Windows/Mixed to UNIX, all files and directories will be changed to be owned by *admin* and *admingrp*, with UNIX permissions of 777(rwxrwxrwx).
- If changing from UNIX to Windows/Mixed, files and directories will be changed to default permissions that allow all users the ability to create and manage their own files and directories and to access other users' files and directories.

Special Share Options

The basic setup and configuration of shares on a SnapScale are handled on the **Security > Shares** page (see Chapter 7, "Security Options"). This section covers more details about the special options and features of share security on your SnapScale.

Hiding Shares

There are three ways a share can be hidden in RAINcloudOS:

- Name the share with a dollar-sign ($) at the end. This is the traditional Windows method of hiding shares; however, it does not truly hide the share since Windows clients themselves filter the shares from share lists. Other protocols can still see dollar-sign shares.
- Hide the share from all protocols (except NFS) by:
  - While creating a share, navigating to **Security > Shares > Create Share > Advanced Share Properties** and checking the **Hide this Share** box.
  - Edit a share by selecting the share, clicking to expand **Advanced Share Properties**, and checking the **Hide this Share** box.

  When a share is hidden this way, the share is invisible to clients, and must be explicitly specified to gain access.

  NOTE: Hidden shares are not hidden from NFS, which cannot access invisible shares. To hide shares from NFS, consider disabling NFS access to the hidden shares.

- Disable individual protocol access to certain shares by:
  - While creating a share, navigating to **Security > Shares > Create Share > Advanced Share Properties** and enabling/disabling specific protocols.
  - Edit a share by selecting a share, clicking to expand **Advanced Share Properties**, and enabling or disabling specific protocols.

Where to Place Shares

For security and backup purposes, it is recommended that administrators restrict access to shares at the root of a storage volume to administrators only. After initialization, all SnapScale clusters have a default share named *SHARE1* that points to the root of the default volume *Volume1*. The share to the root of the volume should only be used by administrators as a "door" into the rest of the directory structure so that, in the event that permissions on a child directory are inadvertently altered to disallow administrative access, access from the root share is not affected. This also allows one root share to be targeted when performing backups of the server. If it is necessary to have the root of the volume accessible, using the Hidden option helps ensure only those that need access to that share can access it.

File and Share Access

The shares feature controls access by users and groups. This section provides information on setting up the shares options to allow proper access to the files.

Cumulative Share Permissions

Share-level permissions on RAINcloudOS are applied cumulatively. For example, if the user "j_doe" has Read-Only share access and belongs to the group "sales", which has Read/Write share access, the result is that the user "j_doe" will have Read/Write share access.

NOTE: Share-level permissions only apply to non-NFS protocols. NFS access is configured independently by navigating to the Security > Shares page, selecting from the table the NFS Access level for the share, and modifying the client access as desired.

Snapshot Shares and On Demand File Recovery

A *snapshot share* is a read-only copy of a live share that provides users with direct access to versions of their files archived locally on the SnapScale via a snapshot. Users who wish to view or recover an earlier version of a file can retrieve it on demand without administrator intervention.

Snapshot shares are created during the course of creating a share. For instructions an accessing snapshot shares, see Chapter 5, "Configuring Share Access."

Creating a Snapshot Share

You create a snapshot share by going to **Security > Shares**. In the **Shares** column, click the share name. At the **Shares Properties** page, expand the **Advanced Share Properties** section, and check the **Create Snapshot Share** box.

For example, assume you create a share to a directory called *sales*, and you select the **Create Snapshot Share** option. When you connect to the server via a file browser or use the **Misc. > Web Home** link in the Site Map, two shares display:

```
SALES
SALES_SNAP
```

The first share provides access to the live volume, and the second share provides access to any archived snapshots. Other than read-write settings (snapshots are read-only), a snapshot share inherits access privileges from its associated live-volume share.

Accessing Snapshots Within the Snapshot Share

A snapshot share contains a series of directories. Each directory inside the snapshot share represents a different snapshot. The directory names reflect the date and time the snapshot was created.

For example, assume the snapshot share named *Sales_SNAP* contains the following four directories:

```
latest
2012-09-25.120000
2012-10-01.000100
2012-10-07.020200
```

The *latest* directory always points to the most recent snapshot (in this case, `2012-10-07.020200`, or October 7th, 2012, at 2:02 a.m.). A user may view an individual file as it existed at a previous point in time or even roll back to a previous version of the file by creating a file copy to the current live volume.

NOTE: The latest subdirectory is very useful for setting up backup jobs, as the name of the directory is always the same and always points to the latest available snapshot.

File-level Security

RAINcloudOS supports two "personalities" of filesystem security on files and directories:

- **Windows ACLs**: Windows NTFS-style filesystem permissions. Windows ACLs fully support the semantics of NTFS ACLs, including configuration, enforcement, and inheritance models (not including the behavior of some built-in Windows users and groups).
- **UNIX**: Traditional UNIX permissions (rwx) for owner, group owner, and other.

By default, volumes are created with the Windows/Mixed security model (Windows-style ACLs for files created by SMB clients and UNIX-style permissions for files created by other protocols and processes), and allow all users to create, delete, and configure permissions on their own files and to access files and directories created by other users.

Security Personalities and Security Models

The security personality of a file or directory is dependent on the security model of the root directory or volume in which the file or directory exists.

Files and directories in a Windows/Mixed security model can have either a Windows or UNIX security personality, depending on the network protocol used to create the file or change permissions on it. Files in a UNIX security model always have the UNIX security personality and can only be set by NFS clients.

Windows ACLs

RAINcloudOS fully supports Windows NTFS-style filesystem ACLs, including configuration, enforcement, and inheritance models. Inside Windows/Mixed root directories, files created and managed by Windows clients have the Windows security personality and behave just as they would on a Windows server. Clients can use the standard Windows 2000, 2003, XP, Vista, or Windows 7 interface to set directory and file permissions for local and Windows domain users and groups on the SnapScale.

Permissions are enforced for the specified users in the same manner for all client protocols, including non-SMB clients that normally have the UNIX security personality. However, if a non-SMB client changes permissions or ownership on a Windows personality file or directory (or deletes and recreates it), the personality will change to UNIX with the UNIX permissions specified by the client.

NOTE: Group membership of NFS clients is established by configuring the local client's user account or the NIS domain. Group membership of SnapScale local users or users ID-mapped to domain users is not observed by NFS clients. Therefore, ACL permissions applied to groups may not apply as expected to NFS clients.

Default File and Folder Permissions

When a file or directory is created by an SMB client, the owner of the file is the user who created the file (except for files created by local or domain administrators, in which case the owner is the **Administrators** group, mapped to the local **admingrp**), and the ACL will be inherited per the inheritance ACEs on the parent directory's ACL. The owner of a file or directory always implicitly has the ability to change permissions, regardless of the permissions established in the ACL. In addition, members of the SnapScale's local admin group, as well as members of Domain Admins (if the server is configured to belong to a domain) always implicitly have *take ownership* and *change ownership* permissions.

Setting File and Directory Access Permissions and Inheritance (Windows)

Access permissions for files and directories with the Windows security personality are set using standard Windows 2003, XP, Vista, 2008, or 7 security tools. RAINcloudOS supports:

- All standard generic and advanced access permissions that can be assigned by Windows clients.
- All levels of inheritance that can be assigned to an ACE in a directory ACL from a Windows client.
- Automatic inheritance from parent directories, as well as the ability to disable automatic inheritance from parents.
- Special assignment and inheritance of the CREATOR OWNER, CREATOR GROUP, Users, Authenticated Users, and Administrators built-in users and groups.

Procedure to set file and directory access permissions and inheritance in Windows:

1. Using a Windows 2003, XP, Vista, 2008, or 7 client, **map a drive** to the SnapScale, logging in as a user with change permissions for the target file or directory.
2. Right-click the file or directory, choose **Properties**, and then select the **Security** tab.
3. Use the **Windows security tools** to add or delete users and groups, to modify their permissions, and to set inheritance rules.

Appendix C

RAINcloudOS Ports

Port Map for RAINcloudOS

The following table outlines the ports used in RAINcloudOS (ROS).

Port #	Layer	ROS Feature	Name	Comment
1	DDP		rtmp	Routing Table Management Protocol
1	TCP & UDP		tcpmux	TCP port service multiplexer
2	DDP		nbp	Name Binding Protocol
22	TCP & UDP	Server > SSH	ssh	Secure Shell (SSH) service
25	TCP & UDP	Server > Email Notification	smtp	Simple Mail Transfer Protocol (SMTP)
67	TCP & UDP	Network > TCP/IP	bootps	Bootstrap Protocol (BOOTP) services; also used by Dynamic Host Configuration Protocol (DHCP) services
68	TCP & UDP	Network > TCP/IP	bootpc	Bootstrap (BOOTP) client; also used by Dynamic Host Control Protocol (DHCP) clients
80	TCP & UDP	Web Management Interface	http	HyperText Transfer Protocol (HTTP) for World Wide Web (WWW) services
81	TCP	Web Management Interface	HTTP	Hypertext Transport Protocol
111	TCP & UDP	• Networking > NFS • Assist • SnapServer Manager	sunrpc	Remote Procedure Call (RPC) Protocol for remote command execution, used by Network Filesystem (NFS) and SnapServer Manager
123	TCP & UDP	Server > Date/Time > Advanced	ntp	Network Time Protocol (NTP)
137	TCP & UDP	Network > Windows/SMB	netbios-ns	NETBIOS Name Services used in Red Hat Enterprise Linux by Samba
138	TCP & UDP	Network > Windows/SMB	netbios-dgm	NETBIOS Datagram Services used in Red Hat Enterprise Linux by Samba
139	TCP & UDP	Network > Windows/SMB	netbios-ssn	NETBIOS Session Services used in Red Hat Enterprise Linux by Samba
389	TCP & UDP	Network > Windows/SMB	ldap	Lightweight Directory Access Protocol (LDAP)

Port #	Layer	ROS Feature	Name	Comment
443	TCP & UDP	• Web Management Interface • SnapServer Manager • SnapExtensions > Snap EDR	https	Secure Hypertext Transfer Protocol (HTTP).
445	TCP & UDP	Network > Windows/SMB	microsoft-ds	Server Message Block (SMB) over TCP/IP
852	TCP	Network > NFS		Used by rpc.mountd
882	UDP	• Snap Finder • SnapServer Manager	Sysbroker	Broadcast Discovery
933	UDP	Network > NFS		Used by rpc.statd
936	UDP	Network > NFS		Used by rpc.statd
939	TCP	Network > NFS		Used by rpc.statd
2005	TCP	SnapExtensions	SnapExtensions	Bridge from Servlet to Snap Extension framework
2049	TCP & UDP	Network > NFS	nfs [nfsd]	Network Filesystem (NFS)
2050	UDP	Network > NFS	mountd	
2051	UDP	Network > NFS	lockd	
2599	UDP	• Snap Finder • SnapServer Manager	Sysbroker	Multicast Discovery
3052	TCP	Server > UPS		Port for monitoring UPS status
8001	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8002	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8003	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications
8005	TCP	Web Management Interface	tomcat	Tomcat Shutdown port
8008	TCP & UDP	Web Management Interface	http-alt	Tomcat - Apache Bridge
9049	TCP	Sysbroker		Sysbroker Shutdown Port
9050	TCP	Sysbroker		Sysbroker RPC Port
10001	TCP	Snap Extension	Snap Extension	Shutdown Port
32780	TCP	Web Management Interface	tomcat	Random Port
32781	TCP	Web Management Interface	tomcat	Random Port
49221	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications Port
49229	TCP	SnapExtensions > SnapEDR	SnapEDR	External Communications Port
1024 - 65535	TCP & UDP	Network > NFS	NFS	Dynamically allocated in runtime for user connections

Master Glossary & Acronym List

NOTE: This is a general Overland Storage glossary and acronym list. Not all items may be found in this document or be used by this product.

1000BASE-T

1000BASE-T (also known as IEEE 802.3ab) is a standard for gigabit Ethernet over copper wiring. It requires, at a minimum, Category 5 cable (the same as 100BASE-TX), but Category 5e (Category 5 enhanced) and Category 6 cable may also be used and are often recommended. 1000BASE-T requires all four pairs to be present and is far less tolerant of poorly installed wiring than 100BASE-TX.

Access Permissions

A rule associated with a share, a file, or a directory on a drive to regulate which users can have access to the share and in what manner.

Address

An address is a data structure or logical convention used to identify a unique entity, such as a particular process or network device.

ACL

Short for *Access Control List*. A mechanism for restricting access to drive directories and files. It is a list of initiator IQNs, along with type of access (read/write or read only) granted to each initiator together with any information required for authentication.

ADS

Short for Active Directory *Service*. The preferred authentication method for Windows XP, Windows 2000, Windows 2000 Advanced Server, and Windows 3000 network users. This authentication allows Active Directory users to connect to shares on the SnapServer. The SnapServer supports the Microsoft Windows 2000 family of servers that run in native ADS mode.

Agent

A program that performs some information-gathering or processing task in the background. SnapServers support Data Protection Agents and can be configured as SNMP agents.

Algorithm

A sequence of steps designed to solve a problem or execute a process.

AllLocalUsers Group

The default group for all local users on SnapServers. Local users are set up by the SnapServer administrator. Network users or Windows domain users are not part of the AllLocalUsers group.

AllUsers Group

A collection of all users. The SnapServer automatically maintains the AllUsers group.

Array

A group of disks that are combined together to create a single large storage area. Up to 64 arrays are supported, each containing up to 16 disks per array. There is no capacity limit for the arrays. In a server context, an array refers to the grouping of hard disks into a RAID set.

ATA

Short for *Advanced Technology Attachment*. A standard interface for connecting storage devices to a PC.

Auto Balance

A feature that automatically balances preferred paths evenly among all available host ports and controller ports. Auto balancing spreads I/O load by utilizing as many host ports and controller ports as possible.

Authentication

The validation of a user's identity by requiring the user to provide a registered login name and corresponding password.

Autonegotiation

An Ethernet feature that automatically negotiates the fastest Ethernet speed and duplex setting between a port and a hub or switch. This is the default setting and is recommended.

Autosensing

An Ethernet feature that automatically senses the current Ethernet speed setting.

Back-end

Front-end and back-end are terms used to characterize program interfaces and services relative to the initial user, human or program, of these interfaces and services. A "front-end" application is one that application users interact with directly. A "back-end" application or program serves indirectly in support of the front-end services, usually by being closer to the required resource or having the capability to communicate with the required resource. The back-end application may interact directly with the front-end or, perhaps more typically, is a program called from an intermediate program that mediates front-end and back-end activities.

Back-off Percent

In order to allow disks from a different family or manufacturer to be used as a replacement for a drive in an array, it is recommended that a small percentage of the drive's capacity be reserved when creating the array. This is user selectable, from 0 to 10 percent. This is sometimes known as Reserved Capacity.

Bar Code

The machine-readable representation of a product code. Bar codes are read by a scanner that passes over the code and registers the product code. The width of black lines and white spaces between varies. Combinations of lines and spaces represent characters. Overland uses 3-of-9 code (Code 39) where each character is represented by 9 bars, 3 of which are wide.

Bonding

A technology that treats two ports as a single channel, with the network using one IP address for the server. SnapServer appliances support load balancing and failover bonding modes.

Bridging

Devices that connect and pass packets between two network segments that use different communications protocol.

Bus or Channel

A common physical path composed of wires or other media, across which signals are sent from one part of a computer to another. A channel is a means of transferring data between modules and adapters, or between an adapter and SCSI devices. A channel topology network consists of a single cable trunk that connects one workstation to the next in a daisy-chain configuration. All nodes share the same medium, and only one node can broadcast messages at a time.

CA

Short for *Certificate Authority*. A trusted third-party in a network that issues and manages security credentials.

CA Antivirus

The antivirus software bundled with the SnapServer as a SnapExtension.

Cache Flush Array

This is the array that is used to automatically flush cache data in a situation where power has failed to some of the disks.

Cat 5 Cable

Short for *Category 5*, it is network cabling that consists of four twisted pairs of copper wire terminated by 8P8C modular connectors. CAT 5 cabling supports frequencies up to 100 MHz and speeds up to 100 Mbps. (CAT 5e cabling supports frequencies up to 1000 MHz and speeds up to 1000 Mbps.) It can be used for ATM, token ring, 1000BASE-T, 100BASE-T, and 10BASE-T networking.

Cat 5 is based on the EIA/TIA 568 Commercial Building Telecommunications Wiring Standard developed by the Electronics Industries Association as requested by the Computer Communications Industry Association in 1985.

Cat 6 Cable

Short for *Category 6*, it is network cabling that consists of four twisted pairs of copper wire terminated by 8P8C modular connectors made to higher standards that help reduce noise caused by crosstalk and system noise. The ANSI/TIA-568-B.2-1 specification states the cable may be made with 22 to 24 AWG gauge wire, so long as the cable meets the specified testing standards.

It is designed for Gigabit Ethernet that is backward compatible with the Category 5/5e and Category 3 cable standards. Cat 6 features more stringent specifications for crosstalk and system noise. The cable standard provides performance of up to 250 MHz and is suitable for 10BASE-T / 100BASE-TX and 1000BASE-T (Gigabit Ethernet).

Chaining

A native SnapServer technology in which all snapshots of a volume depend on successive snapshots for part of their content.

Channel

A communications path between two computers or devices.

CHAP

Short for *Challenge Handshake Authentication Protocol*. A three-way handshake scheme used to verify the identity of remote clients in a network.

If there are security concerns, it is possible to set up authentication of targets and initiators, using the CHAP authentication protocol. With CHAP authentication, an initiator can only connect to a target if it knows the target's password or secret. To set up CHAP, the same secret must be known by both the initiator and target.

Checksum

The result of adding a group of data items that are used for checking the group. The data items can be either numerals or other character strings treated as numerals during the checksum calculation. The checksum value verifies that communication between two devices is successful.

Chunk Size

This is the amount of data that is written on a single drive before the controller moves to the next drive in the stripe.

CIFS

Short for *Common Internet Filesystem*. Also known as SMB. The default Windows protocol for communication between computers. A specification for an Internet file access protocol that complements HTTP and FTP and reduces access time.

daemon

A process that runs in the background.

default gateway

The router used when there is otherwise no known route to a given subnet.

degraded

A RAID state caused by the failure or removal of a disk in which data is consistent, but there is no redundancy.

DHCP

Short for *Dynamic Host Configuration Protocol*. A communications protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a computer network. Each system that connects to the Internet/intranet needs a unique IP address. A SnapServer can be configured to perform as a DHCP server and assign IP addresses with a single subnet.

Disaster Recovery

A strategy that allows a company to return to normal activities after a catastrophic interruption. Through failover to a parallel system or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.

Discovery

Discovery is the process by which an initiator 'discovers' a target. Discovery uses a special type of session, called a Discovery Session, where an initiator connects to a RAID storage controller and asks it to send a list of the targets present on the controller. The target will respond with a list of all the targets to which the initiator has access.

Disk Roaming

This is the process of removing a disk from a controller and putting it back later, either on the same controller, or a different one, and having it recognized as the same disk. The disks may be can be attached to different ports than they were originally attached to, without harm to the data. The disks may be attached to the same ports or different ports on the controller.

DNS

Short for *Domain Name Service*. A network service that translates domain names into IP addresses using a server that maintains a mapping of all host names and IP addresses. Normally, this mapping is maintained by the system administrator, but some servers support dynamic mappings.

DNS A Record

One of the resource records (database records) stored in the zone files of the Domain Name System (DNS). It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

Domain

A set of network resources in Windows 2000/2003/2008, such as users and groups of users. A domain may also include multiple servers on the network. To gain access to these network resources, the user logs into the domain.

Domain Name

The ASCII name that identifies the domain for a group of computers within a network.

DSM

Short for *Device Specific Module*, it is a software module that allows RAID storage array hardware to use Microsoft's MPIO.

DynamicRAID™

DynamicRAID is a powerful SnapServer feature that simplifies management of disk additions and replacements in a RAID environment. All RAID and filesystem capacity management is entirely automated. More capacity can be added over time by just inserting or replacing disks. Filesystem volumes can be added and removed at will because all volumes share the same underlying pool of storage.

Ethernet

The most widely installed LAN technology. 100BASE-T Ethernet provides transmission speeds of up to 100 Mbps. Fast Ethernet or 1000BASE-T provides transmission speeds up to 1000 Mbps and is typically used for LAN backbone systems, supporting workstations with 100BASE-T cards. Gigabit Ethernet (GbE) provides an even higher level of backbone support at 1000 Mbps (one Gigabit or one billion bits per second).

Ethernet Address

The unique six-digit hexadecimal (0-9, A-F) number that identifies the Ethernet interface.

Ethernet Port

The port on a network card to provide Ethernet access to the computer.

Event

Any significant occurrence or error in the system that may require notifying a system administrator or adding an entry to a log.

Expansion Slot

Area in a computer that accepts additional input/output boards to increase the capability of the computer.

F_port

A *Fabric* port within a Fibre Channel switch that provides a point-to-point link attachment to a single N_Port. F_Ports are intermediate ports in virtual point-to-point links between end ports, for example N_Port to F_Port to F_Port to N_Port using a single Fibre Channel fabric switch.

Failback

Failback occurs when a path with a higher priority than the currently active path is restored. In this case, I/O will "fail back" to the higher priority path once it is available again.

Failover

A strategy that enables one Ethernet port to assume the role of another port if the first port fails. If a port fails on a SnapServer, the second port assumes its network identity (if the two Ethernet cards have been configured for failover). When the port comes back online, the original identities are restored. Failover is possible only in a multi-Ethernet configuration.

Failover/Failback

A combination of Failover and Failback. When a preferred path becomes unavailable, another path is used to route I/O until the preferred path is restored. In this case I/O will "fail back" to the preferred path once it is available again.

FC-AL

Short for *Fibre Channel Arbitrated Loop*. An FC-AL is a Fibre Channel network in which up to 126 systems and devices are connected in a loop topology, with each transmitter connecting to the receiver of the device on its logical right. The Fibre Channel Arbitrated Loop protocol used for transmission is different from Fibre Channel switched and point-to-point protocols. Multiple FC-AL loops can be connected via a fabric switch to extend the network.

Fibre Channel

Fibre Channel (FC) is a gigabit-speed network technology which transports SCSI commands over Fibre Channel networks. Fibre Channel was primarily concerned with simplifying the connections and increasing distances, but later designers added the goals of connecting SCSI disk storage, providing higher speeds and far greater numbers of connected devices.

Filesystem

See NFS.

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM). Firmware is often responsible for the behavior of a system when it is first switched on.

FL_port

A *Fabric Loop* port within a Fibre Channel switch that is capable of Fibre Channel Arbitrated Loop operations and is connected to one or more NL_Ports via a Fibre Channel Arbitrated Loop. An FL_Port becomes a shared entry point for public NL_Port devices to a Fibre Channel fabric. FL_Ports are intermediate ports in virtual point-to-point links between end ports that do not reside on the same loop, for example NL_Port to FL_Port to F_Port to N_Port through a single Fibre Channel fabric switch.

Front-end

See Back-end.

FTP

Short for *File Transfer Protocol*. A standard Internet protocol that provides a way to exchange files between computers on the Internet. By default, a SnapServer is set up to be an FTP server.

Full-duplex

A type of transmission that allows communicating systems to both transmit and receive data simultaneously.

Gateway

The hardware or software that bridges the gap between two network subnets. It allows data to be transferred among computers that are on different subnets.

Gigabit Ethernet

Also known as GigE or GbE, this Ethernet standard uses a one Gigahertz (1000 Hz) clock rate to move data.

GID

Short for *Group Identification*. On a SnapServer, the unique ID assigned to each group of users for security purposes.

GuardianOSImage.gsu

An image file used to upgrade the GuardianOS.

HBA

Short for *Host Bus Adapter*. An HBA is an I/O adapter that sits between the host computer's bus and the Fibre Channel loop and manages the transfer of information between the two channels. In order to minimize the impact on host processor performance, the HBA performs many low-level interface functions automatically or with minimal processor involvement.

Half-duplex

A type of transmission that transfers data in one way at a time.

Hidden Share

A share that restricts the display of the share via the Windows (SMB), Web View (HTTP/HTTPS), FTP, and AFP protocols. See also SMB.

Host Bus Adapter

Connects a host system (such as a SnapScale) to other network and storage devices.

Host Name

The unique name by which a computer is known on a network. It is used to identify the computer in electronic information interchange.

Hot Spare

A disk that can automatically replace a damaged disk in a RAID 1, 5, 6, 10, 50 or 60. If one disk in a RAID fails or is not operating properly, the RAID automatically uses the spare to rebuild itself without administrator intervention. A *local* spare is associated with and available only to a single RAID. A *global* spare is associated with a single RAID, but may be used for any RAID in the system.

Hot Swapping

The ability to remove and add disks to a system without the need to power down or interrupt client access to filesystems. Not all components are hot-swappable. Please read installation and maintenance instructions carefully.

HTTP

Short for *Hypertext Transfer Protocol*. An application protocol for transferring files (text, graphic images, sound, video, and other multimedia files) over TCP/IP on the World Wide Web.

HTTPS

Short for *Hypertext Transfer Protocol Secure*. The HTTP protocol using a Secure Sockets Layer (SSL). SSL provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

IDE

Short for *Integrated Drive Electronics*. A standard interface for connecting storage devices to a PC.

Inheritance

In Windows permissions, inheritance is the concept that when permissions for a folder are defined, any subfolders within the defined folder inherit its permissions. This means an administrator need not assign permissions for subfolders as long as identical permissions are desired. Inheritance greatly reduces administrative overhead and also results in greater consistency in access permission management.

Initialization

RAID 5, 6, 50, and 60 disk arrays must have consistent parity before they can be used to protect data. Initialization writes a known pattern to all disks in the array. If you choose not to initialize an array, the array will be trusted. Any disk failure results in data corruption in a trusted array. (It is possible to later perform a parity rewrite that recalculates the parity based on the current data, thus ensuring the data and parity are consistent.)

Initiator Device

A system component that originates an I/O command over an I/O bus or network. An initiator issues the commands; a *target* receives them.

An initiator normally runs on a host computer. It may be either a software driver or a hardware plug-in card, often called a Host Bus Adapter (HBA). A software initiator uses one of the computer's Ethernet ports for its physical connection, whereas the HBA will have its own dedicated port.

Software initiators are readily available for most host operating systems. Hardware initiators are not widely used, although they may be useful in very high performance applications or if 10 Gigabit Ethernet support is required.

Internal Logical Drive

An internal logical drive is identical to a regular logical drive, except it is NOT made visible to a host adapter as a LUN. Instead, internal logical drives are used for setting up snapshot ODAs that are only accessed internally by the RAID controller.

Internet

A global network of networks used to exchange information using the TCP/IP protocol. It allows for electronic mail and the accessing ad retrieval of information from remote sources.

I/O (Input/Output)

The operation of transferring data to or from a device, typically through an interface protocol like CIFS, NFS, or HTTP. The SnapServer presents a filesystem to the user and handles block I/O internally to a RAID array.

IP

Short for *Internet Protocol*. The unique 32-bit value that identifies the location of the server. This address consists of a network address, optional subnetwork address, and host address. It displays as four addresses ranging from 1 to 255 separated by periods.

IQN

Short for *iSCSI Qualified Name*. A name format used in the iSCSI protocol.Initiators and targets have IP addresses, just like any other network entity. They are also identified using an iSCSI name, called the iSCSI Qualified Name (IQN). The IQN should be unique

worldwide. It is made up of a number of components, specifying the date, identifying the vendor in reverse format, and then uniquely identifying the initiator or target. An example of an IQN is:

```
iqn.2001-04.com.example:storage:diskarray-sn-123456789
```

Since these IQNs are rather unwieldy, initiators and targets also use short, user friendly names (sometimes called alias names or just aliases).

iSCSI

Short for *Internet SCSI*. iSCSI is an IP-based storage networking standard for linking data storage facilities. iSCSI is a standard that defines the encapsulation of SCSI packets in TCP and then routing it using IP. It allows block-level storage data to be transported over widely used IP networks.

iSNS Server

Short for *Internet Storage Name Service* Server. A protocol enabling the automatic discovery, configuration, and management of iSCSI devices on a TCP/IP network.

Kerberos

A secure method for authenticating a request for a service used by ADS. Kerberos lets a user request an encrypted "ticket" from an authentication process that can then be used to request a service from a server. The user credentials are always encrypted before they are transmitted over the network.

In Windows 2000/XP, the domain controller is the Kerberos server. The Kerberos key distribution center (KDC) and the origin of group policies are applied to the domain.

LACP

Link Aggregation Control Protocol provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).

LAN

Short for *Local Area Network***.** A network connecting computers in a relatively small area such as a building.

LCD

Short for *Liquid Crystal Display*. An electronic device that uses liquid crystal to display messages.

LED

Short for *Light-Emitting Diode*. An LED is a type of diode that emits light when current passes through it. Visible LEDs are used as indicator lights on electronic devices.

Linux

A UNIX-like operating system that was designed to provide personal computer users a free or very low-cost operating system comparable to traditional and usually more expensive UNIX systems. GuardianOS and RAINcloudOS are based on the Linux operating system.

Load Balancing

A process available only in multi-Ethernet configurations. The Ethernet port transmission load is distributed among two or more network ports (assuming the cards are configured for load balancing). An intelligent software adaptive agent repeatedly analyzes the traffic flow from the server and distributes the packets based on destination addresses.

Local Group/Local User

A group/user defined locally on a SnapServer using the Web Management Interface. The local user is defined by the server administrator. Windows domain, ADS, and NIS users are not considered local.

Logical Drive

A drive that is defined or created from regions of an array, a whole array, or a combination of regions of different arrays. The logical drive appears as a single drive to one or more host systems.

Logical Drive Availability

To accommodate hosts with multiple ports and multiple host systems, it is possible to restrict a logical drive's availability to a particular HBA or controller port. Access can be enabled or disabled for each host port of each controller.

LUN

Short for *Logical Unit Number*. A SCSI or Fibre Channel device identifier. LUN is a subdivision of a SCSI target.

MAC Address

Short for *Media Access Control address*, a hardware address that uniquely identifies each node of a network. In the Open Systems Interconnection (OSI) model, one of two sublayers of the Data Link Control layer concerned with sharing the physical connection to the network among several computers. Each Ethernet port has a unique MAC address. SnapServer appliances with dual-Ethernet ports can respond to a request with either port and have two unique MAC addresses.

Maintenance Mode

A series of HTML pages in the GuardianOS or RAINcloudOS Web Management Interface that allows you to perform repair, upgrade, or reinstall GuardianOS or RAINcloudOS in a disaster recovery situation.

Mapped LUN Number

Each logical drive is presented to the host system with a unique LUN. In certain cases (such as after deleting another logical drive) it may be desirable to change the number that a logical drive is presented as. This can be done at any time, bearing in mind that any attached host systems may need to be rebooted or reconfigured to maintain access to the logical drive.

Mapping table

A table indexed by sequential LUN values, indicating the selected BUS:TARGET:LUN devices. Mapping tables are used by routers and bridges like the GEOi to perform Ethernet-to-SCSI pathing.

MD5 Algorithm

MD5 is a way to verify data integrity, and is much more reliable than checksum and many other commonly used methods.

MIB

Short for *Management Information Base*. A formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). The format of the MIB is defined as part of SNMP.

Mirroring

Used in RAID 1 and 10, a process of storing data on one disk and copying it to one or more disks, creating a redundant storage solution. RAID 1 is the most secure method of storing mission-critical data.

Mounted

A filesystem that is available.

MPIO

Short for *Multipath Input/Output*. A multipath solution built into Microsoft server-grade operating systems. It requires the DSM to work with RAID storage array hardware.

MTU

Short for *Maximum Transfer Unit*. It is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network.

Multihomed

A SnapServer that is connected to two or more networks or has two or more network addresses.

N_port

A *Node* port connects via a point-to-point link to either a single N_Port or a single F_Port. N_Ports handle creation, detection, and flow of message units to and from the connected systems. N_Ports are end ports in virtual point-to-point links through a fabric, for example N_Port to F_Port to F_Port to N_Port using a single Fibre Channel fabric switch.

NAS

Short for *Network Attached Storage***.** Hard disk storage that is set up with its own network address as opposed to being attached to the department computer that is serving applications to a network's workstation users. By removing storage access and its management from the department server, both application programming and files can be served faster because they are not competing for the same processor resources. The NAS device is attached to a local area network (typically an Ethernet network) and assigned an IP address.

NAT

Short for *Network Address Translation*. A technique for passing network traffic through a router whereby one set of IP addresses is used on one side of the router and another set of addresses is used on the other side. This is done to avoid address conflicts and to increase the address space of the internal network.

NDMP

Short for *Network Data Management Protocol*. A protocol standard used by some Network Attached Storage systems to provide an industry standard means to do backup and restores of the NAS system without the need for 3rd party agents to be installed on the NAS device. Also see NDMP.org for further details.

NFS

Short for *Network Filesystem*. A client/server application that allows a computer user to view and optionally store and update files on a remote computer as though they were on the user's own computer. The user's system needs to have an NFS client and the other computer needs the NFS server. The SnapServer is configured as an NFS server by default.

NIC

Short for *Network Interface Card*. A board that provides network communication capabilities to and from a computer.

NIS

Short for *Network Information Service*. A network naming and administration system for smaller networks that was developed by Sun Microsystems. NIS+ is a later version that provides additional security and other facilities. The SnapServer accepts NIS users and groups.

NL_port

A *Node Loop* port is capable of arbitrated loop functions and protocols. An NL_Port connects via an arbitrated loop to other NL_Port and at most a single FL_Port. NL_Ports handle creation, detection, and flow of message units to and from the connected systems. NL_Ports are end ports in virtual point-to-point links through a fabric, for example NL_Port to F_Port to F_Port to N_Port using a single Fibre Channel fabric switch. In the absence of a fabric switch FL_Port, NL_Ports can communicate with other NL_Ports in virtual point-to-point links through a FC-AL open loop circuit often through FC-AL (Arbitrated Loop) hub or loop switch devices.

Node

Any device, including servers, workstations, or tape devices, that are connected to a network; also the point where devices are connected.

Node Name

This is an eight-byte, 16-character hexadecimal number, uniquely identifying a single fibre device. It incorporates the World Wide Name and two additional bytes that are used to specify the format. In a host system with multiple FC ports, all adapters typically use the same Node Name, but unique Port Names.

NTFS

Short for *New Technology File System*. The standard file system used by Windows NT and later versions of the Windows operating system.

NTP

Short for *Network Time Protocol*. A protocol for synchronizing the system clocks of computers over a packet-switched network.

NVRAM

Abbreviation of *Non-Volatile Random Access Memory*, a type of memory that retains its contents when power is turned off.

ODA

The *Overwrite Data Area* is an internal storage area on an array that is dedicated to storing data from a snapshot logical drive. The data stored on the ODA is the data from the logical drive that needed to be overwritten after a snapshot was initiated. The ODAs are mapped on top of internal logical drives. An ODA cannot be accessed externally through a host LUN; it is only accessed internally.

ODA Stripe Size

The read/write block size that the system will use when copying data from the original logical drive to the ODA.

Orphan

A drive that has become disconnected from its RAID either by accidental removal of the disk or the intermittent failure of the drive.

Parity

Error correction data. RAIDs 5, 6, 50, and 60 store equal portions of each file on each disk and distributes parity information for each file across all disks in the group. This distributed parity allows the system to recover from a single disk failure.

Permissions

A security category, such as no access, read-only, or read-write, that determines what operations a user or group can perform on folders or files.

Pool

A pool is a collection of RAID disks, grouped together by the RAID storage controller. iSCSI volumes are created from these pools. New volumes can be created and existing volumes can be extended, provided there is spare capacity in the pool from which the volume was created.

PoP

Short for *Proof of Purchase*. The number used to obtain a license key for an upgrade to third-party applications.

Port Name

This is an eight-byte hexadecimal number, uniquely identifying a single host HBA port. It incorporates the World Wide Name and two additional bytes that are used to specify the format and indicate the port number.

Portal

A target's IP address together with its TCP port number.

POSIX

Short for *Portable Operating System Interface*. A set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to develop programs that could run on multiple platforms without the need to recode.

Preferred Path

The preferred path is the default path. When the path selection policy is set to Failover/Failback, the preferred path is always used if it is available. If the preferred path fails, I/O switches to another path. If it is later restored, I/O switches back to the preferred path.

Protocol

A standardized set of rules that specifies the format, timing, sequencing, and/or error checking for data transmissions.

PTP

Short for *Point-to-Point*. PTP is the common mode of attachment to a single host. PTP is sometimes used to attach to a Fibre Channel switch for SAN connectivity.

Public Access Share

A share that allows all users read/write access to the filesystem.

Quota

A limit on the amount of storage space on a volume that a specific user or NIS group can consume.

RAID

Short for *Redundant Array of Independent Disks*. A data storage scheme where multiple hard drives are combined to form a single logical unit which is highly reliable and gives good performance. Reliability is achieved by mirroring (the copying of data to more than one disk), striping (the splitting of data across more than one disk) and error correction (redundant data is stored to enable faults to be detected and corrected).

RAID 0 (Striped)

RAID 0 is ideal for environments in which performance (read and write) is more important than fault tolerance, or you need the maximum amount of available drive capacity in one volume.

Data is striped across multiple disks so that it can be read and written in parallel. It provides higher performance than a single disk, especially when reading or writing large files, but it is vulnerable to a disk failure. If any disk in the pool fails, the entire pool is effectively lost. For this reason, RAID 0 pools should only be used in cases where the loss of the data is unimportant, for example, because it can easily be recreated from another data source. The capacity of a RAID 0 pool is equal to the total capacity of all the disks making up the pool[1]. For example, a RAID 0 pool made up of 4 x 1 TB disks will have a capacity of 4 TB.

RAID 1 (Mirrored)

RAID 1 is useful for building a fault-tolerant system or data volume, providing excellent availability without sacrificing performance. However, you lose 50 percent of the assigned disk capacity.

RAID 1 is also called disk mirroring: data is stored on two identical disks, so that if one disk fails, the other can still be used to access the data. Write operations are performed in parallel to both disks, so write performance is identical to that of a single disk; read operations can be done to either disk, so effectively read performance is doubled.

1Capacity is usually very slightly less because a small but insignificant amount of space is reserved by the RAID controller to store internal metadata.

If one of the disks fails, it should be replaced. When it is replaced, the RAID pool will automatically be rebuilt by copying all the data from the surviving disk to the new disk. While the rebuild is occurring, there will be a degradation in performance.

Because disks are mirrored, the usable capacity of a pair of RAID 1 disks is only equal to the capacity of a single disk, so that a RAID 1 pool made of 2 x 500 GB disks will have a capacity of 500 GB.

RAID 5 (Striping with Parity)

With a RAID 5 pool, because data is read from many disks in parallel, as for RAID 0, read performance is good. Write performance is slightly lower because, in addition to writing the data, parity data has to be calculated and written. If a hardware RAID controller is used, this will be done using dedicated hardware; if software RAID is used, the work will be done on the main processor of the storage controller.

The capacity of a RAID 5 pool is reduced by exactly one disks worth of capacity, which is required to store the parity data. For example, a RAID 5 pool made up of 3 x 500 GB disks will have a capacity of 1 TB.

In principle, a RAID 5 pool could have a very large number of disks. However, the more disks there are, the greater the chance of a double disk failure. If a single disk fails, the data is no longer protected until the disk has been replaced and the pool has been rebuilt by reconstructing all the data from the failed disk and writing it to the new disk. If the disk capacities are very large, it may take many hours to rebuild the pool. If a second disk fails before the rebuild has completed, all the data in the pool will be lost. That is to say, large capacity disks increase the time taken to rebuild the pool, during which time the pool is vulnerable to a second disk failure. Moreover, the chance of a second disk failure increases as the number of disks in the pool increases.

RAID 5 is similar to RAID 0 in that data is striped across multiple disks. However, one disks worth of space is reserved to store parity data, which can be used to reconstruct the pool in the event of one of its disks failing. With RAID 5, the parity data is distributed across all the disks in the pool. If a single disk fails, each block of data stored on that disk can be reconstructed using the corresponding data block from all the other disks along with the parity block. This means that if a single disk fails, data can still be read, albeit at a rather slower rate (because it needs to be reconstructed, rather than read directly). For this reason, a RAID 5 pool with a disk failure is referred to as a degraded pool.

RAID 6 (Striping with Dual Parity)

RAID 6 is similar to RAID 5 but instead of storing a single disk's worth of parity data, two disk's worth are stored, making the pool capable of withstanding the failure of two disks. However, there is an additional write overhead involved in calculating the double parity data. Since RAID 6 works best with dedicated hardware, RAID 6 is only offered on systems with a hardware RAID controller. Read performance is similar to that of RAID 0 or 5. Since two disks are used for storing parity data, the capacity of a RAID 6 pool made up of 8 x 500 GB disks will be 3 TB.

RAID 10 (Striped Mirroring)

RAID 10 is defined as mirrored stripe sets or also known as RAID 0+1. You can build RAID 10 either directly through the RAID controller (depending on the controller) or by combining software mirroring and controller striping, or vice versa (called RAID 01).

RAID 50

A RAID 50 combines the straight block-level striping of RAID 0 with the distributed single parity of RAID 5. That is, a RAID 0 array striped across RAID 5 elements. It requires at least 6 disks. This can increase the performance by allowing the controller to more efficiently cluster commands together. Fault tolerance is also increased, as one disk can fail in each individual array.

RAID 60

A RAID 60 combines the straight block-level striping of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID 6 elements. It requires at least 8 disks. This can increase the performance by allowing the controller to more efficiently cluster commands together. Fault tolerance is also increased, as two drives can fail in each individual array.

RAINcloudOSImage.gsu

An image file used to upgrade the RAINcloudOS.

Recurring Snapshot

A snapshot that runs at an administrator-specified time and interval.

Restrict Anonymous

A Windows feature in which anonymous users cannot list domain user names and enumerate share names. Microsoft has provided a mechanism in the Registry called restrict anonymous for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names.

The implementation of the restrict anonymous mechanism may prevent the SnapServer from obtaining the list of account names it needs to authenticate Windows domain users.

Resynchronization

A RAID state that describes the process of integrating a new drive into the RAID.

RETMA

Short for *Radio-Electronics-Television Manufacturers' Association*. It is the common name given for a 19-inch distribution frame rack for mounting components.

Rollback

A snapshot feature that allows the administrator to restore a volume to a previous state as archived in a snapshot without resorting to tape.

Round Robin

The Round Robin path selection policy causes all healthy paths to be used for I/O. Paths are used in a round-robin order.

Router

A router is a device that enables connectivity between Ethernet network segments.

SAN

Short for *Storage Area Network*. Data storage connected to a network that provides network clients access to data using block level protocols. To the clients, the data storage devices appear local rather than remote. An iSCSI SAN is sometimes referred to as an IP-SAN.

SAS

Short for *Serial Attached SCSI*. It is a point-to-point serial protocol that replaces parallel SCSI bus technology (multidrop) and uses the standard SCSI command set. It has no termination issues, supports up to 16,384 devices (using expanders), and eliminates clock skew. It consists of an Initiator that originates device service requests, a Target containing logical units that receives device service requests, and a Service Delivery Subsystem that transmits information between the Initiator and the Target.

SCSI

Short for *Small Computer System Interface*. SCSI is an industry standard for connecting peripheral devices and their controllers to an initiator. Storage devices are daisy-chained together and connected to a host adapter. The host adapter provides a shared bus that attached peripherals use to pass data to and from the host system. Examples of devices attached to the adapter include disks, CD-ROM discs, optical disks, and tape drives. In theory, any SCSI device can be plugged into any SCSI controller.

SCSI addressing

Each device supported by a SCSI adapter has its own unique SCSI address, which dictates the device's priority when arbitrating for access to the SCSI bus. A SCSI address of 7 has the highest priority. For a fast/wide SCSI adapter that supports up to 16 devices, the next highest priority address is 6, then 5, 4, 3, 2, 1, 0, 15, 14, 13, 12, 11, 10, 9, and 8. The narrow SCSI adapter supports up to eight devices, including itself. The SCSI address 7 has the highest priority, followed by 6, 5, 4, 3, 2, 1, and 0.

SCSI bus

A SCSI bus provides a means of transferring data between SCSI devices. A SCSI bus is either an 8- or 16-bit bus that supports up to 8 or 16 devices, including itself. The bus can consist of any mix of initiators and targets, with the requirement that at least one initiator and one target must be present.

SCSI device

A SCSI device is a single unit on a SCSI bus that originates or services SCSI commands. A SCSI device is identified by a unique SCSI address. SCSI devices can act as initiators or targets.

SCSI port

A SCSI port is an opening at the back of a router that provides connection between the SCSI adapter and SCSI bus.

Serial Number

The ten-character alphanumeric number assigned by the manufacturer at the factory.

Server Number

A numeric derived from the MAC address of your SnapServer's primary Ethernet port that is used to uniquely identify a SnapServer.

Session

When an initiator wants to establish a connection with a target, it establishes what is known as an iSCSI session. A session consists of one or more TCP/IP connections between an initiator and a target. Sessions are normally established (or re-established) automatically when the host computer starts up, although they also can be established (and broken) manually.

Share

A virtual folder that maps to the root of a volume or a directory on the volume. Permissions are assigned to a share that determine access for specific users and groups.

Share Access

Permissions granted or denied to users and groups that control user and group access to the files.

S.M.A.R.T.

Short for *Self Monitoring, Analysis and Reporting Technology*. A standard mechanism for querying disks to monitor performance and reliability attributes, such as temperature, read error rates and seek times. S.M.A.R.T. systems are built into most modern disks.

SMB

Short for *Server Message Block*. A protocol for Windows clients. SMB uses the TCP/IP protocol. It is viewed as a complement to the existing Internet application protocols such as FTP and HTTP. With SMB, you can access local server files, obtain read-write privileges to local server files, share files with other clients, and restore connections automatically if the network fails.

SMS

Short for *Short Message Service*. Is a means of sending short text messages to a mobile phone.

SMTP

Short for *Simple Mail Transfer Protocol*. A TCP/IP protocol used for sending and receiving email.

Snap EDR

A SnapExtension that copies the contents of a share from one SnapServer to another share on one or more SnapServers. Snap EDR is designed to work with SnapServers and other SnapServer Storage Solutions.

Snapback

The process of restoring a logical drive from a selected snapshot. This process takes place internally in the RAID controller firmware and needs no support from any backup utility.

SnapDRImage

The SnapServer disaster recovery image that saves server-specific settings such as server name, network, RAID, volume and share configuration, local user and group lists, and snapshot schedules.

SnapExtension

A Java application that extends a SnapServer's functionality. SnapExtensions are produced both by SnapServer and third-party vendors.

SnapServer Manager

The SnapServer Manager (SSM) is a Java-based utility for discovering and monitoring SnapServers.

Snapshot

A method for producing a point-in-time image of a logical drive that results in a consistent, stable, point-in-time image of a volume (filesystem) used for backup purposes. In the process of initiating a snapshot, no data is actually copied from the snapshot logical drive. However as new writes are made to a snapshot logical drive, existing data blocks are copied to the ODA before the new data is written to the logical drive.

Snapshot LUN

A special LUN created from a combination of the snapshot logical drives' data and the data contained in the ODA.

Snapshot Number

Identifier that references one of several snapshots of the same logical drive.

Snapshot Pool

Disk space reserved within a RAID for the storage of snapshot data. In the default storage configuration of many SnapServers, twenty percent of the RAID capacity is allocated to the snapshot pool.

Snapshot Share

A virtual folder that allows access to all current snapshots at the same directory level as the original share on which it is based.

SNMP

Short for *Simple Network Management Protocol*. A system to monitor and manage network devices such as computers, routers, bridges, and hubs. SNMP views a network as a collection of cooperating, communicating devices, consisting of managers and agents.

SSH

Short for *Secure Shell*. A service that provides a remote console for special system administration and customer support access to the server. SSH is similar to telnet but more secure, providing strong encryption so that no passwords cross the network in clear text.

SSL

Short for *Secure Sockets Layer*. A protocol for managing the security of a message sent on the Internet. It is a type of technology that provides data encryption, server authentication, message integrity, and client authentication for any TCP/IP connection.

Standalone

A network bonding mode which treats each port as a separate interface. This configuration should be used only in multihomed environments in which network storage resources must reside on two separate subnets.

Static IP Address

An IP address defined by the system administrator rather than by an automated system, such as DHCP. The SnapServer allows administrators to use DHCP-assigned or statically assigned IP addresses.

Storage Area Network

See SAN.

Stripe

The process of separating data for storage on more than one disk. For example, bit striping stores bits 0 and 4 of all bytes on disk 1, bits 1 and 5 on disk 2, etc.

Stripe Size

This is the number of data drives multiplied by the chunk size.

Sub-array

In RAID 50 applications, this is the name given to the individual RAID 5 arrays that are striped together. Each sub-array has one parity drive.

Subnet Mask

A portion of a network that shares a common address component. On TCP/IP networks, subnets are all devices with IP addresses that have the same prefix.

Switch Trunking and Link Aggregation (802.3ad)

This is a computer networking term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

Target

A target is a device (peripheral) that responds to an operation requested by an initiator (host system). Although peripherals are generally targets, a peripheral may be required to act temporarily as an initiator for some commands (for example, SCSI COPY command).

Targets are embedded in iSCSI storage controllers. They are the software that makes the RAID storage available to host computers, making it appear just like any other sort of drive.

TCP/IP

Short for *Transmission Control Protocol/Internet Protocol*. The basic protocol used for data transmission over the Internet.

Telco

Short for *Telephone Company*. When used in reference to a rack, it refers to the two-posted, light-weight rack for center-mounted appliances.

Telnet

A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on a computer and connects it to a server on the network. You enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid user name and password. Telnet is a common way to remotely control Web servers.

Terminator

A terminator refers to the electrical connection at each end of a SCSI bus. The terminator is composed of a set of resisters, or possibly other components. The function of a terminator is to provide a pull-up for open collector drivers on the bus, and also impedance matching to prevent signal reflections at the ends of the cable. SCSI buses require that a terminator be placed on the SCSI connector on the last SCSI peripheral. Data errors may occur in a SCSI bus that is not terminated.

TOE (TCP Offload Engine)

Short for *TCP Offload Engine*. TOE is a technology used in network interface cards to offload processing of the entire TCP/IP stack to the network controller. It is primarily used with high-speed network interfaces, such as gigabit Ethernet and 10 gigabit Ethernet, where processing overhead of the network stack becomes significant.

Topology

Logical layout of the parts of a computer system or network and their interconnections. There are two types of topology: physical and logical. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Logical topology is the method used to pass the information between workstations.

Trap

A signal from a device informing an SNMP management program that an event has occurred.

U

A standard unit of measure for designating the height in computer enclosures and rack cabinets. One U equals 1.75 inches. For example, a 3U server chassis is 5.25 inches high.

UDP

Short for *User Datagram Protocol*. A communications protocol for sending messages between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol but, unlike TCP, does not guarantee reliability or ordering of data packets.

UID

Short for *User Identification*. A unique ID assigned to each user on a SnapServer for security purposes.

Unassigned

The state of a disk that is seated in a slot but has not been incorporated into a RAID.

Unassigned Free Space

The controller keeps a map of all the space that is not assigned to any logical drive. This space is available for creation or expansion. Each unassigned region is individually listed.

UNC

Short for *Universal Naming Convention*. In a network, a way to identify a shared file in a computer without having to specify (or know) the storage device it is on. In the Windows OS, the UNC name format is as follows:

```
\\server_name\share_name\path\file_name
```

UPS

Short for *Uninterruptible Power Supply*. A device that allows a computer to keep running for a short time when the primary power source is lost. It also provides protection from power surges. A UPS device contains a battery that starts when the device senses a loss of power from the primary source.

URL

Short for *Uniform Resource Locator*. A Web address.

USB Port

USB is short for *Universal Serial Bus*. A USB port is a hardware interface for low-speed peripherals such as the keyboard, mouse, joystick, scanner, printer, and telephony devices.

VDS

Short for *Virtual Disk Service*. VDS is a feature of Microsoft Windows (from Windows Server 2003 onwards). It provides a consistent interface for managing storage devices and creating volumes. Each vendor of a storage solution can write their own hardware provider module that enables the standard set of VDS commands to be used with different enclosures. Thus, multiple storage systems by different vendors can be controlled using the same set of VDS commands.

Virtual LUN

See Snapshot LUN.

VLAN

Short for *Virtual LAN*. It consists of a network of computers that behave as if they are connected to the same wire - even though they may actually be physically connected to different segments of a LAN.

Volumes

A logical partition of a RAID's storage space that contains a filesystem. Volumes are created from storage pools, using unused capacity in a pool. They can be extended in size, so long as there is free capacity in the pool.

A volume appear to a host computer just like a regular, physical disk except that it is attached by means of iSCSI instead of traditional disk interconnects such as IDE, SCSI or SATA.

Each volume has an iSCSI target associated with it. The volume is mapped to Logical Unit Number (LUN) 0 of the iSCSI/SCSI target, just like a regular physical disk. Associated with the target is an Access Control List (ACL) that defines which host systems are allowed to access the volume.

When the iSCSI initiator on the host computer connects to the iSCSI target, the iSCSI volume becomes available for use.

VSS

Short for *Volume Shadow Copy Service*. A low level communications interface that enables volumes to be backed up without having to halt all applications that are reading or writing the volumes. Microsoft VSS provides a mechanism for creating consistent point-in-time copies of data known as shadow copies.

Web Management Interface

A Web-based utility used for configuration and ongoing maintenance, such as monitoring server conditions, configuring email alerts for key events, or for SNMP management.

Web View

The Web-browser page that opens when users access a SnapServer using their Web browsers, and displays a list of all shares.

Windows Domain Authentication

Windows-based networks use a domain controller to store user credentials. The domain controller can validate all authentication requests on behalf of other systems in the domain. The domain controller can also generate encrypted challenges to test the validity of user credentials. Other systems use encrypted challenges to respond to CIFS/SMB clients that request access to a share.

WINS

Short for *Windows Internet Naming Service*. The server that locates network resources in a TCP/IP-based Windows network by automatically configuring and maintaining the name and IP address mapping tables.

Workgroup

A collection of computers that are grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name.

Write-Back Cache

A caching method in which modifications to data in the cache aren't copied to the cache source until absolutely necessary. Write-back caching yields somewhat better performance than write-through caching because it reduces the number of write operations to main memory. With this performance improvement comes a slight risk that data may be lost if the system crashes.

Index

Symbols

Numerics

A

B

C

D

R

S

T

U

V

W