SecureTransport

Version 5.4

2 April 2024

Appliance Guide

Platform version 7.2.0

This documentation describes the following Axway software:

Axway SecureTransport 5.4

Contents

About the SecureTransport Appliance Platform

The SecureTransport Appliance Platform provides a ready solution for SecureTransport installation and deployment. It is available either as installed on a hardware server or as a SUSE image you install on your own virtual infrastucture.

This document describes features of the SecureTransport Appliance Platform version 7.2.0 with SecureTransport 5.4 installed and provides some procedures and reference material to help you configure and maintain it.

Who should read this guide

This guide is intended for system administrators who install the SecureTransport Appliance Platform and perform its initial configuration. This guide is also intended for enterprise personnel involved in installing the SecureTransport Appliance and Axway Professional Services personnel.

This guide presumes you have knowledge of:

- Your company's business processes and practices
- Your company's hardware, software, and IT policies
- The Internet, including use of a browser

Related documentation

SecureTransport provides the following documentation:

- *SecureTransport Administrator's Guide* – This guide describes how to use the SecureTransport Administration Tool to configure and administer your SecureTransport Server. The content of this guide is also available in the Administration Tool online help.
- *SecureTransport REST API documentation* – The portal published API documentation derived from the API swagger documents. To access the administrator API documentation, go to SecureTransport Administrator API v1.4. To access the end-user API documentation, go to SecureTransport End-User API v1.4.
- *SecureTransport Appliance Guide* - (Current document) This guide provides the SecureTransport Appliance installation, configuration, and operation instructions. It also provides installation and upgrade instructions on SecureTransport Appliances.
- *SecureTransport Capacity Planning Guide* – This guides provides information useful when planning your production environment for SecureTransport.

- *SecureTransport Developer's Guide* – This guide provides the descriptions and usage of the plug-able information for the SecureTransport Pluggable Transfer Site and how to implement a Pluggable Transfer Site. It also provides Swagger REST API integration instructions and custom Address Book source implementation instructions and custom plugins/exits source implementation instructions.
- *SecureTransport Getting Started Guide* – This guide explains the initial setup and configuration of SecureTransport using the SecureTransport Administrator setup interface.
- *SecureTransport Installation Guide* – This guide explains how to install and uninstall SecureTransport on UNIX-based platforms and Microsoft Windows.
- *SecureTransport Release Notes* – This document contains information about new features and enhancements, information received after the finalization of the rest of the documentation, and a list of known and fixed issues.
- *SecureTransport Security Guide* – This guide provides security information necessary for the secure operation of the SecureTransport product.
- *SecureTransport Software Development Kit (SDK)* – A set of software development tools and examples that allow extending SecureTransport by consuming and implementing available APIs.
- *SecureTransport Upgrade Guide* - This guide explains how to upgrade SecureTransport on UNIX-based platforms and Microsoft Windows.
- *ST Web Client Configuration Guide* - This guide describes how to configure and customize the ST Web Client user interface.
- *ST Web Client User Guide* – This guide describes how to use the ST Web Client.

Go to Axway Support at support.axway.com to view or download documentation. The website requires login credentials and is for customers with active support contracts.

Get more help

Go to Axway Support at support.axway.com to get technical support, download software, documentation and knowledgbase articles. The website requires login credentials and is for customers with active support contracts.

The following support services are available:

- Official documentation
- Product downloads, service packs, and patches
- Information about supported platforms
- Knowledgebase articles
- Access to your cases

When you contact Axway Support with a problem, be prepared to provide the following information for more efficient service:

- Product version and build number
- Database type and version
- Operating system type and version

- Service packs and patches applied
- Description of the sequence of actions and events that led to the problem
- Symptoms of the problem
- Text of any error or warning messages
- Description of any attempts you have made to fix the problem and the results

Training

Axway offers training across the globe, including on-site instructor-led classes and self-paced online learning. For details, go to training.axway.com

Appliance console menu reference 1

The Appliance Console menu consists of subpages, each with several options. The following table provides a quick reference for Appliance Console Menu options organized as they appear in the various subpages, and cross-references to other parts of this document where appropriate.

Console Menu Subpage	Options
Appliance Management	**Reboot/Shut down System** — Reboot or shutdown your appliance. See *Connect to, reboot, and shut down the Appliance* on page 12. **System Management** — Switch between consoles, set time zone & date and work with system files. See *System management tips* on page 25 **Clock/Timezone** — Set the appliance clock and time zone. This is especially useful for clustered machines. See *Set the clock and time zone* on page 25. **Keyboard Layout** — Select a language-based layout for your keyboard. **System Log Files** — Access your appliance's log files. See *Work with system log files* on page 26. **Enable/Disable Independent Wallclock** (*Amazon EC2 images only*) — Enable or disable time sync with the host server of the virtual appliance. When enabled, the virtual appliance will always perform time sync with the host server. The normal system time sync via NTP will have no effect. When disabled, the virtual appliance will not perform the time sync with the host server and will need another time sync method; for example, NTP.
Hardening & Security	**Password Configuration** — Specify rules for your appliance password. See *Manage the appliance password* on page 19. **SuSEFirewall Management** — Enable or disable firewall functionality and configure the firewall. See *Configure SuSEFirewall* on page 17. **Linux Audit Framework** — Enable or disable Linux audit framework functionality and configure the audit framework. See *Configure Linux audit framework* on page 21.

Console Menu Subpage	Options
Network Settings	**View Configuration** — See the current network configuration on one screen. **Set IP version** — Choose between IPv4 and IPv6 and then specify options for that IP version. See *Configure Appliance network settings* on page 13. **Shared Folder Management** — Choose from a list of options for viewing, exporting, and mounting shared folders. See *Manage shared folders* on page 15. **Hostname and Name Server** — See *Configure the DNS server address, host name, and domain name* on page 14. **Edit Host Configuration** — Choose from a list of hosts to configure, add a host or delete a host. See *Edit host configuration* on page 14. **Proxy Configuration** — Specify proxy information for HTTP, HTTPS, and FTP protocols. See *Configure proxies* on page 14.
Support Tools	**Enable Remote Support** — Allows remote accesss to Axway support **Factory Network Reset** — If you have incorrectly configured the network settings, this function resets them.

Appliance installation prerequisites 2

Note Non-root installation is not supported on appliances.

SecureTransport 5.4 is available as a 64-bit virtual appliance running SUSE 12 SP4 in the following format:

- **Appliance image** (Can be used on VMWare installs.) – `Appliance_Platform_7.2.0_Appliance_ap-x86-64_<BuildNumber>.iso`

where `<BuildNumber>` is the actual build number for the release, for example, `BN299`.

To make a virtual machine available for use, refer to the Amazon Elastic Compute Cloud (EC2) or VMware documentation.

Review and understand the following information before starting the installer:

- Before booting the ISO image, make sure the floppy is disabled in the BIOS setup panel: otherwise the SLES installation might not complete successfully.
- A minimum of 40 GB of hard drive space is required.
- When you start an appliance or virtual appliance, press **Alt+F2** to switch to tty2 and access the Linux login.

To connect to SLES on your SecureTransport Appliance using SSH, use port 10022. (After you install SecureTransport, you will use port 22 to connect to SecureTransport using SFTP or SCP). You can change the SLES SSH port number after installation by editing `/etc/ssh/sshd_config`.

The following topics provide additional appliance prerequisite information:

- *Configure Appliance network settings* on page 13 - Provides how to instructions for setting appliance network configuration parameters.
- *Configure the DNS server address, host name, and domain name* on page 14 - Provides how to instructions for configuring the DNS server address and host name.

For additional SecureTransport installation prerequisite information, see the *SecureTransport Installation Guide*.

Install SecureTransport on the Appliance 3

You use the Appliance Console menu to install SecureTransport on an SecureTransport Appliance. Installation on the Appliance Platform offers some general options like choice of database and standalone or cluster installation. For example, you can install SecureTransport Server or Edge using an embedded database server in a Standard Cluster or stand-alone. Alternatively, you can use an external Microsoft SQL Server or an Oracle database in an Enterprise Clustering (EC) option. Regardless of the setup, you must have a license.

Check the pre-installation information and prerequisites before you install.

This procedure is an example of the interaction when SecureTransport Server is not already installed on the system. Multiple instances of SecureTransport Server or Edge are not supported in a production environment.

1. Connect to your virtual appliance to open the console menu.
2. On the Appliance Console Menu, enter **C** (SecureTransport Configuration) to display the SecureTransport Configuration menu.
3. Enter **I** (Install SecureTransport) to begin installation.
4. Choose your setup preference from the available options:
    - Single — Install SecureTransport on a single machine in standalone mode. Standalone SecureTransport can use either embedded or external database. The latter option requires an Oracle or Microsoft SQL Server database server and a license for the Enterprise Cluster option.

      – For an *embedded database* installation, see the *Installing SecureTransport to use the embedded database* section of the *SecureTransport Installation Guide*.

      – For an *external database* installation, see the *Installing SecureTransport Server in an Enterprise Cluster or to use an external database* section of the *SecureTransport Installation Guide*.
    - Enterprise Cluster — Install SecureTransport as a node in an Enterprise cluster: either as Server or Edge. This option requires an Oracle or Microsoft SQL Server database server and a license for the Enterprise Cluster option.
    - Standard Cluster — Install SecureTransport as a node in a Standard cluster: either as Server or Edge. This option uses the embedded database.
5. Follow the prompts. Provide all the required information and confirm installation.

The installer displays a progress indicator. It can take several minutes to install SecureTransport. When the installation is complete, the SecureTransport Configuration menu is once again displayed.

Connect to, reboot, and shut down the Appliance 4

This topic describes how to reboot, and shut down the appliance. It also describes how to connect to the Appliance Console Menu.

Connect to the console

To access the virtual Appliance Console Menu, connect to the Console of your machine. Only connecting directly to the machine gives you complete control over the appliance. Console 1, the (blue) Appliance Console Menu, is the first screen you see when you power up the virtual appliance.

Reboot the Appliance

To do this, use the Configuration Menu and follow these steps:

1. Connect to the console: the Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **A**, Appliance Management.
3. On the Appliance Management menu, type **R**, Reboot System.

   Type **Y** to confirm.

   The Appliance reboots and the Appliance Console Menu is displayed.

Shut down the appliance

To do this, use the Configuration Menu and follow these steps:

1. Connect to the console: the Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **A**, Appliance Management.
3. On the Appliance Management menu, type **S**, Shutdown System.

   Type **Y** to confirm.

   The Appliance shuts down.

Configure Appliance network settings 5

In this topic you will learn how to:

Additionally, you can see *Manage shared folders* on page 15

Configure the network

Use the following procedures to configure the IP version, network interface card, boot protocol, default gateway, and static routes.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **N**, Network Settings. The Network Settings menu is displayed.
3. Set the IP version by pressing **4** to select IPv4, or **6** to select IPv6.
4. Specify a default gateway. Type **G**, Default Gateway, and enter the IP address of the gateway.
5. Type **I**, Network Interface.

   The Network Interface Configuration menu appears on display.
6. If available, select the interface boot protocol. Press **T** for Static or **H** for DHCP.
7. If you choose Static, press **I** to enter an IP address and **N** to enter a netmask.
8. (Optional) Type **E** to delete the configuration file for the NIC you selected above.
9. Press **S** to save your settings or **C** to cancel the operation.

Configure the DNS server address, host name, and domain name

1. Connect to the console. The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **N**, Network Settings. The Network Settings menu is displayed.
3. Type **H**, Hostname and Name Server.
4. Enter the correct values for your network in the fields. Use the tab keys to navigate among fields and the arrow keys to navigate within fields.
5. Press **F10** to save your changes. The Network Settings menu is displayed.

Edit host configuration

Use the Host Configuration screen to add, edit, or delete host configurations.

1. Connect to the console. The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **N**, Network Settings. The Network Settings menu is displayed.
3. Type **E**, Edit Host Configuration.

   The Host Configuration screen is displayed with your cursor in the list of current hosts.

   Use the arrow keys to navigate within the list of hosts. Use the Tab key to navigate among buttons and fields on the screen. Use the Enter key to invoke highlighted commands.
4. Add, edit, or delete host configurations as needed.

Note When you are configuring SecureTransport in cluster environment, verify that the hosts file configuration is correct across all nodes.

Configure proxies

Use the following procedure to configure proxies for the appliance.

1. Connect to the console. The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **N**, Network Settings.
3. On the Network Settings menu, type **P**, Proxy Configuration.
4. The Proxy Configuration page displays. On this screen, you use **Alt+<key>** combinations to choose highlighted options. For example, **Alt+E** selects Enable Proxy.
5. On the Proxy Configuration page, type **Alt+E** and then press Enter to enable the proxy and make the remaining fields on the page available.

6. Use the Tab key to cycle through the fields on the page. Specify values for each of the following fields as necessary:

Field	Description
HTTP Proxy URL	Name of the HTTP proxy server
HTTPS Proxy URL	Name of the HTTPS proxy server
FTP Proxy URL	Name of the FTP proxy server

7. *(optional)* Use the same proxy for all protocols. Type **Alt+a** to use the value you specified in the HTTP Proxy URL field for all protocols.
8. *(optional)* Specify domains for which no proxies should be used. Type **Alt+D** to move the cursor to the No Proxy Domains field, and then enter the names or addresses for which there should be no proxies used.
9. *(optional)* Specify a user name and password for proxy authentication. Type **Alt+U** and then enter a user name. Type **Alt+P** and then enter a password.
10. *(optional)* Type **Alt+O** to test the proxy settings.

Manage shared folders

You access the Shared Folder Management screen from the Network Configuration screen. Use the Shared Folder Management screen to view shared folders, export local shared folders, and mount NFS or CIFS remote folders.

View shared folders

Use the View shared folders option to view external shares currently mounted on the system.

1. On the Network Settings screen, type **S**, Shared Folder Management.

   The Shared Folder Management screen is displayed.
2. Type **V**, View Shared Folders.

   A list of shared folders is displayed.

Export local folders

Use the Export local folders option to view external shares currently mounted on the system.

1. On the Network Settings screen, type **S**, Shared folder management.

   The Shared Folder Management screen is displayed.
2. On the Shared Folder Management screen, type **E**, Export local folder.
3. Follow instructions on the screen.

Manage NFS Mount remote folders

Use the NFS Mount remote folders option to configure new NFS network shared folders and manage existing folders.

1. On the Network Settings screen, type **S**, Shared folder management.

   The Shared Folder Management screen is displayed.

2. Type **N**, NFS Mount remote folders.

   The NFS Client Configuration - NFS Shares screen is displayed. If you already have folders configured, this screen displays a list of them.

3. Choose from the following:
   - Select **A**, Add, to add a folder. When you select Add, a screen is displayed to allow you to configure a remote folder.
   - Navigate down the list to select a folder and then select **E**, Edit, to edit the selected folder.
   - Navigate down the list to select a folder and then select **D**, Delete, to delete the selected folder.

4. Select **O**, OK, to apply configuration to the system.

Manage CIFS Mount remote folders

Use the CIFS Mount remote folders option to configure new CIFS network shared folders and manage existing folders.

1. On the Network Settings screen, type **S**, Shared folder management.

   The Shared Folder Management screen is displayed.

2. On the Shared Folder Management screen, type **C**, CIFS Mount remote folder.

3. Follow instructions on the screen.

Manage your appliance firewall 6

Use the Appliance Console Menu to configure the firewall and proxy for the appliance.

Configure SuSEFirewall

Use the following procedure to configure a firewall for your appliance.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **H**, Hardening & Security.
3. On the Hardening & Security menu, type **S**, SuSEFirewall Management.
4. On the SuSE Firewall Management menu, type **F**, SuSEFirewall Configuration.
5. From the SuSE Firewall Configuration menu, use the arrow keys to move between sections in the menu on the left and the tab key to move between choices on the right. The SuSE Firewall Configuration menu is divided into the following sections:

Section	Details
Start-up	Enable the Firewall to start as soon as the appliance powers up, or disable the Firewall so that it starts manually. In the box below the start-up box, you can also start or stop the Firewall manually.
Interfaces	Assign each network device attached to your appliance to the appropriate zone.
Allowed Services	Add servers and services to the list to allow the services to continue functioning. Listing them does create an exception in the Firewall protection. Unnecessary services should not be listed because this creates holes in the Firewall security. The Allowed Services menu item has an Advanced Option that allows you to enter port numbers to enable in the firewall zone.
Masquerading	Accept data from a source network and redirect it to another port by checking the Masquerade Networks box. Then, list both the source network and port in the Redirect Requests to the Masqueraded IP box.

Section	Details
Broadcast	Allow broadcasts from certain zones to reach your appliance. To accept broadcasts from a certain zone, uncheck the corresponding box.
IPsec Support	Activate IPsec to use virtual private networks or to specify security levels for employees who access the network remotely. Checking the box enables IPsec support.
Logging Level	Use the drop-down menus to select whether you want to log all, only the critical, or none of the accepted and non-accepted packets. Highlight the menu and press the down key to view the drop down menu, then select your desired logging style and press **Enter**.
Custom Rules	Add custom rules and protocol for a source network and its destination port.

6. Once each section of the Firewall Configuration menu is set, a summary is displayed to confirm all changes. Type **Alt+F**, Finish, to complete the configuration.

For more information about any of the configuration options, press **Alt+H** to open online help.

Manage appliance passwords 7

In addition to setting passwords, the appliance platform allows you to manage your appliance password, including requirements for defining password complexity rules.

Set the appliance password

Use this procedure to set your appliance password. Setting a new password requires that you know the current password and that the new password meet complexity rules. See *Manage the appliance password* on page 19 for information about specifying password complexity rules.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **H**, Hardening & Security.
3. On the Hardening & Security menu, type **P**, Password Configuration.
4. From the Password Configuration menu, type **M**, Modify root/console menu password, to change the appliance console password. The appliance prompts you for your old password. You must enter the correct password to proceed. If you enter an incorrect password, you are returned to the Password Configuration menu.

Note The default password after installation: axway

Note Whenever you are prompted to type the password, the keys you type are not displayed on the screen. Type the password and press **Enter**, and the next prompt or menu is displayed.

Manage the appliance password

Use the following information to help you manage complexity rules for passwords and Appliance Console Menu password protection.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **H**, Hardening & Security.
3. On the Hardening & Security menu, type **P**, Password Configuration.
4. Set password complexity.
   a. Change password complexity rules. Type **U**, Update password complexity rules.
   b. The menu displays a series of prompts where you specify the minimum number of characters, numerical characters, upper case characters, lower case characters and

special characters your password should contain to be valid.

c. At the end of the prompts, type **y** to save your changes or type **n** to discard them.

5. (optional) Reset password complexity back to the default. On the Password Configuration menu, type **R**.
6. (optional) Type **E** to enable or **D** to disable password protection for the Appliance Console Menu. If you enable it, when you connect to the appliance, the log in prompt displays and you must log in to see the Appliance Console Menu. If you disable password protection, when you connect to the appliance, you see the Appliance Console Menu without having to log in.
7. When the changes are complete, type **B** to return to the Hardening & Security menu.

Configure Linux audit framework

8

Use the following procedure to configure the Linux audit framework. The Linux audit framework is disabled by default.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **H**, Hardening & Security.
3. On the Hardening & Security menu, type **L**, Linux Audit Framework.
4. On the Hardening & Security menu, type **L**, Linux Audit Framework Configuration.
5. The Linux Audit Framework Configuration page displays. On this screen, you use **Alt+<key>** combinations to choose highlighted options. For example, **Alt+I** takes you to the Log File path where you can type in the file path.
6. Use the Tab key to cycle through the fields on the page. Specify values for each of the following fields as necessary:

Field	Description
Dispatcher	The audit dispatcher can be used to send event notifications in addition to - or instead of - writing them to the audit log. In the Dispatcher window, type **I** to manually type in the file path and dispatcher program name, or type **L** to select the program on the computer.
Disk space	Select and assign the disk space rules on the window that opens. Options include rules on what to do when disk space is starting to run low, when admin space is running low, and when the disk is full or there is an error.
Rules for 'auditctl'	Set the audit framework rules. For more information, see *Configure audit framework rules* on page 23.
Log File	Set the file path for the audit log file.
Select File	Opens a window from which the audit log file can be chosen.
Format	Set the audit log file format to one of these two options: • **RAW** - Information is stored as it is sent. • **NOLOG** - Information is not written to a file.

Field	Description
Flush	Set whether the audit log is written to disk, how, and how often. The options are: • **NONE** - The audit data will not be written to a file. • **INCREMENTAL** - The audit data will be written to the file in the increments specified. • **DATA** - Keeps the data part of the disk file in sync at all times. • **SYNC** - Includes both data and metadata.
Frequency (Number of Records)	Sets the number of records before the data is written to the audit log file.
Max File Size	Set the maximum file size, in megabytes, of the audit log.
Maximum File Size Action	Set the action to be performed when the audit log file size reaches the maximum. Use the up and down arrow keys to make your selection. The options are: • **IGNORE** - Ignore the maximum file size set and continue recording in the audit log file. • **SYSLOG** - Write to the system log. • **SUSPEND** - Stop recording in the audit log file. • **ROTATE** - Rotate between the different audit log files. • **KEEP_LOGS** - Save the audit log file and start another.
Number of Log Files	Set the number of log files to keep.
Computer Name Format	Set the format of the computer name to be used. Use the up and down arrow keys to make your selection. The options are: • **None** - No special computer name format. • **Hostname** - The hostname will be used. • **FQD** - The fully qualified domain name will be used. • **User** - The specified user-defined name will be used. Type **E** to specify the user-defined name.
User Defined Name	This field appears only when "User" is chosen for the Computer Name Format. Enter the user-defined name that will be used as the computer name format.

7. Once each section of the Linux Audit Framework Configuration is set, type **Alt+F**, Finish, to complete the configuration.

For more information about any of the configuration options, press **Alt+H** to open online help.

Configure audit framework rules

By configuring the Linux audit framework rules, you can specify which system components are audited:

- System calls
- File and directory watches
- Basic system parameters

Use the following procedure to access the Configuration of Linux Audit Framework (LAF) screen:

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **H**, Hardening & Security.
3. On the Hardening & Security menu, type **L**, Linux Audit Framework.
4. On the Hardening & Security menu, type **L**, Linux Audit Framework Configuration.
5. On the Linux Audit Framework Configuration page, type **T** to access the rules screen.
6. Use the Tab key to cycle through the fields on the page and the up and down arrows to view the information in the `audit.rules` box. Specify values for each of the following fields as necessary:

Field	Description
Set Enabled Flag	Set the enabled flag to one of these options: • **Auditing enabled** - Turns auditing on. • **Auditing disabled** - Turns auditing off. • **Rules are locked (until next boot)** - Locks the auditing rules until the next time the system is booted.
audit.rules	Edit the rules for the audit subsystem.
Check Syntax	Check the syntax of the audit rules for errors.
Restore 'audit.rules'	Reset the audit rules to the state before changes were made.
Restore and Reset	Restore and reset all settings to the state before changes were made.
Load	Load the modified audit rules.

Audit system parameters

The following audit system parameters can be used:

Parameter	Description
-D	Deletes any preexisting rules to avoid problems with new rules.
-b	Sets the number of outstanding audit buffers. If no more buffers are available, the failure flag is checked for action.
-f	Sets the failure flag, which controls the reaction to critical errors. Value options: • **0** - Silent • **1** - Print a failure message (printk) • **2** - Shutdown the system (panic). There is a risk of data loss and corruption with this option.
-e	Sets the enable flag, which enables or temporarily disables the audit. Value options: • **0** - Disables the audit. • **1** - Enables the audit and the audit contexts for system calls. • **2** - Enables the audit and audit contexts and locks down the configuration.
-w	Sets a file system watch. Example: `-w /etc/audit/audit.rules -p rxwa`
-p	Sets permission filtering. In the example `-w /etc/audit/audit.rules -p rxwa`, permission filtering is turned on for read, write, execute, and attribute change.
-k	Attaches a text string to a recorded event. Example: `-w /var/log/audit/ -k LOG_audit`. This helps with searches using the ausearch log analyzer.

The above information was adapted from https://www.suse.com/.

System management tips 9

In this topic you will learn how to:

Set the clock and time zone

You can use the Clock and Time Zone menu for clustered machines. The time server should be set so that the clustered machines are always in sync.

1. On the Appliance Management menu, type **T**, Clock/Timezone.
2. In the Clock and Time Zone panel, select a region. If you select **Global**, the Time Zone panel displays all possible time zones. If you select a different region, the Time Zone panel displays only time zones for that region.
3. In the Time Zone panel, select your time zone. Use the tab key to navigate between panels.
4. (optional) Display the correct local time. Type **Alt+H** to set the appliance hardware clock to UTC (Coordinated Universal Time.)
5. In the Date and Time panel, you can select **Change** to manually manage the date and time or to synchronize the date and time with the NTP Server.
6. From the Clock and Time Zone menu, select **OK**.

Switch between consoles

Console 1 is the Appliance Console Menu (blue); it is the first screen you see when you power up the appliance. Consoles 2-6 allow you to log in directly to the operating system.

To switch from one virtual console to another, use the **Alt+Fn** keyboard combination, where Fn is a value between 1 and 6. For example:

- From console 6 (Linux kernel), use the key combination **Alt+F1** to go to console 1.
- From console 1, use the key combination **Alt+F6** to go to console 6.

Note Using **Alt+F4** might close the currently opened window of most browsers.

Work with system log files

The Appliance Console Menu provides you with access to system log files.

1. Connect to the console. See *Connect to the console* on page 12 for more information.

   The Appliance Console Menu is displayed.
2. On the Appliance Console Menu, type **A**, Appliance Management.
3. On the Appliance Management menu, type **L**, System Log Files.
4. Use the up and down arrow keys to choose a log file to view and then the left and right arrow keys to choose one the following:
   - **Live View** — displays a read-only view of the latest log entries
   - **Full View** — displays a read-only view of the entire selected log file.

Migrate SecureTransport Appliance from 7.1.x to 7.2.0 10

You can install and run SecureTransport 5.4 on both Axway Appliance Platform version 7.1.x and version 7.2.0. The latest 7.2.0 version of the operating system of the Appliance is compatible with SecureTransport 5.4 only and requires a clean installation. In order to upgradeAxway Appliance Platform version 7.1.x to 7.2.0, adhere to the instructions strictly.

Prerequisites

If you are currently using a SecureTransport version earlier than 5.4, you must first upgrade SecureTransport to version 5.4. For more information, see the *SecureTransport* 5.4 *Upgrade guide*.

Procedure

After you have SecureTransport 5.4 installed on the Axway Appliance, download the appropriate upgrade file from the Axway Technical support website and perform these steps:

1. **Create a full back-up copy** of your existing SecureTransport implementation and configuration.
2. Proceed with the latest image of Axway Appliance. Note that the SLES image installation will **erase all existing data**.

Post-migration steps

After migration, check all the OS settings and reconfigure them if needed. Then, restore the backup created in step 1 to bring your SecureTransport 5.4 deployment back.

Update SecureTransport Appliance 11

To install security updates on your Axway appliance, run the following command:

```
zypper up
```

After first run you will be prompted to accept the Axway GPG key:

New repository or package signing key received:

```
Repository:  appliance-platform-updates
Key Name:  Axway SecureTransport Appliance <BU.426.ST.Appliance@axway.com>
Key Fingerprint:  2F4811E2 87CEED53 F951BF78 B006F0E8 9DBDD9E8
Key Created:  Thu 18 Apr 2019 11:46:05 AM EEST
Key Expires:  (does not expire)
Subkey:  2C76DDE85142DCC3 2019-04-18 [expires: 2021-04-17]
Rpm Name:  gpg-pubkey-9dbdd9e8-5cb8394d
```

You must accept the key to receive the updates.

Note Your firewall should be configured to allow access to `axway.bintray.com` from your Axway Appliance.

Uninstall SecureTransport from an Appliance 12

This section explains how to uninstall SecureTransport from the Axway Appliance using the Appliance Console Menu.

Note In a cluster environment, stop all of the protocol servers and services on the node you want to uninstall and remove this node from the cluster before you uninstall it. For details refer to the *SecureTransport Administrator's Guide*.

1. Open the Appliance Console Menu.
    - Connect to your virtual appliance
2. On the Appliance Console Menu, enter **C** (SecureTransport Configuration) to display the SecureTransport Configuration menu.
3. Enter **U** (Uninstall SecureTransport). The Appliance Console prompts you to confirm uninstallation.
4. Enter **Y** to display a second confirmation prompt. Enter **Y** again to confirm uninstallation.

SecureTransport Appliance SAN card 13

The following topics describe how to configure the optional SAN card for the Axway Appliance and gives its specifications:

- *Configure a SUSE Linux Enterprise High Availability cluster with OCFS2* on page 30 – Provides how to instructions for configuring a SuSE Linux Enterprise High Availability (SLEHA) cluster.
- *SAN fiber card specifications on page 45* – Lists the SAN fiber card specifications.

Configure a SUSE Linux Enterprise High Availability cluster with OCFS2

This section describes all of the prerequisite tasks that you must complete before you begin configuring SLEHA cluster with OCFS2:

- Enable loading of fiber card driver
- Initialize multipath
- Create multipath.conf file
- Enable multipath
- Configure NTP client
- Configure the ssh client

Enable loading of fiber card driver

Comment out or remove the line containing `blacklist qla2xxx` in `/etc/modprobe.d/50-blacklist.conf`. If no other changes are made this, should be the last line in the file.

Initialize multipath

Depending on the number of your fiber cards and number of LUNs exported on SAN, block devices initialized by the OS may vary. In this case, there is only one called `sdb`.

Run the following command:

```
multipath -ll
```

If there is no output or not every block device representing SAN is listed, initialize each block device as:

```
node115:~ # multipath /dev/sdb
create: 360014056e1d398a52894c8e99d7de877 undef LIO-ORG,IBLOCK
size=2.0G features='0' hwhandler='1 alua' wp=undef
`-+- policy='service-time 0' prio=50 status=undef
  `- 3:0:0:0 sdb 8:16 undef ready running
```

A device named `dm-name-360014056e1d398a52894c8e99d7de877` should now appear in `/dev/disk/by-id`.

If you have more than one device, repeat the task for each of the rest.

Create multipath.conf file

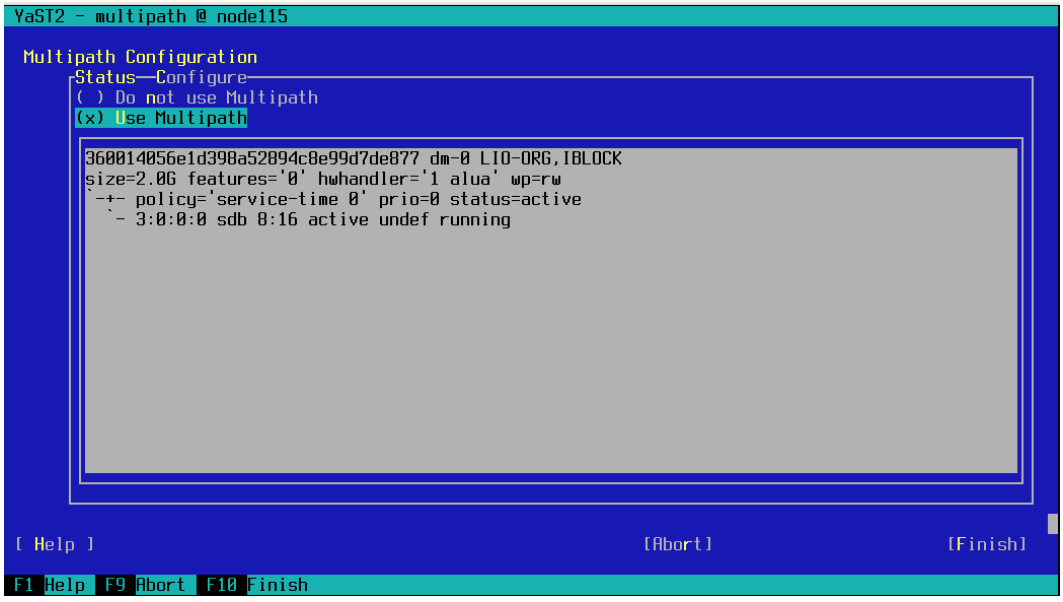
Create the file `/etc/multipath/multipath.conf` with the following content

```
blacklist {
       devnode "^sda[0-9]*"
}
```

Note If you are planning to decrease the watchdog timeout, you may need to decrease the multipath timeouts. The default value of `max_polling_interval` is 5. The default value of `max_polling_interval` is `4 * polling_interval`. It should be less than the watchdog timeout.

Enable multipath

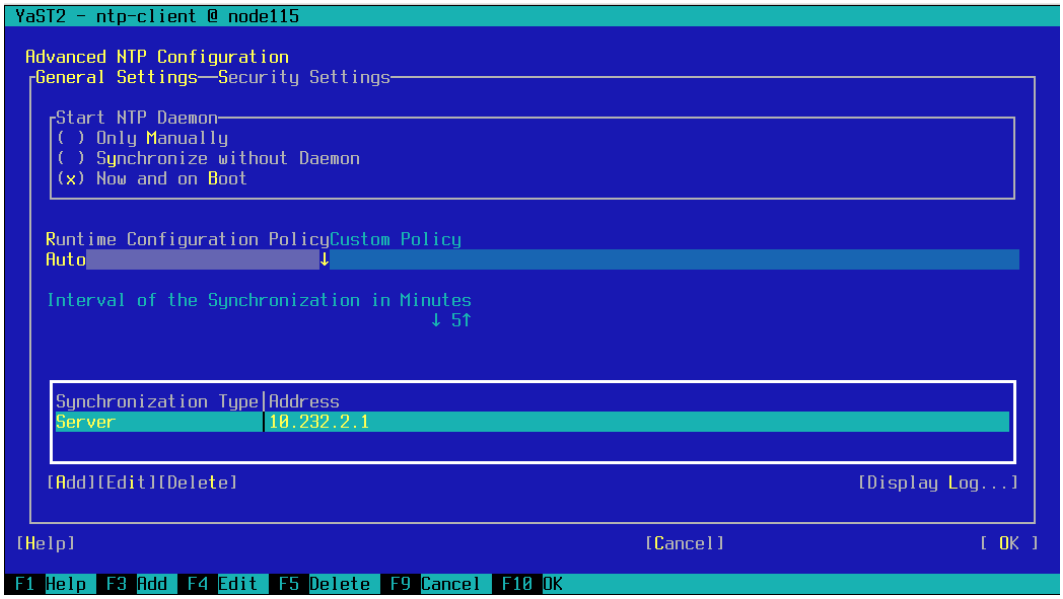
Run `yast multipath` and select **Use multipath**.



Press Finish and reboot the appliance. If after the restart your system enters in Emergency mode, provide root password and verify your multipath configuration.

Configure NTP

Run `yast ntp` and configure your local ntp servers. Select **Now and on Boot** for NTP startup.



Configure the ssh client

Add records for every node in `/etc/hosts` file.

Edit, or create if not present `/root/.ssh/config`. Add port 10022 as a default SSH port on Axway Appliance. For example, if there are two nodes:

```
Host st-appliance1 st-appliance2
Port 10022
```

The steps in the following topics need to be performed to configure a SUSE Linux Enterprise High Availability (SLEHA) OCFS2 cluster using the optional SAN card on Axway appliances:

- *Setup SLEHA with OCFS2 using multicast on the first node* on page 33 - Provides configuration instructions for setting SLEHA with OCFS2 using multicast on the first node of a cluster.
- *Setup N-th node in a cluster using multicast* on page 43 - Provides configuration instructions for setting up the N-th node in a cluster using mulicast.
- *Setup SLEHA cluster to use unicast* on page 43 - Provides configuration instructions for setting up a SLEHA cluster to use unicast.

- *Verify cluster configuration* on page 45 - Provides a procedure for checking the cluster configuration.
- *Remove a node from a SLEHA cluster* on page 45 - Provides configuration instructions for removing a node from a SLEHA cluster.
- *Test STONITH configuration* on page 45 - Provides a procedure for testing the STONITH configuration.

For additional SUSE configuration information, refer to the following links:

- SUSE Linux Enterprise High Availability Extension 12 SP4 High Availability Guide
- Manual Cluster Setup (YaST)

Setup SLEHA with OCFS2 using multicast on the first node

To setup SLEHA with OCFS2 using multicast on the first node:

Caution Make sure you fulfill the following prerequisites.

1. Create SBD partition
2. Initialize SBD
3. Initialize the cluster
4. Configure SBD STONITH resource
5. Configure Distributed Lock Manager (DLM)
6. Configure OCFS2

Create SBD partition

Use the `fdisk` utility to create SBD partition on your storage.

Note In an environment where all nodes have access to shared storage, a small partition of the device is formatted for use with SBD. The size of the partition depends on the block size of the used disk (for example, 1 MB for standard SCSI disks with 512 byte block size or 4 MB for DASD disks with 4 kB block size). The initialization process creates a message layout on the device with slots for up to 255 nodes.

- Press `p` to see current partition table
- Press `n` to create new partition
- Press `p` for primary partition
- Select the correct size of your SBD
- Press `w` to write the partition table

```
node115:~ # fdisk /dev/disk/by-id/dm-name-
```

```
360014056e1d398a52894c8e99d7de877

Welcome to fdisk (util-linux 2.33.2).
Changes will remain in memory only, until you decide to write
them.
Be careful before using the write command.


Command (m for help): p
Disk /dev/disk/by-id/dm-name-360014056e1d398a52894c8e99d7de877:
2 GiB, 2147483648 bytes, 4194304 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 4194304 bytesDisklabel
type: dos
Disk identifier: 0x228d0281

Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (8192-4194303, default 8192):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (8192-4194303,
default 4194303): +1M

Created a new partition 1 of type 'Linux' and of size 1 MiB.

Command (m for help): w
The partition table has been altered.
```

Caution If you see a message saying "Failed to add partition 1 to system: Invalid argument", reboot the system and continue with the setup.

Initialize SBD

Run the following command:

```
node115:~ # sbd -d /dev/disk/by-id/dm-name-
```

```
360014056e1d398a52894c8e99d7de877-part1 -4 180 -1 90
create
Initializing device /dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1

Creating version 2.1 header on device 4 (uuid: 73e6e254-
703c-43bd-acd5-538a7f3d42ad)
Initializing 255 slots on device 4
Device /dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1 is initialized.
```

- Use `-4` option to specify the msgwait timeout. In the example above, it is set to 180 seconds.
- Use `-1` option to specify the watchdog timeout. In the example above, it is set to 90 seconds. The minimum allowed value for the emulated watchdog is 15 seconds.
- You may use the following formula for timeout configuration:

```
Timeout (msgwait) >= (Timeout (watchdog) * 2)
 stonith-timeout = Timeout (msgwait) + 20%
```

Caution The following should be executed on all cluster nodes, not only on the first one!

1. After SBD is initialized, edit the file `/etc/sysconfig/sbd` and search for "SBD_DEVICE=".
2. Edit the line and replace it with your SBD device:

```
SBD_DEVICE="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1"
```

3. Enable sbd service on all nodes:

```
node115:~ # systemctl enable sbd
Created symlink from
/etc/systemd/system/corosync.service.requires/sbd.serv
ice to /usr/lib/systemd/system/sbd.service.
Created symlink from
/etc/systemd/system/pacemaker.service.requires/sbd.ser
vice to /usr/lib/systemd/system/sbd.service.
Created symlink from
/etc/systemd/system/dlm.service.requires/sbd.service
to /usr/lib/systemd/system/sbd.service.
```

Initialize the cluster

Run the following command:

```
node115:~ # sleha-init
  Generating SSH key
  Configuring csync2
  Generating csync2 shared key (this may take a while)...done
  csync2 checking files...done

Configure Corosync:
  This will configure the cluster messaging layer.  You will
need
  to specify a network address over which to communicate
(default
  is eth0's network, but you can use the network address of any
  active interface).

  IP or network address to bind to [10.134.64.115]
  Multicast address [239.124.194.226]
  Multicast port [5405]

Configure SBD:
  If you have shared storage, for example a SAN or iSCSI
target,
  you can use it avoid split-brain scenarios by configuring
SBD.
  This requires a 1 MB partition, accessible to all nodes in
the
  cluster.  The device path must be persistent and consistent
  across all nodes in the cluster, so /dev/disk/by-id/* devices
  are a good choice.  Note that all data on the partition you
  specify here will be destroyed.

Do you wish to use SBD (y/n)? y
SBD is already configured to use /dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1 - overwrite (y/n)? n
  Initializing SBD......done
  Hawk cluster interface is now running. To see cluster status,
open:
    https://10.134.64.115:7630/
  Log in with username 'hacluster', password 'linux'
WARNING: You should change the hacluster password to something
more secure!
  Waiting for cluster..............done
```

```
  Loading initial cluster configuration

Configure Administration IP Address:
  Optionally configure an administration virtual IP
  address. The purpose of this IP address is to
  provide a single IP that can be used to interact
  with the cluster, rather than using the IP address
 of any specific cluster node.

Do you wish to configure a virtual IP address (y/n)? n
  Done (log saved to /var/log/ha-cluster-bootstrap.log)
```

- If you have more than one network interface, enter the address of the interface dedicated for the pacemaker. If you have only one interface configured press enter.
- Press `y` on prompt Do you wish to use SBD
- Press `n` when prompted to overwrite the configuration
- Press `n` on prompt for virtual IP address

Configure SBD STONITH resource

1. Run the `crm configure` command.
2. Type `property stonith-enabled="true"`. This is the default configuration as clusters without STONITH are not supported. In case STONITH has been deactivated for testing purposes, make sure this parameter is set to `true` again.
3. Type `property stonith-watchdog-timeout=0`.
4. Type `property stonith-timeout="240s"` A `stonith-timeout` value of 240 would be appropriate if the `msgwait` timeout value for SBD was set to 60 seconds.
5. Type `verify` to check your configuration.
6. Type `commit` to save the changes.
7. Type `edit stonith-sbd` to add your STONITH device. This runs Vi mode.

```
primitive stonith-sbd stonith:external/sbd \
 params pcmk_delay_max=30s \
 params sbd_device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1"
```

8. Type `verify` to check your configuration
9. Type `commit` to save the changes
10. Type `show` to see the configuration

```
crm(live/node115)configure# show
node 176570483: node115
primitive stonith-sbd stonith:external/sbd \
        params pcmk_delay_max=30s \
        params sbd_device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1"property cib-
bootstrap-options: \
        have-watchdog=true \
        dc-version="1.1.23+20200622.28dd98fad-3.6.1-
1.1.23+20200622.28dd98fad" \
        cluster-infrastructure=corosync \
        cluster-name=hacluster \
        stonith-enabled=true \
        stonith-watchdog-timeout=0 \
        stonith-timeout=240s
rsc_defaults rsc-options: \
        resource-stickiness=1 \
        migration-threshold=3
op_defaults op-options: \
        timeout=600 \
        record-pending=true
```

Configure Distributed Lock Manager (DLM)

1. Run the `crm configure` command.
2. Type `primitive dlm ocf:pacemaker:controld op monitor interval="60" timeout="60"`.
3. Type `group g-storage dlm`.
4. Type `clone cl-storage g-storage meta interleave=true target-role=Started`.
5. Type `verify` to check your configuration.
6. Type `commit` to save the changes.
7. Type `show` to see the configuration. See *Verify cluster configuration* on page 45.

```
crm(live/node115)configure# show
node 176570483: node115
primitive dlm ocf:pacemaker:controld \
        op monitor interval=60 timeout=60
```

```
primitive stonith-sbd stonith:external/sbd \
        params pcmk_delay_max=30s \
        params sbd_device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1"
group g-storage dlmclone cl-storage g-storage \
        meta interleave=true target-role=Started
property cib-bootstrap-options: \        have-
watchdog=true \
        dc-version="1.1.23+20200622.28dd98fad-3.6.1-
1.1.23+20200622.28dd98fad" \
        cluster-infrastructure=corosync \
        cluster-name=hacluster \
        stonith-enabled=true \
        stonith-watchdog-timeout=0 \
        stonith-timeout=240srsc_defaults rsc-options:
\
        resource-stickiness=1 \
        migration-threshold=3
op_defaults op-options: \
        timeout=600 \
        record-pending=true
```

Configure OCFS2

1. Create partition for OCFS2
2. Create OCFS2 filesystem
3. Mount OCFS2 file system

Create partition for OCFS2

You may skip this step if you already have partition on your SAN.

Use the `fdisk` utilty to create additional partition on your SAN:

```
node115:~ # fdisk /dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877

Welcome to fdisk (util-linux 2.33.2).
Changes will remain in memory only, until you decide
to write them.
```

```
Be careful before using the write command.


Command (m for help): nPartition type
   p   primary (1 primary, 0 extended, 3 free)
   e   extended (container for logical
partitions)Select (default p): p
Partition number (2-4, default 2):
First sector (10240-4194303, default 16384):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (16384-
4194303, default 4194303):

Created a new partition 2 of type 'Linux' and of size
2 GiB.

Command (m for help): w
The partition table has been altered.
```

1. Press `n` for new partition.
2. Press `p` for primary partition.
3. Select the number of partition.
4. Select the size of partition.
5. Press `w` to save the partition table.

You may need to reboot your system.

Create OCFS2 filesystem

Run the following command:

```
node115:~ # mkfs.ocfs2 /dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part2
mkfs.ocfs2 1.8.5
Cluster stack: pcmk
Cluster name: hacluster
Stack Flags: 0x0
NOTE: Feature extended slot map may be enabled
Label:
Features: sparse extended-slotmap backup-super unwritten
inline-data strict-journal-super xattr indexed-dirs
```

```
refcount discontig-bg append-dio
Block size: 4096 (12 bits)
Cluster size: 4096 (12 bits)
Volume size: 2139095040 (522240 clusters) (522240 blocks)
Cluster groups: 17 (tail covers 6144 clusters, rest cover
32256 clusters)
Extent allocator size: 4194304 (1 groups)
Journal size: 67108864
Node slots: 2
Creating bitmaps: done
Initializing superblock: done
Writing system files: done
Writing superblock: done
Writing backup superblock: 1 block(s)
Formatting Journals: done
Growing extent allocator: done
Formatting slot map: done
Formatting quota files: done
Writing lost+found: done
mkfs.ocfs2 successful
```

For more information about mkfs.ocfs2 options, refer to man page. Also see man tunefs.ocfs2.

Mount OCFS2 file system

1. Run the `crm configure` command and type:

```
primitive ocfs2-1 ocf:heartbeat:Filesystem \

params device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part2"
directory="/sanmount" \ fstype="ocfs2" options="acl" \

op monitor interval="20" timeout="40" \

op start timeout="60" op stop timeout="60" \

meta target-role="Started"
```

Where `/dev/disk/by-id/dm-name-360014056e1d398a52894c8e99d7de877-part2` is your OCFS2 partition and `/sanmount` is directory where it should be mounted

2. Type `modgroup g-storage add ocfs2-1` to add ocfs2 primitive to g-storage group.
3. Type `verify` to check your configuration.
4. Type `commit` to save the changes.
5. Type `show` to see the configuration.

```
node115:~ # crm configure
crm(live/node115)configure# primitive ocfs2-1
ocf:heartbeat:Filesystem \   >   params
device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part2"
directory="/sanmount" \
   >   fstype="ocfs2" options="acl" \


   >   op monitor interval="20" timeout="40" \
   >   op start timeout="60" op stop timeout="60" \
   >   meta target-role="Started"
crm(live/node115)configure# modgroup g-storage add
ocfs2-1
crm(live/node115)configure# verify
crm(live/node115)configure# commit
crm(live/node115)configure# show
node 176570483: node115
primitive dlm ocf:pacemaker:controld \
        op monitor interval=60 timeout=60primitive
ocfs2-1 Filesystem \
        params device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part2"
directory="/sanmount" fstype=ocfs2 options=acl \
        op monitor interval=20 timeout=40 \
       op start timeout=60 interval=0 \        op stop
timeout=60 interval=0 \
        meta target-role=Startedprimitive stonith-sbd
stonith:external/sbd \
        params pcmk_delay_max=30s \
        params sbd_device="/dev/disk/by-id/dm-name-
360014056e1d398a52894c8e99d7de877-part1"group g-
storage dlm ocfs2-1
clone cl-storage g-storage \
        meta interleave=true target-role=Started
```

```
property cib-bootstrap-options: \
        have-watchdog=true \
        dc-version="1.1.23+20200622.28dd98fad-3.6.1-
1.1.23+20200622.28dd98fad" \
        cluster-infrastructure=corosync \
        cluster-name=hacluster \
        stonith-enabled=true \
        stonith-watchdog-timeout=0 \
        stonith-timeout=240s
rsc_defaults rsc-options: \
        resource-stickiness=1 \
        migration-threshold=3
op_defaults op-options: \
        timeout=600 \
        record-pending=true
crm(live/node115)configure#
```

6. Type `quit` to exit the crm shell.
7. Run `mount | grep ocfs2` to check whether the filesystem is mounted:

Setup N-th node in a cluster using multicast

To setup the N-th node in a cluster using multicast:

Caution Make sure you fulfill the following prerequisites.

1. Run `sleha-join`.
2. Enter the alias for the first node. Be sure this alias is present in `/root/.ssh/config`.
3. Enter the root password for the first node when prompted.
4. Run `mount | grep ocfs2` to check if OCFS2 mount is present.

Setup SLEHA cluster to use unicast

If your environment does not use multicast, change the configuration from multicast to unicast on each of the cluster nodes as follows:

1. Run **yast2 cluster** to display the SLEHA cluster configuration.

   ```
   #yast2 cluster
   ```

2. Navigate to **Cluster > Communication Channels > Transport** and change communications from `multicast` to `unicast`.
3. Navigate to **Cluster > Communication Channels > Member Address** and add all of the cluster nodes IP addresses.
4. Verify your configuration

```
st-appliance:~ # crm configure show
node 176570481: st-appliance
node 176570482: st-appliance2
primitive dlm ocf:pacemaker:controld \
     op monitor interval=60 timeout=60
primitive ocfs2-1 Filesystem \
     params device="/dev/disk/by-id/wwn-0x6001405256f3afcbf294600bbd48d488-
part2" directory="/shared_storage" fstype=ocfs2 options=acl \
     op monitor interval=20 timeout=60 \
     op_params timeout=60 \
     op stop timeout=60 interval=0 \
     meta target-role=Started
primitive stonith-sbd stonith:external/sbd \
     params sbd_device="/dev/disk/by-id/wwn-
0x6001405256f3afcbf294600bbd48d488-part1" \
     meta target-role=Started \
     op monitor interval=20 timeout=20 start-delay=20
group g-storage dlm ocfs2-1
clone cl-storage g-storage \
     meta interleave=true target-role=Started
     property cib-bootstrap-options: \
     have-watchdog=true \
     dc-version="1.1.19+20181105.ccd6b5b10-3.10.1-
1.1.19+20181105.ccd6b5b10" \
     cluster-infrastructure=corosync \
     cluster-name=hacluster \
     stonith-enabled=true \
     placement-strategy=balanced
rsc_defaults rsc-options: \
    resource-stickiness=1 \
```

```
    migration-threshold=3
op_defaults op-options: \
    timeout=600 \
    record-pending=true
```

Verify cluster configuration

Run **crm configure show** to view the cluster resource configuration.

For each node, there should be a `stonith external/sbd` resource created.

Also there is a HA Web Console for viewing the cluster status and configuration, running on port 7630 on each of the cluster nodes. Username: **hacluster** password: **linux**

Remove a node from a SLEHA cluster

1. Login as a root user to any cluster node, except the one that is being removed.
2. Run one of the following commands:

   `sleha-remove -c <hostname>`

   or

   `sleha-remove -c <IP address>`,

   where `<hostname>` or `<IP address>` is the hostname or the IP address of the node to be removed.

Test STONITH configuration

To test the STONITH configuration, run the **crm node fence <hostname>** command from the shell.

```
#crm node fence <hostname>
```

Where `<hostname>` is the hostname of the node.

The command will fence the node and cause a reboot.

SAN fiber card specifications

This section describes the optional SAN card that can be used with the ST5850 and ST6850 appliances.

Note This card is only offered when you purchase the appliance. It is not available separately.

The following information is provided to help you use the SAN card properly.

- The optional SAN card is a QLogic SANblade QLE2462. Ensure you only connect compatible SAN devices to this card. For a list of compatible devices, contact QLogic. For the full SANblade QLE2462 datasheet, search for it on the QLogic web site.
- The card is dual-channel (Dual Port 4-Gbps Fiber Channel (FC) to PCI Express Host Bus Adapter [HBA])
- Bus Interface: PCI Express x4
- Data Rate: 4/2/1 Gbps auto-negotiation (4.2480/2.1240/1.0625 Gbps)