Symantec NetBackup™ Appliance Security Guide

Release 2.6.0.4

Symantec

Symantec NetBackup Appliance Security Guide

Documentation version 2.6.0.4

Legal Notice

Copyright © 2014 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and NetBackuop are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

About the NetBackup Appliance Security Guide

This chapter includes the following topics:

About the NetBackup Appliance Security Guide

The NetBackup Appliance is developed with security as a primary need from inception. The Linux operating system, the core NetBackup application, and each element of the appliances are tested for vulnerabilities using both industry standards and Symantec Security products. This ensures that the exposure to unlawful access and resulting data loss or theft is minimized.

Each release of new software as well as hardware is verified for vulnerabilities before release. Depending on the severity of issues found, Symantec will address them using a patch or through a scheduled major release. To reduce the risk of unknown threats, Symantec will also be regularly updating third-party packages and modules used in the product as part of their maintenance release cycles

The goal of this guide is to describe the security features implemented in the *2.6.x.x* release of the NetBackup Appliance and includes the following chapters and sub-sections:

NetBackup Appliance Authentication

This chapter talks about the authentication features implemented in the NetBackup Appliance and includes the following sections:

Table 1-1 Sections on authentication

Section name	Description	Link
Authentication types in NetBackup Appliance	This section describes the types of users, user accounts, and processes allowed to access the NetBackup Appliance.	See "Authentication types in NetBackup Appliance" on page 25.
About configuring LDAP supported users	This section describes the prerequisites and process to configure LDAP supported users.	See "About configuring LDAP supported users" on page 26.
About configuring Active Directory supported users	This section describes the prerequisites and process to configure Active Directory supported users.	See "About configuring Active Directory supported users" on page 26.
Authentication of NetBackupCLI administrators	This section introduces the role of the NetBackup CLI user.	See "Authentication of NetBackupCLI administrators" on page 27.
About user name and password specifications	This section describes the user name and password credentials.	See "About User name and Password Specifications" on page 28.

NetBackup Appliance Authorization

This chapter describes the features implemented for authorizing users accessing the NetBackup Appliance and includes the following sections:

Table 1-2 Sections on authorization

Section name	Description	Link
About NetBackup Appliance authorization	This section describes the key characteristics of the authorization process of the NetBackup Appliance.	See "About NetBackup Appliance Authorization" on page 34.

Table 1-2 Sections on authorization *(continued)*

Section name	Description	Link
About supported user roles - NetBackup Appliance Administrator	This section describes the NetBackup Appliance Administrator user role.	See "About supported user roles - NetBackup Appliance Administrator" on page 34.
About supported user roles - Appliance NetBackup CLI user	This section describes the NetBackup CLI user role.	See "About supported user roles - Appliance NetBackup CLI user" on page 35.

NetBackup Appliance IPS and IDS

This chapter describes the SCSP implementation for the NetBackup Appliance using the following sections:

Table 1-3 Sections on IPS and IDS policies

Section name	Description	Link
Introduction to Symantec Critical System Protection (SCSP)	This section introduces the Symantec Critical System Protection (SCSP) feature implemented with the appliances.	See "Introduction to Symantec Critical System Protection (SCSP)" on page 39.
About NetBackup Appliance Intrusion Prevention Policy (IPS)	This section describes the IPS policy used to protect the appliances.	See "About NetBackup Appliance Intrusion Prevention Policy (IPS)" on page 40.
About NetBackup Appliance Intrusion Detection Policy (IDS)	This section describes the IDS policy used to monitor the appliances.	See "About NetBackup Appliance Intrusion Detection Policy (IDS) " on page 41.
Overriding the Symantec Intrusion Security policy	This section describes the procedure to override the IPS policy applied to the appliances.	See "Overriding the Symantec Intrusion Security policy (IPS)" on page 42.
Re-enable the Symantec Intrusion Security policy	This section describes the procedure to re-enable the IPS policy applied to the appliances.	See "Re-enable the Symantec Intrusion Security policy" on page 45.

Table 1-3 Sections on IPS and IDS policies *(continued)*

Section name	Description	Link
Reviewing SCSP events	This section describes the SCSP events based on their level of security.	See "Reviewing SCSP events" on page 47.
About NetBackup Appliance authorization	This section describes the key characteristics of the authorization process of the NetBackup Appliance.	See "About SCSP Protection using the Unmanaged Mode" on page 50.

NetBackup Appliance Log Files

This chapter lists the NetBackup Appliance log files and the options to view the log files, using the following sections:

Table 1-4 Working log sections

Section name	Description	Link
About working with log files	This chapter provides an overview on all the different types of logs that you can view for the NetBackup Appliance.	See "About working with log files" on page 58.
About using the Collect Log files wizard	This chapter describes the usage of the Collect Log files wizard present on the NetBackup Appliance Web Console.	See "About using the Collect Log files wizard" on page 60.
Viewing log files using the Support command	This chapter describes the procedure to view log files using the support command.	See "Viewing log files using the Support command" on page 61.
Locating NetBackup Appliance log files using the Browse command	This chapter describes the usage of Browse command to view log files.	See "Locating NetBackup Appliance log files using the Browse command" on page 62.
Gathering device logs with the DataCollect command	This chapter describes the procedure to gather device logs.	See "Gathering device logs with the DataCollect command" on page 63.

NetBackup Appliance Operating System Security

This chapter describes the security implementation for the NetBackup Appliance operating system, using the following sections:

Table 1-5 Operating System sections

Section name	Description	Link
About Operating System Security	This section describes the different update types made to the operating system to improve the security of the overall NetBackup Appliance.	See "About Operating System Security" on page 67.
Listing Products and Operating System Components within the NetBackup Appliance Installation	This section lists the products and operating system components with the NetBackup Appliance.	See "Listing Products and Operating System Components within the NetBackup Appliance Installation" on page 68.
Listing Disabled login for service account	This section lists the disabled service accounts.	See "Disabled Service Accounts" on page 69.

NetBackup Appliance Data Security

This chapter describes the data security implementation for the NetBackup Appliance, using the following sections:

Table 1-6 Data security sections

Section name	Description	Link
About Data Security	This section lists the measures taken to improve data security.	See "About Data Security" on page 71.
About Data Integrity	This section lists the measures taken to improve data integrity.	See "About Data Integrity" on page 72.
About Data Classification	This section lists the measures taken to improve data classification.	See "About Data Classification" on page 73.
About Data Encryption	This section lists the measures taken to improve data encryption.	See "About Data Encryption " on page 74.

NetBackup Appliance Web Security

This chapter describes the web security implementation for the NetBackup Appliance, using the following sections:

Table 1-7 Web security sections

Section name	Description	Link
About NetBackup Appliance Web Console Security Updates	This section lists the security updates for NetBackup Appliance Web Console.	See "About NetBackup Appliance Web Console Security Updates " on page 76.
About SSL certification	This section lists the SSL certification updates for NetBackup Appliance Web Console.	See "About SSL certification" on page 77.
Implementing third-party SSL certificates	This section lists the procedure to implement third-party SSL certificates.	See "Implementing third-party SSL certificates" on page 78.

NetBackup Appliance Network Security

This chapter describes the network security implementation for the NetBackup Appliance, using the following sections:

Table 1-8 Network security sections

Section name	Description	Link
About IPsec Channel Configuration	This section describes the IPsec configuration for NetBackup Appliances.	See "About IPsec Channel Configuration" on page 80.
About NetBackup Appliance 52xx ports	This section describes the port information for NetBackup Appliances.	See "About the NetBackup Appliance 52xx ports" on page 82.

NetBackup Appliance Call Home Security

This chapter describes the Call Home security implementation for the NetBackup Appliance, using the following sections:

Table 1-9 Call Home security sections

Section name	Description	Link
About AutoSupport	This section describes the AutoSupport feature in the NetBackup Appliance.	See "About AutoSupport " on page 85.
About Call Home	This section describes the Call Home feature in the NetBackup Appliance.	See "About Call Home" on page 86.

Table 1-9 Call Home security sections *(continued)*

Section name	Description	Link
About SNMP	This section describes the SNMP feature in the NetBackup Appliance.	See "About SNMP" on page 90.

NetBackup Appliance IPMI Security

This chapter describes the guidelines adopted to secure IPMI configuration, using the following sections:

Table 1-10 IPMI security sections

Section name	Description	Link
Introduction to IPMI configuration	This section describes IPMI and how it is configured with the NetBackup Appliance.	See "Introduction to IPMI configuration" on page 92.
Listing the Recommended IPMI settings	This section lists the recommended IPMI settings for a secure configuration.	See "Recommended IPMI settings" on page 92.

Appendices

This chapter describes the guidelines adopted to secure IPMI configuration, using the following sections:

Table 1-11 Appendix listed in the Security Guide

Section name	Description	Link
Appendix A: Operating system packages removed from the NetBackup Appliance	This section lists the packages removed from the NetBackup Appliance operating system.	See "Listing Operating system packages removed from the NetBackup Appliance" on page 99.

Intended Audience

This guide is intended for the end users that include security administrators, backup administrators, system administrators, and IT technicians who are tasked with maintaining the NetBackup Appliance.

What's new in NetBackup Appliance 2.6.x.x security feature?

For NetBackup Appliance 2.6.x.x the security implementation has been improved with the addition of the following features:

- The NetBackup Appliance Web Console is now available only over HTTPS on the default port 443; port 80 over HTTP has been disabled. Please use https://<appliance-name> to log in to the Web Console, where appliance-name is the fully qualified domain name (FQDN) of the Appliance and can also be an IP address.
- The client installation media share for NFS and CIFS are disabled for security reasons, as a default, in the NetBackup Appliance 2.6.0.4 version. You can use the `Settings > Share ClientInstall Open` command from the NetBackup Appliance Shell Menu to enable the client share.
- You can now configure the Active Directory server to register users and user groups with the appliance. The feature is currently available only from the NetBackup Appliance Shell menu, using the `Settings > Security > Authentication > Active Directory` command.
- You can grant the NetBackup CLI user role to LDAP/AD users and user groups that grants them the permissions to run all the NetBackup commands through the NetBackup Appliance Shell Menu. The maximum number of user groups that can be granted NetBackup CLI role is 9.
- You can set a login banner, to be displayed after a user logins to the NetBackup Appliance Shell Menu via SSH. The `Settings >Security > PolicyBanner` command has been added to set a new login banner.

Generic security guidelines

Symantec recommends the following guidelines for server and user configuration:

- Only one authentication type (LDAP or Active Directory) can be configured on the NetBackup Appliance at a given point of time.
- The Active Directory server and users can be configured only using the `Main > Settings > Security > Authorization > Active Directory` commands from NetBackup Appliance Shell Menu.
- A Login Banner can be applied, for SSH logins, using the `Settings > Security > PolicyBanner` command from the NetBackup Appliance Shell Menu.
- A maximum of nine(9) user groups can be assigned to the NetBackup CLI role.

- The NetBackup CLI user role cannot be assigned to a local user.
- Two users with the same user ID, should not be added to the same NetBackup Appliance. Such conflicting user IDs lead to security issues. For example, there are two users with the same name 'John Doe', one is an Active Directory user and the other is a local user. Both these users should have different user IDs to access the NetBackup Appliance, like 'John_Doe1' and 'John_Doe_new'.

See "About the authentication feature" on page 20.

See "About the authorization feature" on page 32.

About the NetBackup Appliance documentation

The following documents help to ensure that you can successfully install, configure, and use your appliance. All these documents are posted on the Symantec Support website at the following URL:

http://www.symantec.com/docs/DOC2792

Table 1-12 NetBackup Appliance documentation

Guide	Description
Symantec NetBackup™ Appliance Administrator's Guide	The *Symantec NetBackup™ Appliance Administrator's Guide* contains the following types of information: ■ Deployment information ■ Administering your appliance ■ Monitoring information
Symantec NetBackup™ Appliance Command Reference Guide	The *Symantec NetBackup™ Appliance Command Reference Guide* provides a complete list of the commands that are available for you to use through the NetBackup Appliance Shell Menu.
Symantec NetBackup Appliance Release Notes	This document contains information about NetBackup appliance, version 2.6.0.4. It contains brief descriptions of new features within the release, operational notes that apply to the release update, and any known issues.
Symantec NetBackup Appliance Troubleshooting Guide	This document contains the latest troubleshooting information for the NetBackup appliances.
Symantec NetBackup Appliance Capacity Planning and Performance Tuning Guide	This document contains information on how to optimize your backup environment and your NetBackup appliance. It helps you to analyze your backup requirements and design a system that best fits your needs.

Table 1-12 NetBackup Appliance documentation *(continued)*

Guide	Description
Symantec NetBackup Appliance Security Guide	This document describes the security features in NetBackup Appliance and how to use those features to ensure that your appliance environment is secure.
Symantec NetBackup Appliance Third-party Legal Notices	The *Symantec NetBackup Appliance Third-party Legal Notices* document lists the third-party software that is included in this product, and it contains attributions for the third-party software. This document is available from the following website: http://www.symantec.com/about/profile/policies/eulas/

For additional information about the appliance hardware, refer to the following documents:

- *Symantec NetBackup 5220 Appliance and Symantec Storage Shelf Product Description*
- *Symantec NetBackup 5230 Appliance and Symantec Storage Shelf Product Description*

Chapter 2

NetBackup Appliance Authentication

This chapter includes the following topics:

About the authentication feature

Table 2-1 describes the options provided for authenticating new users using the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu:

Note: You need use the NetBackup Appliance Shell Menu to configure the Active Directory server and register the AD users and user groups.

Table 2-1 Authentication feature

	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Path	**Settings > Authentication > Server Configuration** tab	`Main > Settings > Security > Authentication` command

Table 2-1 Authentication feature *(continued)*

	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
LDAP configuration	You can configure the LDAP server and perform the following tasks: ■ Add details of a new LDAP server. ■ Import the settings of an existing LDAP server. ■ Identify and attach the SSL certificate for the LDAP server. ■ Add, Edit, and Delete attribute mappings for the LDAP server. ■ Add, Edit, and Delete configuration parameters for the LDAP server. ■ Export current LDAP configuration as an xml file. These can be imported to configure the server on other appliances. ■ Disable the configured LDAP server. ■ Unconfigure the disabled LDAP server. Use the **Settings > Authentication > User Configuration** tab to add LDAP users from the NetBackup Appliance Web Console.	**LDAP server configuration commands** ■ `Configure` - Configure LDAP Authentication. ■ `Enable` - Use this command to enable LDAP Authentication. ■ Import the settings of an existing LDAP server. ■ `Certificate` - Identify and attach the SSL certificate for the LDAP server. ■ `Attribute` - Add, Edit, and Delete attribute mappings for the LDAP server. ■ `Map` - Set and view the NSS Map attributes or object classes. ■ `ConfigParam` - Add, Edit, and Delete configuration parameters for the LDAP server. ■ `Export` - Export current LDAP configuration as an xml file. These can be imported to configure the server on other appliances. ■ `Disable` - Disable the configured LDAP server. ■ `Unconfigure` - Unconfigure the disabled LDAP server. ■ `Status` - View configuration status. ■ `Show` - View configuration details. ■ `Users` - Add and remove LDAP users.* ■ `Groups` - Add and remove LDAP user groups. (The maximum number of user groups that can be granted NetBackupCLI role is 9.)* ■ `List` - List users and user groups.*

Table 2-1 Authentication feature *(continued)*

	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
AD configuration tasks	You cannot configure Active Directory server or register AD users from theNetBackup Appliance Web Console.	**Active Directory server configuration** ■ `Configure` - Add details of a new Active Directory server. ■ `Unconfigure` - Unconfigure the disabled Active Directory server. ■ `Status` - View configuration status. ■ `Users` - Add and remove Active Directory users.* ■ `Groups` - Add and remove Active Directory user groups.* The maximum number of user groups that can be granted NetBackupCLI role is 9. ■ `List` - List users and user groups.*
Local user tasks	Use the **Settings > Authentication > User Configuration** tab to add local users from the NetBackup Appliance Web Console.	**Local user configuration*** ■ `Users` - Add or remove local users. ■ `Clean` - Delete all the local users. ■ `Password` - Change the password for a local user. ■ `List` - List users and user groups.

* - these tasks can be performed using the **Settings > Authentication > User Configuration** tab from the NetBackup Appliance Web Console.

Accounts available on the NetBackup Appliance

The following accounts are available on the NetBackup Appliance:

Table 2-2 NetBackup Appliance accounts

User account	Description
Administrators	This user role is provided administrative privileges to manage the NetBackup Appliance. The Administrator is allowed to log on, view, and perform all functions on theNetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. It is important that when you add new users or user groups, you also grant them administrative permissions. See "About supported user roles - NetBackup Appliance Administrator" on page 34.
NetBackup CLI administrators	This user role is solely restricted to run NetBackup CLI and does not have access outside the scope of NetBackup software directories. Once these users login, they are taken to a restricted NetBackup Appliance Shell Menu from where they can manage NetBackup. The NetBackup CLI users do not have access to NetBackup Appliance Web Console or NetBackup Appliance Shell Menu. See "About supported user roles - Appliance NetBackup CLI user" on page 35.
Maintenance	This user account is specifically used by the Symantec support through the NetBackup Appliance Shell Menu (after an administrative login). It is used specifically to perform maintenance activity or troubleshoot the appliance.
AppComm	This service account is used for internal process communication.
sisips	This is an internal user role for implementing the SCSP policies.

root	This is a restricted account and accessible only to perform maintenance tasks by the Symantec Support . If you try to access the root account the following message is displayed:
	
	`Permission Denied !! Access to the root account requires overriding the Symantec Intrusion Security Policy.`
	
	`Please refer to the appliance security guide for overriding instructions.`
	
	Warning: Please note that you can override the Symantec Intrusion Security Policy to gain access to the root account. However, doing this is not recommended as it puts the system under risk and makes the system vulnerable to attack. See "Overriding the Symantec Intrusion Security policy (IPS)" on page 42.

Authentication types in NetBackup Appliance

The NetBackup Appliance lets you directly add local users on the appliance and also register users from your LDAP server or Active Directory. Table 2-3 desrcibes the types of users that can be added to a NetBackup Appliance:

Table 2-3 User types

User type	Description	Notes
Local user or Native user	A local user is added to the appliance database, and is not referenced to an external directory-based server like the LDAP server or Active Directory. At the time of initial configuration the Symantec Support team or Field engineers help you obtain the user credentials for the first local user.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to managed local users. ■ You use the `Settings > Security > Authorization > Local user` command from the NetBackup Appliance Shell Menu to manage local users. ■ You cannot add local user groups. ■ You can only assign the Administrator access permissions to a local user.
LDAP supported users	An LDAP (Lightweight Directory Access Protocol) user or user group needs to be registered with the NetBackup Appliance. Once the user has been registered you can grant or revoke the appropriate permissions.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add LDAP users or user groups. ■ You can use the `Settings > Security > Authorization > LDAP` command from the NetBackup Appliance Shell Menu to add LDAP users and user groups. ■ The maximum number of LDAP user groups that can be granted NetBackupCLI role is 9. ■ You can assign the Administrator or NetBackup CLI access permissions.
Active Directory supported users	An Active Directory user or user group needs to be registered with the NetBackup Appliance. Once the user has been registered you can grant or revoke the appropriate permissions.	■ You can use the `Settings > Security > Authorization > Active Directory` command from the NetBackup Appliance Shell Menu to add AD users and user groups. ■ The maximum number of AD user groups that can be granted NetBackupCLI role is 9. ■ You can assign the Administrator or NetBackup CLI access permissions.

For detailed instructions to configure new users please refer to the 'Settings > Authentication' section in the *Symantec NetBackup™ Appliance Administrator's Guide*.

About configuring LDAP supported users

The NetBackup Appliance uses PAM plug-ins to support various authentication methods. One of them is an LDAP PAM plug-in. This is used to support the LDAP Authentication method by which users belonging to an LDAP (Lightweight Directory Access Protocol) directory can be configured to log on to the appliance.

Pre-requisites to configure the LDAP Server

- Software version 2.6 or higher must be installed on the NetBackup Appliances
- LDAP schema must be RFC 2307 or RFC 2307bis compliant
- The following Firewall ports must be open:
  - LDAP 389
  - LDAP OVER SSL/TLS 636
  - HTTPS 443
- LDAP integration with a NetBackup 52xx series appliance also depends on the distributed LDAP PAM plug-ins, as part of the Linux operating system used in the appliance.

Configuring the LDAP server

Before registering the LDAP users with the NetBackup Appliance, LDAP Authentication needs to be configured on the Appliance. Once this configuration is complete the NetBackup Appliance can access user information and authenticate the users across all your LDAP Authentication configured appliances. To configure LDAP Authentication, you can use either of the following options:

- **Settings > Authentication > Server configuration** page from the NetBackup Appliance Web Console
- `Settings > Security > Authentication > LDAP` command from the NetBackup Appliance Shell Menu

For detailed instructions to configure the LDAP server, refer to the 'Settings > Authentication' section in the *Symantec NetBackup™ Appliance Administrator's Guide*.

About configuring Active Directory supported users

The LDAP PAM plug-in can also be used to support the Active Directory authentication method by which users belonging to an Active Directory server can be configured to log on to the appliance. Active Directory is considered as another type of user directory with a schema installed on it by UNIX services.

Pre-requisites to configure the Active Directory server

- Software version 2.6 or higher must be installed on the NetBackup Appliances.
- Ensure that your Active Directory is set up with all the required identities and groups.
- Ensure the authorized domain user credentials are utilized to configure the AD server with the NetBackup Appliance.
- Configure the NetBackup Appliancewith a DNS server that can forward DNS requests to an AD DNS server. Alternatively, configure the appliance to use the AD DNS server as the name service data source.
- The AD integration with a NetBackup 52xx series appliance also depends on the distributed LDAP PAM plug-ins, as part of the Linux operating system used in the appliance

Configuring the Active Directory server

Before you add new users from the Active Directory, you need to configure it with your appliances. Once this configuration is complete the NetBackup Appliance can access user information and authenticate the users across all your appliances.

You can configure the Active Directory server using the `Security > Authentication > ActiveDirectory` command from theNetBackup Appliance Shell Menu.

For detailed instructions to configure the Active Directory server, refer to the 'Main > Settings > Security > Authentication ' section in the *Symantec NetBackup Appliance Command Reference Guide*.

Authentication of NetBackupCLI administrators

In addition to the administrative privileged identities, you can create local users who have NetBackup CLI role. These NetBackup CLI roles are solely restricted to run NetBackup Commands with superuser privileges and do not have access outside the scope of NetBackup software directories. Once these users logins, they are taken to a restricted NetBackup Appliance Shell Menu from where they can run the NetBackup commands. The NetBackup CLI users do not have access to NetBackup Appliance Web Console or NetBackup Appliance Shell Menu.

You can use the `Manage > NetBackupCLI > Create user_name` command from the NetBackup Appliance Shell Menu to create a NetBackup CLI user. You do not require to provide any additional permissions for enabling the NetBackup CLI administrator.

About User name and Password Specifications

You can refer to the following specifications while assigning a new user name and a password:

Note: The `Manage > NetBackupCLI > Create interface` command is used to create local users with NetBackup CLI role. All the local user and password specifications apply to these users.

User name specifications

The user name for the NetBackup Appliance user account must be in the format that the selected authentication system accepts. Table 2-4 lists the user name specifications for each user type.

Table 2-4 User name specifications

Description	Administrator (Local user)	NetBackup CLI (Local user)	LDAP/AD user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP and the AD policy
Minimum length	2 characters	2 characters	Determined by the LDAP and the AD policy
Restrictions	User names must not start with: ■ number ■ special character	User names must not start with: ■ number ■ special character	Determined by the LDAP and the AD policy
Space inclusion	User names must not include spaces.	User names must not include spaces.	Determined by the LDAP and the AD policy

Password specifications

The NetBackup Appliance password policy has been updated to increase security on the appliance. The password for the NetBackup Appliance user account must be in the format that the selected authentication system accepts. Table 2-5 lists the password specifications for each user type.

Table 2-5 Password specifications

Description	Administrator (Local user)	NetBackup CLI (Local user)	LDAP/AD user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP and the AD policy.
Minimum length	Passwords must contain at least eight characters	Passwords must contain at least eight characters	Determined by the LDAP and the AD policy.
Requirements	■ One lowercase letter (a-z). ■ One number (0-9). ■ Dictionary words are considered as weak passwords and are not accepted. ■ The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	■ One lowercase letter (a-z). ■ One number (0-9). ■ Dictionary words are considered as weak passwords and are not accepted. ■ The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP and the AD policy.
Space inclusion	Passwords must not include spaces.	Passwords must not include spaces.	Determined by the LDAP and AD policy,
Minimum password age	0 day **Note:** The administrator can manage the password age of the users using the `Settings > Password` command from theNetBackup Appliance Web Console. For more information, refer to the *Symantec NetBackup™ Appliance Command Reference Guide*.	0 day **Note:** The administrator can manage the password age of the users using the `Manage > NetBackupCLI > PasswordExpiry` command from theNetBackup Appliance Web Console. For more information, refer to the *Symantec NetBackup™ Appliance Command Reference Guide*.	Determined by the LDAP and AD policy
Maximum password age	99999 days (doesn't expire)	99999 days (doesn't expire)	Determined by the LDAP and AD policy

Table 2-5 Password specifications *(continued)*

Description	Administrator (Local user)	NetBackup CLI (Local user)	LDAP/AD user
Password history	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP and AD policy
Password expiry	Not applicable as the password does not expire	Use the `Manage > NetBackupCLI > PasswordExpiry` command to manage the NetBackup CLI password.	Determined by the LDAP and AD policy
Password lockout	None	None	Determined by the LDAP and AD policy
Lockout duration	None	None	Determined by the LDAP and AD policy

Note: To increase the security of your environment, Symantec recommends that you change the default admin and maintenance passwords upon initial login to the appliance. You can use the **Settings > Password Management** page from the NetBackup Appliance Web Console or `Settings > Password` command from the NetBackup Appliance Shell Menu, to change the password.

Warning: The NetBackup Appliance does not support setting the Maintenance account password, using commands like `yppasswd root` or `passwd root`. The password set in this fashion is overwritten once the system is upgraded. You should use the NetBackup Appliance Shell Menu to change the Maintenance password.

Password encryption

The NetBackup Appliance adopts the following password encryption measures:

- Blowfish symmetric-key block cipher password hashing for hashing passwords of local users of the appliance.
- Passwords in transit include the following:
  - SSH login where the password is protected by the SSH protocol

- NetBackup Appliance Web Console login where the password is protected by the HTTPS communication

For detailed instructions to change password, refer to the 'Settings > Password Management' section in the *Symantec NetBackup™ Appliance Administrator's Guide*.

Chapter 3

NetBackup Appliance Authorization

This chapter includes the following topics:

About the authorization feature

Table 3-1 describes the options provided for Authorizing new users using theNetBackup Appliance Web Console and NetBackup Appliance Shell Menu:

Table 3-1 Authorization feature

	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Path	**Settings > Authentication > User Management** tab	`Main > Settings > Security > Authorization`

Table 3-1 Authorization feature *(continued)*

	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
User management	■ Add and remove Local users. ■ Add and remove LDAP users and user groups. **Note:** You cannot add Active Directory users from the NetBackup Appliance Web Console you can only manage access permissions for the Active Directory users.	Use the `Main > Settings > Security > Authentication` command to add Local users, LDAP users and Active Directory users.
Grant permissions	■ Grant permission to users and user groups as an Administrators ■ Grant permission to users and user groups as a NetBackup CLI user. ■ Revoke Administrator permissions ■ Revoke NetBackup CLI permissions	**Authorization** command: ■ `Grant` - Grant access permissions. ■ Grant administrative permissions to Local users, LDAP user, LDAP user groups, AD user, and AD user groups. ■ Grant NetBackup CLI user permissions to LDAP users, LDAP user groups, AD user, and AD user groups. ■ `List` - List all users and groups. ■ `Revoke` - Revoke access permissions. ■ Revoke administrative permissions from Local users, LDAP user, LDAP user groups, AD user, and AD user groups. ■ Revoke NetBackup CLI user permissions from LDAP users, LDAP user groups, AD user, and AD user groups. ■ `SyncGroupMembers` - Synchronize members of registered groups.

In addition to the `Authorization` and `Authentication` commands, you can also set a Login Banner using the `Settings > Security > PolicyBanner` command from the NetBackup Appliance Shell Menu. The 2.6.0.3 version of the NetBackup

Appliance enables you to set a login banner, which is displayed whenever any user tries to access the NetBackup Appliance Shell Menu using SSH.

About NetBackup Appliance Authorization

The NetBackup Appliance authorization has the following characteristics:

- Ability to prevent unintended access to the NetBackup Appliance by password protecting logins to the appliance.
- Access to shared data is provided only to authorized NetBackup Appliance users and NetBackup processes.
- Data stored within an appliance cannot inherently protect itself from unintended modification or deletion by a malicious user that knows of admin credentials to the appliance.
- Access to NetBackup Appliance Shell Menu must be done only by using SSH. You can also directly connect a monitor and keyboard to the appliance and login using your admin credentials.

  Note: The 2.6.0.3 version of the NetBackup Appliance enables you to set a login banner, which is displayed whenever any user tries to access the NetBackup Appliance Shell Menu by SSH. You can use the `Settings > Security > PolicyBanner` command to set a new login banner. For more information refer to *Symantec NetBackup Appliance Command Reference Guide*.

- Access to NetBackup Appliance Web Console is only done access HTTPS requests.
- Access to FTP, Telnet, and rlogin are disabled on all appliances.

Note: The NetBackup Appliance does not limit login attempts and enforce lockout policies. These features will be implemented in the future releases.

About supported user roles - NetBackup Appliance Administrator

The NetBackup Appliance provides access control mechanisms to prevent unauthorized access to the data backed up on appliances. These mechanisms include administrative user logins that provide elevated privileges to modify appliance configurations, monitoring the appliance and so on.

Note: Only Admin role is authorized to configure and manage NetBackup Appliance. There by ruling out all other user roles.

The Admin login credentials should be provided only to an authorized system administrator to prevent unauthorized and inappropriate modification of appliance configuration or backup data contained in the expansion disk storage. An admin can access the NetBackup Appliance using SSH access to NetBackup Appliance Shell Menu or HTTPS access to the NetBackup Appliance Web Console.

A local, LDAP, or Active Directory user needs to have the permissions of an admin user role to access and administer the various tasks on the NetBackup Appliance. After you have added a new user or a user group use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to grant the user or group the permissions of an Admin user role

The admin as a superuser can perform all the following tasks:

- Initial configuration
- Monitor hardware, storage, and SCSP logs
- Manage storage configuration, additional servers, licenses and so on
- Update configuration settings like Date and Time, Network, Notifications and so on.
- Restore the NetBackup Appliance.
- Decommission a NetBackup Appliance.
- Apply patches to a NetBackup Appliance.

For more information about the tasks you can perform as an NetBackup Appliance Admin, refer to *Symantec NetBackup™ Appliance Administrator's Guide*.

About supported user roles - Appliance NetBackup CLI user

The user functionality for the Appliance NetBackup CLI user is improved for better usability. A NetBackup CLI user can execute all NetBackup commands, view logs, edit NetBackup touch files, edit NetBackup notify scripts. The NetBackup CLI users share a common home directory.

When NetBackup CLI users log onto the Appliance, they are given a restricted NetBackup Appliance shell from where the NetBackup commands can be executed. Table 3-2 lists the rights and restrictions for a NetBackup CLI user.

Table 3-2 Rights and Restrictions of the Appliance NetBackup CLI user

Rights	Restrictions
The NetBackup CLI user can use the NetBackup Appliance Shell Menu to: ■ Run NetBackup CLI and access the NetBackup directories and files ■ Modify or create NetBackup notify scripts, using the `cp-nbu-notify` command to create and edit the scripts. **Note:** The notify script restriction has been lifted from versions 2.6.0.2 and higher. See "Loading the NetBackup notify scripts" on page 37. ■ Run the following NetBackup commands and for the following directories that contain the NetBackupCLI: NetBackupCLI Directory Path ■ `/usr/openv/netbackup/bin/*` ■ `/usr/openv/netbackup/bin/admincmd/*` ■ `/usr/openv/netbackup/bin/goodies/*` ■ `/usr/openv/volmgr/bin/*` ■ `/usr/openv/volmgr/bin/goodies/*` ■ `/usr/openv/pdde/pdag/bin/mtstrmd` ■ `/usr/openv/pdde/pdag/bin/pdcfg` ■ `/usr/openv/pdde/pdag/bin/pdusercfg` ■ `/usr/openv/pdde/pdconfigure/pdde` ■ `/usr/openv/pdde/pdcr/bin/*`	The following restrictions are placed on NetBackup CLI administrator ■ The NetBackup CLI user does not have access outside the NetBackup software directories. ■ They cannot edit the `bp.conf` file directly using an editor. Use the `bpsetconfig` command to set an attribute. ■ The `cp-nbu-config` command supports creating and editing NetBackup touch configuration files only in the `/usr/openv/netbackup/db/config` directory. ■ They cannot use the `man` or `-h` command to see the help of any other command.

How to run NetBackup commands as Appliance NetBackupCLI user:

There are two ways to run commands as NetBackupCLI user:

- Using the restricted NetBackup Appliance Shell Menu
- Using absolute path ["sudo"] for example,

  `bppllist`

  or

  `/usr/openv/netbackup/bin/admincmd/bpplist`

Loading the NetBackup notify scripts

The `cp-nbu-notify` utility is similar to `cp-nbu-config` utility that is added to the NetBackup Appliance to modify the NetBackup notify scripts, like the `start` and `exit` notification scripts to be run after each job.

The NetBackup CLI users can modify the notify scripts from the following script locations:

- `/usr/openv/netbackup/bin`
- `/usr/openv/volmgr/bin`

Note: The `cp-nbu-notify` assumes that the notify script pre-exists either in the actual location as a sample file or its goodies directory as a template. If a sample or template notify script does not exist in these directories, then the script that you may try to load is not considered valid.

To install or edit the notify scripts:

1. Login to the appliance as a NetBackupCLI user and then create the notify script in the home directory.
2. Enter `cp-nbu-notify` command to install the script:

   ```
   cp-nbu-notify <notify-script>
   ```

   The appliance displays the following messages:

   ```
   NetBackup Appliance admin must review and
   approve this operation.
   Enter admin password:
   ```

3. When the command prompts for admin password, enter the Appliance admin password (not the NetBackupCLI password). The password is needed for security purpose to make sure that the notify script is approved by the Appliance admin.

   When the password is successfully verified the notify script is automatically loaded in the right location.

   Note: The source notify script must exist in the home directory or its subdirectory.

Caution: You can only copy the notify scripts. Not any other scripts in the NetBackup install path. Execution of any external script through the notify script can lead to a security issue.

See “About supported user roles - Appliance NetBackup CLI user” on page 35.

Chapter 4

NetBackup Appliance Intrusion Prevention and Intrusion Detection Systems

This chapter includes the following topics:

Introduction to Symantec Critical System Protection (SCSP)

The Symantec Critical System Protection (SCSP) is a solution offered by the Symantec Data Center Security team to protect servers in data centers. It offers policy-based protection and helps secure servers using host-based intrusion

prevention and detection technology. It uses the least privileged containment approach and also helps security administrators manage multiple appliances centrally in your data center. The SCSP security agent along with NetBackup Appliance Intrusion Prevention (IPS) and Intrusion Detection (IDS) policy has been integrated with the NetBackup Appliance to provide the following features:

- **Harden Linux OS components** - prevent or contain malware from harming the integrity of the underlying host system as a result of OS vulnerabilities.
- **Protect the Data** - tightly limit access to appliance data to only those programs and activities needing access regardless of system privileges.
- **Harden the Application stack** - lock down appliance application binaries and configuration settings such that changes are tightly controlled by the application or trusted programs/scripts.
- **Expand detection and audit capabilities** - provide enhanced visibility into important user or system actions to ensure a valid and complete audit trail that addresses compliance regulations (such as PCI) as a compensating control.
- **Support centralized Managed mode operations** - allows customers to use central CSP manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by CSP.

About NetBackup Appliance Intrusion Prevention Policy (IPS)

The NetBackup Appliance Intrusion Prevention policy features are:

- Real-time tight confinement of the NetBackup Appliance OS processes and common applications like:
  - `nscd` - which caches DNS requests to cut down on remote DNS lookups.
  - `cron`
  - `syslog-ng`
  - `klogd`
  - `rpcd` for NFS
    - `rpc.idmapd`
    - `rpc.mountd`
    - `rpc.statd`
    - `rpcbind`

- Self-Protection for the SCSP Agent itself, to ensure the security and the monitoring features of SCSP are not compromised
- Lock-down of system binaries except by identified and trusted applications and users/groups.
- Confinements that protect the system from having apps trying to install software (such as `sbin`) or change system configuration settings, such as`hosts file`, and so on.
- Prohibits applications from executing critical system calls such as `mknod`, `modctl`, `link`, `mount`, and so on.
- Prohibit unauthorized users or applications from accessing backed up data such as `/advanceddisk`, `/cat`, `/disk`, `/usr/openv/kms`, `/opt/NBUAppliance/db/config/data` and so on.
- Restricted access to the root account by maintenance user. See "Overriding the Symantec Intrusion Security policy (IPS)" on page 42.

About NetBackup Appliance Intrusion Detection Policy (IDS)

The Intrusion Detection System (IDS) policy is a detection policy enabled by an SCSP agent. The IDS policy includes the detection engine that monitors significant system events and critical configuration changes in real time like:

- User logins, logouts, and failed log on attempts
- Sudo commands
- User addition, deletion, password changes
- Group addition, deletion, member modifications
- System auto start change options
- Modifications to all system directories and files (which includes Core system files, core system configuration files, installation programs, common daemon files)
- NetBackup start/stop services
- Detected system attacks from UNIX Rootkit File / Directory Detection, UNIX Worm File/Directory Detection, Malicious Module Detection, Suspicious Permission Change Detection, and so on
- NetBackup Appliance shell operations for maintenance, root, and NetBackup CLI users

- Audit all the NetBackup Appliance Shell Menu and NetBackup Appliance Web Console activity.

Overriding the Symantec Intrusion Security policy (IPS)

For the version 2.6.0.2 and higher the NetBackup Appliance discourages accessing the root account using the `elevate` command using the `Support > Maintenance` menu. If you try to access the elevate command the following message is displayed:

```
Permission Denied !! Access to the root account requires
overriding the Symantec Intrusion Security Policy.

Please refer to the appliance security guide for
overriding instructions.
```

Warning: Please note that you can override the Symantec Intrusion Security Policy to gain access to the root account. However, doing this is not recommended as it puts the system under risk and makes the system vulnerable to attack.

Note: You can use the NetBackup CLI user role to run NetBackup commands, without overriding the security policy. See "About supported user roles - Appliance NetBackup CLI user" on page 35.

You can use the following procedure to override the Symantec Intrusion Policy.

Note: Every activity under the maintenance account will be logged.

Overriding the security policy disables only the prevention mode. Detection mode and logging on the appliance will still be enabled.

To override the Symantec Intrusion security policy:

1. Log on to the NetBackup Appliance Shell Menu as an Administrator.
2. Run the `Support > Maintenance` command.

3 To enter your Maintenance account, run the following command, and provide the password when you receive a prompt.

```
NBAppl.Support > Maintenance

<!--Maintenance Mode--!>

maintenance's password:
```

4 In the Maintenance mode, type the following command to override the Symantec Intrusion Security Policy:

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
```

The appliance displays the following message:

```
Symantec Critical Protection Policy Override

Agent Version: 5.2.9 (build 739)

Current Policy: NetBackup Appliance Prevention Policy, r19

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Not overridden

To override the policy and disable protection,
enter your login password.

Password:
```

5 Enter your maintenance password.

The appliance then displays the following options:

```
Choose the type of override that you wish to perform:

1. Override Prevention except for Self Protection

2. Override Prevention Completely

Choice?
```

6 Enter `1` to override prevention except for self protection.

Note: Symantec recommends that you use Option 1. Selecting **Option 1** allows modification only to theNetBackup Appliance Shell Menu and NOT to the SCSP Agent.

The appliance displays the following options:

```
Choose the amount of time after which to automatically re-enable:

1. 15 minutes

2. 30 minutes

3. 1 hour

4. 2 hours

5. 4 hours

6. 8 hours

7. never
```

7 Enter the appropriate number from 1 to 7 based on the time required to debug the Symantec support case.

The appliance displays the following message:

```
Enter a comment. Press Enter to continue.

Disabling the security policy for
debugging a Symantec
support case no - XYZ
```

8 Enter a relevant comment as to why the override is required.

The appliance overrides the policy and displays the following message:

```
Please wait while the policy is being overridden.
........

The policy was successfully overridden.
maintenance - !> elevate
```

You should now have access to the root account for debugging the appliance.

See “Re-enable the Symantec Intrusion Security policy” on page 45.

Re-enable the Symantec Intrusion Security policy

You can use the following procedure to re-enable the Intrusion Security policy (IPS) from the maintenance mode.

To re-enable the Symantec Intrusion security policy:

1. Log on to the NetBackup Appliance Shell Menu as an Administrator.
2. Run the `Support > Maintenance` command.
3. To enter your Maintenance account, run the following command, and provide the password when you receive a prompt.

```
NBAppl.Support > Maintenance

<!--Maintenance Mode--!>

maintenance’s password:
```

4 In the Maintenance mode, type the following command to re-enable the Symantec Intrusion security policy:

```
/opt/Symantec/scspagent/IPS/sisipsoverride.sh
```

The appliance displays the following message:

```
Symantec Critical Protection Policy Override

Agent Version: 5.2.9 (build 739)

Current Policy: NetBackup Appliance Prevention Policy, r19

Policy Prevention: Enabled

Policy Override: Allowed

Override State: Overriden

Overide Type: Prevention Overriden except for Self-Protection

Overide User: maintenance

Previous Comment: This is an example.

Auto re-enable in: 13 minutes, 31 seconds


Do you wish to:

1. Re-enable the Policy.
2. Extend the Override Time.
```

5 Enter `1` to re-enable the Symantec Intrusion security policy.

The appliance displays the following message:

```
Enter a comment. Press Enter to continue.

The policy is re-enabled.
```

6 Enter a relevant comment.

The appliance re-enables the policy and displays the following message:

```
Please wait while the policy is being re-enabled.

......

The policy was successfully re-enabled.
```

See "Overriding the Symantec Intrusion Security policy (IPS)" on page 42.

Reviewing SCSP events

You can use the **Monitor > SCSP Event View** menu to view the Symantec Critical System Protection (SCSP) logs.

These audit logs can help detecting security breach or abnormal activity on your appliance. An event in the audit log includes the following details:

- When - Displays the timestamp of the logged event.
- Who - Displays which user had logged on when the event took place.
- What - Displays the description of the event and the resource involved.
- How - Displays the Process Name, Process ID, Operation Permissions, Sandbox Details.
- Severity - Displays the severity of the log.
- Enforcement Action - Displays whether the event was allowed or denied.

The SCSP logs are retrieved and are represented using the following severity types:

Severity types	Description	Events example

Information	Events with a severity as Info contain information about normal system operation.	For example the following message provides the basic information relating to a generic event.
		
		`general CLISH message`
		`Event source:`
		`SYSLOG PID: 30315`
		`Complete message:`
		`May 21 06:58:55`
		`nb-appliance`
		`CLISH[30315]:`
		`User admin`
		`executed Return`

Notice	Events with a severity as Notice contain information about normal system operation.	An event that helps confirm the successful execution of an event is recorded as a Notice. For example the following message helps the user to understand that the event has been successfully executed.
		
		`successful SUDO to root`
		`Event source: SYSLOG`
		`[sudo facility]`
		`Command: /bin/su From`
		`Username: AppComm To`
		`Username: root`
		`Port: unknown`

Severity types	Description	Events example
Warning	Events with a severity as Warning indicate unexpected activity or problems that have already been handled by Symantec Critical System Protection. These Warning messages might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access to the specific resources if necessary.	For example, the following event helps to identify and unexpected activity, like the inbound connection from a local IP address. `Inbound connection allowed from <IPaddress> to local address.`
Major	Events with a severity as Major imply a more serious effect than Warning and less effect than Critical.	For example, the following event helps to identify unauthorized access. `General luser message Event source:SYSLOG Complete message: Feb 5 21:57 luser Unauthorized user by luser Denying access to system.`
Critical	Events with a severity as Critical indicate activity or problems that might require administrator intervention to correct.	For example, the following event can help to identify critical events that can affect the appliance in an unexpected manner. `Group Membership for "group1" CHANGED from 'admin1' to 'admin2'`

For more information about retrieving SCSP audit logs, refer to the **Monitor > SCSP Events**section in the *Symantec NetBackup 52xx Appliance Administrator's Guide*.

For information about the Operating System logs, such as syslogs and other NetBackup Appliance logs, See “About working with log files” on page 58.

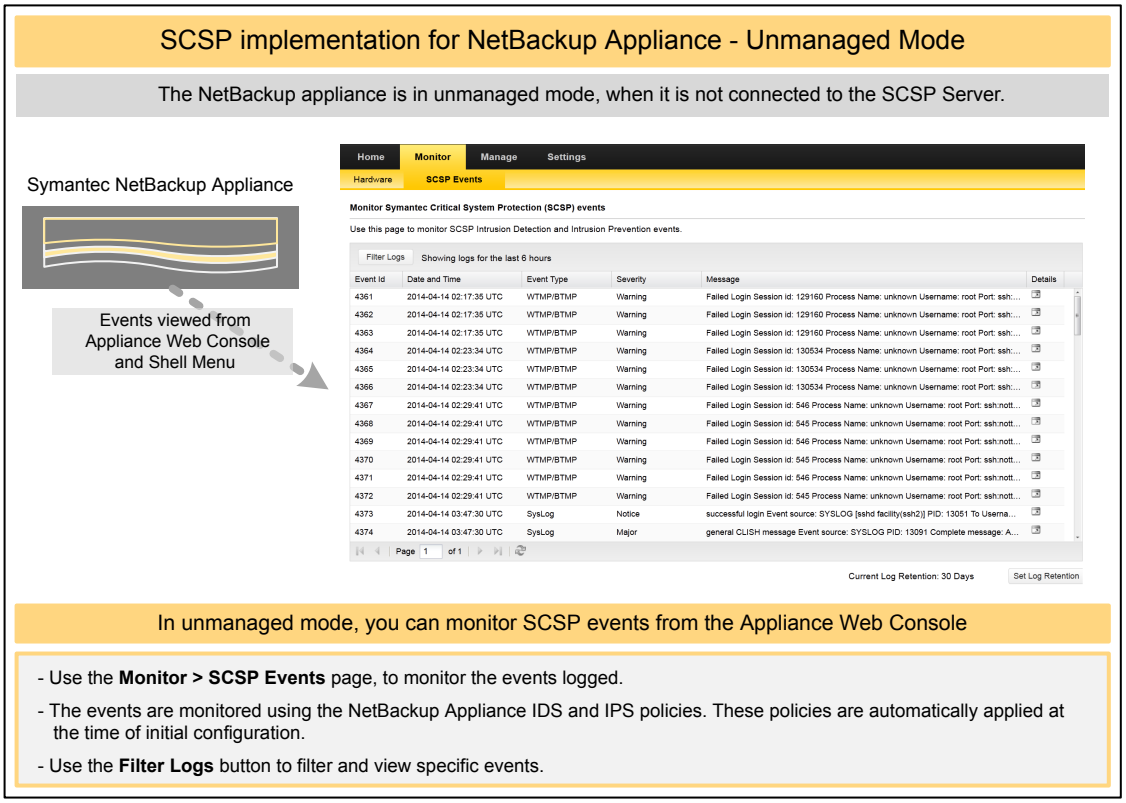
About SCSP Protection using the Unmanaged Mode

The SCSP protection is offered in unmanaged mode and in managed mode. The unmanaged mode is the default mode in which a NetBackup Appliance is configured. In unmanaged mode, the appliance is protected and audited without the use of an external SCSP server. The SCSP agent is baked in the appliance, it protects and audits the appliance using NetBackup Appliance Prevention and Detection Policy upon startup.

Note: The unmanaged mode is recommended for administrators who are the sole owners of the NetBackup Appliance and are primarily involved in backup administration.

The **Monitor > SCSP Events** page on the NetBackup Appliance Web Console is used to monitor the events on an appliance for any abnormal activity. Figure 4-1 illustrates the implementation of unmanaged mode:

Figure 4-1 SCSP implementation in Unmanaged mode



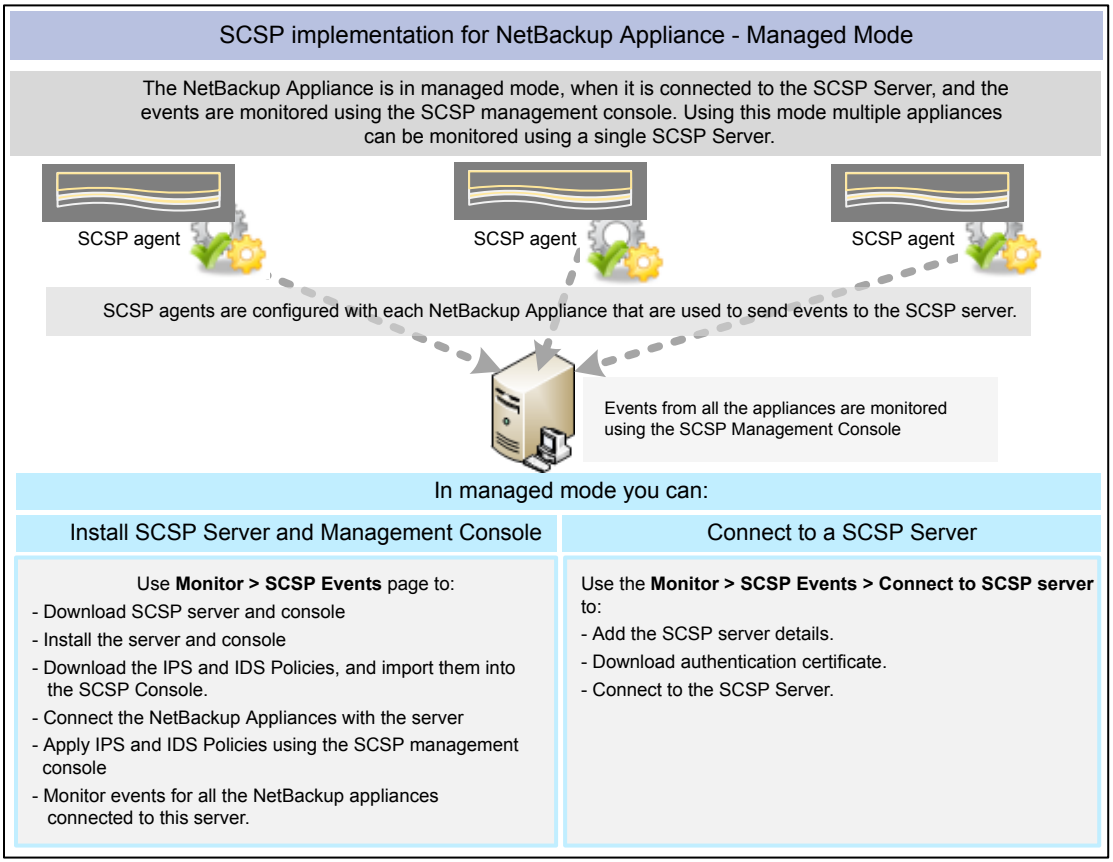
SCSP agent setup

From the version 2.6.0.2 and later of the NetBackup Appliance, the SCSP version of 5.2.8 (June 2012) is replaced with SCSP version 5.2.9 MP3 (July 2013) binaries and the NetBackup Appliance IPS and IDS policies.

About SCSP Protection using the Managed Mode

In managed mode, an external SCSP server can be used to communicate with and manage the SCSP agent on the appliance. The external SCSP server can be used to manage multiple appliances. You can download the SCSP server (data center security server), console, and policies from the NetBackup Appliance Web Console. Managed mode is recommended for use only by security administrators or by existing SCSP customers who have in-depth knowledge of SCSP. Figure 4-2 illustrates the implementation of managed mode:

Figure 4-2 SCSP implementation in managed mode



Benefits of using the managed mode

- Helps to provide separate tools catering to the Backup Administrators role and the Security Administrator role.
- Provides centralized and secure management of Multiple Appliances using a single SCSP server and console.
- Provides the ability to archive and export logs.
- Provides a common console for monitoring, reporting, and setting up alerts.
- Extends the NetBackup Appliance IPS and IDS policies on top of Symantec Baseline to meet your data center standards.
- Provides links to instantly download SCSP Server and Console from the NetBackup Appliance Web Console.

Downloading the SCSP server and console installable

The following procedure describes how to download the SCSP server and console from the **SCSP Event** page.

To download the SCSP server and console:

1. Log in to the NetBackup Appliance Web Console.
2. Click **Monitor > SCSP Event**.
3. The appliance displays the **SCSP Event** page. It displays the audit logs for the last 6 hours.
4. From the **Symantec Critical System Protection Downloads** section, use the **SCSP Server and Console** link to download the installation package for the SCSP server and console.

   The `scsp_server_5.2.9_MP3_EN.zip` file is downloaded to your local folders.
5. Extract the contents from the `scsp_server_5.2.9_MP3_EN.zip` file.

   The `scsp_server_5.2.9_MP3_EN > SCSPInstall` folder, contains the following:

   - `server.exe` - used to install the Symantec Critical System Protection Management Server 5.2.9 on your local computer.
     An installation wizard is displayed to help you install Symantec Critical System Protection Management Server 5.2.9 on your local computer. For more information about installing the SCSP management server, refer to *Symantec Critical System Protection 5.2.9 Installation Guide*. To download the latest installation guide, refer to DOC5944.
   - `console.exe` - used to install the Symantec Critical System Protection management console.
     An installation wizard is displayed to help you install the management console. For more information about installing the SCSP management console, refer to *Symantec Critical System Protection 5.2.9 Installation Guide*. To download the latest installation guide, refer to DOC5944.

See "Downloading NetBackup Appliance IPS and IDS policies" on page 53.

See "About SCSP Protection using the Managed Mode" on page 51.

Downloading NetBackup Appliance IPS and IDS policies

The following procedure describes how to download the NetBackup Appliance IPS policy and IDS policy, from the **SCSP Event** page.

To download NetBackup Appliance IPS and IDS policies:

1. Log in to the NetBackup Appliance Web Console.
2. Click **Monitor > SCSP Event**.

   The appliance displays the **SCSP Event** page. It displays the audit logs for the last 6 hours.
3. From the **Symantec Critical System Protection Downloads** section, use the **NetBackup Appliance IPS and IDS Policies** link to download the polices to be applied to the SCSP server.

   The `SCSPPolicies.zip` file is downloaded to your local folders.
4. Extract the contents from the `SCSPPolicies.zip` file.

   The `SCSPPolicies.zip` file contains the following policy compressed files:

   - `NetBackup Appliance Detection Policy.zip` - contains the IDS policy. This policy is an “after-the-fact” IDS for monitoring important significant events and optionally taking remediation actions on events of interest.
   - `NetBackup Appliance Prevention Policy.zip` - contains the IPS policy. This policy is an “in-line” IPS that can proactively block unwanted resource access behaviors before they can be acted upon by the operating system.

Note: These policies help to validate the events that take place on appliance and can be monitored by either using the **Monitor > SCSP Event** page in an unmanaged mode or the SCSP Management Server 5.2.9.

---

5 From the **Connect to SCSP Server** section, of the **SCSP Event** page, click **Connect**. This will let you connect your NetBackup Appliance to the SCSP server for applying the IDS and the IPS policy. See "Connecting to the SCSP server" on page 55.

6 Log on to the Symantec Critical System Protection Management Server 5.2.9, using the management console. Connect to your NetBackup Appliance and apply the IDS policy and IPS policy. For instructions on installing and setting up SCSP server in your environment, refer to the Symantec Critical System Protection Admin and Install guide.

See "Applying the NetBackup Appliance IPS and IDS policies" on page 56.

Warning: You must apply the downloaded IPS and IDS policies before connecting your NetBackup Appliance to the installed SCSP server. If the policy is not applied and the appliance is connected to the SCSP server it remains in an unprotected state.

See "Downloading the SCSP server and console installable" on page 53.

See "About SCSP Protection using the Managed Mode" on page 51.

Connecting to the SCSP server

The following procedure describes how to connect to the SCSP server from the **SCSP Events** page.

The **SCSP Events** page displays the **Connect to SCSP server** section that is used to connect to the SCSP server.

To connect to the SCSP server

1 Log in to the NetBackup Appliance Web Console.

2 Click **Monitor > SCSP Audit Logs**.

The appliance displays the **SCSP Events** page. It displays the audit logs for the last 6 hours.

3 Click on the **Connect** button, to connect to the SCSP server.

The appliance displays the **Connect to SCSP Server** dialog box.

4 Enter a complete and valid host name / IP address of the SCSP server in the **Host Name / IP** field.

5 Enter the port number of the SCSP server in the **Port** field.

Note: You cannot add an SCSP server without providing its authentication certificate. You can either download the certificate from the site or point to a downloaded certificate earlier, from your local folders.

6 Select the **Download authentication certificate from the site** radio button to download the authentication certificate from the SCSP server site.

The appliance displays certificate details.

7 Click on the **Accept Certificate** button, to accept the certificate.

The appliance displays the **Certificate issued** message.

OR

8 Select the **Provide location of an existing certificated** radio button, to enter the location of the certificate from your local folders.

9 Click on the **Connect** button to connect to the SCSP server.

The appliance connects to the SCSP Server and displays the following message:

Connected successfully to SCSP server.

See "About SCSP Protection using the Managed Mode" on page 51.

See "Downloading NetBackup Appliance IPS and IDS policies" on page 53.

See "Downloading the SCSP server and console installable" on page 53.

Applying the NetBackup Appliance IPS and IDS policies

You can use the NetBackup Appliance Web Console to download the NetBackup Appliance IPS and IDS policies. To apply these polices using the SCSP management console, use the following procedure:

To apply the IPS and IDS policies to an NetBackup Appliance agent or group

1 Log on to your SCSP server using the management console.

2 In the management console, click **Policies**.

3 Under the **Policies** tab, click **Prevention** or **Detection**.

4 On the **Policies** page, in the **Policies** tree, navigate to the downloaded `NetBackup Appliance Detection Policy.zip` and `NetBackup Appliance Prevention Policy.zip`. These policies can be downloaded from the **Monitor > SCSP Events** page on the NetBackup Appliance Web Console. See "Downloading NetBackup Appliance IPS and IDS policies" on page 53.

5 On the **Policies** page, select a policy to apply, and then right-click **Apply Policy**.

Warning: Do not apply any other existing prevention or detection workspace policy found on the policy page. This can cause serious damage to the system and can make the system non-responsive. Only the NetBackup Appliance policies, imported from theNetBackup Appliance Web Console, should be applied to the NetBackup Appliance 2.6.0.2 version or higher.

---

6 On the **Assets** page and click **Refresh** to ensure that the policy is applied. The red flag should then disappear ensuring that the agent successfully processed the policy changes.

You should now see events from all connected appliances under one page (SCSP Console).

For more information about the Policies tab and other tasks to be performed using policies, refer to 'Managing policies' section from the *Symantec Critical System Protection 5.2.9 Administration Guide*.

See "About SCSP Protection using the Managed Mode" on page 51.

See "Downloading the SCSP server and console installable" on page 53.

See "Connecting to the SCSP server" on page 55.

Chapter 5

NetBackup Appliance Log Files

This chapter includes the following topics:

About working with log files

As you define and troubleshoot a problem, always try to capture potentially valuable information. NetBackup Appliance has the ability to capture hardware-, software-, system-, and performance-related data. These log files capture information such as how the appliance has been running, whether there are any issues such as unconfigured volumes or arrays, temperature issues, batteries not being found, etc. These log files are stored in specific directories and can be accessed using the following methods:

Table 5-1 lists the methods you can use to access the various appliance logs.

Table 5-1 Viewing log files

From...	Using...	Logs collected..
NetBackup Appliance Web Console	You can use the **Collect Log files** wizard from the NetBackup Appliance Web Console to collect log files from an appliance. See "About using the Collect Log files wizard" on page 60.	■ Logs created by the NetBackup Copy Logs tool (`nbcplogs`) ■ Appliance logs including high availability, hardware, and event logs ■ Operating system logs ■ All logs related to Media Server Deduplication Pool (MSDP) ■ All logs related to the NetBackup Appliance Web Console ■ Diagnostic information about NetBackup and the operating system ■ Hardware and storage device logs
NetBackup Appliance Web Console	You can use the **Monitor > SCSP Audit View** screen from the NetBackup Appliance Web Console to retrieve the audit logs of an appliance. See "Reviewing SCSP events" on page 47.	NetBackup appliance's audit logs
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > Browse` commands to open the `LOGROOT/>` prompt. You can use commands like `ls` and `cd` to work with the appliance log directories and obtain the various logs. See "Viewing log files using the Support command" on page 61.	■ NetBackup appliance configuration log ■ NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory ■ NetBackup appliance operating system (OS) installation log ■ NetBackup administrative web user interface log and the NetBackup web server log ■ NetBackup 52xx appliance device logs

Table 5-1 Viewing log files *(continued)*

From...	Using...	Logs collected..
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > VxLogView Module` *`ModuleName`* commands to access the NetBackup Appliance VxUL (unified) logs. You can also use the `Main > Support > Share Open` commands and use the desktop to map, share, and copy the VxUL logs.	NetBackup Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace`
NetBackup Appliance Shell Menu	You can use the `Main > Support > DataCollect` commands to collect storage device logs. See "Gathering device logs with the DataCollect command" on page 63.	NetBackup 5xxx storage device logs
NetBackup-Java applications	If you encounter problems with the NetBackup-Java applications, you can use the scripts in this section to gather the required information for contacting support.	Logs relating to the NetBackup-Java applications

About using the Collect Log files wizard

You can use the **Collect Log files** wizard from the NetBackup Appliance Web Console to collect log files from an Appliance. The wizard lets you collect different

types of log files like NetBackup, Appliance, operating system, PureDisk, GUI, NBSU (NetBackup Support Utility), DataCollect and so on.

You can collect log files from a 52x0 Appliance.

After you have generated the log files you can email them to recipients, download them to your computer, or upload them to Symantec Support. For information about the Appliance Diagnostics Center,

See "About working with log files" on page 58.

Viewing log files using the Support command

You can use the following section to view the log file information.

To view logs using the `Support > Logs > Browse` command:

1. Enter browse mode using the `Main_Menu` > `Support` > `Logs` followed by the `Browse` command in the NetBackup Appliance Shell Menu. The `LOGROOT/>` prompt appears.
2. To display the available log directories on your appliance, type `ls` at `LOGROOT/>` prompt.
3. To see the available log files in any of the log directories, use the `cd` command to change directories to the log directory of your choice. The prompt changes to show the directory that you are in. For example, if you changed directories to the `GUI` directory, the prompt appears as `LOGROOT/GUI/>`. From that prompt you can use the `ls` command to display the available log files in the `GUI` log directory.
4. To view the files, use the `less <FILE>` or `tail <FILE>` command. Files are marked with `<FILE>` and directories with `<DIR>`.

See "Locating NetBackup Appliance log files using the Browse command" on page 62.

To view NetBackup Appliance unified (VxUL) logs using the `Support > Logs` command:

1. You can view the NetBackup Appliance unified (VxUL) logs with the `Support > Logs > VXLogView` command. Enter the command into the shell menu and use one of the following options:
   - `Logs VXLogView JobID` *`job_id`*
     Use to display debug information for a specific job ID.
   - `Logs VXLogView Minutes` *`minutes_ago`*
     Use to display debug information for a specific timeframe.

- `Logs VXLogView Module module_name`

  Use to display debug information for a specific module. The available module names are: `All`, `CallHome`, `Checkpoint`, `Common`, `Config`, `Database`, `Hardware`, `HWMonitor`, `Network`, `RAID`, `Seeding`, `SelfTest`, `Storage`, `SWUpdate`, `Commands`, `CrossHost`, and `Trace`.

2 If you want, you can copy the unified logs with the `Main > Support > Share Open` command. Use the desktop to map, share, and copy the logs.

Note: The NetBackup Appliance unified logs are not the same as the NetBackup unified logs, such as `nbpem` or `nbjm`. NetBackup Appliance has its own set of unified logs. To collect the NetBackup unified logs, use the Collect Logs Wizard and select **NetBackup**.

You can also use the `Main_Menu > Support > Logs` commands to do the following:

- Upload the log files to Symantec Technical Support.
- Set log levels.
- Export or remove CIFS and NFS shares.

Note: The NetBackup Appliance VxUL logs are no longer archived by a cron job, or a scheduled task. In addition, log recycling has been enabled, and the default number of log files has been set to 50.

Refer to the *NetBackup Appliance Command Reference Guide* for more information on the above commands.

See "About working with log files" on page 58.

Locating NetBackup Appliance log files using the Browse command

Table 5-2 provides the location of the logs and the log directories that are accessible with the `Support > Logs > Browse` command.

Table 5-2 NetBackup Appliance log file locations

NetBackup appliance logs	Log file location
NetBackup appliance configuration log	`<DIR> APPLIANCE config_nb_factory.log`

Table 5-2 NetBackup Appliance log file locations *(continued)*

NetBackup appliance logs	Log file location
NetBackup appliance selftest report	`<DIR> APPLIANCE` `selftest_report`
NetBackup appliance host change log	`<DIR> APPLIANCE` `hostchange.log`
NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory	`<DIR> NBU` ■ `<DIR> netbackup` ■ `<DIR> openv` ■ `<DIR> volmgr`

NetBackup appliance operating system (OS) installation log	`<DIR> OS`
	`boot.log`
	`boot.msg`
	`boot.omsg`
	`messages`

NetBackup deduplication (PDDE) configuration script log	`<DIR> PD` `pdde-config.log`
NetBackup Administrative web user interface log and the NetBackup web server log	`<DIR> WEBGUI` ■ `<DIR> gui` ■ `<DIR> webserver`
NetBackup appliance device logs	`/tmp/DataCollect.zip` You can copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.

See "About working with log files" on page 58.

Gathering device logs with the DataCollect command

You can use the `DataCollect` command from the `Main > Support` shell menu to gather device logs. You can share these device logs with the Symantec Support team to resolve device-related issues.

Along with the operating system, IPMI, and storage logs, the DataCollect command now collects the following logs as well:

- Patch logs
- Veritas File System logs
- Test hardware logs
- CPU information
- Disk performance logs
- Memory information
- Hardware information

To gather device logs with the DataCollect command

1. Log on to the administrative NetBackup Appliance Shell Menu.
2. Open the Support menu. To open the support menu, use the following command:

   ```
   Main > Support
   ```

   The appliance displays all the sub-tasks in the support menu.

3 Enter the `DataCollect` command to gather storage device logs.

The appliance initiates the following procedure:

```
appliance123.Support > DataCollect
Gathering release information
Gathering dmidecode logs
Gathering ipmitool sel list logs
Gathering fwtermlog logs
Gathering AdpEventLog logs
Gathering smartctl logs
Gathering disk performance logs
Gathering ipmiutil command output
Gathering cpu information
Gathering memory information
Gathering sdr logs
Gathering adpallinfo logs
Gathering encinfo logs
Gathering cfgdsply logs
Gathering ldpdinfo logs
Gathering pdlist logs
Gathering fru logs
Gathering adpbbucmd logs
Gathering os logs
Gathering adpalilog logs
Gathering dfinfo logs
Gathering vxprint logs
Gathering Test Hardware logs
Gathering patch logs


All logs have been collected in /tmp/DataCollect.zip
Log file can be collected from the appliance shared folder
 - \\appliance123\logs\APPLIANCE
Share can be opened using Main->Support->Logs->Share Open

=======================End of DataCollect=================
All logs have been collected in /tmp/DataCollect.zip
```

The appliance generates the device log in the `/tmp/DataCollect.zip` file.

4 Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.

5 You can send the `DataCollect.zip` file to the Symantec Support team to resolve your issues.

See "About working with log files" on page 58.

Chapter 6

NetBackup Appliance Operating System Security

This chapter includes the following topics:

About Operating System Security

The NetBackup Appliance software is installed and runs the Linux operating system provided by Symantec, also known as Appliance OS. The OS included in the NetBackup Appliance version 2.6 comes with the following security enhancements:

- Updated and trimmed operating system platform, which enables packaging and installing the customized SLES 11 SP1, Storage Foundation, NetBackup packages, and third-party tools on a compatible and a robust hardware platform.
  See "Listing Products and Operating System Components within the NetBackup Appliance Installation" on page 68.
  See "Listing Operating system packages removed from the NetBackup Appliance" on page 99.
- SCSP-based intrusion prevention feature that hardens the Appliance operating system, Backed up Media and Data by isolating and sandboxing each process and all the system files thus ensuring system integrity
- Regular scan of the NetBackup Appliance with industry-recognized vulnerability scanners. Typically every three months there is a Maintenance release which includes the latest security updates related to OS or 3rd party components such

as tomcat/openssl/java and so on. If Security threats are identified between release schedules, please reach out to Symantec for a known resolution.

- Reduced the burden of operating system maintenance and further harden the NetBackup Appliance OS against potential security exploitation by removing OS packages that are not used by the platform.
- Removed or disabled non users and unused service accounts.
  See "Disabled Service Accounts" on page 69.
- The NetBackup Appliance has edited the tunable kernel parameters to secure the appliance operating system against attacks such DoS attacks. The `sysctl` setting `net.ipv4.tcp_syncookies` has been added to `/etc/sysctl.conf` configuration file to implements TCP Syncookies.
- Disabled unnecessary runlevel services. The appliance operating systems uses runlevels to determine the services that should be running and to allow specific work to be done on the system.
- Disabled `FTP`, `telnet`, `rlogin (rsh).`
- Usage limited to `ssh`, `scp`, `sftp` are used.
- Disabled TCP Forwarding for SSH by adding `AllowTcpForwarding no` and `X11Forwarding no` to`/etc/ssh/sshd_config`
- The UMASK value determines the file permission for newly created files. It specifies the permissions which should not be given by default to the newly created file. Although the default value of UMASK in most UNIX systems is 022. The UMASK is set to 077 for the NetBackup Appliance.
- Searched and fixed the permissions of all the world writeable files found in the NetBackup Appliance.
- Searched and fixed the permissions of all the orphaned and unowned files and directories found in the NetBackup Appliance.

Listing Products and Operating System Components within the NetBackup Appliance Installation

The Table 6-1 lists the components of the base appliance operating system and the Symantec products installed along with the NetBackup Appliance:

Table 6-1 Symantec products and OS components installed with NetBackup Appliance

Products / OS components	Version
Symantec Storage Foundation with special patches and performance tunings	6
Symantec Critical System Protection	SCSP Agent 5.2.9 MP3
NetBackup	7.6.x.x
NetBackup Appliance Web Console	2.6.x.x
NetBackup Appliance Shell Menu	2.6.x.x
Hardware monitoring software	2.2
Linux operating system Provided by Symantec	SUSE Linux Enterprise Server with security fixes found with service pack one 11SP1
WAN Optimization Kernel	2.6.16.60-0.101.1

See "About Operating System Security" on page 67.

Disabled Service Accounts

The following list of service accounts have been disabled for the NetBackup Appliance operating system:

- Batch jobs daemon
- bin
- daemon
- DHCP server daemon
- FTP account
- User for haldaemon
- User for OpenLDAP
- Mailer daemon
- Manual pages viewer
- User for D-BUS
- Name server daemon

- News system
- nobody
- NTP daemon
- PolicyKit
- Postfix Daemon
- SSH daemon
- Novell Customer Center User
- UNIX-to-UNIX CoPy system
- wwwrun WWW daemon Apache
- NBE Web service ntbecmlpi

See “About Operating System Security” on page 67.

Chapter 7

NetBackup Appliance Data Security

This chapter includes the following topics:

About Data Security

NetBackup Appliances support policy driven mechanism to protect data on clients as well as NetBackup servers. The following measures are implemented to improve data security by avoiding data leaks and improving protection:

- Real-time intrusion detection mechanisms are in place to audit access to confidential data stored on NetBackup Appliance.
- Logging and real-time tracking of all restores.
- Access to the backed up data is authorized to only appliance users and processes.
- NetBackup Appliance ensures that all backup data in the Deduplication Pool (MSDP) are marked with Cyclic Redundancy Check (CRC) digital signatures when the backup takes place. A maintenance task continuously re-computes the CRC digital signatures and compares it with the original signature to detect if there has been any unwanted tampering or corruption in the Deduplication Pool.

- Unintended access to appliance storage is prevented by password protecting logins to the appliance.
- Access to shared data limited to authorized users only and NetBackup processes. See "Disabled Service Accounts" on page 69.
- Usage of HTTPS protocol and port 443 to connect to the Symantec AutoSupport server to upload hardware and software information using the Call Home feature. Symantec support uses this information to resolve any issues that you might report. This information is retained for 90 days and purged at the Symantec Secure Operations Center.
- Support "Checkpoints" that lets you easily roll back the entire system to a point in time to undo any misconfiguration. The checkpoint captures the following components:
  - Appliance operating system
  - Appliance software
  - NetBackup software
  - Tape media configuration on the master server
  - Networking configuration
  - LDAP configuration if it exists
  - Fiber channel configuration
  - Any previously applied patches

  Note: Critical components like NetBackup Catalog, KMS database, or NBAC database may need additional configuration.

NetBackup Appliance software has no in-built transmission/session security unless it is HTTP (Web service) protocol. Symantec recommends deploying VPN (Virtual Private Networks) solutions like IPSec, between NetBackup hosts if appliance software is running in an untrusted network environment.

About Data Integrity

The Deduplication Pool storage in NetBackup Appliance provides the following data integrity checks to ensure that successful data restores:

Continuous end-to-end verification of backup data, stored in the Deduplication Pool

Any inadvertent data modifications that can cause data corruption are automatically detected and rectified if possible. Any unrecoverable data corruption issues are reported to the storage administrator by the NetBackup Console's Disk Reports UI (**NetBackup Administration Console > Reports > Disk Reports**).

Continuous Cyclic Redundancy Check (CRC) verification of backup data, stored in the Deduplication Pool

A CRC value is computed for each object created for the backup job in the Deduplication pool. A background process continuously verifies the CRC signatures to ensure that backup data is not tampered with and can be restored successfully when needed. The deduplication pool design naturally isolates any data corruption from uncorrupted portions of the pool, preventing corruption from spreading throughout the deduplication pool.

About Data Classification

A data classification represents a set of backup requirements, which makes it easier to configure backups for data with different requirements. For example, a backup with a gold classification must go to a storage lifecycle policy with a gold data classification. The NetBackup Appliance supports the same data classification attributes as NetBackup.

The NetBackup Data Classification attribute specifies the classification of the storage lifecycle policy that stores the backup. For example, a backup with a gold classification must go to a storage unit with a gold data classification.

NetBackup provides the following default data classifications:

- Platinum
- Gold
- Silver
- Bronze

This attribute is optional and applies only when the backup is to be written to a storage lifecycle policy. If the list displays **No data classification**, the policy uses the storage selection that is displayed in the **Policy storage** list. If a data classification is selected, all the images that the policy creates are tagged with the classification ID.

About Data Encryption

The NetBackup Appliance offers the following encryption methodologies to protect both data at rest and in flight:

- Transmit data in encrypted formats and using secure tunnels. These configurations can be made by client-side encryption and also replication. If these options are not used, once the data is out of NetBackup Appliances we rely on Network infrastructure for securing data in flight.
- Provides blowfish128-bit encryption in MSDP and allows encryption of each block with a unique key, further enhancing security.
- Supports encryption using NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. See "KMS support " on page 74.
- Supports NetBackup Access Control (NBAC) functionality that incorporates the NetBackup Product Authentication and Authorization into NetBackup Appliance master servers.

KMS support

The NetBackup Appliance supports encryption managed by NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. With version 2.6 and later, KMS is supported on a NetBackup Appliance configured as a Master or a Media Server. Regenerating the data encryption key is the only supported method of recovering KMS on an Appliance Master Server.

It has the following key features:

- It does not require an additional license.
- It is a master server-based symmetric key management service.
- It can be administered as a Master Server with tape devices connected to it or to another NetBackup Appliance.
- It manages symmetric cryptography keys for tape drives, that conform to the T10 standard (such as LTO4 or LTO5).
- It is designed to use volume pool-based tape encryption.
- It can be used with tape hardware, that has built-in hardware encryption capability.
- It can be managed by a NetBackup CLI administrator using the NetBackup Appliance Shell Menu or the KMS Command Line Interface (CLI).

Note: In the versions earlier than 2.6 of the NetBackup Appliance, KMS is only supported when the appliance is configured as a Media Server. A non-Appliance Master Server is required to administrate KMS with devices connected to a NetBackup Appliance.

About the keys used under KMS

The KMS generates keys from passcodes or auto-generates keys. The Table 7-1 lists the files associated with KMS that hold the information about the keys.

Table 7-1 KMS files

KMS files	Description	Location
Key file or key database	This is the most important file for KMS. It contains the data encryption keys.	/usr/openv/kms/db/KMS_DATA.dat
Host Master Key	It contains the encryption key that encrypts and protects the KMS_DATA.dat key file using AES 256.	/usr/openv/kms/key/KMS_HMKF.dat
Key Protection Key	It is the encryption key that encrypts and protects individual records in the KMS_DATA.dat key file using AES 256. Currently the same key protection key is used to encrypt all of the records.	/usr/openv/kms/key/KMS_KPKF.dat

Chapter 8

NetBackup Appliance Web Security

This chapter includes the following topics:

About NetBackup Appliance Web Console Security Updates

The NetBackup Appliance Web Console is updated in v2.6.x.x to include the following support:

Tomcat version 6.0.37

The NetBackup Appliance software release v2.6 includes the updated Tomcat version 6.0.37 to improve performance and increase security. The Tomcat server is configured to prevent the cookies to be accessed through client-side scripts. With the updated version of Tomcat, the browser does not reveal the cookies to a third party even if a user tries to use cross-site scripting (XSS) flaws.

Apache Struts 2.3.15.1

The Apache Struts version is updated to 2.3.15.1. This update contains the latest security vulnerability fixes, like the web server disclosing details about the server application modules.

Java version JRE 1.7

The Java version is updated to JRE 1.7 update 45. This Critical Patch Update contains 40 new security fixes for Oracle Java SE, from which, four are applicable to server deployments of Java.

See "About SSL certification" on page 77.

About SSL certification

The Secure Socket Layer protocol creates an encrypted connection between your appliances web server and your LDAP server or your local servers allowing for information to be transmitted without the problems of eavesdropping, data tampering, or message forgery. To enable SSL on your NetBackup Appliance Web Console, you need an SSL certificate that identifies you and installs it on the appliance's web server.

Symantec Product Authentication Service issues self-signed SSL certificates. The NetBackup Appliance uses a self-signed certificate hierarchy. The key algorithm used to generate the SSL certificate key is SHA1with RSA. All the Low strength ciphers, such as, SSLv2 and Diffie-Hellman are disabled.

You can also set the SSL certificates for an LDAP PAM Authentication module that enables you to establish a secure connection, between the NetBackup Appliance LDAP PAM module and the LDAP server.

Third-party certificates

You can manually add and implement third-party certificates for the Web service support. The appliance uses the Java keystore as the repository of security certificates. A Java keystore (JKS) is a repository of security certificates, like authorization certificates or public key certificates that are used for instance in SSL encryption.

Note: The procedure to implement third-party certificates varies with the type of PKCS (Public-key Cryptography Standards) used. For more information on implementing third-party certificates using PKCS# 7 and PKCS# 12 standard formats, refer to section 'Implementing third-party SSL certificates' section from the*Symantec NetBackup™ Appliance Administrator's Guide*.

See "About NetBackup Appliance Web Console Security Updates " on page 76.

Implementing third-party SSL certificates

You can manually add and implement third-party certificates for the web service support. The appliance uses the Java KeyStore as the repository of security certificates. A Java KeyStore (JKS) is a repository of security certificates, like authorization certificates or public key certificates that are used for instance in SSL encryption. If you want to implement third-party certificates, use the following procedure:

To implement third-party SSL certificates:

1 Prepare keystore file for web services. The procedure varies with the type of PKCS (Public-key Cryptography Standards) you use, the following table describes the steps to use PKCS# 7 and PKCS# 12 standard formats

PKCS format	Preparing keystore files
PKCS#7 or X.509 format	You can use the following link: https://knowledge.verisign.com/support/ssl-certificates-support/index.html

PKCS#12 format	1 Convert PEM formatted x509 Cert and Key to a PKCS# 12, using the following commands:
	`openssl pkcs12 export -in server.crt -inkey server.key -out server.p12 -name some-alias -CAfile ca.crt -caname root`
	For more information on `openssl` usage, refer to http://www.openssl.org/.
	Note: Ensure that you put a password on the PKCS #12 file. When the password is not applied to the file, you may get a null reference exception when you try to import the file
	2 Convert the pkcs12 file to a Java Keystore using the following commands:
	`keytool -importkeystore -deststorepass changeit -destkeypass changeit -destkeystore server.keystore -srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass some-password -alias some-alias`
	For more information on `keytool` usage, refer to http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

2 Shutdown webservice using the following command:

```
/etc/init.d/nbappws stop
```

3. Replace the existing keystore file with your new keystore file. The default file name is `/opt/SYMCnbappws/Security/keystore`.
4. Correct the following information in the configuration files:
   - Change the `keystoreFile` and `keystorePass` settings in the `/opt/SYMCnbappws/config/server.xml`.
   - Change the `keystoreFile` and `keystorePass` settings in the `/opt/SYMCnbappws/webserver/conf/server.xml`.
   - Change the `javax.net.ssl.trustStore` and `javax.net.ssl.trustStorePassword` settings in the `/opt/SYMCnbappws/bin/startgui.sh`.
5. Startup webservice using the following command:

   ```
   /etc/init.d/nbappws start
   ```

Chapter 9

NetBackup Appliance Network Security

This chapter includes the following topics:

About IPsec Channel Configuration

The NetBackup Appliance uses IPsec channels to secure communication between two appliances, thus helping to secure data in transit. All other communication between NetBackup Appliance and non-appliance, like the NetBackup master servers, would be non-IPsec.

IPsec security works at IP level and allows securing IP traffic between two hosts. Device certificates are provisioned to the Master and Media appliances, these certificates are then enabled for configuring IPsec channels. This enables a secure interaction of the master and media servers. The device certificates used are x509 certificates issued by Versign CA.

The appliance performs the following validation checks before establishing IPsec channel:

- Validate the authenticity of the certificates using the x509 cert validate.
- Validate whether the device certificate corresponds to the IP.
- Validate and update security associations in both directions of the communication.

The hosts are detected after the device certificates are recognized. Only after this is IPsec channel is configured and enabled.

Managing IPsec configuration

You can use the following commands from the NetBackup Appliance Shell Menu to manage IPsec channel:

Table 9-1 IPsec commands

Command	Description
`Network > Security > Configure`	You can use this command to configure IPsec between any two hosts. You can define the hosts by the host name. You can also identify them by the user ID and password.
`Network > Security > Delete`	You can use this command to remove IPsec policies for a list of remote hosts on a local system. You can use this command to remove IPsec policies for a list of remote hosts on a local system. Remove IPsec policies for a list of remote hosts on a local system. Use the Hosts variable to define one or more host names. Use a comma to separate multiple host names.
`Network > Security > Export`	Use this command to export the IPsec credentials. The *`EnterPasswd`* field is used to answer the question, `"Do you want to enter a password?"`. You must enter a value of yes or no in this field. In addition, you must specify a path that defines where you want to place the exported credentials. **Note:** The IPsec credentials are removed during a reimage process. The credentials are unique for each appliance and are included as part of the original factory image. The IPsec credentials are not included on the USB drive that is used to reimage the appliance.
`Network > Security > Import`	Use this command to import the IPsec credentials. The `EnterPasswd` field is used to answer the question, `"Do you want to enter a password?"`. You must enter a value of yes or no in this field. In addition, you must specify a path that defines where you want to place the imported credentials.
`Network > Security > Provision`	Use this command to provision IPsec policies for a list of remote hosts on a local system. Use the *`Hosts`* variable to define one or more host names. Use a comma to separate multiple host names.

Table 9-1 IPsec commands *(continued)*

Command	Description
`Network > Security (IPsec) > Refresh`	Use this command to reload the IPsec configuration. The `[Auto]` option defines whether the configurations on all referenced hosts are refreshed or not. You can enter `[Auto]` or `[NoAuto]`. The default value is `[NoAuto]`.
`Network > Security > Show`	Display the IPsec policies for a local host or a provided host. The `[[Verbose]]` option is used to define whether the output is verbose or not. The values that you can enter in this field are `[VERBOSE]` or `[NoVERBOSE]`. The default value is `[NoVERBOSE]`. The `[[HostInfo] ]` option can contain the following information that is separated by a comma. The host name, the user ID (optional), and the password (optional).
`Network > Security > Unconfigure`	Use this command to unconfigure IPsec between any two hosts. The *`Host1Info`* variable can contain the following information that is separated by a comma. The host name, the user ID (optional), and the password (optional). The *`[Host2info]`* variable can contain the host name, the user ID (optional), and the password (optional).

You can use the `Main > Network > Security` command from the NetBackup Appliance Shell Menu to configure the IPSec channel between two hosts. For more information of configuring IPsec channels, refer to the *Symantec NetBackup™ Appliance Command Reference Guide*.

About the NetBackup Appliance 52xx ports

In addition to the ports used by NetBackup, the 52xx appliances also provide for both in-band and out-of-band management. The out-of-band management is through a separate network connection, the Remote Management Module (RMM), and the Intelligent Platform Management Interface (IPMI). Open these ports through the firewall as appropriate to allow access to the management services from a remote laptop or KVM (keyboard, video monitor, mouse).

Warning: The NetBackup Appliance Web Console is now available only over HTTPS on the default port 443; port 80 over HTTP has been disabled. Please use `https://<appliance-name>` to log in to the Web Console, where appliance-name is the fully qualified domain name (FQDN) of the Appliance and can also be an IP address.

Table 9-2 lists the ports open for inbound communication to the NetBackup Appliance.

Table 9-2 Inbound ports

Port	Service	Description
22	ssh	In-band management CLI
443	HTTPS	In-band management GUI
443	HTTPS	Out-of-band management (ISM+ or RM*)
5900	KVM	CLI access, ISO & CDROM redirection
623	KVM	(optional, used if open)
7578	RMM	CLI access
5120	RMM	ISO & CD-ROM redirection
5123	RMM	Floppy redirection
7582	RMM	KVM
5124	HTTPS	CD ROM
5127		USB or Floppy
2049	HTTPS	NFS++
445		CIFS (for the Log/Install shares)

+ NetBackup Integrated storage manager

* Symantec Remote Management – Remote Console

++ Once the NFS service is shut down, the vulnerability scanners do not pick up these ports as threats.

Note: Ports 7578, 5120, and 5123 are for the unencrypted mode. Ports 7528, 5124, and 5127 are for the encrypted mode.

Table 9-3 list the ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 9-3 Outbound ports

Port	Service	Description
443	HTTPS	Call Home notifications to Symantec
162**	SNMP	Outbound traps and alerts
443	HTTPS	Download SCSP certificate

** This port number can be changed within the appliance configuration to match the remote server.

The complete list of all the applicable ports is available in the *Symantec NetBackup Network Ports Reference Guide*.

Chapter 10

NetBackup Appliance Call Home Security

This chapter includes the following topics:

About AutoSupport

The AutoSupport feature lets you register the appliance and your contact details at the Symantec support website . Symantec support uses this information to resolve any issue that you report. The information allows Symantec support to minimize downtime and provide a more proactive approach to support.

Provide the registration details for your appliance using one of the following provisions:

- The appliance initial configuration on the **Registration** page
- The NetBackup Appliance Web Console by navigating to **Settings > Notification > Registration** page
- The NetBackup Appliance Shell Menu by running the `Settings > Alerts > CallHome Registration` command. For more information about this command, refer to the *NetBackup Appliance Command Reference Guide*.

You can register by entering the following basic information:

- Name: Your name, company name
- Address, where the appliance is physically located: City, street, state, ZIP Code

- Contact information: Phone number, email address

The support infrastructure is designed to allow Symantec support to help you in the following ways:

- Proactive monitoring lets Symantec support to automatically create cases, fix issues, and dispatch any appliance parts that might be at risk.
- The AutoSupport infrastructure within Symantec analyzes the Call Home data from appliance. This analysis provides proactive customer support for hardware failures, reducing the need for backup administrators to initiate support cases.
- With AutoSupport ability, Symantec support can begin to understand how customers configure and use their appliances, and where improvements would be most beneficial.
- Send and receive status and alert notifications for the appliance.
- Receive hardware and software status using Call Home.
- Provide more insight into the issues and identify any issues that might further occur as a result of the existing issue.
- View reports from the Call Home data to analyze patterns of hardware failure, and see usage trends. The appliance sends health data every 30 minutes.

The information that you provide for appliance registration helps Symantec support to initiate resolution of any issue that you report. However, if you want to provide additional details such as a secondary contact, phone, rack location, and so on, you can visit https://my.symantec.com.

About Call Home

Your appliance can connect with a Symantec AutoSupport server and upload hardware and software information. Symantec support uses this information to resolve any issues that you might report. The appliance uses the HTTPS protocol and uses port 443 to connect to the Symantec AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

AutoSupport in appliance uses the data that is gathered by Call Home to provide proactive monitoring for the appliance. If Call Home is enabled, the appliance uploads hardware and software information (or the Call Home data) to Symantec AutoSupport server periodically at an interval of 15 minutes

If you determine that you have a problem with a piece of hardware, you might want to contact Symantec support. The Technical Support engineer uses the serial number of your appliance and assesses the hardware status from the Call Home data. To know the serial number of your appliance from theNetBackup Appliance Web Console, go to the **Monitor > Hardware > Health details** page. To determine

the serial number of your appliance using the shell menu, go to the `Monitor > Hardware` commands. For more information about the `Monitor > Hardware` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Use the **Settings > Notification** page to configure Call Home from the NetBackup Appliance Web Console. Click **Alert Configuration** and enter the details in the **Call Home Configuration** pane.

Table 10-1 describes how a hardware failure is reported when the feature is enabled or disabled.

Table 10-1 What happens when Call Home is enabled or disabled

Monitoring enabled or disabled	Hardware failure routine
Call Home enabled	When a hardware failure occurs, the following sequence of alerts occur: ■ The appliance uploads the following hardware and software information to a Symantec AutoSupport server: ■ CPU ■ Disk ■ Fan ■ Power supply ■ RAID group ■ Temperatures ■ Adapter ■ PCI ■ Fibre Channel HBA ■ Network card ■ Partition information ■ MSDP statistics ■ 52xx Storage Shelf - Status of disk, fan, power supply, and temperature ■ The appliance generates a local alert by email to notify you of the hardware failure. The appliance also generates an SNMP trap.
Call Home disabled	No data is sent to the Symantec AutoSupport server. Your system does not report hardware errors to Symantec to enable faster problem resolution.

See "Configuring Call Home from the NetBackup Appliance Shell Menu" on page 88.

See "About AutoSupport " on page 85.

Configuring Call Home from the NetBackup Appliance Shell Menu

You can configure the Call Home details from the **Settings > Notification** page.

You can configure the following Call Home settings from the NetBackup Appliance Shell Menu:

- Enabling and disabling Call Home from the NetBackup Appliance Shell Menu
- Configuring a Call Home proxy server from the NetBackup Appliance Shell Menu
- Testing whether or not Call Home works correctly by running the `Settings > Alerts > CallHome > Test` command.

If you enable Call Home, you can use the `Settings > Alerts > CallHome Registration` command to configure the contact details for your appliance by entering the following information:

- The name of the person who is the first point of contact and responsible for the appliance.
- The address of the contact person.
- The phone number of the contact person.
- The email address of the contact person.

To learn more about the `Main > Settings > Alerts > CallHome` commands, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

For a list of the hardware problems that cause an alert, see the following topics:

See "About Call Home" on page 86.

Enabling and disabling Call Home from the NetBackup Appliance Shell Menu

You can enable or disable Call Home from both, the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. Call Home is enabled by default.

To enable or disable Call Home from the NetBackup Appliance Shell Menu

1. Log on to the NetBackup Appliance Shell Menu.
2. To enable Call Home, run the `Main > Settings > Alerts > CallHome Enable` command.
3. To disable Call Home, run the `Main > Settings > Alerts > CallHome Disable` command.

For more information on `Main > Settings > Alerts > CallHome` commands, refer to the *Symantec NetBackup Appliance Command Reference Guide*.

Configuring a Call Home proxy server from the NetBackup Appliance Shell Menu

You can configure a proxy server for Call Home, if required. If the appliance environment has a proxy server between the environment and external Internet access, you must enable the proxy settings on the appliance. The proxy settings include both a proxy server and a port. The proxy server must accept https connections from the Symantec AutoSupport server. This option is disabled by default.

To add a Call Home proxy server from the NetBackup Appliance Shell Menu

1. Log on to NetBackup Appliance Shell Menu.
2. To enable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Enable` command.
3. To add a proxy server, run the `Main > Settings > Alerts > CallHome Proxy Add` command.
   - You are prompted to enter the name of the proxy server. The proxy server name is the TCP/IP address or the fully qualified domain name of the proxy server.
   - After you have entered a name for the proxy server, you are prompted to enter the port number for the proxy server.
   - Further, you are required to answer the following:

     ```
     Do you want to set credentials for proxy server? (yes/no)
     ```

   - On answering *yes*, you are prompted to enter a user name for the proxy server.
   - After you have entered the user name, you are prompted to enter a password for the user. On entering the required information, the following message is displayed:

     ```
     Successfully set proxy server
     ```

4. To disable proxy settings, run the `Main > Settings > Alerts > CallHome Proxy Disable` command.

Further, you can also use the NetBackup Appliance Shell Menu to enable or disable proxy server tunneling for your appliance. To do so, run the `Main > Settings > CallHome Proxy EnableTunnel` and `Main > Settings > Alerts > CallHome Proxy DisableTunnel` commands. Proxy server tunneling lets you provide a secure path through an untrusted network.

Understanding the Call Home workflow

This section explains the mechanism that Call Home uses to upload data from your appliance to the Symantec AutoSupport server.

Call Home uses HTTPS (secure and encrypted protocol) with port number 443 for all communication with Symantec AutoSupport servers. For Call Home to work correctly, ensure that your appliance has Internet access either directly, or through a proxy server to reach the Symantec AutoSupport servers. AutoSupport, a mechanism that monitors the appliance proactively, uses the Call Home data to analyze and resolve any issues that the appliance may encounter.

The transmission of the Call Home data is done using the NetBackup Product Improvement Program Agent. The agent communicates using Secure Socket Layer (SSL) over port 443. All communications are initiated by the appliance. Your appliance needs access to both, https://telemetrics.symantec.com and https://www.symappmon.com.

The appliance Call Home feature uses the following workflow to communicate with AutoSupport servers:

- Access a port to https://www.symappmon.com every 15 minutes.
- Perform a self-test operation to https://www.symappmon.com.
- If the appliance encounters an error state, all hardware logs from past three days are gathered along with the current log.
- The logs are then uploaded to the Symantec AutoSupport server for further analysis and support. These error logs are also stored on the appliance. You can access these logs from `/log/upload/<date>` folder.
- If the error state persists three days later, the logs will be re-uploaded.

See “About Call Home” on page 86.

See “About AutoSupport ” on page 85.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager model and agent model. This model consists of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

About the Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.2682.1).

These OIDs form a tree. An MIB associates each OID with a readable label and various other parameters that are related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages. This information is saved as a MIB file.

You can check the details of the SNMP MIB file from the **Setting > Notifications > Alert Configuration** page. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** pane.

Chapter 11

NetBackup Appliance IPMI Security

This chapter includes the following topics:

Introduction to IPMI configuration

You can configure the IPMI sub-system for your appliances. The Intelligent Platform Management Interface (IPMI) sub-system is beneficial when an unexpected power outage shuts down the connected system. This sub-system operates independently of the operating system and can be connected by using the remote management port, located on the rear panel of the appliance.

You can configure the IPMI sub-system and the Symantec Remote Management tool using the BIOS setup. The Symantec Remote Management tool provides an interface to use the remote management port. It lets you monitor and manage your appliance from a remote location.

Recommended IPMI settings

This section lists the recommended IPMI settings to ensure a secure IPMI configuration.

Users

The following recommendations must be kept in mind while creating IPMI users:

- Don’t allow accounts with null user name or password.
- Recommended to have one administrative user.
- Recommended to disable anonymous user.
- Recommended to delete vendor accounts and create your own user name and passwords.
- Recommended to set 16-20 characters of password on each user to avoid brute force attacks

Login

The following recommendations must be kept in mind while creating applying login settings for the IPMI users:

Table 11-1 Login security settings

Settings	Recommended values
Failed login attempts	3
User Lockout time (min)	60 seconds
Force HTTPS	Yes The 'Force HTTPS' check-box must be enabled to ensure that the IPMI connection always takes place over HTTPS.
Web Session Timeout	1800

LDAP Settings

Symantec recommends that you should enable LDAP authentication, if possible in your environment.

SSL Upload

Symantec recommends that you import a new/custom ssl certificate.

Remote Session

Table 11-2 Remote session security settings

Settings	Recommended values
KVM Encryption	AES
Media Encryption	Enable

Cipher recommendation

- Do NOT set cipher to zero on the IPMI channel

  Warning: If the cipher 0 enabled on a channel, it allows anyone to perform any IPMI action with no authentication, effectively subverting IPMI security entirely. Disable it at all costs.

- Only use ciphers 3, 8, and 12.

Ethernet connection settings

Recommended to have a dedicated Ethernet connection for IPMI, that is you should avoid sharing the server's physical connection.

- Use a static IP
- Avoid DHCP

Disable Services that aren't used

In future version of IPMI, you will have the ability to disable SSH and HTTP services from the Symantec Remote Management Console or the command line interface.

For more information, refer to http://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html.

Replacing the default IPMI SSL certificate

Symantec recommends that the default IPMI SSL certificate used to access the IPMI web interface be replaced with either a certificate signed by a trusted internal or external Certificate Authority (in PEM format), or by a self-signed certificate. You can use the following procedure to create a minimal self-signed certificate on a Linux computer and import it into the IPMI web interface:

To create a minimal self-signed certificate on a Linux computer and import it into the IPMI web interface:

1 Run the following command to generate the private key called `ipmi.key`:

```
$ openssl genrsa -out ipmi.key 2048

Generating RSA private key, 2048 bit long modulus

.....+++

 .+++

 e is 65537 (0x10001)
```

2 Generate a certificate signing request called `ipmi.csr` using `ipmi.key`, filling in each field with their appropriate values:

Note: To avoid extra warnings in your browser, set the CN to the fully qualified domain name of the IPMI interface. You are about to enter is what is called a Distinguished Name or a DN.

```
$ openssl req -new -key ipmi.key -out ipmi.csr
```

Refer to the following guidelines to enter information to be incorporated into your certificate request:

Country Name (2 letter code) [AU]:	Enter your Country's name. For example, US.
State or Province Name (full name) [Some-State]:	Enter your State's or Province's name. For example, OR.
Locality Name (eg, city) []:	Enter your Locality name. For example, Springfield.
Organization Name (eg, company) [Internet Widgits Pty Ltd]:	Enter your Organization's name. For example, Symantec.
Organizational Unit Name (eg, section) []:	Enter your Organization Unit's name.
Common Name (eg, YOUR name) []:	Enter `hostname.your.company`.
Email Address []:	Enter your email address. For example, `email@your.company .`
A challenge password []:	Enter the appropriate challenge password, which is the extra attribute to be sent with your certificate request.
An optional company name []:	Enter the appropriate optional company name, which is the extra attribute to be sent with your certificate request.

Note: Enter '.', to leave any field blank.

3 Sign `ipmi.csr` with `ipmi.key` and create a certificate called `ipmi.crt` that is valid for 1 year:

```
$ openssl x509 -req -in ipmi.csr

-out ipmi.crt -signkey ipmi.key

-days 365

 Signature ok

 subject=/C=US/ST=OR/L=Springfield

/O=Symantec/OU=Your OU/

CN=hostname.your.company/

emailAddress=email@your.company


Getting Private key
```

4 Concatenate `ipmi.crt` and `ipmi.key` to create a certificate in PEM format called `ipmi.pem`.

```
$ cat ipmi.crt ipmi.key > ipmi.pem
```

5 Copy `ipmi.pem` to a host that has access to the appliance's IPMI web interface.

6 Login to your Symantec Remote Management (IPMI web interface).

7 Click **Configuration > SSL**.

The appliance displays the **SSL Upload** page.

8 From the **SSL Upload** page, click **Choose File** to import the certificate.

9 Select the `ipmi.pem` and click **Upload**.

10 A warning may appear that says an SSL certificate already exists, press **OK** to continue.

11 To import the key, click **Choose File** again (notice it says **New Privacy Key** next to the button).

12 Select the `ipmi.pem` and click **Upload**.

13 A confirmation appears stating that the certificate and key were uploaded successfully, press **OK** to restart the Web service.

14 Close and reopen the Symantec Remote Management (IPMI web interface) interface to verify that the new certificate is being presented.

Appendix A

Operating system packages removed from the NetBackup Appliances

This appendix includes the following topics:

Listing Operating system packages removed from the NetBackup Appliance

For Appliance 2.6.0.x an effort has been taken to reduce the burden of operating system maintenance and further harden the NetBackup Appliance against potential security exploitation. As a result of these efforts, the base operating system packages have been reviewed and several that are not used by the platform have been removed

Table A-1 List of known packages removed from the Appliance platform as of 2.6.x.x:

Apache Web services	compat-32bit	expat-32bit
LP Daemon (Print Server)	compat-libstdc++	gettext
SNMP Server Daemon	compat-openssl097g	gettext-32bit
aaa_skel	compat-openssl097g-32bit	glib2-32bit
ash	curl-32bit	gnome-filesystem
binutils-32bit	db	hfsutils

Table A-1 List of known packages removed from the Appliance platform as of 2.6.x.x: *(continued)*

blocxx	db-32bit	igb
boost	db42	ixgbe
bootsplash-theme-SuSE-SLES	dbus-1-mono	jfsutils
bzip2-32bit	e2fsprogs-32bit	jre
compat	evms	kernel-smp
ldapcpplib	open-iscsi	sitar
libapr-util1	openct-32bit	sles-admin_en
libapr1	openldap2-client-32bit	sles-heartbeat_en
libart_lgpl	openssl-32bitresmgr-32bit	sles-preparetion_en
libgssapi	perl-Compress-Zlib	sles-startup_en
libgssapi-32bit	perl-TermReadKey	sles-stor_evms_en
libpcap-32bit	portmap	smpppd
libusb-32bit	powersave	sqlite-32bit
liby2util	powersave-libs	util-linux-crypto
libzypp-zmd-backend	powersave-libs-32bit	wol
linux32	readline	wvdial
log4net	readline-32bit	wvstrams
mkisofs	resmgr	xntp
mktemp	resmgr-32bit	yast2-cd-creator
mono-core	rrdtool	yast2-heartbeat
mono-core-32bit	rug	yast2-iscsi-client
ncompress	samba-client-32bit	yast2-iscsi-server
ncursesportmap	sas_ir_snmp	yast2-mail-aliases
ncurses-32bit	sas_snmp	yast2-powertweak
net-snmp	scsi	yast2-theme-NLD
nfs-utils	sensors	zmd

Table A-1 List of known packages removed from the Appliance platform as of 2.6.x.x: *(continued)*

ntfsprogs	siga	zmd-inventory

Note: If you have installed any of the above packages on the 2.5.x or 2.0.x versions of the NetBackup Appliance functionality of these packages may fail or degrade after the appliance is upgraded to version 2.6. Symantec does not support the installation of packages outside of those installed as part of the initial configuration.

See "About Operating System Security" on page 67.

Index

R

S

T

U