Veritas NetBackup™ Appliance Security Guide

Release 3.2 (5250)

VERITAS™

Veritas NetBackup Appliance Security Guide

Last updated: 2020-05-19

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1 About the NetBackup appliance Security Guide 7

About the NetBackup appliance Security Guide 7

Chapter 2 User authentication 15

About user authentication on the NetBackup appliance 15
User types that can authenticate on the NetBackup appliance 18
About configuring user authentication 21
Generic user authentication guidelines 24
About authenticating LDAP users 24
About authenticating Active Directory users 26
About authentication using smart cards and digital certificates 27
About authenticating Kerberos-NIS users 29
About the appliance login banner 30
About user name and password specifications 31
About STIG-compliant password policy rules 35

Chapter 3 User authorization 37

About user authorization on the NetBackup appliance 37
About authorizing NetBackup appliance users 39
NetBackup appliance user role privileges 41
About the Administrator user role 42
About the NetBackupCLI user role 43

Chapter 4 Intrusion prevention and intrusion detection systems 46

About Symantec Data Center Security on the NetBackup appliance 47
About the NetBackup appliance intrusion prevention system 49
About the NetBackup appliance intrusion detection system 50
Reviewing SDCS events on the NetBackup appliance 51

Running SDCS in unmanaged mode on the NetBackup appliance 53
Running SDCS in managed mode on the NetBackup appliance 53

Chapter 5 Log files 55

About NetBackup appliance log files 55
Viewing log files using the Support command 57
Where to find NetBackup appliance log files using the Browse command 58
Gathering device logs on a NetBackup appliance 59
Log Forwarding feature overview 61

Chapter 6 Operating system security 64

About NetBackup appliance operating system security 64
Major components of the NetBackup appliance OS 66
Vulnerability scanning of the NetBackup appliance 66

Chapter 7 Data security 68

About data security 68
About data integrity 69
About data classification 70
About data encryption 70
KMS support 71

Chapter 8 Web security 75

About SSL usage 75
Implementing third-party SSL certificates 76

Chapter 9 Network security 86

About IPsec Channel Configuration 86
About NetBackup appliance ports 89
About the NetBackup Appliance firewall 90

Chapter 10 Call Home security 94

About AutoSupport 94
Data security standards 95
About Call Home 95
Configuring Call Home from the NetBackup Appliance Shell Menu 97

Enabling and disabling Call Home from the appliance shell menu 98
Configuring a Call Home proxy server from the NetBackup Appliance Shell Menu 98
Understanding the Call Home workflow 99
About SNMP 100
About the Management Information Base (MIB) 100

Chapter 11 Remote Management Module (RMM) security 102

Introduction to IPMI configuration 102
Recommended IPMI settings 102
RMM ports 104
Enabling SSH on the Remote Management Module 106
Replacing the default IPMI SSL certificate 106

Chapter 12 STIG and FIPS conformance 111

OS STIG hardening for NetBackup appliance 111
Unenforced STIG hardening rules 125
FIPS 140-2 conformance for NetBackup appliance 131

Appendix A Security release content 133

NetBackup Appliance security release content 133

Index 136

Chapter 1

About the NetBackup appliance Security Guide

This chapter includes the following topics:

- About the NetBackup appliance Security Guide

About the NetBackup appliance Security Guide

NetBackup appliances are developed from their inception with security as a primary need. Each element of the appliance, including its Linux operating system and the core NetBackup application, is tested for vulnerabilities using both industry standards and advanced security products. These measures ensure that exposure to unauthorized access and resulting data loss or theft is minimized.

Each new version of NetBackup appliance software and hardware is verified for vulnerabilities before release. Depending on the severity of issues found, Veritas releases a patch or provides a fix in a scheduled major release. To reduce the risk of unknown threats, Veritas regularly updates the third-party packages and modules in the product as part of regular maintenance release cycles.

The goal of this guide is to describe the security features implemented in NetBackup appliance 3.2 and includes the following chapters and sub-sections:

NetBackup appliance user authentication

This chapter talks about the authentication features of the NetBackup appliance and includes the following sections:

Table 1-1 Sections featuring authentication

Section name	Description	Link
About user authentication on the NetBackup appliance	This section describes the types of users, user accounts, and processes allowed to access the appliance.	See "About user authentication on the NetBackup appliance" on page 15.
About configuring user authentication	This section describes the configuration options for the various types of users that can authenticate on the appliance.	See "About configuring user authentication" on page 21.
About authenticating LDAP users	This section describes the prerequisites and process to configure the appliance to register and authenticate LDAP users.	See "About authenticating LDAP users" on page 24.
About authenticating Active Directory users	This section describes the prerequisites and process to configure the appliance to register and authenticate Active Directory (AD) users.	See "About authenticating Active Directory users" on page 26.
About authenticating Kerberos-NIS users	This section describes the prerequisites and process to configure the appliance to register and authenticate Kerberos-NIS users.	See "About authenticating Kerberos-NIS users" on page 29.
About the appliance login banner	This section describes the login banner feature where you can set a text banner to appear when a user tries to authenticate on the appliance.	See "About the appliance login banner" on page 30.
About user name and password specifications	This section describes the user name and password credentials.	See "About user name and password specifications" on page 31.

NetBackup Appliance user authorization

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

Table 1-2 Sections on authorization

Section name	Description	Link
About user authorization on the NetBackup appliance	This section describes the key characteristics of the authorization process of the NetBackup appliance.	See "About user authorization on the NetBackup appliance" on page 37.
About authorizing NetBackup appliance users	This section describes the administrative options for authorizing appliance users with various access permissions.	See "About authorizing NetBackup appliance users" on page 39.
About the Administrator user role	This section describes the Administrator user role.	See "About the Administrator user role" on page 42.
About the NetBackupCLI user role	This section describes the NetBackupCLI user role.	See "About the NetBackupCLI user role" on page 43.

NetBackup Appliance intrusion prevention and intrusion detection systems

This chapter describes the Symantec Data Center Security: Server Advanced (SDCS) implementation for the NetBackup appliance using the following sections:

Table 1-3 Sections on IPS and IDS policies

Section name	Description	Link
About Symantec Data Center Security on the NetBackup appliance	This section introduces the SDCS feature implemented with the appliances.	See "About Symantec Data Center Security on the NetBackup appliance" on page 47.
About the NetBackup appliance intrusion prevention system	This section describes the IPS policy that is used to protect the appliances.	See "About the NetBackup appliance intrusion prevention system" on page 49.
About the NetBackup appliance intrusion detection system	This section describes the IDS policy that is used to monitor the appliances.	See "About the NetBackup appliance intrusion detection system" on page 50.

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

Section name	Description	Link
Reviewing SDCS events on the NetBackup appliance	This section describes the SDCS events based on their level of security.	See "Reviewing SDCS events on the NetBackup appliance" on page 51.
Running SDCS in unmanaged mode on the NetBackup appliance	This section briefly describes the default security management on the appliance.	See "Running SDCS in unmanaged mode on the NetBackup appliance" on page 53.
Running SDCS in managed mode on the NetBackup appliance	This section describes how you can manage appliance security as part of a centralized SDCS environment.	See "Running SDCS in managed mode on the NetBackup appliance" on page 53.
Overriding the NetBackup appliance intrusion prevention system policy	This section describes the procedure to override the IPS policy that is applied to the appliances.	
Re-enabling the NetBackup appliance intrusion prevention system policy	This section describes the procedure to re-enable the IPS policy that is applied to the appliances.	

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 NetBackup appliance log files" on page 55.
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 57.

Table 1-4 Working log sections *(continued)*

Section name	Description	Link
Locating NetBackup Appliance log files using the Browse command	This chapter describes the usage of Browse command to view log files.	See "Where to find NetBackup appliance log files using the Browse command" on page 58.
Gathering device logs with the DataCollect command	This chapter describes the procedure to gather device logs.	See "Gathering device logs on a NetBackup appliance" on page 59.

NetBackup Appliance operating system security

Table 1-5 Operating system sections

Section name	Description	Link
About NetBackup appliance operating system security	This section describes the different update types that are made to the operating system to improve the security of the overall NetBackup appliance.	See "About NetBackup appliance operating system security" on page 64.
Major components of the NetBackup appliance OS	This section lists the products and operating system components of the NetBackup appliance.	See "Major components of the NetBackup appliance OS" on page 66.
Vulnerability scanning of the NetBackup appliance	This section lists some of the security scanners that Veritas uses to verify the security of the appliance.	See "Vulnerability scanning of the NetBackup appliance" on page 66.

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 that are taken to improve data security.	See "About data security" on page 68.

Table 1-6 Data security sections *(continued)*

Section name	Description	Link
About Data Integrity	This section lists the measures that are taken to improve data integrity.	See "About data integrity" on page 69.
About Data Classification	This section lists the measures that are taken to improve data classification.	See "About data classification" on page 70.
About Data Encryption	This section lists the measures that are taken to improve data encryption.	See "About data encryption " on page 70.

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 SSL certificates	This section lists the SSL certification updates for NetBackup Appliance Web Console.	
Installing third-party SSL certificates	This section lists the procedure to install third-party SSL certificates.	

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 86.
About NetBackup appliance ports	This section describes the port information for NetBackup Appliances.	See "About NetBackup appliance ports" on page 89.

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 94.
About Call Home	This section describes the Call Home feature in the NetBackup appliance.	See "About Call Home" on page 95.
About SNMP	This section describes the SNMP feature in the NetBackup appliance.	See "About SNMP" on page 100.

NetBackup Appliance IPMI security

This chapter describes the guidelines that are 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 102.
Listing the Recommended IPMI settings	This section lists the recommended IPMI settings for a secure configuration.	See "Recommended IPMI settings" on page 102.

Intended Audience

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

Note: The tasks and procedures in this document must be performed on a configured appliance. Local user commands cannot be used successfully before the appliance role is configured. Any attempted local user commands including, but not limited to granting user permissions, fail if the appliance role is not configured. If you attempt to run local user commands before role configuration, those same commands also fail after you complete the role configuration. Other commands can also exhibit unexpected or undesired behavior. To prevent this situation, it is a best practice to avoid attempting any local user commands until after the appliance role has been configured.

Chapter 2

User authentication

This chapter includes the following topics:

- About user authentication on the NetBackup appliance
- About configuring user authentication
- About authenticating LDAP users
- About authenticating Active Directory users
- About authentication using smart cards and digital certificates
- About authenticating Kerberos-NIS users
- About the appliance login banner
- About user name and password specifications

About user authentication on the NetBackup appliance

The NetBackup appliance is administered and managed through user accounts. You can create local user accounts, or register users and user groups that belong to a remote directory service. Each user account must authenticate itself with a user name and password to access the appliance. For a local user, the user name and password are managed on the appliance. For a registered remote user, the user name and password are managed by the remote directory service.

In order for a new user account to log on and access the appliance, you must first authorize it with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role.

Table 2-1 describes the user accounts that are available on the appliance.

Table 2-1 NetBackup appliance account types

Account name	Description
admin	The **admin** account is the default Administrator user on the NetBackup appliance. This account provides full appliance access and control for the default Administrator user. New appliances are shipped with the following default logon credentials: ■ User name: **admin** ■ Password: **P@ssw0rd** When mounting or mapping shares from an appliance, make note of the following: ■ Windows: Only the local **admin** account is authorized to mount or map Windows CIFS shares. ■ Linux: Only users with a root access account can issue the mount command directly to mount NFS shares.
AMSadmin	The **AMSadmin** account provides full access to the following appliance interfaces: ■ Appliance Management Console ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup Administration console For complete details about this account, see the *Veritas Appliance Management Guide*.
maintenance	The **maintenance** account is used by Veritas Support through the NetBackup Appliance Shell Menu (after an administrative log-on). This account is used specifically to perform maintenance activity or to troubleshoot the appliance. **Note:** This account is also used to make GRUB changes, and for single user mode boot when the STIG option is enabled.

Table 2-1 NetBackup appliance account types *(continued)*

Account name	Description
nbasecadmin	The **nbasecadmin** account is used by the Security Administrator user for role-based access control (RBAC) and managing backup and restore operations in NetBackup. Starting with appliance release 3.1.2, this user is created automatically when you perform the initial configuration on an appliance master server or when you upgrade an appliance master server. Once created, this account is assigned the default appliance password. When this user first logs in to the NetBackup Appliance Shell Menu, they are prompted to change the default password for the account. **Note:** This user cannot log in to the NetBackup Web UI until the default password is changed. After the default password has been changed, by default, the **nbasecadmin** user is allowed the following access and privileges: ■ NetBackup Web UI Access to the NetBackup Web UI lets this user set user roles for other NetBackup users, manage all NetBackup security settings, and perform backup and restore operations. **Note:** Starting with software version 3.2, you can assign backup and restore privileges to the **nbasecadmin** user. If you are upgrading from an earlier version, you must manually add the backup and restore privileges to the **nbasecadmin** user account. For details, see the *NetBackup Web UI Security Administrator's Guide*. ■ NetBackup Appliance Shell Menu Log in to the NetBackup Appliance Shell Menu to change the password for the account. Access is limited to the `Main > Settings > Password` view. This view is visible to the `nbasecadmin` user and all appliance local users that have **No Role** assigned on the appliance. When the `nbasecadmin` user is logged in to the shell menu, only the following menu items are available: **Exit** **Password** The access rules for the **nbasecadmin** user can also be changed to allow more privileges. To access the NetBackup Web UI, this user can open a browser window and enter the URL `https:<appliance master server host name>/webui`. For more information about RBAC and NetBackup user role management, see the *NetBackup Web UI Security Administrator's Guide*.

The following describes the accounts that are available only for internal users. These accounts do not allow system access through the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.

Table 2-2 NetBackup appliance internal account types

Account name	Description
sisips	The `sisips` account is an internal user for implementing the SDCS policies.

root	The `root` account is a restricted user that is only accessed by Veritas Support to perform maintenance tasks. If you try to access this account, the following message is displayed:
	
	`Permission Denied !! Access to the root account requires overriding the Intrusion Security Policy.`
	
	`Please refer to the appliance security guide for overriding instructions.`

nbcopilotxxxx	Supports authentication for access from the master to the media server.
nbwebsvc	Does not support authentication.

See "About authorizing NetBackup appliance users" on page 39.

User types that can authenticate on the NetBackup appliance

You can directly add local users on the appliance, or register users from an LDAP server, Active Directory (AD) server, or NIS server. Registering remote users offers the benefit of letting you leverage your existing directory service for user management and authentication. Table 2-3 describes the types of users that can be added to a NetBackup appliance.

Note: Local user commands cannot be used successfully before the appliance role is configured. Any attempted local user commands including, but not limited to granting user permissions, fail if the appliance role is not configured. If you attempt to run local user commands before role configuration, those same commands also fail after you complete the role configuration. Certain commands can also exhibit unexpected or undesired behavior. To prevent these situations, it is a best practice to avoid attempting any local user commands until after the appliance role has been configured.

Table 2-3 NetBackup appliance user types

User type	Description	Notes
Local (native user)	A local user is added to the appliance database and is not referenced to an external directory-based server like an LDAP server. Once the user has been added, you can then grant or revoke the appropriate appliance access permissions.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage local users. ■ You can use the `Settings > Security > Authentication > LocalUser` command from the NetBackup Appliance Shell Menu to add and delete local users, as well as change their passwords. ■ You cannot add local user groups. ■ A local user can have the Administrator or NetBackupCLI role. **Note:** You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.
LDAP	An LDAP (Lightweight Directory Access Protocol) user or user group exists on an external LDAP server. After configuring the appliance to communicate with the LDAP server, you can register those users and user groups with the appliance. Once the user has been registered (added), you can then grant or revoke the appropriate appliance access permissions. See "About authenticating LDAP users" on page 24.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage LDAP users and user groups. ■ You can use the `Settings > Security > Authentication > LDAP` command from the NetBackup Appliance Shell Menu to add and delete LDAP users and user groups. ■ You can assign the Administrator or NetBackupCLI role to an LDAP user or user group. **Note:** The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.

Table 2-3 NetBackup appliance user types *(continued)*

User type	Description	Notes
Active Directory	An Active Directory (AD) user or user group exists on an external AD server. After configuring the appliance to communicate with the AD server, you can register those users and user groups with the appliance. Once the user has been registered (added), you can then grant or revoke the appropriate appliance access permissions. See "About authenticating Active Directory users" on page 26.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage AD users and user groups. ■ You can use the `Settings > Security > Authentication > ActiveDirectory` command from the NetBackup Appliance Shell Menu to add and delete AD users and user groups. ■ You can assign the Administrator or NetBackupCLI role to an AD user or user group. **Note:** The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.
Kerberos-NIS	A NIS (Network Information Service) user or user group exists on an external NIS server. Unlike the LDAP and AD implementations, configuring the appliance to communicate with the NIS domain requires Kerberos authentication. You must have an existing Kerberos service associated with your NIS server before you can configure the appliance to register the NIS users. After configuring the appliance to communicate with the NIS server and the Kerberos server, you can register the NIS users and user groups with the appliance. Once the user has been registered (added) to the appliance, you can then grant or revoke the appropriate appliance access permissions. See "About authenticating Kerberos-NIS users" on page 29.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage NIS users and user groups. ■ You can use the `Settings > Security > Authentication > Kerberos` command from the NetBackup Appliance Shell Menu to add and delete NIS users and user groups. ■ You can assign the Administrator or NetBackupCLI role to a NIS user or user group. **Note:** The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.

For detailed instructions on configuring new users, refer to the *NetBackup Appliance Administrator's Guide*.

About configuring user authentication

Table 2-4 describes the options that are provided in the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu for configuring the appliance to authenticate various types of users and grant them access privileges.

Table 2-4 User authentication management

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Local (native user)	Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add local users. See "About authorizing NetBackup appliance users" on page 39.	The following commands and options are available under `Settings > Security > Authentication > LocalUser`: ■ `Clean` - Delete all of the local users. ■ `List` - List all of the local users that have been added to the appliance. ■ `Password` - Change the password of a local user. ■ `Users` - Add or remove one or more local users.

Table 2-4 User authentication management *(continued)*

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
LDAP	You can perform the following LDAP configuration tasks under **Settings > Authentication > LDAP**: ■ Add a new LDAP configuration. ■ Import a saved LDAP configuration from an XML file. ■ Add, edit, and delete configuration parameters for the LDAP server. ■ Identify and attach the SSL certificate for the LDAP server. ■ Add, edit, and delete attribute mappings for the LDAP server. ■ Export the current LDAP configuration (including users) as an XML file. This file can be imported to configure LDAP on other appliances. ■ Disable and re-enable the LDAP configuration. ■ Unconfigure the LDAP server. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add LDAP users and user groups. See "About authorizing NetBackup appliance users" on page 39.	The following commands and options are available under `Settings > Security > Authentication > LDAP`: ■ `Attribute` - Add or delete LDAP configuration attributes. ■ `Certificate` - Set, view, or disable the SSL certificate. ■ `ConfigParam` - Set, view, and disable the LDAP configuration parameters. ■ `Configure` - Configure the appliance to allow LDAP users to register and authenticate with the appliance. * ■ `Disable` - Disable LDAP user authentication on the appliance. ■ `Enable` - Enable LDAP user authentication on the appliance. ■ `Export` - Export the existing LDAP configuration as an XML file. ■ `Groups` - Add or remove one or more LDAP user groups. Only the user groups that already exist on the LDAP server can be added to the appliance. ■ `Import` - Import the LDAP configuration from an XML file. ■ `List` - List all of the LDAP users and user groups that have been added to the appliance. ■ `Map` - Add, delete, or show NSS map attributes or object classes. ■ `Show` - View the LDAP configuration details. ■ `Status` - View the status of LDAP authentication on the appliance. ■ `Unconfigure` - Delete the LDAP configuration. ■ `Users` - Add or remove one or more LDAP users. Only the users groups that already exist on the LDAP server can be added to the appliance.

Table 2-4 User authentication management *(continued)*

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Active Directory	You can perform the following AD configuration tasks under **Settings > Authentication > Active Directory**: ■ Configure a new Active Directory configuration. ■ Unconfigure an existing Active Directory configuration. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add Active Directory users and user groups. See "About authorizing NetBackup appliance users" on page 39.	The following commands and options are available under `Settings > Security > Authentication > ActiveDirectory`: ■ `Configure` - Configure the appliance to allow AD users to register and authenticate with the appliance. ■ `Groups` - Add or remove one or more AD user groups. Only the user groups that already exist on the AD server can be added to the appliance. ■ `List` - List all of the AD users and user groups that have been added to the appliance. ■ `Status` - View the status of AD authentication on the appliance. ■ `Unconfigure` - Delete the AD configuration. ■ `Users` - Add or remove one or more AD users. Only the users that already exist on the AD server can be added to the appliance.
Kerberos-NIS	You can perform the following Kerberos-NIS configuration tasks under **Settings > Authentication > Kerberos-NIS** : ■ Configure a new Kerberos-NIS configuration. ■ Unconfigure an existing Kerberos-NIS configuration. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add Kerberos-NIS users and user groups. See "About authorizing NetBackup appliance users" on page 39.	The following commands and options are available under `Settings > Security > Authentication > Kerberos`: ■ `Configure` - Configure the appliance to allow NIS users to register and authenticate with the appliance. ■ `Groups` - Add or remove one or more NIS user groups. Only the user groups that already exist on the NIS server can be added to the appliance. ■ `List` - List all of the NIS users and user groups that have been added to the appliance. ■ `Status` - View the status of NIS and Kerberos authentication on the appliance. ■ `Unconfigure` - Delete the NIS and Kerberos configuration. ■ `Users` - Add or remove one or more NIS users. Only the users that already exist on the NIS server can be added to the appliance.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

- Only one remote user type (LDAP, Active Directory (AD), or NIS) can be configured for authentication on an appliance. For example, if you currently authenticate LDAP users on an appliance, you must remove the LDAP configuration on it before changing to AD user authentication.
- The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.
- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.
- You cannot add a new user or a user group to an appliance with the same user name, user ID, or group ID as an existing appliance user.
- Do not use group names or user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for LDAP, AD, or NIS users.
- The appliance does not handle ID mapping for LDAP or NIS configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.

See "About user authentication on the NetBackup appliance" on page 15.

About authenticating LDAP users

The NetBackup appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Lightweight Directory Access Protocol (LDAP) users. This functionality allows users belonging to an LDAP directory service to be added and authorized to log on to a NetBackup appliance. LDAP is considered as another type of user directory with a schema installed on it by UNIX services.

Pre-requisites for using LDAP user authentication

The following describes the pre-requisites and requirements for using LDAP user authentication on the appliance:

- The 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
- Ensure that the LDAP server is available and is set up with the users and user groups that you want to register with the appliance.

  Note: As a best practice, do not use group names or user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for LDAP users.

- The appliance does not handle ID mapping for LDAP configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.

Configuration methods for LDAP user authentication

Before registering new LDAP users and user groups on the appliance, you must configure the appliance to communicate with the LDAP server. Once the configuration is complete, the appliance can access the LDAP server user information for authentication.

To configure LDAP user authentication, use one of the following methods:

- **Settings > Authentication > LDAP** from the NetBackup Appliance Web Console.
- `Settings > Security > Authentication > LDAP` from the NetBackup Appliance Shell Menu.

For detailed instructions on how to configure and manage LDAP user authentication on the appliance, refer to the *NetBackup Appliance Administrator's Guide* and the *NetBackup Appliance Commands Reference Guide*.

2FA

Starting with appliance release 3.2, NetBackup appliances support two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI. The following describes the 2FA support for the 3.2 release:

- The **nbasecadmin** user or any user with the NetBackup Adminstrator role can configure 2FA for the NetBackup Web UI.
- 2FA is only supported for AD or LDAP domain users with the NetBackup™ Web UI. The 2FA feature is not currently supported through the NetBackup Appliance Shell Menu or NetBackup Appliance Web Console.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.

For details about how to enable 2FA, see the following topic:

See "About authentication using smart cards and digital certificates" on page 27.

About authenticating Active Directory users

The NetBackup appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Active Directory (AD) users. This functionality allows users belonging to an AD service to be added and authorized to log on to a NetBackup appliance. AD is considered as another type of user directory with a schema installed on it by UNIX services.

Pre-requisites for using Active Directory user authentication

The following describes the pre-requisites and requirements for using AD user authentication on the appliance:

- Ensure that the AD service is available and is set up with the users and user groups that you want to register with the appliance.

  Note: As a best practice, do not use group names or user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for AD users.

- Ensure that the authorized domain user credentials are used to configure the AD server with the appliance.
- Configure the appliance with 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.

Configuration methods for Active Directory user authentication

Before registering new AD users and user groups on the appliance, you must configure the appliance to communicate with the AD service. Once the configuration is complete, the appliance can access the AD server user information for authentication.

Configure AD authentication using one of the following methods:

- **Settings > Authentication > Active Directory** page from the NetBackup Appliance Web Console.
- `Settings > Security > Authentication > ActiveDirectory` commands from the NetBackup Appliance Shell Menu.

For detailed instructions on how to configure and manage AD user authentication on the appliance, refer to the *NetBackup Appliance Administrator's Guide* and the *NetBackup Appliance Commands Reference Guide*.

2FA

Starting with appliance release 3.2, NetBackup appliances support two-factor authentication (2FA) for Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Web UI. The following describes the 2FA support for the 3.2 release:

- The **nbasecadmin** user or any user with the NetBackup Adminstrator role can configure 2FA for the NetBackup Web UI.
- 2FA is only supported for AD or LDAP domain users with the NetBackup™ Web UI. The 2FA feature is not currently supported through the NetBackup Appliance Shell Menu or NetBackup Appliance Web Console.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.
  For details about how to enable 2FA, see the following topic:

FSee "About authentication using smart cards and digital certificates" on page 27.

About authentication using smart cards and digital certificates

The NetBackup Web UI supports authentication of Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users with a digital certificate or smart card, including CAC and PIV. This authentication method only supports one AD or LDAP domain for each appliance master server domain and is not available for local domain users. You must configure LDAP for NetBackup, even if LDAP is already configured on the appliance.

Note: Perform this configuration separately for each appliance master server domain where you want to use this authentication method.

Ensure that you add the AD or the LDAP domain before you add access rules for domain users or configure the domain for smart card authentication. Use the `vssat` command to add AD or LDAP domains.

To add the AD or the LDAP domain for NetBackup

1. Log on to the appliance master server as a NetBackupCLI user.
2. Run the `vssat` command.

```
vssat addldapdomain -d DomainName -s server_URL -u user_base_DN
-g group_base_DN -t schema_type -m admin_user_DN
```

Replace the variables in the above command as per the following descriptions:

- *DomainName* is a symbolic name that uniquely identifies an LDAP domain.
- *server_URL* is the URL of the LDAP directory server for the given domain. The LDAP server URL must start with either `ldap://` or `ldaps://`. Starting with `ldaps://` indicates that the given LDAP server requires SSL connection. For example `ldaps://my-server.myorg.com:636`.
- *user_base_DN* is the LDAP-distinguished name for the user container. For example, `ou=user,dc=mydomain,dc=myenterprise,dc=com`.
- *group_base_DN* is the LDAP-distinguished name for the group container. For `example, ou=group,dc=mydomain,dc=myenterprise,dc=com`.
- *schema_type* specifies which type of LDAP schema to use. The two default schema types that are supported are `rfc2307` or `msad`.
- *admin_user_DN* is a string that contains the DN of the administrative user or any user that has search permission to the user container, or user subtree as specified by `UserBaseDN`. If the user container is searchable by anyone including an anonymous user, you can configure this option as an empty string. For example, `--admin_user=`. This configuration allows anyone to search the user container.

3 Verify that the specified AD or LDAP domain was successfully added using `vssat validateprpl`. Note that you can also use the `vssat` command with the following options:

- `vssat removeldapdomain` removes an LDAP domain from the authentication broker.
- `vssat validategroup` checks the existence of a user group in domain provided.
- `vssat validateprpl` checks the existence of a user in domain provided.

For more details on the `vssat` command, see the *Veritas NetBackup Commands Reference Guide*

Configure role-based access control

After adding the AD and LDAP domains for NetBackup, you can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure role-based access control for the NetBackup web UI. For more information about configuring RBAC for NetBackup appliance users, see the *NetBackup Web UI Security Administrator's Guide*.

Configure authentication for a smart card or digital certificate

You can use the `nbasecadmin` user to log on to the NetBackup Web UI and configure authentication for a smart card or digital certificate. Refer to the *NetBackup Web UI Security Administrator's Guide* for steps on performing the following procedures required for the configuration:

- Configure NetBackup Web UI to authenticate users with a smart card or digital certificate.
- Edit the configuration for smart card authentication.
- Add a CA certificate that is used for smart card authentication.
- Delete a CA certificate that is used for smart card authentication.

About authenticating Kerberos-NIS users

The NetBackup appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Network Information Service (NIS) users. This functionality allows users belonging to a NIS directory service to be added and authorized to log on to a NetBackup appliance. NIS is considered as another type of user directory with a schema installed on it by UNIX services.

Configuring the appliance to authenticate NIS users requires Kerberos authentication. You must have an existing Kerberos service associated with your NIS domain before you can configure the appliance to register the NIS users.

Pre-requisites for using NIS user authentication with Kerberos

The following describes the pre-requisites and requirements for using NIS user authentication on the appliance:

- Ensure that the NIS domain is available and is set up with the users and user groups that you want to register with the appliance.
- The appliance does not handle ID mapping for NIS configuration. Veritas recommends that you reserve a user ID and group ID range of 1000 to 1999 for appliance users only.

Note: As a best practice, do not use group names or user names that are already used for appliance local users or NetBackupCLI users. Additionally, do not use the appliance default names **admin** or **maintenance** for NIS users.

- Ensure that the Kerberos server is available and properly configured to communicate with the NIS domain.
- Due to the strict time requirements in Kerberos, always use an NTP server to synchronize time between the appliance, the NIS server, and the Kerberos server.

Configuration methods for NIS user authentication with Kerberos

Before registering new NIS users and user groups on the appliance, you must configure the appliance to communicate with the NIS server and the Kerberos server. Once the configuration is complete, the appliance can access the NIS domain user information for authentication.

To configure Kerberos-NIS authentication, use one the following methods:

- **Settings > Authentication > Kerberos-NIS** page from the NetBackup Appliance Web Console.
- `Settings > Security > Authentication > Kerberos` commands from the NetBackup Appliance Shell Menu.

For detailed instructions on how to configure and manage Kerberos-NIS user authentication on the appliance, refer to the *NetBackup Appliance Administrator's Guide* and the *NetBackup Appliance Commands Reference Guide*.

About the appliance login banner

The NetBackup appliance provides the ability to set a text banner that appears when a user attempts to log on to the appliance. You can use the login banner to communicate various kinds of messages to users. Typical uses for the login banner include legal notices, warning messages, and company policy information.

The NetBackup Administration Console also supports a login banner. By default, when you set a login banner for the appliance, the banner is not used by NetBackup. However, during the appliance login banner configuration you can choose to propagate the banner to NetBackup so that it appears whenever a user attempts to log into the NetBackup Administration Console.

Table 2-5 describes the appliance interfaces that support the login banner. Once a login banner is set, it appears in each of the appliance interfaces that support it, such as the NetBackup Appliance Shell Menu and SSH. However, the login banner can be optionally turned on and off for the NetBackup Administration Console.

Table 2-5 Appliance interfaces that support the login banner

Interface	Notes
NetBackup Appliance Shell Menu	The login banner appears before a user attempts to log on the NetBackup Appliance Shell Menu.
IPMI console session	The login banner appears in an IPMI console session once a user name is specified, but before a password is requested.
NetBackup Appliance Web Console	The login banner appears every time the appliance is accessed through a web browser. The login banner can only be dismissed by clicking the **Agree** button.
NetBackup Administration Console (optional)	The login banner appears whenever a user attempts to log on to the appliance using the NetBackup Administration Console. This feature uses the pre-existing login banner functionality that is a part of NetBackup. For more information, refer to the *NetBackup Administrator's Guide, Volume I*.

Use `Settings > Notifications > LoginBanner` in the NetBackup Appliance Shell Menu to configure the login banner. Refer to the *NetBackup Appliance Commands Reference Guide* for more information.

Or configure the login banner from the NetBackup Appliance Web Console by following the path **Settings > Notification > Login Banner**. Refer to the *NetBackup appliance Administrator's Guide* for more information.

About user name and password specifications

The user name for the NetBackup appliance user account must be in the format that the selected authentication system accepts. Table 2-6 lists the user name specifications for each user type.

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

Table 2-6 User name specifications

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP, AD, or NIS policy
Minimum length	2 characters	2 characters	Determined by the LDAP, AD, or NIS policy
Restrictions	User names must not start with: ■ Number ■ Special character	User names must not start with: ■ Number ■ Special character	Determined by the LDAP, AD, or NIS policy
Space inclusion	User names must not include spaces.	User names must not include spaces.	Determined by the LDAP, AD, or NIS policy

Password specifications

The NetBackup appliance password policy has been updated to increase security on the appliance. The password for the appliance user account must be in the format that the selected authentication system accepts. Table 2-7 lists the password specifications for each user type.

Table 2-7 Password specifications

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP, AD, or NIS policy
Minimum length	Passwords must contain at least eight characters.	Passwords must contain at least eight characters.	Determined by the LDAP, AD, or NIS policy

Table 2-7 Password specifications *(continued)*

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Requirements	■ One uppercase letter ■ 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 uppercase letter ■ 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, AD, or NIS policy
Space inclusion	Passwords must not include spaces.	Passwords must not include spaces.	Determined by the LDAP, AD, or NIS policy
Minimum password age	0 day	0 day **Note:** You can manage the user password age using the `Manage > NetBackupCLI > PasswordExpiry` command from the NetBackup Appliance Shell Menu. For more information, refer to the *NetBackup Appliance Command Reference Guide*.	Determined by the LDAP, AD, or NIS policy
Maximum password age	99999 days (doesn't expire)	99999 days (doesn't expire)	Determined by the LDAP, AD, or NIS policy

Table 2-7 Password specifications *(continued)*

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote 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, AD, or NIS policy
Password expiry	Not applicable as the password does not expire	Use the `Manage > NetBackupCLI > PasswordExpiry` command to manage NetBackupCLI user passwords.	Determined by the LDAP, AD, or NIS policy
Password lockout	None	None	Determined by the LDAP, AD, or NIS policy
Lockout duration	None	None	Determined by the LDAP, AD, or NIS policy

Note: To increase the security of your appliance environment, Veritas recommends that you change the default `admin` and `maintenance` account passwords upon initial login to the appliance. You can use the **Settings > Password** page from the NetBackup Appliance Web Console or the `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 `passwd`. A password that is set in this fashion is overwritten once the system is upgraded. You should use the NetBackup Appliance Shell Menu to change the Maintenance account password.

Password protection

The NetBackup appliance uses the following password protection measures:

- The SHA-512 hashing algorithm is used for protecting the passwords of all customer-accessible local appliance users (local users, NetBackupCLI users, the Administrator user, and the Maintenance user). Whenever you create a new

local appliance user, or change an existing local appliance user password, the password is hashed using SHA-512.

Note: If you are upgrading from NetBackup appliance software version earlier than 2.6.1.1, Veritas recommends that you eventually change the passwords of all the local appliance users after the upgrade so that they use the latest default SHA-512 hashing algorithm.

- The password history is set to 7, meaning that the old passwords are protected and logged up to seven times. If you try to use the old password as the new password, the appliance displays a token manipulation error.
- Passwords in transit include the following:
  - An SSH login where the password is protected by the SSH protocol.
  - A NetBackup Appliance Web Console login where the password is protected by HTTPS communication.

For detailed password instructions, refer to the *NetBackup Appliance Administrator's Guide*.

About STIG-compliant password policy rules

To comply with the Security Technical Implementation Guides (STIGs), NetBackup appliances automatically enforce a higher security password policy when the STIG option is enabled.

After the STIG option is enabled, all current user passwords that were created under the default policy remain valid. Once you are ready to change any user passwords, the STIG-compliant policy rules must be followed.

The following describes the STIG-compliant password policy rules:

- Minimum characters: 15
- Minimum numbers: 1
- Minimum lowercase characters: 1
- Minimum uppercase characters: 1
- Minimum special characters: 1
- Maximum consecutive repeating characters: 2
- Maximum consecutive repeating characters of the same class: 4
- Minimum number of different characters: 8

- Minimum days for password change: 1
- Maximum days for password change: 60
- Dictionary words are not valid or accepted.
- The last seven passwords cannot be reused

Note: Password policy that is displayed on the interface is not translated in other languages. The password policy is displayed in English on Japanese and Chinese interfaces.

Login lockout enforcement

When the STIG option is enabled, it enforces a login lockout for any user that enters three consecutive incorrect passwords within 15 minutes. The lockout condition is in effect for seven days. To clear a lockout condition, contact Technical Support for assistance.

Maintenance account password changes on STIG-enabled appliances

Starting with appliance release 3.1.2, the STIG password age policy delays maintenance account password changes in the following scenarios:

- For 24 hours, after you enable the STIG option.
- For 24 hours, after you upgrade a STIG-enabled appliance to 3.1.2 or later.

Any attempt to change the maintenance account password within 24 hours of either of these events results in failure. Make sure that you wait at least 24 hours after these events before you change the maintenance account password.

See “OS STIG hardening for NetBackup appliance” on page 111.

Chapter 3

User authorization

This chapter includes the following topics:

- About user authorization on the NetBackup appliance
- About authorizing NetBackup appliance users
- About the Administrator user role
- About the NetBackupCLI user role

About user authorization on the NetBackup appliance

The NetBackup appliance is administered and managed through user accounts. You can create local user accounts, or register users and user groups that belong to a remote directory service. In order for a new user account to log on and access the appliance, you must first authorize it with a role. By default, a new user account does not have an assigned role, and therefore it cannot log on until you grant it a role.

Table 3-1 NetBackup appliance user roles

Role	Description
Administrator	A user account that is assigned the Administrator role is provided administrative privileges to manage the NetBackup appliance. An Administrator user is allowed to log on, view, and perform all functions on the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. These user accounts have permissions to log on to the appliance and run NetBackup commands with superuser privileges. See "About the Administrator user role" on page 42.

Table 3-1 NetBackup appliance user roles *(continued)*

Role	Description
NetBackupCLI	A user account that is assigned the NetBackupCLI role is solely restricted to run a limited set of NetBackup CLI commands and does not have access outside the scope of NetBackup software directories. Once these users log on to the appliance, they are taken to a restricted shell menu from where they can manage NetBackup. The NetBackupCLI users do not have access to the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. See "About the NetBackupCLI user role" on page 43.
AMSadmin	A user account that is assigned the `AMSadmin` role is provided administrative privileges to access the Appliance Manager that is hosted on the AMS. An AMSadmin user is allowed to perform all the functions on the Appliance Manager and centrally manage multiple appliances. The AMSadmin user cannot log on the NetBackup Appliance Shell Menu for AMS. An Administrator can create AMSadmin users.

The following list describes some of the characteristics of NetBackup appliance authorization:

- Ability to prevent unintended access to the appliance by password protecting logins.
- Access to shared data is provided only to authorized appliance users and NetBackup processes.
- Data that is stored within an appliance cannot inherently protect itself from unintended modification or deletion by a malicious user that knows the admin credentials to the appliance.
- Network access to the NetBackup Appliance Shell Menu is only allowed through SSH, and the NetBackup Appliance Web Console over HTTPS. You can also directly connect a monitor and keyboard to the appliance and log on using administrative credentials.
- Access to `FTP`, `Telnet`, and `rlogin` are disabled on all appliances.

Note: Starting with software version 3.1, the NetBackup appliance limits login attempts and enforces lockout policies only when the STIG feature is enabled. For more information, refer to the following topic: See "About STIG-compliant password policy rules" on page 35.

Note: Starting with NetBackup Appliance release 3.1.2, the `Telnet` packaged has been removed from VxOS to comply with the STIG feature when it is enabled on NetBackup appliances. The `Telnet` protocol is not secure or encrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security, and is included in VxOS.

About authorizing NetBackup appliance users

Table 3-2 describes the options that are provided for authorizing new and existing users or user groups through the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu:

Table 3-2 User authorization management

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage users	The following options are available under **Settings > Authentication > User Management** ■ View all of the users that have been added to the appliance. ■ Expand and view all belonging users to a single user group. ■ Add and delete local users. ■ Add and delete LDAP/AD/Kerberos-NIS users and user groups.	Use the `Settings > Security > Authentication` commands to add, delete, and view appliance users. See "About configuring user authentication" on page 21.

Table 3-2 User authorization management *(continued)*

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage user permissions (roles)	The following options are available under **Settings > Authentication > User Management**: ■ Grant and revoke the Administrator role for users and user groups. ■ Grant and revoke the NetBackupCLI role for users and user groups. ■ Synchronize members of registered user groups with Administrator role.	The following commands and options are available under `Main > Settings > Security > Authorization`: ■ `Grant` Grant the Administrator and NetBackupCLI roles to specific users and users groups that have been added to the appliance. ■ `List` List all of the users and user groups that have been added to the appliance, along with their designated roles. ■ `Revoke` Revoke the Administrator and NetBackupCLI roles from specific users and users groups that have been added to the appliance. ■ `SyncGroupMembers` Synchronize members of registered user groups.

Notes about user management

- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from theNetBackup Appliance Shell Menu.
- The NetBackupCLI role can be assigned to a maximum of nine user groups at any given time.
- Active Directory (AD) user groups and user names support the use of a hyphen character in those names. The hyphen must appear between the first and the last character of a user name or a user group name. AD user names and user group names cannot begin or end with a hyphen.

- You can list all users of a group that has maximum to 2000 users from theNetBackup Appliance Web Console. To list all of a group that has more than 2000 users, use the `List` command from theNetBackup Appliance Shell Menu.

NetBackup appliance user role privileges

User roles determine the access privileges that a user is granted to operate the system or to change the system configuration. The user roles that are described in this topic are specific to LDAP, Active Directory (AD), and NIS users.

The following describes the appliance user roles and their associated privileges:

Table 3-3 User roles and privileges

User role	Privileges
NetBackupCLI	Users can only access the NetBackup CLI. See "About the NetBackupCLI user role" on page 43.
Administrator	Users can access the following: ■ NetBackup Appliance Web Console ■ NetBackup Appliance Shell Menu ■ NetBackup Administration Console See "About the Administrator user role" on page 42.
AMSadmin	A user account that is assigned the **AMSadmin** role is provided administrative privileges to access the Appliance Management Console that is hosted on the AMS. An AMS user is allowed to perform all the functions on the Appliance Management Console and centrally manage multiple appliances. The AMS user cannot log on the NetBackup Appliance Shell Menu for AMS. An Administrator can create AMS users.

A role can be applied to an individual user, or it can be applied to a group that includes multiple users.

A user cannot be granted privileges to both user roles. However, a NetBackupCLI user can also be granted access to the NetBackup Appliance Shell Menu in the following scenarios:

- The user with the NetBackupCLI role is also in a group that is assigned the Administrator role.
- The user with the Administrator role is also in a group that is assigned the NetBackupCLI role.

Note: When granting a user to have privileges to the NetBackupCLI and the NetBackup Appliance Shell Menu, an extra step is required. The user must enter the `switch2admin` command from the NetBackup CLI to access the NetBackup Appliance Shell Menu.

Granting privileges to users and user groups can be done as follows:

- From the NetBackup Appliance Web Console, on the **Settings > Authentication > User Management** page, click on the **Grant Permissions** link.
- From the NetBackup Appliance Shell Menu, use the following commands in the `Settings > Security > Authorization` view:

```
Grant Administrator Group
Grant Administrator Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
Grant AMS Group
Grant AMS Users
```

See "About configuring user authentication" on page 21.

See "About authorizing NetBackup appliance users" on page 39.

About the Administrator user role

The NetBackup appliance provides access control mechanisms to prevent unauthorized access to the backup data on the appliances. These mechanisms include administrative user accounts that provide elevated privileges to modify appliance configurations, monitoring the appliance, and so on. Only the users that are assigned the Administrator role are authorized to configure and manage the NetBackup appliance.

The Administrator role should be provided only to authorized system administrators to prevent unauthorized and inappropriate modification of the appliance configuration or the backup data that is contained in the expansion disk storage.

An Administrator user can access the appliance using the NetBackup Appliance Shell Menu through SSH, or the NetBackup Appliance Web Console over HTTPS.

An Administrator user as a superuser can perform all the following tasks:

- Perform appliance initial configuration.
- Monitor hardware, storage, and SDCS logs.
- Manage storage configuration, additional servers, licenses and so on.

- Update configuration settings like **Date and Time**, **Network**, **Notification**, etc.
- Restore the appliance.
- Decommission the appliance.
- Apply patches to the appliance.
- Mount or map shares. The following limitations apply:
  - Windows: Only the local **admin** user is authorized to mount or map Windows CIFS shares.
  - Linux: Only users with a root access account can issue the mount command directly to mount NFS shares.

A local, LDAP, Active Directory (AD), or NIS user needs to have the permissions of the Administrator user role to access and administer the 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 Administrator user permissions.

About the NetBackupCLI user role

A NetBackupCLI user can execute all NetBackup commands, view logs, edit NetBackup touch files, and edit NetBackup notify scripts. NetBackupCLI users 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 log on, they are taken to a restricted shell from where they can run the NetBackup commands. The NetBackupCLI users share a home directory and do not have access to the NetBackup Appliance Web Console or the NetBackup Appliance Shell Menu.

The NetBackupCLI role can be assigned to a maximum of nine user groups at any given time. To create a local NetBackupCLI user, use the `Manage > NetBackupCLI > Create` command from theNetBackup Appliance Shell Menu. For more information, see the *NetBackup Appliance Commands Reference Guide*.

Note: You cannot grant the NetBackupCLI role to an existing local user.

Table 3-4 lists the rights and restrictions of NetBackupCLI users.

Table 3-4 Privileges and restrictions of the appliance NetBackupCLI user

Privileges	Restrictions
The NetBackupCLI user can use the NetBackup Appliance Shell Menu to do the following: ■ Run the NetBackup CLI and access the NetBackup directories and files. ■ Modify or create NetBackup notify scripts using the `cp-nbu-notify` command. ■ Run the following NetBackup commands and for the following directories that contain the NetBackup CLI: ■ `/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 NetBackupCLI users: ■ NetBackupCLI users do not have access outside of 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 a NetBackupCLI user

Use one of the following methods to run commands as a NetBackupCLI user:

- Restricted shell.
- Absolute path [“`sudo`”]. For example: `bppllist` or `/usr/openv/netbackup/bin/admincmd/bpplist`

How to run special directive operations

Special directive operations can fail if the special directive files and commands are not in the correct NetBackup list or path. One example of a special directive operation is when you specify an alternate restore path.

Appliance users that need to run NetBackup commands to access special directive files as a NetBackupCLI user, must do the following to ensure successful operation:

- Add the `/home/nbusers` path to the NetBackup `bpcd whitelist`.
- Add the special directive commands to the `/home/nbusers` directory.

For details about adding entries to the NetBackup `bpcd whitelist`, refer to the `BPCD_WHITELIST_PATH` configuration option in the following documents:

NetBackup Administrator's Guide, Volume 1

NetBackup Commands Reference Guide

Chapter 4

Intrusion prevention and intrusion detection systems

This chapter includes the following topics:

- About Symantec Data Center Security on the NetBackup appliance
- About the NetBackup appliance intrusion prevention system
- About the NetBackup appliance intrusion detection system
- Reviewing SDCS events on the NetBackup appliance
- Running SDCS in unmanaged mode on the NetBackup appliance
- Running SDCS in managed mode on the NetBackup appliance

About Symantec Data Center Security on the NetBackup appliance

Note: After an upgrade, the appliance SDCS agent is automatically set to unmanaged mode. If an appliance was running in managed mode before upgrade, make sure to reset that appliance back to managed mode after the upgrade is completed.

You must also update the appliance IPS and IDS policies on your SDCS management server. You cannot use the older policies to manage an appliance that is running the newer software version after upgrade. The new policies can be downloaded from the **Monitor > SDCS Events** page of the NetBackup Appliance Web Console. Also note that any custom rules or support exceptions you might have for the IPS and IDS policies are not available after an upgrade

Symantec Data Center Security: Server Advanced (SDCS) is a security solution offered by Symantec to protect servers in data centers. The SDCS software is included on the appliance and is automatically configured during appliance software installation. SDCS offers policy-based protection and helps secure the appliance using host-based intrusion prevention and detection technology. It uses the least-privileged containment approach and also helps security administrators centrally manage multiple appliances in a data center. The SDCS agent runs at startup and enforces the customized NetBackup appliance intrusion prevention system (IPS) and intrusion detection system (IDS) policies. The overall SDCS solution on the appliance provides the following features:

- Hardened Linux OS components
  Prevents or contains malware from harming the integrity of the underlying host system as a result of OS vulnerabilities.
- Data protection
  Tightly limits appliance data access to only those programs and activities that need access, regardless of system privileges.
- Hardened appliance stack
  Appliance application binaries and configuration settings are locked down such that changes are tightly controlled by the application or trusted programs and scripts.
- Expanded detection and audit capabilities
  Provides 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.

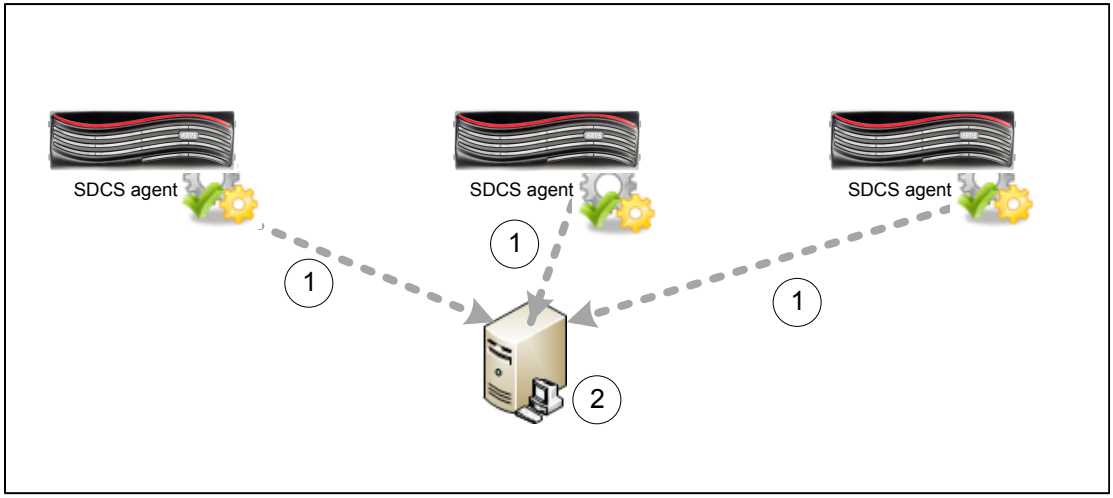
- Centralized managed mode operations
  Lets you use a central SDCS manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by SDCS.

The SDCS implementation on the appliance can operate in an unmanaged mode or a managed mode. By default, SDCS operates in an unmanaged mode and helps secure the appliance using host-based intrusion prevention and detection technology. The NetBackup appliance is in unmanaged mode, when it is not connected to the SDCS server. In unmanaged mode, you can monitor SDCS events from the NetBackup Appliance Web Console. Use the **Monitor > SDCS Events** page, to monitor the events logged. The events are monitored using the NetBackup appliance IDS and IPS policies. These policies are automatically applied at the time of initial configuration. Click **Filter Logs** to filter and view specific events.

In managed mode, the SDCS agent on the appliance continues to protect the appliance while also connecting to an external SDCS server for centralized management and log analysis. In managed mode, the appliance is connected to the SDCS server and the events are monitored using the SDCS management console. Using this mode multiple appliances can be monitored using a single SDCS server. SDCS agents are configured with each NetBackup appliance that are used to send events to the SDCS server.

Figure 4-1 illustrates SDCS in managed mode.

Figure 4-1 SDCS implementation in managed mode



To set up managed mode, you can install the SDCS server and management console and then connect the appliance to an SDCS server.

Use **Monitor > SDCS Events** page to:

- Download NetBackup Appliance IPS and IDS policies
- Apply these polices using the SDCS management console
- Connect the NetBackup appliances with the server
- Monitor events for all the NetBackup appliances connected to this server.

Use **Monitor > SDCS Events > Connect to SDCS server** to:

- Add SDCS server details
- Download authentication certificate
- Connect to the SDCS server

For complete information about the SDCS implementation on the appliance, refer to the *NetBackup Appliance Security Guide*.

About the NetBackup appliance intrusion prevention system

The appliance intrusion prevention system (IPS) consists of a custom Symantec Data Center Security (SDCS) policy that runs automatically at startup. The IPS policy is an in-line policy that can proactively block unwanted resource access behaviors before they can be acted upon by the operating system.

The following list contains some of the IPS policy features:

- Real-time tight confinement of the appliance operating system processes and common applications, such as the following:
  - `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 SDCS agent itself to ensure that the security features and monitoring features of SDCS are not compromised.

- Lock-down of access to system binaries, except by identified and trusted applications, users, and user groups.
- Confinements that protect the system from the applications that try to install software, such as `sbin`) or change system configuration settings, such as `hosts` file.
- Prohibits applications from executing critical system calls such as `mknod`, `modctl`, `link`, `mount`, and so on.
- Prohibits unauthorized users or applications from accessing backup 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.

About the NetBackup appliance intrusion detection system

The appliance intrusion detection system (IDS) consists of a custom Symantec Data Center Security (SDCS) policy that runs automatically at startup. The IDS policy is a real-time policy for monitoring significant system events and critical configuration changes, while optionally taking remediation actions on events of interest.

The following list contains some of the events that the IDS policy monitors:

- User logons, logouts, and failed log on attempts
- Sudo commands
- User addition, deletion, and password changes
- User group addition, deletion, and member modifications
- System auto-start option changes
- Modifications to all system directories and files, including core system files, core system configuration files, installation programs, and common daemon files
- NetBackup services start and stop
- Detected system attacks from UNIX rootkit file/directory detection, UNIX worm file/directory detection, malicious module detection, suspicious permission change detection, and so on
- Audit of all the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu activity, including shell operations for maintenance, root, and NetBackupCLI users.

Reviewing SDCS events on the NetBackup appliance

You can use the **Monitor > SDCS Events** page to view the Symantec Data Center Security (SDCS) logs. These audit logs can help in detecting security breaches and abnormal activity on the 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, and Sandbox Details.
- Severity - Displays the severity of the event.
- Enforcement Action - Displays whether the event was allowed or denied.

The SDCS events are retrieved and are represented using the severity types that are described in Table 4-1

Table 4-1 SDCS event 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`

Table 4-1 SDCS event severity types *(continued)*

Severity types	Description	Events example

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`

Warning	Events with a severity as Warning indicate unexpected activity or problems that have already been handled by SDCS. 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.`

Table 4-1 SDCS event severity types *(continued)*

Severity types	Description	Events example
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 SDCS audit logs, refer to the *NetBackup Appliance Administrator's Guide*.

For information about the appliance operating system logs, such as syslogs and other appliance logs, See "About NetBackup appliance log files" on page 55.

Running SDCS in unmanaged mode on the NetBackup appliance

The Symantec Data Center Security (SDCS) implementation on the appliance operates in an unmanaged mode or a managed mode. The unmanaged mode is the default mode in which the appliance is configured. In unmanaged mode, the appliance is protected and audited without the use of an external SDCS server. Even in an unmanaged mode, both the IDS and IPS policies are applied and the appliance is protected at startup.

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

You can monitor SDCS events from the NetBackup Appliance Web Console (**Monitor > SDCS Events**) and the NetBackup Appliance Shell Menu (`Main_Menu > Monitor > SDCS`).

Running SDCS in managed mode on the NetBackup appliance

The SDCS implementation on the appliance can operate in an unmanaged mode or a managed mode. In managed mode, an external SDCS server is used to communicate with and manage the SDCS agent on one or more appliances. The

SDCS server uses the same IPS and IDS policies that are used in managed mode. You can download the SDCS policies from the NetBackup Appliance Web Console.

Managed mode is recommended for use only by security administrators or by existing SDCS customers who have in-depth knowledge of SDCS.

Benefits of using the managed mode:

- Helps to provide separate tools that cater to the backup administrator role and the security administrator role.
- Provides centralized security management of multiple appliances using a single SDCS server and console.
- Provides the ability to archive and export logs.
- Provides a common console for monitoring, reporting, and setting up alerts.
- Extends the IPS and IDS policies on top of Symantec baseline to meet your data center standards.

To configure the appliance in SDCS managed mode

1. Ensure that your SDCS console is available to connect to the SDCS server and that the server is available to connect to the appliance.

   If you need the SDCS console and server software, you can download them from https://my.veritas.com.

2. Download the IPS and IDS policies from the appliance and import them using the SDCS console. The policies are available for download directly from the NetBackup Appliance Web Console under **Monitor > SDCS Events**.

3. Connect the appliance to the SDCS server. You can connect to the SDCS server from the NetBackup Appliance Web Console under **Monitor > SDCS Events** or from the NetBackup Appliance Shell Menu using under `Monitor > SDCS`.

4. Use the SDCS console to apply the IPS and IDS policies to the connected appliance.

Chapter 5

Log files

This chapter includes the following topics:

- About NetBackup appliance log files
- Viewing log files using the Support command
- Where to find NetBackup appliance log files using the Browse command
- Gathering device logs on a NetBackup appliance
- Log Forwarding feature overview

About NetBackup appliance log files

Log files help you to identify and resolve any issues that you may encounter with your appliance.

The NetBackup appliance has the ability to capture hardware-, software-, system-, and performance-related data. Log files capture information such as appliance operation, issues such as unconfigured volumes or arrays, temperature or battery issues, and other details.

Table 5-1 describes the methods you can use to access the appliance log files.

Table 5-1 Viewing log files

From	Access methods	Log details
NetBackup Appliance Web Console	You can use the **Monitor > SDCS Audit View** screen from the NetBackup Appliance Web Console to retrieve the audit logs of an appliance. See "Reviewing SDCS events on the NetBackup appliance" on page 51.	Appliance audit logs

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

From	Access methods	Log details
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > Browse` command to open the `LOGROOT/>` prompt. You can use the `ls` and `cd` commands to traverse the appliance log directories. See "Viewing log files using the Support command" on page 57.	■ Appliance configuration log ■ Appliance command log ■ Appliance debug log ■ NetBackup logs, Volume Manager logs, and the NetBackup logs that are contained in the `openv` directory ■ Appliance operating system (OS) installation log ■ NetBackup administrative web user interface log and the NetBackup web server log ■ NetBackup 52xx appliance device logs
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > VxLogView Module` *`ModuleName`* command to access the appliance VxUL (unified) logs. You can also use the `Main > Support > Share Open` command and use the desktop to map, share, and copy the VxUL logs. See "Viewing log files using the Support command" on page 57.	Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedup` ■ `TaskService` ■ `AuthService`

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

From	Access methods	Log details
NetBackup Appliance Shell Menu	You can use the `Main > Support > DataCollect` command to collect the storage device logs. See "Gathering device logs on a NetBackup appliance" on page 59.	Appliance 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

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 `OS` directory, the prompt appears as `LOGROOT/OS/>`. From that prompt you can use the `ls` command to display the available log files in the `OS` 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 "Where to find NetBackup appliance log files using the Browse command" on page 58.

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.

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

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

- Upload the log files to Veritas 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 NetBackup appliance log files" on page 55.

Where to find 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

Appliance log	Log file location
Configuration log	`<DIR> APPLIANCE config_nb_factory.log`
Selftest report	`<DIR> APPLIANCE selftest_report`

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

Appliance log	Log file location
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`

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`
Device logs	`/tmp/DataCollect.zip` (software versions up to 3.1.2) `/log/DataCollect.zip` (software versions 3.2 and later) You can copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.

See "About NetBackup appliance log files" on page 55.

Gathering device logs on a NetBackup appliance

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

The DataCollect command collects the following logs:

- Release information
- Disk performance logs
- Command output logs
- iSCSI logs

  Note: The iSCSI logs can be found in /var/log/messages and /var/log/iscsiuio.log.

- CPU information
- Memory information
- Operating system logs
- Patch logs
- Storage logs
- File system logs
- Test hardware logs
- AutoSupport logs
- Hardware information
- Sysinfo logs

To gather device logs with the DataCollect command

1. Log on to the NetBackup Appliance Shell Menu.
2. From the `Main > Support` view, type the following command to gather device logs:

   `DataCollect`

   For appliance software versions up to 3.1.2, the appliance generates the device log in the `/tmp/DataCollect.zip` file.

   For appliance software versions 3.2 and later, the appliance generates the device log in the `/log/DataCollect.zip` file.
3. Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
4. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

See "About NetBackup appliance log files" on page 55.

Log Forwarding feature overview

The Log Forwarding feature lets you send appliance logs to an external log management server. Starting with software version 3.0, NetBackup appliances support forwarding syslogs. A syslog is an OS system log that contains user and system level activities in the form of events. Use this feature to help increase security and to help achieve general compliance initiatives such as HIPPA, SOX, and PCI. The currently supported log management servers are HP ArcSight and Splunk.

NetBackup appliances use the Rsyslog client to forward logs. In addition to HP ArcSight and Splunk, other log management servers that support the Rsyslog client can also be used to receive syslogs from the appliance. Refer to the log management server documentation to verify Rsyslog client support.

Secure log transmission

To secure the log transmission from the appliance to the log management server, you can use the TLS (Transport Layer Security) option. NetBackup appliance currently supports only TLS Anonymous Authentication for log forwarding.

To enable TLS, the appliance and the log management servers each require unique preparation as follows:

- Appliance requirements
  Before you configure and enable the log forwarding feature, the appliance requires the following certificate and private key files in the X.509 file format:
  - `ca-server.pem`
    A root CA certificate from which the log management server certificate is derived.
  - `nba-rsyslog.pem`
    A certificate for the appliance to communicate with a log management server, that also includes any intermediary CA certificates.
  - `nba-rsyslog.key`
    A private key that corresponds to the certificate used to communicate with the `syslog` management server.

  You can upload these files to the appliance through an NFS or a CIFS share.
- Configuration requirements for HP ArcSight servers
  You must set up an Rsyslog server with TLS settings on the HP ArcSight server to receive encrypted logs from the appliance. Then, configure the Rsyslog server to forward the decrypted logs to the HP ArcSiight server. See the `www.rsyslog.com` website for guides on setup and configuration.
- Configuration requirements for Splunk servers

You must first configure TLS on these servers, and then configure the log forwarding feature on the appliance. Refer to your Splunk documentation for the appropriate TLS configuration details.

Configuration

The feature must be configured from the shell menu with the following `Main > Settings > LogFowarding` command options:

- `LogForwarding Enable`
  Configures the feature functionality.
- `LogForwarding Disable`
  Deletes the configuration and disables the feature.
- `LogForwarding Interval`
  Sets how often logs are forwarded. Select from 0 (continuous), 15, 30, 45, or 60 minutes.
- `LogForwarding Share`
  Opens or closes an NFS or a CIFS share on the appliance for obtaining the required certificate and private key files. The share paths are the following:
  NFS: `<appliance.name>:/inst/logforwarding`.
  CIFS: `\\<appliance.name>\logforwarding`
- `LogForwarding Show`
  Shows the current configuration and status.

After you enter the `LogForwarding > Enable` command, prompts appear to guide you through the configuration as described in the following table:

Table 5-3 `LogForwarding > Enable` command prompts

Prompt	Description
Server name or IP	Enter the name or the IP address of the external log management server.
Server port	Enter the appropriate port number on the external log management server.
Protocol	Select either UDP or TCP.
Interval	Set how often logs are forwarded.

Table 5-3 `LogForwarding > Enable` command prompts *(continued)*

Prompt	Description
Enable TLS	Select to enable TLS for secure log transmissions to the log management server. Currently, only the X.509 file format is supported. The following certificate and private key files must be uploaded to the appliance to use TLS: ■ `ca-server.pem` ■ `nba-rsyslog.pem` ■ `nba-rsyslog.key`

For complete configuration and command information, refer to the following documents:

NetBackup Appliance Administrator's Guide

NetBackup Appliance Commands Reference Guide

Chapter 6

Operating system security

This chapter includes the following topics:

- About NetBackup appliance operating system security
- Major components of the NetBackup appliance OS
- Vulnerability scanning of the NetBackup appliance

About NetBackup appliance operating system security

NetBackup appliances use the Veritas operating system (VxOS), which is a customized Linux operating system. Each NetBackup appliance software release includes the latest versions of VxOS and NetBackup software. In addition to regular security patches and updates, VxOS includes the following security enhancements and features:

- An updated and trimmed Red Hat Enterprise Linux (RHEL)-based OS platform that enables the packaging and installation of all the necessary software components on a compatible and a robust hardware platform.
- Hardening for VxOS based on security standards from the National Institute of Standards and Technology (NIST) and RHEL. Additional security is provided by Symantec Data Center Security (SDCS).
- Symantec Data Center Security: Server Advanced (SDCS) intrusion prevention and intrusion detection software that hardens VxOS and protects the backup data by isolating and sandboxing each process and all system files.
- Regular scan of the appliance with industry-recognized vulnerability scanners. Any discovered vulnerabilities are patched in regular releases of the appliance software and with emergency engineering binaries (EEBs). If security threats

are identified between release schedules, you can contact Veritas Support for a known resolution.

- Unused service accounts are removed or disabled.
- VxOS includes edited kernel parameters that secure the appliance against attacks such as denial of service (DoS). For example, the `sysctl` setting `net.ipv4.tcp_syncookies` has been added to `/etc/sysctl.conf` configuration file to implement TCP SYN cookies.
- Unnecessary runlevel services are disabled. VxOS uses runlevels to determine the services that should be running and to allow specific work to be done on the system.
- `FTP`, `telnet`, and `rlogin (rsh)` are disabled. Usage is limited to `ssh`, `scp`, and `sftp`.

Note: Starting with NetBackup Appliance release 3.1.2, the `telnet` packaged has been removed from VxOS to comply with the STIG feature when it is enabled on NetBackup appliances. The `telnet` protocol is not secure or encrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security, and is included in VxOS.

- TCP forwarding for SSH is disabled with the addition of `AllowTcpForwarding no` and `X11Forwarding no` to `/etc/ssh/sshd_config`.
- IP forwarding is disabled in VxOS and does not allow routing on the TCP/IP stack. This feature prevents a host on one subnet from using the appliance as a router to access a host on another subnet.
- NetBackup appliances do not allow IP aliasing (configuring multiple IP addresses) on the network interface. This feature prevents access to multiple network segments on one NIC port.
- The UMASK value determines the file permission for newly created files. It specifies the permissions that should not be given by default to the newly created file. Although the default value of UMASK in most UNIX systems is 022, UMASK is set to 077 for the NetBackup appliance.
- The permissions of all the world-writable files that are found in VxOS are searched and fixed.
- The permissions of all the orphaned and unowned files and directories that are found in VxOS are searched and fixed.

- Starting with software version 3.1, SMBv1 protocol has been disabled and replaced with SMBv2 protocol. SMBv1 protocol is vulnerable to ransomware attacks such as `WannaCry` and `Petya`, and is no longer considered as secure. SMBv2 is now the minimum supported protocol for NetBackup appliances.

Major components of the NetBackup appliance OS

Table 6-1 lists the major software components of the appliance operating system (VxOS).

Table 6-1 Major software components included in VxOS for appliance version 3.1.2.

Software component	Version
Red Hat Enterprise Linux (RHEL)	7.6
Veritas InfoScale	7.2 **Note:** The Veritas InfoScale installation is modified and tuned for maximum performance on the appliance.
Symantec Data Center Security: Server 6.8 Advanced (SDCS)	6.8.0 (build 309)
Java Runtime Environment (JRE)	1.8.0_221-1
Apache Tomcat	9.0.14-1
RabbitMQ	rabbitmq-server-3.7.13-1
MongoDB	3.2.9
Intel IPMI Utils	3.1.2-3

Vulnerability scanning of the NetBackup appliance

Veritas regularly tests the NetBackup appliance with industry-recognized vulnerability scanners. Any new vulnerabilities that pose a security threat to the appliance are then patched in routine software releases. For high-severity vulnerabilities, Veritas may choose to issue a patch in an emergency engineering binary (EEB) to urgently address a potential security threat. The following table describes the software products that were used for this release.

Table 6-2 Vulnerability scanning software and versions

Security scanner	Version
Nessus™ Professional	8.7.2
QualysGuard™	11.5.21-1

Chapter 7

Data security

This chapter includes the following topics:

- About data security
- About data integrity
- About data classification
- About data encryption

About data security

NetBackup appliance supports policy driven mechanisms 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.

- Usage of HTTPS protocol and port 443 to connect to the Veritas AutoSupport server to upload hardware and software information using the Call Home feature. Veritas Technical Support uses this information to resolve any issues that you might report. This information is retained for 90 days and purged at the Veritas 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 the NetBackup Catalog and the KMS database may need additional configuration.

NetBackup appliance software has no in-built transmission/session security unless it is HTTP (Web service) protocol. Veritas 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:

- Transmits data in encrypted formats by 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 transmitted from the appliance, the network infrastructure is used for securing data in flight.

- Starting with NetBackup appliance version 3.0 (NetBackup version 8.0), MSDP provides AES encryption. If your environment uses encrypted MSDP, new incoming data gets encrypted with AES 128-bit (default) or AES 256-bit. For more information, see the following NetBackup documents:
  Veritas NetBackup Deduplication Guide
  Veritas NetBackup Security and Encryption Guide
- Supports encryption using NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. See "KMS support " on page 71.

KMS support

The NetBackup appliance supports encryption managed by NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. KMS is supported on master and media server appliances. Regenerating the data encryption key is the only supported method of recovering KMS on an appliance master server.

The following describes the KMS key features:

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

About the keys used under KMS

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

Table 7-1 KMS files

KMS files	Description	Location
Key file or key database	This file is critical for KMS, as it contains the data encryption keys.	/usr/openv/kms/db/KMS_DATA.dat
Host Master Key	This file 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	This encryption key 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

Configuring KMS

To configure KMS on an appliance master server, you must log in as a NetBackupCLI user. For information about this user, refer to the following topic:

See "About the NetBackupCLI user role" on page 43.

To create a NetBackupCLI user, see the *NetBackup Appliance Commands Reference Guide*.

The following describes how to configure and enable KMS on an appliance.

To configure and enable KMS on an appliance

1. Log in to the appliance master server as a NetBackupCLI user.
2. Create an empty database using the nbkms command, as follows:

```
[nbcli@myappliance~]# nbkms -createemptydb
```

3. Start nbkms. For example:

```
[nbcli@myappliance~]# nbkms
```

4. Create a Key group. For example:

```
[nbcli@myappliance~]# nbkmsutil -createkg -kgname KMSKeyGroupName
```

5. Create an active key. For example:

```
[nbcli@myappliance~]# nbkmsutil -createkey -kgname KMSKeyGroupName
-keyname KMS KeyName
```

Enabling KMS encryption for MSDP

After KMS has been configured and is running on the master server, you can enable KMS encryption for MSDP on all of the media servers that are associated with the master server.

To enable KMS encryption for MSDP on an appliance media server, you must log in as a NetBackupCLI user. For information about this user, refer to the following topic:

See "About the NetBackupCLI user role" on page 43.

To create a NetBackupCLI user, see the *NetBackup Appliance Commands Reference Guide*.

The following describes how to enable KMS encryption for MSDP on an appliance.

To enable KMS encryption for MSDP

1. Log in to the appliance media server as a NetBackup CLI user.
2. Change the following options in the order as shown:

   - `nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSType --value=0`
   - `nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSServerName --value=<master server hostname>`
   - `nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSKeyGroupName --value=msdp`
   - `nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KeyName --value=<KMS KeyName>`
   - `nbcli@myappliance:~> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSEnable --value=true`
   - `pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=ContentRouter --option=ServerOptions --value=verify_so_references,fast,encrypt`

     Repeat this step on all media servers that are associated with the master server

3 Stop and restart the NetBackup services with the following commands:

- `bp.kill_all`
- `bp.start_all`

4 To verify that KMS encryption for MSDP is enabled on the media server, run a backup job on the server, then run the following command:

```
crcontrol --getmode
```

Chapter 8

Web security

This chapter includes the following topics:

- About SSL usage
- Implementing third-party SSL certificates

About SSL usage

The Secure Socket Layer (SSL) protocol creates an encrypted connection between the appliance web server and the appliance web console, and other local servers. This type of connection allows for a more secure information transfer without the problems of eavesdropping, data tampering, or message forgery. To enable SSL on the appliance web server, you need an SSL certificate that identifies the appliance host.

The appliance uses self-signed certificates for client and host validation. The appliance certificate is generated using a 2048 bit RSA public key that is hashed with the SHA256 algorithm and signed with RSA encryption. For secure communications, the appliance uses only TLS v1.2 and later protocol.

Note: Warnings such as **SSL Certificate Cannot be Trusted** or **SSL Self-Signed Certificate** can be avoided by replacing the default self-signed certificate with a custom CA issued certificate.

SSL certificates are also supported for secure communications between the appliance and various external servers, such as LDAP and Syslog.

Third-party certificates

Third-party certificates are used for SSL encryption and authentication. By default, a host ID-based certificate issued by the NetBackup Certificate Authority (NBCA) is deployed on the master and media servers during role configuration.

Starting from 3.2, NetBackup appliance also supports host ID-based certificates issued by an External Certificate Authority (ECA) for NetBackup. An ECA can be used as an alternative to the NBCA for providing host verification and security on new installations as well as upgraded appliances.

You can import external certificates on a NetBackup Appliance master or media server from the NetBackup Appliance Shell Menu. For more information, see the *Veritas NetBackup Appliance Commands Reference Guide*. You can also import external certificates on a NetBackup Appliance media server while configuring its role. For more information, see the *Veritas NetBackup Appliance Initial Configuration Guide*.

Additionally, to configure the ECA to the NetBackup Appliance infrastructure services such as mongodb, tomcat, and nginx, see the following topic:

Note: You must deploy the same external certificate for both NetBackup and NetBackup Appliance layers. Note that separate certificates for NetBackup and NetBackup Appliance layers are not supported.

Implementing third-party SSL certificates

Use the steps in this section to manually deploy and configure the external certificates for NetBackup Appliance layer. You must deploy the same external certificate for both NetBackup and NetBackup Appliance. Note that separate certificates for NetBackup and NetBackup Appliance layers are not supported.

Refer to the following table for different types of certificates used in NetBackup Appliance.

Table 8-1 Types of third-party certificates

Certificate type	Description
Appliance host certificate	The Appliance host certificate is based on the X.509 or PKCS#7 standard. The certificate is encoded in either DER (binary) or PEM (text) format. Veritas recommends that you use RSA public and private keys of length 2048 bits or higher. **Note:** Ensure that the **CN** part of the certificate Subject field specifies the fully qualified hostname of the appliance **SubjectAlternativeName** certificate extension must contain all the appliance hostnames and IP addresses by which the appliance can be reached. You must include the fully qualified hostnames and the short names.
Appliance host private key (corresponding to the host certificate)	The Appliance host private key must be in PKCS#8 standard and encoded in PEM format. We recommend using **appliance** as the passphrase for encryption. Using any other passphrase can cause issues while connecting to MongoDB, after the certificates are replaced during an upgrade.
(Optional) Intermediary CA certificates	Intermediary CA certificates form a certificate chain from the appliance host certificate to the root CA certificate. These certificates are only required if the host certificates are issued by a CA other than the root CA.
Root CA certificates	These include the root CA certificates of the Appliance certificate chain and its peers. If the appliance needs to interact with the hosts that have certificates from different Certificate Authorities, you must have all those intermediary and root CA certificates ready in a file called cacerts.pem.

Note: The Appliance host certificate, private key, and its intermediary CA certificates can all be in a single PEM file.

Prerequisites

Ensure that you have read through prerequisites and performed the necessary steps, before installing the third-party certificates.

- To implement the third-party certificates in NetBackup appliance you must log in with the root account. Ensure that you have privileges to access the maintenance account, override the Symantec Data Center security, and log in with the root account.
- To prevent errors, ensure that the certificate files meet the following criterion:
  - All certificate files must have a suffix of `.pem` or `.cer` and include `"-----BEGIN CERTIFICATE-----"` at the beginning of the certificate.
  - All certificate files must contain the host name and FQDN in the subject alternative name (SAN) field of the certificate. If the certificate is used in a HA environment, the SAN field must contain the VIP, host name, and FQDN.
  - Subject name and common name fields must not be left empty.
  - Subject fields must be unique for each host.
  - Subject fields can contain a maximum of 255 characters.
  - Server and client authentication attributes must be set in the certificate.
  - Only ASCII 7 characters can be used in the subject and SAN fields of the certificate.
- The private key must be in the PKCS#8 PEM format and it must begin with a header line of `-----BEGIN ENCRYPTED PRIVATE KEY-----` or `-----BEGIN PRIVATE KEY-----`
- NetBackup Appliance's web service uses the PKCS#12 standard and requires certificate files to be in the X.509 (.pem) format. If you obtained the certificate and private key in any other format you must first convert them to the X.509 (.pem) format. See the table below for steps on converting your certificate files to the required format with the help of OpenSSL. You can download OpenSSL from http://www.openssl.org.

Table 8-2 Procedure to convert certificate files to the required format

Certificate file format	Certificate file suffix	Procedure to convert the certificate file to the required format
DER	.DER or .der	Convert DER format to an X.509 (.pem) format using the following command: `openssl x509 -inform der -in cert.der -outform pem -out cert.pem`

Table 8-2 Procedure to convert certificate files to the required format *(continued)*

Certificate file format	Certificate file suffix	Procedure to convert the certificate file to the required format

	.p7b	If the certificate file does not contain the "---BEGIN PKCS7—" string, use the following command to convert it to an X.509 (.pem) format:
		`openssl pkcs7 -inform der -in cacerts.der.p7b -out cacerts.p7b`
		`openssl pkcs7 -print_certs -in cacerts.p7b -out cacerts.pem`

p7b	.p7b	If the certificate file contains the "---BEGIN PKCS7—" string, use the following command to convert it to an X.509 (.pem) format: `openssl pkcs7 -print_certs -in cacerts.p7b -out cacerts.pem`

Assuming that your appliance host certificate, appliance host private key, and root CA certificate files are named as `server.pem`, `serverkey.pem`, and `cacerts.pem` respectively, perform the following steps to configure third-party certificates in NetBackup Appliance.

Step 1: Install the certificate files to the existing Java KeyStore and TrustStore

Third-party certificates are stored in a Java KeyStore (JKS). A Java KeyStore (JKS) is a repository of security certificates that is used by Java-based services such as the Tomcat web server.

The root CA SSL certificate is loaded into a Java TrustStore that is used by the NetBackup Web Management Console. This TrustStore is part of the NetBackup catalog backup.

To install certificate files to the existing Java KeyStore and TrustStore in NetBackup Appliance, perform the following steps:

1. Log on to the maintenance account using SSH and override the Symantec Data Center Security protection.
2. Log on to the appliance using the root account.
3. Copy the appliance host certificate, private key, and CA certificate files to a temporary directory such as `/tmp`.

4 Ensure that all certificate files are in X.509 PEM format. These files typically have a suffix of `.pem` or `.cer`. and contain a header line `-----BEGIN CERTIFICATE-----` at the beginning of the certificate, see

5 Convert the PEM formatted X.509 certificate (`server.pem`) and private key (`serverkey.pem`), to the PKCS#12 format using the CA certificate file `cacerts.pem`. Type the following command:

```
openssl pkcs12 -export -in server.pem -inkey serverkey.pem -out
server.p12 -name tomcat -CAfile cacerts.pem -caname root
```

Note: When the OpenSSL command prompts for the import password, type the private key's passphrase. When it prompts for the export password, type **appliance**.

6 Copy the NetBackup Appliance's webservice KeyStore file to your working directory, as follows:

```
cp /opt/apache-tomcat/security/keystore ./keystore
```

7 Import the PKCS#12 file (`server.p12`) to the Java KeyStore, type the following command:`keytool -importkeystore -deststorepass appliance -destkeypass appliance -destkeystore keystore -srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass appliance -alias tomcat`

To prevent any exceptions from occurring, ensure the following:

- Specify `appliance` as the password for the `-deststorepass` and `-destkeypass` options. Note that only alphanumeric characters are supported for the password.
- Specify `tomcat` for the `-alias` option.

8 Run the following command to ensure that all the DNS values are correctly applied to the entry in Java KeyStore.

```
keytool -list -v -alias tomcat -keystore keystore -storepass
appliance
```

9 At the bottom of the `cacerts.pem` certificate authority (CA) certificate file, ensure that you have included the chain of intermediary CA certificates (if any) up to the root CA certificate.

10 Import the CA certificate file `cacerts.pem` to the Java TrustStore. The Java TrustStore is used by the NetBackup Web Management Console. Type the following commands:

```
keytool -import -noprompt -trustcacerts -file cacerts.pem -alias
vxosrootcachain -keystore keystore -storepass appliance
```

If the `cacerts.pem` file consists of multiple intermediary CA certificates, ensure that you split the certificates into separate files as indicated by the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` tags in the certificate. You can then run the command separately for each CA certificate file.

```
keytool -import -noprompt -trustcacerts -file cacertn.pem alias
vxosrootcachain[n] -keystore keystore -storepass appliance
```

Where `cacertn` represents each of the individual certificate files (for example, `cacert1.pem`, `cacert2.pem`, ... , `cacertn.pem`.

Step 2: Shutdown the database and relevant web services

To shutdown the database and relevant web services, type the following commands:

```
systemctl stop nginx
service as-alertmanager stop
service as-analyzer stop
service as-transmission stop
/opt/IMAppliance/scripts/infraservices.sh webserver stop
/opt/IMAppliance/scripts/infraservices.sh database stop
```

Step 3: Install the new Java KeyStore in the Tomcat web server

To install the new KeyStore in the Tomcat web server, perform the following steps:

1. Backup the existing web server KeyStore file using the following command

```
cp /opt/apache-tomcat/security/keystore
/opt/apache-tomcat/security/keystore.orig
```

2. Replace the existing KeyStore file with the new KeyStore file:

```
cp ./keystore /opt/apache-tomcat/security/keystore
```

3. Set the permissions for the new KeyStore file using the following command:

```
chmod 700 /opt/apache-tomcat/security
chmod 600 /opt/apache-tomcat/security/keystore
chown –R tomcat:tomcat /opt/apache-tomcat/security
```

Step 4: Copy the certificate files to the default location

Perform the following steps:

1. Copy the certificate files to `/etc/vxos-ssl/servers/certs`.

```
cp serverkey.pem /etc/vxos-ssl/servers/certs
cp server.pem /etc/vxos-ssl/servers/certs
cp cacerts.pem /etc/vxos-ssl/servers/certs
```

2. Concatenate the private key (`serverkey.pem`) and certificate (`server.pem`).

```
cat /etc/vxos-ssl/servers/certs/server.pem >>
/etc/vxos-ssl/servers/certs/serverkey.pem
```

3. Set the required file permissions for the certificate files, as follows:

```
chown root:infra /etc/vxos-ssl/servers/certs/serverkey.pem
chown root:infra /etc/vxos-ssl/servers/certs/server.pem
chown root:infra /etc/vxos-ssl/servers/certs/cacerts.pem

chmod 440 /etc/vxos-ssl/servers/certs/serverkey.pem
chmod 440 /etc/vxos-ssl/servers/certs/server.pem
chmod 440 /etc/vxos-ssl/servers/certs/cacerts.pem
```

Step 5: Configure MongoDB to use the new certificate files

To configure the third-party SSL certificates in MongoDB, perform the following steps:

1. Concatenate the private key (`serverkey.pem`) and certificate (`server.pem`).

   ```
   cat /etc/vxos-ssl/servers/certs/server.pem >>
   /etc/vxos-ssl/servers/certs/serverkey.pem
   ```

2. Edit the line containing **PEMKeyFile** in `/etc/mongod.conf`, and add `/etc/vxos-ssl/servers/certs/serverkey.pem`.
3. Edit the line containing **PEMKeyPassword** in `/etc/mongod.conf`, and add the passphrase of the private key.
4. Edit `/etc/mongod.conf`, and add the following:

   ```
   server_cert=/etc/vxos-ssl/servers/certs/serverkey.pem
   client_cert=/etc/vxos-ssl/servers/certs/cacerts.pem
   pem_password=<passphrase of the private key>
   ```

5. Type the following commands to start the mongodb and web service:

   ```
   /opt/IMAppliance/scripts/infraservices.sh database start
   /opt/IMAppliance/scripts/infraservices.sh webserver start
   ```

Step 6: Configure the NGINX gateway server to use the new certificate files

To configure the third-party SSL certificates in NGINX gateway, perform the following:

1. Ensure that `/etc/nginx/conf.d/appsol.conf` is writable.

   Edit the lines containing **ssl_certificate** and **ssl_certificate_key** to point to the certificates and private key (concatenated with the certificate):

   ```
   ssl_certificate /etc/vxos-ssl/servers/certs/server.pem;
   ssl_certificate_key /etc/vxos-ssl/servers/certs/serverkey.pem;
   ```

2. Ensure that `/etc/nginx/locations/appsol.conf` is writable.

   Edit the lines containing **proxy_ssl_certificate** and **proxy_ssl_certificate_key** to point to the certificates and private key (concatenated with the certificate):

   ```
   proxy_ssl_certificate /etc/vxos-ssl/servers/certs/server.pem;
   proxy_ssl_certificate_key /etc/vxos-ssl/servers/certs/serverkey.pem;
   ```

3. Type the following commands to start the NGINX server:

   ```
   systemctl start nginx
   ```

Step 8: Start the auto support services

Type the following commands to start the Auto Support Service:

```
service as-alertmanager start
service as-analyzer start
service as-transmission start
```

Step 9: Deploy the third-party certificates on NetBackup Appliance master servers

Every third-party CA SSL certificate that is applied on a NetBackup Appliance media server must also be deployed on the associated NetBackup Appliance master server.

Ensure that you run the following command on the master server for each third-party root CA SSL certificate deployed on its associated media servers.

- For a UNIX-based NetBackup Appliance master server, run the following commands:

  ```
  /usr/openv/java/jre/bin/keytool -importcert -storepass `cat
  /usr/openv/var/global/jkskey` -keystore
  /usr/openv/var/global/wsl/credentials/truststoreMSDP
  -file <path to root CA certificate file>
  -alias <descriptive label for root CA certificate>
  ```

- For a Windows-based NetBackup Appliance master server, use a text editor or a shell or command utility such as *type* to read the `jkskey` file stored at `\Program Files\Veritas\NetBackup\var\global\jkskey`. Run the following command to replace the KeyStore password:

  ```
  \Program Files\Veritas\NetBackup\jre\bin\keytool" -importcert
  -keystore "C:\Program
  Files\Veritas\NetBackup\var\global\wsl\credentials\truststoreMSDP"
  -storepass <keystore password> -file "<path to root CA certificate
  file>" -alias <descriptive label for root CA certificate>
  ```

  Note: The`jkskey` file contains the NetBackup password for the Java KeyStore files that are used by the NetBackup Web Management Console. Any changes made to the`jkskey` file can cause a system failure.

Chapter 9

Network security

This chapter includes the following topics:

- About IPsec Channel Configuration
- About NetBackup appliance ports
- About the NetBackup Appliance firewall

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 Verisign 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.

Table 9-1 IPsec commands *(continued)*

Command	Description
`Network > Security > Import`	Depending on which NetBackup Appliance model you are using, use either of the following commands: ■ On 5230, 5240,5330, and 5340 NetBackup Appliances, use the `Import [EnterPasswd] [PathValue]` command. 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. ■ On 5250 NetBackup Appliances, a copy of the IPsec credentials is stored on the SSD. You can use the `Import` command to import the IPsec credentials from the SSD. IPsec credentials are unique for each appliance and are included as part of the original factory image. Because IPsec credentials are removed during a reimage or factory reset process, you must manually import the credentials to enable secure communication between appliances.
`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.
`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).

Table 9-1 IPsec commands *(continued)*

Command	Description
`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 *NetBackup Appliance Command Reference Guide*.

About NetBackup appliance ports

In addition to the ports used by NetBackup software, NetBackup 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). You can 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).

For a list of the appliance ports that are open by default before and after the initial configuration, refer to the following topic:

See "About the NetBackup Appliance firewall" on page 90.

Note: The NetBackup Appliance Web Console is available only over HTTPS on the default port 443. 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 outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 9-2 Outbound ports

Port	Service	Description
443	HTTPS	Call Home notifications to Veritas Download SDCS certificate
161	SNMP Polling	Download appliance updates
162**	SNMP	Download appliance updates
22	SFTP	Log uploads to Veritas
25	SMTP	Email alerts
389	LDAP	
636	LDAPS	
514	rsyslog	Log forwarding

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

Note: To see a list of Remote Management Module (RMM) ports, see the following topic:

See "RMM ports" on page 104.

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

About the NetBackup Appliance firewall

Starting with NetBackup Appliance release 3.1.2, a firewall policy provides added network security for the appliance. This feature changes the firewall default zone from "trusted" to "public". To provide maximum security, specific incoming connections are opened automatically while others are blocked automatically during the following operations:

- Initial configuration
- Role configuration (part of the initial configuration)
- Add node or remove node (high availability configuration)
- Upgrades

Exception rules help to ensure that connections between master and media servers remain open during the described operations and keep unnecessary ports blocked.

The following tables describe the open ports on the appliance before and after the initial configuration takes place.

Table 9-3 shows the NetBackup Appliance ports that are open by default, before the appliance initial configuration has been completed.

Table 9-3 Factory default open NetBackup Appliance ports (before appliance initial configuration)

Port	Protocol	Usage
22	TCP	SSH
111	TCP/UDP	Sunrpc, Portmapper
137	UDP	NetBIOS Name Service (Samba)
138	UDP	NetBIOS Datagram Service (Samba)
139	TCP	NetBIOS Session Service (Samba)
162	TCP/UDP	SNMP
443	TCP	HTTPS
445	TCP	Samba
867	TCP	NFS mount
2049	TCP/UDP	NFS
20048	UDP	`mountd`
27017	TCP/UDP	Mongo **Note:** This port opens only when you add the partner node to complete the high availability (HA) setup or when you remove a node from the HA setup. After a node is added or removed, the port is closed.

Table 9-4 shows the NetBackup ports that are open by default, after the appliance initial configuration has been completed.

Table 9-4 Open NetBackup ports on NetBackup Appliances (after appliance initial configuration)

1025-5000	TCP	Veritas NDMP, `SERVER_PORT_WINDOW`

Table 9-4 Open NetBackup ports on NetBackup Appliances (after appliance initial configuration) *(continued)*

1556	TCP	Veritas PBX
5637	TCP/UDP	NetBackup Cloud Storage Server Configuration, Deduplication to Cloud
7394	TCP	Veritas Granular Restore Technology (GRT)
8443	TCP	NetBackup VMware
10000	TCP/UDP	Veritas NDMP agent
10082	TCP/UDP	MSDP, Deduplication Engine (`spoold`), HA, Migration
10102	TCP/UDP	MSDP, Deduplication Manager (`spad`), HA, Migration
13701-13723	TCP	Veritas Granular Restore Technology (GRT)
13720	TCP	Support for 271 media role configuration
13724	TCP	`vnetd`
13782	TCP	Veritas `vnet_async`

Synchronize or view the open NetBackup ports on the appliance

The following commands have been added to let you synchronize or view the current open NetBackup ports on the appliance:

```
Main > Settings > Security > Ports > ModifyNBUPortRange
```

Note the following about using this command:

- Before you can run this command, the appliance must be configured with the master server or the media server role.
- Before you run this command, you must first modify the open NetBackup ports using the `SERVER_PORT_WINDOW` option in the NetBackup Java console. Then, run this command to synchronize the appliance ports with the open NetBackup ports.

Note: The `ModifyNBUPortRange` command does not let you change the default NetBackup VMware port assignment of 8443. VMware requires the use of port 8443 by default for both the appliance and NetBackup.

```
Main > Settings > Security > Ports > Show
```

For more information about these commands, see the *NetBackup Appliance Commands Reference Guide*.

Chapter 10

Call Home security

This chapter includes the following topics:

- About AutoSupport
- About Call Home
- About SNMP

About AutoSupport

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

The MyAppliance portal is the unified address that you register the appliance and edit registration details.

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

- Proactive monitoring lets Veritas support to automatically create cases, fix issues, and dispatch any appliance parts that might be at risk.
- The AutoSupport infrastructure within Veritas 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, Veritas 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 Veritas 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.veritas.com.

Data security standards

All data that is transmitted to Veritas from an appliance is done with industry standard high encryption methods. The following data security standards are applied to all AutoSupport data sent between the client and server, and the data communication between the different components inside the client:

- RSA 2048 bit keys for server authentication
- AES 128/256 bit keys for data encryption
- SHA1, SHA2 (256/384 bit) hashes for message authentication

About Call Home

Your appliance can connect with a Veritas AutoSupport server and upload hardware and software information. Veritas 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 Veritas AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

AutoSupport uses the data that Call Home gathers to provide proactive monitoring for the appliance. If Call Home is enabled, the appliance uploads information or data to the Veritas AutoSupport server at a default interval of 24 hours.

If you determine that you have a problem with your appliance, you might want to contact Veritas support. The Technical Support engineer uses the serial number of your appliance and assesses the status from the Call Home data.

To obtain 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 failure is reported when the feature is enabled or disabled.

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

Monitoring status	Failure routine

Call Home enabled	When a failure occurs, the following sequence of alerts occur:
	■ The appliance uploads all the monitored hardware and software information to a Veritas AutoSupport server. The list following the table contains all the relevant information.
	■ The appliance generates 3 kinds of email alerts to the configured email address.
	  ■ An error message by email to notify you of the failure once an error is detected.
	  ■ A resolved message by email to inform you of any failure once an error is resolved.
	  ■ A 24-hour summary by email to summarize all of the currently unresolved errors in the recent 24 hours.
	■ The appliance also generates an SNMP trap.

Call Home disabled	No data is sent to the Veritas AutoSupport server. Your system does not report errors to Veritas to enable faster problem resolution.

The following list contains all the information that is monitored and sent to Veritas AutoSupport server for analysis.

- CPU
- Disk
- Fan
- Power supply
- RAID group
- Temperatures
- Adapter
- PCI
- Fibre Channel HBA
- Network card

- Partition information
- MSDP statistics
- Storage connections
- Storage status
- 52xx Storage Shelf - Status of disk, fan, power supply, and temperature
- 53xx Primary Storage Shelf - Status of disk, fan, power supply, temperature, battery backup unit (BBU), controller, volume, and volume group
- 53xx Expansion Storage Shelf - Status of disk, fan, power supply, and temperature
- NetBackup appliance software version
- NetBackup version
- Appliance model
- Appliance configuration
- Firmware versions
- Appliance, storage, and hardware component serial numbers

See "Configuring Call Home from the NetBackup Appliance Shell Menu" on page 97.

See "About AutoSupport " on page 94.

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 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.

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

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

See "About Call Home" on page 95.

Enabling and disabling Call Home from the appliance shell menu

You can enable or disable Call Home from the appliance shell menu. Call Home is enabled by default.

Note: For Call Home to work properly, you need to register your appliance. You can register your appliance from the **Appliances > My Appliances** page of the MyAppliance portal.

To enable or disable Call Home from the shell menu

1. Log on to the 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 the NetBackup appliance `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Commands 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 Veritas 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 the 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 Veritas AutoSupport server.

Call Home uses HTTPS (secure and encrypted protocol) with port number 443 for all communication with Veritas 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 Veritas 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 appliance initiates all communications. On the appliance, make sure that you enable the proxy and/or the firewall to outbound 443/TCP TLS socket connections to the following site:`https://api.appliance.veritas.com`

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

- Access a port to `https://api.appliance.veritas.com` every 24 hours.
- Perform a self-test operation to `https://api.appliance.veritas.com`
- If the appliance encounters an error state, all logs from past three days are gathered along with the current log.

- The logs are then uploaded to the Veritas 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 95.

See "About AutoSupport " on page 94.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It uses either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for transport, depending on configuration. 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.

NetBackup appliance 3.2 supports SNMP v2.

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, 1.3.6.1.4.1.48328.1).

These OIDs form a tree. A 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 view the details of the SNMP MIB file from the **Settings > Notifications > Alert Configuration** page of the web console. To configure the appliance SNMP manager to receive hardware monitoring related traps, click **View SNMP MIB file** in the **SNMP Server Configuration** page.

You can also view the SNMP MIB file with the `Settings > Alerts > SNMP ShowMIB` command in the Shell Menu of your appliance.

Chapter 11

Remote Management Module (RMM) security

This chapter includes the following topics:

- Introduction to IPMI configuration
- Recommended IPMI settings
- RMM ports
- Enabling SSH on the Remote Management Module
- Replacing the default IPMI SSL certificate

Introduction to IPMI configuration

You can configure the Intelligent Platform Management Interface (IPMI) sub-system for your appliances. The 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 Veritas Remote Management tool using the BIOS setup. The Veritas 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

Use the following recommendations when creating IPMI users:

- Do not create accounts with null user names or passwords.
- Limit the number of administrative users to one.
- Disable any anonymous users.
- To mitigate the CVE-2013-4786 vulnerability:
  - Use strong passwords to help prevent offline dictionary attacks and brute force attacks. The recommended password length is 16-20 characters.
  - Change the default user password (`sysadmin`) as soon as possible.
  - Use Access Control Lists (ACLs) or isolated networks to limit access to the IPMI interface.
  - Keep the IPMI protocol port (623) turned off when not in use to mitigate security risks associated with the IPMI protocol (CVE-2013-4786). For more information, see https://nvd.nist.gov/vuln/detail/CVE-2013-4786.

Login

Use the following recommendations when applying login settings for IPMI users:

Table 11-1 Login security settings

Settings	Recommended values
Failed login attempts	3
User Lockout time (min)	60 seconds
Force HTTPS	Yes Enable **Force HTTPS** to ensure that the IPMI connection always takes place over HTTPS.
Web Session Timeout	1800

LDAP Settings

Veritas recommends that you enable LDAP authentication.

SSL Upload

Veritas recommends that you import a new or a custom SSL certificate.

Remote Session

Table 11-2 Remote session security settings

Settings	Recommended value
KVM Encryption	AES-256
Media Encryption	Enable

You can also log in to the appliance shell menu by using iKVM over HTML5.

Note: The HTML5 option is available only on appliances with firmware (BIOS) versions 00.01.0016 or later.

Cipher recommendation

To help prevent IPMI user actions or activity with no authentication, specific ciphers should be disabled. For further assistance, contact Technical Support and inform the representative to reference article number 000127964.

Ethernet connection settings

Use a dedicated Ethernet connection for IPMI and avoid sharing the physical server connection.

- Use a static IP.
- Avoid using DHCP.

RMM ports

The following ports become visible when you configure the Remote Management Module.

Table 11-3 RMM ports

Port	Service	Description	Default state on 5240	Default state on 5340
80	HTTP	Out-of-band management (ISM+ or RM*)	Disabled	Disabled
443	HTTP	Out-of-band management (ISM+ or RM*)	Enabled	Enabled
5120	RMM	ISO & CD-ROM redirection	Enabled	Disabled

Table 11-3 RMM ports *(continued)*

Port	Service	Description	Default state on 5240	Default state on 5340
5124	RMM (Secured)	CDROM	Disabled	Enabled
22 or 66	SSH		Disabled	Disabled
(UDP) 623	IPMI over LAN		Disabled	Disabled
Ports specific to 5340				
5900	KVM	CLI access, ISO & CDROM redirection	N/A	Disabled
5902	KVM (Secured)	CLI access, ISO & CDROM redirection	N/A	Enabled
623	RMM	Floppy redirection	N/A	Disabled
627	RMM (Secured)	Floppy redirection	N/A	Enabled
Ports specific to 5240				
7578	KVM	CLI access	Enabled	N/A
7582	KVM (Secured)	CLI access	Disabled	N/A
5123	RMM	Floppy redirection	Enabled	N/A
5127	RMM (Secured)	USB or floppy	Disabled	N/A

+ NetBackup Integrated storage manager

* Veritas Remote Management – Remote Console

Note: Ports 7578, 5120, and 5123 are for the unencrypted mode. Ports 7582, 5124, and 5127 are for the encrypted mode.

Enabling SSH on the Remote Management Module

During installation, port 20 (ssh) is blocked automatically for IPMI on the Remote Management Module. Follow these steps to enable SSH.

To enable SSH on the Remote Management Module

1. Log in to the Veritas Remote Management Module.
2. On the **Configuration** tab, in the left pane, select **Security Settings**.
3. Under **Optional Network Services**, select the **Enable** check box next to **SSH**.
4. Click **Save**.

Replacing the default IPMI SSL certificate

Veritas 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, Veritas.
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=Veritas/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 Log in to your Veritas 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 Veritas Remote Management (IPMI web interface) interface to verify that the new certificate is being presented.

Chapter 12

STIG and FIPS conformance

This chapter includes the following topics:

- OS STIG hardening for NetBackup appliance
- Unenforced STIG hardening rules
- FIPS 140-2 conformance for NetBackup appliance

OS STIG hardening for NetBackup appliance

The Security Technical Implementation Guides (STIGs) provide technical guidance for increasing the security of information systems and software to help prevent malicious computer attacks. This type of security is also referred to as hardening.

Starting with software version 3.1, you can enable OS STIG hardening rules for increased security. These rules are based on the following profile from the Defense Information Systems Agency (DISA):

STIG for Red Hat Enterprise Linux 7 Server - Version 0.1.43

To enable these rules, use the following command:

`Main_Menu > Settings > Security > Stig Enable`, followed by the maintenance password.

Note the following about enabling STIG:

- When the option is enabled, a list of the enforced rules appears. The command output also shows exceptions to any rules that are not enforced.
- This command does not allow individual rule control.

- For appliances (nodes) in a high availability (HA) setup, this feature must be enabled manually on each node to ensure correct operation after a switchover.
- Once the option is enabled, a factory reset is required to disable the associated rules.
- If Lightweight Directory Access Protocol (LDAP) is configured, it is recommended that you set it up to use Transport Layer Security (TLS) before you enable the option.

Note: If you have enabled the STIG feature on an appliance and you need to upgrade it or install an EEB on it, do not plan such installations during the 4:00am - 4:30am time frame. By following this best practice, you can avoid interrupting the automatic update of the `AIDE` database and any monitored files, which can cause multiple alert messages from the appliance.

The following describes the hardening rules that are enforced after the option is enabled. Each rule is identified by a Common Configuration Enumerator (CCE) identifier, a short rule description, and a Security Content Automation Protocol (SCAP) scanner severity level. Software version 3.1 addresses rules with high and medium scanner severity levels.

Rules enforced after enabling the option

- CCE-27127-0: Enable randomized layout of virtual address space.
  Scanner severity level: Medium
- CCE-26900-1: Disable core dumps for `SUID` programs.
  Scanner severity level: Low
- CCE-27050-4: Restrict access to kernel message buffer.
  Scanner severity level: Low
- CCE-80258-7: Disable the `kdump` kernel crash analyzer.
  Scanner severity level: Medium
- CCE-27220-3: Build and test `AIDE` database.
  Scanner severity level: Medium
- CCE-26952-2: Configure periodic execution of `AIDE`.
  Scanner severity level: Medium
- CCE-27303-7: Modify the system login banner.
  Scanner severity level: Medium
- CCE-27082-7: Set SSH client alive account.
  Scanner severity level: Medium

- CCE-27314-4: Enable SSH warning banner.
  Scanner severity level: Medium
- CCE-27437-3: Ensure that `auditd` collects information on the use of privileged commands.
  Scanner severity level: Medium
- CCE-27309: Set boot loader password.
  Scanner severity level: High
- CCE-80374-2: Configure notification of `AIDE` scan results.
  Scanner security level: Medium
- CCE-80375-9: Configure AIDE to verify Access Control Lists (ACLs).
  Scanner severity level: Medium
- CCE-80376-7: Configure AIDE to verify extended attributes.
  Scanner severity level: Medium
- CCE-27375-5: Configure `auditd_space_left_action` on low disk space.
  Scanner severity level: Medium
- CCE-27341-7: Configure `auditd` to use `audispd_syslog_plugin`.
  Scanner security level: Medium
- CCE-27353-2: Record events that modify the system discretionary access controls (`fremovexattr`).
  Scanner severity level: Medium
- CCE-27410-0: Record events that modify the system discretionary access controls (`lremovexattr`).
  Scanner severity level: Medium
- CCE-27367-2: Record events that modify the system discretionary access controls (`removexattr`).
  Scanner severity level: Medium
- CCE-27204-7: Record attempts to alter the logon and logout events.
  Scanner severity level: Medium
- CCE-27347-4: Ensure that `auditd` collects unauthorized access attempts to files.
  Scanner severity level: Medium
- CCE-27447-2: Ensure that `auditd` collects information on successful exporting to media.
  Scanner severity level: Medium
- CCE-27206-2: Ensure that `auditd` collects file deletion events by the user.

Scanner severity level: Medium

- CCE-27129-6: Ensure that `auditd` collects information on kernel module loading and unloading.
  Scanner severity level: Medium
- CCE-27333-4: Set the password rule for maximum consecutive repeating characters.
  Scanner severity level: Medium
- CCE-27512-3: Set the password rule for maximum consecutive repeating characters from the same character class.
  Scanner severity level: Medium
- CCE-27214-6: Set the password strength for minimum digit (numeric) characters.
  Scanner severity level: Medium
- CCE-27293-0: Set the password rule for minimum length.
  Scanner severity level: Medium
- CCE-27200-5: Set the password strength for minimum uppercase characters.
  Scanner severity level: Medium
- CCE-27360-7: Set the password strength for minimum special characters.
  Scanner severity level: Medium
- CCE-27345-8: Set the password strength for minimum lowercase characters.
  Scanner severity level: Medium
- CCE-26631-2: Set the password strength for minimum different characters.
  Scanner severity level: Medium
- CCE-27115-5: Disable `modprobe` loading of the USB storage driver.
  Scanner severity level: Medium
- CCE-27350-8: Set the number of failed password attempts to deny access.
  Scanner severity level: Medium
- CCE-80353-6: Configure the root account for failed password attempts.
  Scanner severity level: Medium
- CCE-27297-1: Set the interval for counting failed password attempts.
  Scanner severity level: Medium
- CCE-27002-5: Set the password minimum age.
  Scanner severity level: Medium
- CCE-27051-2: Set the password maximum age.
  Scanner security level: Medium

- CCE-27081-9: Limit the number of concurrent login sessions allowed for each user.
  Scanner severity level: Low
- CCE-80522-6: Set the maximum age (period of time after which the set password expires and must be changed) for the existing password.
  Scanner severity level: Medium
- CCE-80521-8: Set the minimum age (period of time a password must be used before it can be changed) for the existing password .
  Scanner severity level: Medium
- CCE-27339-1: Record the events that modify the system's discretionary access controls (chmod).
  Scanner severity level: Medium
- CCE-27364-9: Record the events that modify the system's discretionary access controls (chown).
  Scanner severity level: Medium
- CCE-27393-8: Record the events that modify the system's discretionary access controls (fchmod).
  Scanner severity level: Medium
- CCE-27388-8: Record the events that modify the system's discretionary access controls (fchmodat).
  Scanner severity level: Medium
- CCE-27356-5: Record the events that modify the system's discretionary access controls (fchown).
  Scanner severity level: Medium
- CCE-27387-0: Record the events that modify the system's discretionary access controls (fchownat).
  Scanner severity level: Medium
- CCE-27389-6: Record the events that modify the system's discretionary access controls (fsetxattr).
  Scanner severity level: Medium
- CCE-27083-5: Record the events that modify the system's discretionary access controls (lchown).
  Scanner severity level: Medium
- CCE-27280-7: Record the events that modify the system's discretionary access controls (lsetxattr).
  Scanner severity level: Medium

- CCE-27213-8: Record the events that modify the system's discretionary access controls (setxattr).
  Scanner severity level: Medium
- CCE-27206-2: Ensure that `auditd` collects file deletion events executed by the user (rename).
  Scanner severity level: Medium
- CCE-80413-8: Ensure that `auditd` collects file deletion events executed by the user (renameat).
  Scanner severity level: Medium
- CCE-80412-0: Ensure that `auditd` collects file deletion events executed by the user (rmdir).
  Scanner severity level: Medium
- CCE-27206-2: Ensure that `auditd` collects file deletion events executed by the user (unlink).
  Scanner severity level: Medium
- CCE-80662-0: Ensure that `auditd` collects file deletion events executed by the user (unlinkat).
  Scanner severity level: Medium
- CCE-80446-8: Ensure that `auditd` collects information on kernel module loading (insmod).
  Scanner severity level: Medium
- CCE-80417-9: Ensure that `auditd` collects information on kernel module loading and unloading (modprobe).
  Scanner severity level: Medium
- CCE-80416-1: Ensure that `auditd` collects information on kernel module unloading (rmmod).
  Scanner severity level: Medium
- CCE-80384-1: Record attempts to alter logon and logout events (lastlog).
  Scanner severity level: Medium
- CCE-80382-5: Record attempts to alter logon and logout events (tallylog).
  Scanner severity level: Medium
- CCE-80398-1: Ensure that `auditd` collects information on the use of privileged commands (chage).
  Scanner severity level: Medium
- CCE-80404-7: Ensure that `auditd` collects information on the use of privileged commands (chsh).

Scanner severity level: Medium

- CCE-80410-4: Ensure that `auditd` collects information on the use of privileged commands (crontab).
  Scanner severity level: Medium
- CCE-80397-3: Ensure that `auditd` collects information on the use of privileged commands (gpasswd).
  Scanner severity level: Medium
- CCE-80403-9: Ensure that `auditd` collects information on the use of privileged commands (newgrp).
  Scanner severity level: Medium
- CCE-80411-2: Ensure that `auditd` collects information on the use of privileged commands (pam_timestamp_check).
  Scanner severity level: Medium
- CCE-80395-7: Ensure that `auditd` collects information on the use of privileged commands (passwd).
  Scanner severity level: Medium
- CCE-80406-2: Ensure that `auditd` collects information on the use of privileged commands (postdrop).
  Scanner severity level: Medium
- CCE-80407-0: Ensure that `auditd` collects information on the use of privileged commands (postqueue).
  Scanner severity level: Medium
- CCE-80408-8: Ensure that `auditd` collects information on the use of privileged commands (ssh-keysign).
  Scanner severity level: Medium
- CCE-80400-5: Ensure that `auditd` collects information on the use of privileged commands (su).
  Scanner severity level: Medium
- CCE-80401-3: Ensure that `auditd` collects information on the use of privileged commands (sudo).
  Scanner severity level: Medium
- CCE-80405-4: Ensure that `auditd` collects information on the use of privileged commands (umount).
  Scanner severity level: Medium
- CCE-80396-5: Ensure that `auditd` collects information on the use of privileged commands (unix_chkpwd).

Scanner severity level: Medium

- CCE-80399-9: Ensure that `auditd` collects information on the use of privileged commands (userhelper).
  Scanner severity level: Medium
- CCE-27461-3: Ensure that `auditd` collects system administrator actions.
  Scanner severity level: Medium
- CCE-80433-6: Record the events that modify user/group information (`/etc/group`).
  Scanner severity level: Medium
- CCE-80432-8: Record the events that modify user/group information (`/etc/gshadow`).
  Scanner severity level: Medium
- CCE-80430-2: Record the events that modify user/group information (`/etc/security/opasswd`).
  Scanner severity level: Medium
- CCE-80435-1: Record the events that modify user/group information (`/etc/passwd`).
  Scanner severity level: Medium
- CCE-80431-0: Record the events that modify user/group information (`/etc/shadow`).
  Scanner severity level: Medium
- CCE-27309-4: Set boot loader password in grub2.
  Scanner severity level: High
- CCE-80377-5: Configure aide to use fips 140-2 for validating hashes.
  Scanner severity level: Medium

Rules always enforced

The following rules are always enforced and cannot be disabled. Hardening of these rules complies with the specifications described in "NIST Special Publication 800-123". For more information, refer to the following:

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

- CCE-80165-4: Configure the kernel parameter to ignore ICMP broadcast echo requests.
  Scanner severity level: Medium
- CCE-80156-3: Disable the kernel parameter for sending ICMP redirects by default.
  Scanner severity level: Medium

- CCE-80156-3: Disable the kernel parameter for sending ICMP redirects for all interfaces.
  Scanner severity level: Medium
- CCE-27212-0: Enable auditing for the processes that start before the audit daemon.
  Scanner severity level: Medium
- CCE-26957-1: Ensure that the Red Hat GPG key is installed.
  Scanner severity level: High
- CCE-27096-7: Ensure that the `AIDE` package is installed.
  Scanner severity level: Medium
- CCE-27351-6: Install the `screen` package.
  Scanner severity level: Medium
- CCE-27268-2: Restrict serial port root logins.
  Scanner severity level: Low
- CCE-27318-5: Restrict virtual console root logins.
  Scanner severity level: Medium
- CCE-27401-9: Disable `telnet` service
  Scanner severity level: High
- CCE-27471-2: Disable SSH access without a password.
  Scanner severity level: High
- CCE-27286-4: Prevent login to accounts without a password.
  Scanner severity level: High
- CCE-27511-5: Disable **Ctrl-Alt-Del** reboot activation.
  Scanner severity level: High
- CCE-27320-1: Allow only SSH protocol version 2.
  Scanner severity level: High
- CCE-27294-8: Do not allow direct root logins.
  Scanner severity level: Medium
- CCE-80157-1: Disable the kernel parameter for IP forwarding.
  Scanner severity level: Medium
- CCE-80158-9: Configure the kernel parameter for accepting ICMP redirects for all interfaces.
  Scanner severity level: Medium
- CCE-80163-9: Configure the kernel parameter for accepting ICMP redirects by default.

Scanner severity level: Medium

- CCE-27327-6: Disable the Bluetooth kernel modules.
  Scanner severity level: Medium
- CCE-80179-5: Configure the kernel parameter for accepting source-routed packets for all interfaces.
  Scanner severity level: Medium
- CCE-80220-7: Disable the GSSAPI authentication.
  Scanner severity level: Medium
- CCE-80221-5: Disable the Kerberos authentication.
  Scanner severity level: Medium
- CCE-80222-3: Enable the use of strict mode checking.
  Scanner severity level: Medium
- CCE-80224-9: Disable compression or set compression to delayed.
  Scanner severity level: Medium
- CCE-27455-5: Use only FIPS approved MACs.
  Scanner severity level: Medium
- CCE-80378-3: Verify the user that owns `/etc/cron.allow`.
  Scanner severity level: Medium
- CCE-80379-1: Verify the group that owns `/etc/cron.allow`.
  Scanner severity level: Medium
- CCE-80372-6: Disable SSH support for user-known hosts.
  Scanner severity level: Medium
- CCE-80373-4: Disable SSH support for `rhosts` RSA authentication.
  Scanner severity level: Medium
- CCE-27363-1: Do not allow SSH environment options.
  Scanner severity level: Medium
- CCE-26989-4: Ensure that `gpgcheck` is globally activated.
  Scanner severity level: High
- CCE-80349--4: Ensure that the installed OS is certified.
  Scanner severity level: High
- CCE-27175-9: No UID except zero.
  Scanner severity level: High
- CCE-27498-5: Disable the auto-mounter.
  Scanner severity level: Medium

- CCE-80134-0: No files not owned by user.
  Scanner severity level: Medium
- CCE-80135-7: No file permissions not owned by group.
  Scanner severity level: Medium
- CCE-27211-2: `sysctl_kernal_exec_shield`.
  Scanner severity level: Medium
- CCE-27352-4: Verify that all account password hashes are shadowed.
  Scanner severity level: Medium
- CCE-27104-9: Set the password hashing algorithm `systemauth`.
  Scanner severity level: Medium
- CCE-27124-7: Set the password hashing algorithm `logindefs`.
  Scanner severity level: Medium
- CCE-27053-8: Set the password hashing algorithm `libusercon`.
  Scanner severity level: Medium
- CCE-27078-5: Disable pre-linking software.
  Scanner severity level: Low
- CCE-27116-3: Install the PAE kernel on supported 32-bit x86 systems.
  Scanner severity level: Low
- CCE-27503-2: All GIDs referenced in `/etc/password` must be defined in `/etc/group`.
  Scanner severity level: Low
- CCE-27160-1: Password pam retry.
  Scanner severity level: Low
- CCE-27275-7: Display login attempts.
  Scanner severity level: Low
- CCE-80350-2: Remove `no_authenticate` on `sudo`.
  Scanner severity level: Medium
- CCE-26961-3: Ensure that SELinux is not disabled in `/etc/default/grub`.
  Scanner severity level: Medium
- CCE-80245-4: Uninstall the `vsftpd` package.
  Scanner severity level: High
- CCE-80216-5: Enable the OpenSSH service.
  Scanner severity level: Medium
- CCE-27407-6: Enable the `auditd` service.

Scanner severity level: Medium

- CCE-27361-5: Verify that firewalld is enabled.
  Scanner severity level: Medium
- CCE-80544-0: Ensure that users cannot change GNOME3 session idle settings.
  Scanner severity level: Medium
- CCE-80371-8: Ensure that users cannot change GNOME3 screensaver settings.
  Scanner severity level: Medium
- CCE-80563-0: Ensure that users cannot change GNOME3 screensaver lock after idle period.
  Scanner severity level: Medium
- CCE-80112-6: Enable GNOME3 screensaver lock after idle period.
  Scanner severity level: Medium
- CCE-80370-0: Set GNOME3 screensaver lock delay after activation period.
  Scanner severity level: Medium
- CCE-80110-0: Set GNOME3 screensaver inactivity timeout.
  Scanner severity level: Medium
- CCE-80564-8: Ensure that users cannot change the GNOME3 screensaver idle activation.
  Scanner severity level: Medium
- CCE-80162-1: Configure the kernel parameter for accepting source-routed packets by default.
  Scanner severity level: Medium
- CCE-80111-8: Enable GNOME3 screensaver idle activation.
  Scanner severity level: Medium
- CCE-80105-0: Disable GDM guest login.
  Scanner severity level: High
- CCE-80104-3: Disable GDM automatic login.
  Scanner severity level: High
- CCE-80108-4: Enable the GNOME3 login smartcard authentication.
  Scanner severity level: Medium
- CCE-27279-9: Configure the SELinux policy.
  Scanner severity level: High
- CCE-80148-0: Add the `nosuid` option to removable media partitions.
  Scanner severity level: Low

- CCE-80136-5: Ensure that all world-writable directories are owned by a system account.
  Scanner severity level: Low
- CCE-80174-6: Ensure that the system is not acting as a network sniffer.
  Scanner severity level: Medium
- CCE-80438-5: Configure multiple DNS servers in `/etc/resolv.conf`.
  Scanner severity level: Low
- CCE-27358-1: Deactivate wireless network interfaces.
  Scanner severity level: Medium
- CCE-27287-2: Require authentication for Single User mode.
  Scanner severity level: Medium
- CCE-27434-0: Configure the kernel parameter for accepting IPv4 source-routed packets for all interfaces.
  Scanner severity level: Medium
- CCE-80447-6: Configure the Firewalld Ports.
  Scanner severity level: Medium
- CCE-80380-9: Ensure that `cron` is able to log in to Rsyslog.
  Scanner severity level: Medium
- CCE-80354-4: Set the UEFI boot loader password.
  Scanner severity level: Medium
- CCE-80517-6: Boat loader is not installed on removeable media.
  Scanner severity level: Medium
- CCE-27394-6: Configure the `auditd` mail_acct action on low disk space.
  Scanner severity level: Medium
- CCE-80434-4: Ensure that home directories are created for new users.
  Scanner severity level: Medium
- CCE-80536-6: Ensure that the default umask is set correctly for interactive users.
  Scanner severity level: Medium
- CCE-26923-3: Limit password reuse.
  Scanner severity level: Medium
- CCE-26892-0: Set the GNOME3 login warning banner text.
  Scanner severity level: Medium
- CCE-26970-4: Enable GNOME3 login warning banner.
  Scanner severity level: Medium

- CCE-27218-7: Remove the X Windows package group.
  Scanner severity level: Medium
- CCE-80215-7: Install the OpenSSH server package.
  Scanner severity level: Medium
- CCE-27311-0: Verify Permissions on SSH Server public *.pub key files.
  Scanner severity level: Medium
- CCE-27485-2: Verify Permissions on SSH Server private *_key key files.
  Scanner severity level: Medium
- CCE-80223-1: Enable Use of Privilege Separation.
  Scanner severity level: Medium
- CCE-27295-5: Use Only FIPS 140-2 Validated Ciphers.
  Scanner severity level: Medium
- CCE-80225-6: Enable SSH Print Last Log.
  Scanner severity level: Medium
- CCE-27445-6: Disable SSH root login.
  Scanner severity level: Medium
- CCE-27377-1: Disable SSH support for .rhosts files.
  Scanner severity level: Medium
- CCE-27413-4: Disable host-based authentication.
  Scanner severity level: Medium
- CCE-27458-9: Mount remote file systems with Kerberos Security.
  Scanner severity level: Medium
- CCE-80214-0: Ensure tftp daemon uses secure mode.
  Scanner severity level: Medium
- CCE-80213-2: Uninstall the tftp-server package.
  Scanner severity level: High
- CCE-27165-0: Uninstall the telnet-server package.
  Scanner severity level: High
- CCE-27342-5: Uninstall the rsh-server package.
  Scanner severity level: High
- CCE-80514-3: Remove user host-based authentication files.
  Scanner severity level: High
- CCE-80513-5: Remove host-based authentication files.
  Scanner severity level: High

- CCE-27399-5: Uninstall the `ypserv` package.
  Scanner severity level: High
- CCE-80240-5: Mount remote file systems with `nosuid`.
  Scanner severity level: Medium
- CCE-80436-9: Mount remote file systems with `noexec`.
  Scanner severity level: Medium
- CCE-80205-8: Ensure that the default umask is set correctly in `login.defs`.
  Scanner severity level: Medium

See “Unenforced STIG hardening rules” on page 125.

Unenforced STIG hardening rules

This topic describes the Security Technical Implementation Guide (STIG) rules that are not currently enforced on NetBackup appliance. Rules in this list may not be enforced for reasons including, but not limited to the following:

- Enforcement of the rule is planned for a future appliance software release.
- An alternate method is used to provide protection that meets or exceeds the method described in the rule.
- The method described in the rule is not used or supported on NetBackup appliance.

The following describes the STIG rules that are not currently enforced:

- CCE-26876-3: Ensure that `gpgcheck` is enabled for all `yum` package repositories.
  Scanner severity level: High
- CCE-27209-6: Verify and correct the file permissions for the rpm.
  Scanner severity level: High
- CCE-27157-7: Verify file hashes with rpm.
  Scanner severity level: High
- CCE-80127-4: Install McAfee Antivirus
  Scanner severity level: High
- CCE-26818-5: Install intrusion detection software.
  Scanner severity level: High
- CCE-27334-2: Ensure SELinux state is enforcing.
  Scanner severity level: High
- CCE-80226-4: Enable encrypted X11 forwarding.
  Scanner severity level: High

- CCE-27386-2: Ensure that the default SNMP password is not used.
  Scanner severity level: High
- CCE-80126-6: Install the Asset Configuration Compliance Module (ACCM).
  Scanner severity level: Medium
- CCE-80369-2: Install the Policy Auditor (PA) module.
  Scanner severity level: Medium
- CCE-27277-3: Disable `modprobe` loading of the USB storage driver.
  Scanner severity level: Medium
- CCE-27349-0: Set default `firewalld` zone for incoming packets.
  Scanner severity level: Medium
- CCE-80170-4: Install `libreswan` package.
  Scanner severity level: Medium
- CCE-80223-1: Enable use of privilege separation.
  Scanner severity level: Medium
- CCE-80347-8: Ensure that `gpgcheck` is enabled for local packages.
  Scanner severity level: High
- CCE-80348-6: Ensure that `gpgcheck` is enabled for repository metadata.
  Scanner severity level: High
- CCE-80358-5: Install the `dracut_fips` package.
  Security scanner level: Medium
- CCE-80359-3: Enable FIPS mode in the `GRand Unified Bootloader` version 2 (GRUB2).
  Scanner severity level: Medium
- CCE-27557-8: Set an interactive session timeout to terminate idle sessions.
  Scanner severity level: Medium
- CCE-80377-5: Configure AIDE to FIPS 140-2 for validating hashes.
  Scanner severity level: Medium
- CCE-80351-0: Ensure that users re-authenticate for privilege escalation (`sudo_NOPASSWD`).
  Scanner severity level: Medium
- CCE-27355-7: Set account expiration following inactivity.
  Scanner severity level: Medium
- CCE-80207-4: Enable smart card login.
  Scanner severity level: Medium
- CCE-27370-6: Configure `auditd_admin_space_left_action` on low disk space.

Security scanner level: Medium

- CCE-27295-5: Use only approved ciphers.
  Scanner severity level: Medium
- CCE-26548-8: Disable kernel support for USB from the `bootloader` configuration.
  Scanner severity level: Low
- CCE-27128-8: Encrypt partitions.
  Scanner severity level: High
- CCE-26895-3: Ensure that software patches are installed.
  Scanner security level: High
- CCE-27279-9: Configure the SE Linux policy.
  Scanner severity level: High
- CCE-27399-5: Uninstall the `ypserv` package.
  Scanner severity level: High
- CCE-80128-2: Enable service nails.
  Scanner severity level: Medium
- CCE-80129-0: Update virus scanning definitions.
  Scanner severity level: Medium
- CCE-27288-0: Make sure that no daemons are unconfined by SE Linux. Make sure that all daemons are confined by SE Linux.
  Scanner severity level: Medium
- CCE-27326-8: Make sure that no device files are unlabeled by SE Linux./Make sure that all device files are labeled by SE Linux.
  Scanner severity level: Medium
- CCE-80354-4: Set the UEFI boot loader password.
  Scanner severity level: Medium
- CCE-80171-2: Verify any configured `IPSec` tunnel connections.
  Scanner severity level: Medium
- CCE-26960-5: Disable booting from USB devices in boot firmware.
  Scanner severity level: Low
- CCE-27194-0: Assign a password to prevent changes to the boot firmware configuration.
  Scanner severity level: Low
- CCE-80516-8: Configure the SSSD LDAP backend client CA certificate.
  Scanner severity level: Medium
- CCE-80515-0: Configure the SSSD LDAP backend client CA certificate location.

Scanner severity level: Medium

- CCE-80546-5: Configure the SSSD LDAP backend to use TLS for all transactions.
  Scanner severity level: Medium
- CCE-80437-7: Configure PAM in SSSD services.
  Scanner severity level: Medium
- CCE-80519-2: Install smart card packages for multi factor authentication.
  Scanner severity level: Medium
- CCE-80520-0: Configure certificate status checking for smart cards.
  Scanner severity level: Medium
- CCE-80526-7: User initialization files must be group-owned by the primary user.
  Scanner severity level: Medium
- CCE-80523-4: User initialization files must not run world-writable programs.
  Scanner severity level: Medium
- CCE-80527-5: User initialization files must be owned by the primary user.
  Scanner severity level: Medium
- CCE-80524-2: Ensure that the user's path contains only local directories.
  Scanner severity level: Medium
- CCE-80528-3: All interactive users must have a defined home directory.
  Scanner severity level: Medium
- CCE-80529-1: All interactive users home directories must exist.
  Scanner severity level: Medium
- CCE-80534-1: All user files and directories in the home directory must be group-owned by the primary user.
  Scanner severity level: Medium
- CCE-80533-3: All user files and directories in the home directory must be owned by the primary user.
  Scanner severity level: Medium
- CCE-80535-8: All user files and directories in the home directory must have permissions set to mode 0750 or less.
  Scanner severity level: Medium
- CCE-80532-5: All interactive user home directories must be group-owned by the primary user.
  Scanner severity level: Medium
- CCE-80531-7: All interactive user home directories must be owned by the primary user.

Scanner severity level: Medium

- CCE-80525-9: Ensure that all user initialization files have permissions set to mode 0740 or less.
  Scanner severity level: Medium
- CCE-80530-9: All interactive user home directories must have permissions set to mode 0750 or less.
  Scanner severity level: Medium
- CCE-80393-2: Record any attempts to run `chcon`.
  Scanner severity level: Medium
- CCE-80391-6: Record any attempts to run `semanage`.
  Scanner severity level: Medium
- CCE-80660-4: Record any attempts to run `setfiles`.
  Scanner severity level: Medium
- CCE-80392-4: Record any attempts to run `setsebool`.
  Scanner severity level: Medium
- CCE-80661-2: Ensure that `auditd` collects information on kernel module loading (create_module).
  Scanner severity level: Medium
- CCE-80415-3: Ensure that `auditd` collects information on kernel module unloading (delete_module).
  Scanner severity level: Medium
- CCE-80547-3: Ensure that `auditd` collects information on kernel module loading and unloading (finit_module).
  Scanner severity level: Medium
- CCE-80414-6: Ensure that `auditd` collects information on kernel module loading (init_module).
  Scanner severity level: Medium
- CCE-80383-3: Record attempts to alter logon and logout events (faillock).
  Scanner severity level: Medium
- CCE-80402-1: Ensure that `auditd` collects information on the use of privileged commands (sudoedit).
  Scanner severity level: Medium
- CCE-80385-8: Record unauthorized (unsuccessful) access attempts to files (create).
  Scanner severity level: Medium

- CCE-80390-8: Record unauthorized (unsuccessful) access attempts to files (ftruncate).
  Scanner severity level: Medium
- CCE-80386-6: Record unauthorized (unsuccessful) access attempts to files (open).
  Scanner severity level: Medium
- CCE-80388-2: Record unauthorized (unsuccessful) access attempts to files (open_by_handle_at).
  Scanner severity level: Medium
- CCE-80387-4: Record unauthorized (unsuccessful) access attempts to files (openat).
  Scanner severity level: Medium
- CCE-80389-0: Record unauthorized (unsuccessful) access attempts to files (truncate).
  Scanner severity level: Medium
- CCE-80381-7: Shutdown system when auditing failures occur.
  Scanner severity level: Medium
- CCE-80439-3: Configure the time service maxpoll interval.
  Scanner severity level: Low
- CCE-80541-6: Configure `audispd` plugin to send logs to remote server.
  Scanner severity level: Medium
- CCE-80539-0: Configure the `disk_full_action` option in the `audispd's` plugin.
  Scanner severity level: Medium
- CCE-80540-8: Encrypt audit records sent with the `audispd` plugin.
  Scanner severity level: Medium
- CCE-80538-2: Configure the `network_failure_action` option in the `audispd's` plugin.
  Scanner severity level: Medium
- CCE-80542-4: Configure `firewalld` to rate limit connections.
  Scanner severity level: Medium
- CCE-26828-4: Disable DCCP support.
  Scanner severity level: Medium
- CCE-81153-9: Add the nosuid option to `/home`.
  Scanner severity level: Low
- CCE-80543-2: Map system users to the appropriate SELinux role.
  Scanner severity level: Medium

- CCE-80545-7: Verify and correct ownership of an rpm.
  Scanner severity level: High
- CCE-80512-7: Prevent unrestricted mail relaying.
  Scanner severity level: Medium
- CCE-26884-7: Set the lockout time for failed password attempts.
  Scanner severity level: Medium

See "OS STIG hardening for NetBackup appliance" on page 111.

FIPS 140-2 conformance for NetBackup appliance

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for validating cryptography modules. The FIPS 140-2 standard specifies the security requirements for cryptographic modules and applies to both the hardware and the software components. It also describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information about the FIPS 140-2 standard and its validation program, click on the following links:

https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

https://csrc.nist.gov/projects/cryptographic-module-validation-program

The NetBackup Cryptographic Module is FIPS validated. NetBackup MSDP and VxOS (Veritas Operating System) use this module and starting with NetBackup Appliance release 3.1.1, you can enable the FIPS 140-2 standard for NetBackup MSDP. Starting with NetBackup Appliance release 3.1.2, you can enable the FIPS 140-2 standard for VxOS.

Once FIPS for VxOS is enabled, the `sshd` uses the following FIPS approved ciphers:

- aes128-ctr
- aes192-ctr
- aes256-ctr

Older SSH Clients are likely to prevent access to the appliance after FIPS for VxOS is enabled. Check to make sure that your SSH client supports the listed ciphers, and upgrade to the latest version if necessary. Default cipher settings are not typically FIPS-compliant, which means you may need to select them manually in your SSH client configuration.

You can enable the FIPS 140-2 standard for NetBackup MSDP and VxOS with the following commands:

- `Main Menu > Settings > Security > FIPS Enable MSDP`, followed by the maintenance password.
  Enabling or disabling the `MSDP` option terminates all jobs that are currently in progress and restarts the NetBackup services. As a best practice, it is recommended that you first stop all jobs manually before you enable or disable this feature.

  Note: If you have upgraded from a previous version of NetBackup appliance, ensure that you enable MSDP only after your existing data has been converted to use FIPS compliant algorithms. To check the current status of the data conversion use the `crcontrol --dataconvertstate` command. Enabling MSDP before the status is set to **Finished** can cause data restoration failures.

- `Main Menu > Settings > Security > FIPS Enable VxOS`, followed by the maintenance password.
  Enabling or disabling the `VxOS` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.
- `Main Menu > Settings > Security > FIPS Enable All`, followed by the maintenance password.
  Enabling or disabling the `All` option reboots the appliance and disconnects all logged in users from their sessions. As a best practice, it is recommended that you provide advanced notice to all users before you enable or disable this feature.

Note: In a NetBackup Appliance high availability (HA) setup, you can enable the FIPS feature on both nodes only after you have completed configuration of the HA setup. The FIPS configuration must match on both the nodes. If FIPS is enabled on either node before the HA setup is completed, you must disable FIPS on that node before you complete the HA setup.

For complete information about FIPS commands, see the *NetBackup Appliance Commands Reference Guide*.

Appendix A

Security release content

This appendix includes the following topics:

- NetBackup Appliance security release content

NetBackup Appliance security release content

The following list contains the known security issues that were fixed and that are now included in this release of NetBackup appliance software:

General release content for version 3.2

The appliance software has been updated to the RHEL7.6 Kernel. Many packages and libraries have been updated that address the following security vulnerabilities:

CVE-2017-3735

CVE-2018-0495

CVE-2018-0732

CVE-2018-0737

CVE-2018-0739

CVE-2018-1092

CVE-2018-1094

CVE-2018-1118

CVE-2018-1120

CVE-2018-1130

CVE-2018-1259

CVE-2018-5344

CVE-2018-5391

CVE-2018-5407

CVE-2018-5743

CVE-2018-5803

CVE-2018-5848

CVE-2018-7208

CVE-2018-7456

CVE-2018-7568

CVE-2018-7569

CVE-2018-7642

CVE-2018-7643

CVE-2018-7740

CVE-2018-7757

CVE-2018-8781

CVE-2018-8905

CVE-2018-8945

CVE-2018-10322

CVE-2018-10372

CVE-2018-10373

CVE-2018-10534

CVE-2018-10535

CVE-2018-10689

CVE-2018-10844

CVE-2018-10845

CVE-2018-10846

CVE-2018-10878

CVE-2018-10879

CVE-2018-10881

CVE-2018-10883

CVE-2018-10902

CVE-2018-10940

CVE-2018-12327

CVE-2018-13033

CVE-2018-13405

CVE-2018-14348

CVE-2018-14618

CVE-2018-16838

CVE-2018-16843

CVE-2018-16845

CVE-2018-16871

CVE-2018-16884

CVE-2018-17101

CVE-2018-18311

CVE-2018-18397

CVE-2018-18557

CVE-2018-18559

CVE-2018-18661

CVE-2018-19039

CVE-2018-20699

CVE-2018-1000026

CVE-2019-3778

CVE-2019-3811

CVE-2019-3813

CVE-2019-3862

CVE-2019-3880

CVE-2019-5953

CVE-2019-6133

CVE-2019-6454

CVE-2019-9824

CVE-2019-10160

CVE-2019-11085

CVE-2019-11811

CVE-2019-1000020

Index

A

Active Directory user
    configure authentication 23
AD supported users
    configure server 26
    pre-requisites 26
appliance log files
    Browse command 58
appliance ports 89
appliance security
    about 7
authentication
    AD 18
    LDAP 18
    local user 18
    NIS
        Kerberos 18
authorization 37
    Administrator 42
    NetBackupCLI user 43
AutoSupport
    customer registration 94

B

Browse command
    appliance log files 58

C

Call Home
    alerts 95
    workflow 99
Call Home proxy server
    configuring 98
collect logs
    commands 57
    datacollect 59
    log file location 57
    types of logs 57

D

data classification 70
data encryption 70
    KMS support 71
data integrity 69
    CRC verification 70
    end-to-end verification 69
data security 68
datacollect
    device logs 59

I

intrusion detection system
    about 50
intrusion prevention system
    about 49
IPMI security
    recommendations 102
IPMI SSL certificate 106
IPsec
    network security 86

K

Kerberos
    authenticate NIS 29

L

LDAP authentication pre-requisites 24
LDAP configuration methods 25
LDAP supported users
    configure server 24
    pre-requisites 24
LDAP user
    configure authentication 22
local user
    configure authentication 21
log files
    introduction 55
log forwarding
    configuration 62

log forwarding *(continued)*
overview 61
secure log transmission 61
login banner
about 30

M

Management Information Base (MIB) 100

N

NetBackupCLI
run NetBackup commands 44
special directive operations 44
network security
IPsec 86
NIS configuration methods 30
NIS supported users
configure server 29
pre-requisites 29
NIS user
configure authentication 23
NIS user authentication pre-requisites 29
notifications 95

O

operating system
major components 66
security highlights 64
OS STIG hardening 111

P

password
credentials 31
encryption 31
password policy rules
STIG compliant 35
privileges
user role 41

R

replacing
IPMI SSL certificate 106

S

Simple Network Management Protocol (SNMP) 100
SSL usage 75
Symantec Data Center Security
about 47
IDS policy 50
IPS policy 49
managed mode 47, 53
unmanaged mode 47, 53

T

Third-party certificates 75

U

unenforced STIG rules 125
user 15
Active Directory 23
add 39
admin 15
Administrator 15
AppComm 15
authorize 39
Kerberos-NIS 23
LDAP 22
local 21
Maintenance 15
manage role
permissions 40
NetBackupCLI 15
root 15
sisips 15
user authentication
configure 21
guidelines 24
user group
add 39
manage role
permissions 40
user name credentials 31
user role privileges
NetBackup appliance 41

V

vulnerability testing 66