Veritas NetBackup™ Appliance Security Guide

Release 5.3

VERITAS™

Veritas NetBackup Appliance Security Guide

Last updated: 2024-08-28

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

https://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:

https://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

This chapter includes the following topics:

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 security patch or provides a fix in a scheduled major or maintenance release. To reduce the risk of 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 5.3 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 14.
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 19.
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 25.
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 Smart Card authentication	This section describes the prerequisites and process to configure the appliance for authentication with smart cards.	See "About authentication using smart cards and digital certificates" on page 27.
About single sign-on (SSO)	This section describes the prerequisites and process to configure single sign-on.	See "About single sign-on (SSO) authentication and authorization" on page 33.
About multifactor authentication	This section describes the prerequisites and process to configure multifactor authentication.	See "About multifactor authentication" on page 36.
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 39.
About user name and password specifications	This section describes the user name and password credentials.	See "About user name and password specifications" on page 40.

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 45.
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 47.
About the Administrator user role	This section describes the Administrator user role.	See "About the Administrator user role" on page 50.
About the NetBackupCLI user role	This section describes the NetBackupCLI user role.	See "About the NetBackupCLI user role" on page 51.

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 57.
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 59.

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

Section name	Description	Link
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 60.
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 61.
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 63.
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 63.

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 65.
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 67.
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 68.

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

Section name	Description	Link
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 69.

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 74.
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 76.

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 79.
About Data Integrity	This section lists the measures that are taken to improve data integrity.	See "About data integrity" on page 80.
About Data Classification	This section lists the measures that are taken to improve data classification.	See "About data classification" on page 81.
About Data Encryption	This section lists the measures that are taken to improve data encryption.	See "About data encryption " on page 81.

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 describes the SSL certification updates for the NetBackup Appliance Web Console.	See "About SSL usage" on page 87.
About implementing external certificates	This section describes the procedure to install third-party SSL certificates.	See "About implementing external certificates" on page 88.

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 93.
About NetBackup appliance ports	This section describes the port information for NetBackup Appliances.	See "About NetBackup appliance ports" on page 93.

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 98.

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

Section name	Description	Link
About Call Home	This section describes the Call Home feature in the NetBackup appliance.	See "About Call Home" on page 99.
About SNMP	This section describes the SNMP feature in the NetBackup appliance.	See "About SNMP" on page 104.

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 106.
Listing the Recommended IPMI settings	This section lists the recommended IPMI settings for a secure configuration.	See "Recommended IPMI settings" on page 107.

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

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 primary server or when you upgrade an appliance primary 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. The **nbasecadmin** user can also assign NetBackup roles to local users on the appliance, or to users registered on an LDAP server or Active Directory (AD) server. See "About user authorization in NetBackup" on page 55. **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 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 primary server FQDN>/webui` For more information about RBAC and NetBackup user role management, see the *NetBackup Web UI 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.`
nbcopilotxxxx	Supports authentication for access from the primary to the media server.
nbwebsvc	Does not support authentication.

See "About authorizing NetBackup appliance users" on page 47.

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 or an Active Directory (AD) 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, NetBackupCLI, or AMSadmin 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 25.	■ 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.

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 47.	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 47.	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 47.	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.

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

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Smart Card Authentication	NA	Enable authentication with smart cards as follows: ■ Configure remote authentication with OpenLDAP or ActiveDirectory under `Settings > Security > Authentication > LDAP` ■ Add CA certificate under `Settings > Security > Certificate AddCACertificate`. ■ Configure DNS to resolve the OCSP URI under `Network > DNS Add Nameserver`. ■ Configure and enable smart card authentication under `Settings > Security > Authentication > SmartCard`. You can also enable authentication for smart cards by logging in to the appliance as a NetBackupCLI user and running the following command: `vssat addldapdomain` See "About authentication using smart cards and digital certificates" on page 27.

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

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Single sign-on (SSO) authentication	NA	Enable SSO authentication for web console users as follows: ■ Configure remote authentication with ActiveDirectory under `Settings > Security > Authentication > ActiveDirectory`. ■ Authorize SSO users and user groups under `Settings > Security > Authorization`. ■ Configure the identity provider (IDP) for SSO under `Settings > Security > Authentication > SingleSignOn`. To configure SSO, click this link to obtain the following documents: *NetBackup Appliance Security Guide* *NetBackup Appliance Commands Reference Guide*

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

User type	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Multifactor authentication	NA	The following commands and options are available under `Settings > Security > Authentication > MFA`: ■ `Configure` - Configure multifactor authentication for the current user. ■ `Enforce` - Enforce multifactor authentication for all appliance users. ■ `Reset` - Reset the multifactor authentication configuration for a user that is unable to log in. ■ `Show GlobalEnforcement` - Check if multifactor authentication is enforced for all users. ■ `Show Key` - Show the key and the QR code for the current user. ■ `Unconfigure` - Unconfigure multifactor authentication for the current user. If multifactor authentication is enforced, users can unconfigure it only within the grace period. See "About multifactor authentication" on page 36.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

- Only one remote user type (LDAP, or Active Directory/AD 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 or AD 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 only for local appliance users. For remote AD and LDAP users, reserve a user ID and group ID range greater than 1999.
- NetBackup appliance uses general CIFS shares for some of its internal operations such as storing patches and installation files, uploading logs to support, forwarding logs to an external server, and uploading OST plug-ins. Starting with appliance software version 4.0, you must manage access to the general CIFS shares for all local users and Active Directory users and user groups (except the **admin** user). Use the `Settings > Security > Authentication > CIFSShare` command to manage access to the general CIFS shares.
  - Guest users: Replace a Guest user by creating a new local user.
  - Existing local users: Change the passwords for these users.

See "About user authentication on the NetBackup appliance" on page 14.

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.
- UNIX mode must be enabled on the Active Directory server.
- 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*.

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.
- If AD requires communication with a Kerberos server for user authentication, in certain situations, network restrictions or firewall rules can prevent Kerberos traffic to port 88 on AD domain controllers. To prevent this issue, ensure that you open port 88 in the network firewall.

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*.

About authentication using smart cards and digital certificates

The following describes the supported interfaces for Smart Card Authentication.

2FA

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

Starting with appliance release 5.0, NetBackup appliances support two-factor authentication (2FA) for Lightweight Directory Access Protocol (LDAP) domain users with the NetBackup Appliance Web UI.

2FA for NetBackup Web UI

- The **nbasecadmin** user or any user with the NetBackup Adminstrator role can configure 2FA for the NetBackup Web UI.
- 2FA configuration requires separate AD or LDAP configuration for NetBackup, even if AD or LDAP is already configured on the appliance.

2FA for NetBackup Appliance Web UI

Any user with the NetBackup Appliance administrator role can configure 2FA for the NetBackup Appliance Web UI. 2FA configuration requires configuring LDAP (with the directory type as OpenLDAP or ActiveDirectory) on the appliance.

For details about how to configure, enable or disable 2FA for the Appliance Web UI, see the following topic:

See “Smart card authentication for NetBackup Appliance Web UI” on page 30.

Smart card Authentication for NetBackup Web UI

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 primary server domain and is not available for local domain users.

Note: Perform this configuration separately for each appliance primary 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 primary 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*

Smart card authentication for NetBackup Appliance Web UI

Ensure that you perform the following three steps before you perform authentication for the Appliance Web UI.

Note: You can perform the steps in any order.

---

1. Configure LDAP authentication with the directory type as OpenLDAP or ActiveDirectory.

   Settings > Security > Authentication > LDAP

2. Add and grant roles to LDAP users who will be authenticated by the appliance.

   Settings > Security > Authentication > LDAP > Users Add

   Settings > Security > Authorization > Grant

3. Add all the certificates in the CA chain to the appliance. Intermediate certificates on the card do not have to be added.

   Settings > Security > Certificates > AddCACertificate

The smart card command menu allows you to configure and display parameters related to the Appliance Web UI smart card authentication. You can also enable or disable this feature.

Settings > Security > Authentication > SmartCard

Table 2-5 Smart card menu commands

Command	Description
`Configure MappingAttribute`	The `Configure` command configures the appliance smart card authentication. It has one required and one optional configuration parameter. The `MappingAttribute` parameter specifies if the Common Name (CN) or the User Principal Name (UPN) of the certificate on the smart card is used to authenticate a user and determine that user's role. Enter CN or UPN. It is a required parameter. CN can be used if the CN in the certificates matches the CN field of the user records in the remote databases, OpenLDAP or ActiveDirectory. UPN can be used if the UPN in the certificates matches the UPN field of the user records in OpenLDAP or ActiveDirectory. When LDAP is, configured the `directoryType` is specified as OpenLDAP or ActiveDirectory.
`Configure OCSPURI`	The `OCSPURI` parameter (Online Certificate Status Protocol) determines if the certificate on the smart card has been revoked. It is an optional parameter. If present, this parameter overrides the OCSP URI present in the certificate. The URI is an FQDN or IPv4 address. An IPv6 address is not supported for the OCSP URI. **Note:** If authentication with smart card fails even after all the necessary steps have been performed, use the **SmartCard > Show** command and verify that the parameters, including the OCSP URI, if present, are correct. Verify that a name server which can resolve the OCSP URI is configured in the Network menu by navigating to **Network > DNS Show**
`Disable`	Disables smart card authentication.
`Enable`	Enables smart card authentication. You can enable smart card authentication only if LDAP has been configured, CA certificates have been added and smart card authentication has been configured.
`Show`	Displays a table which shows if smart card authentication is enabled, the selected mapping attribute, and the OCSP URI, if one was entered.

Smart card authentication for NetBackup Appliance Shell Menu

This topic provides the following information to configure smart card authentication for the NetBackup Appliance Shell Menu (shell menu):

- Order of steps
- Smart card SSH menu commands

Order of steps

1. Enable smart card authentication for SSH. You must first enable the feature before you can add the public key (step 3).
2. Configure the mapping attribute to determine which field in the remote database is used to search for the public key.
3. Add the public key for a local user. You can use either a public key file or a certificate file method.
4. (Optional) Choose to enable or disable password authentication for SSH login.

Table 2-6 Smart card SSH menu commands

Command	Description

`Configure MappingAttribute CN/UPN`
`Configure PublicKey Add filetype <username>`
`Configure PublicKey Remove <username>`
	The `Configure` command configures the appliance smart card authentication and is used to configure the following parameters:
	MappingAttribute is for either CN (Common Name) or UPN (User Principle Name). This attribute determines which of those fields in the remote database is used to search for the public key.
	`Configure PublicKey Add filetype <username>` adds a public key for a local user. Here, *filetype* is either `CertificateFile` or `PublickeyFile`. For `CertificateFile` configurations, copy and paste the certificate content directly. For `PublickeyFile` configurations, locate the public key in the certificate file and copy it, then paste it directly.
	Note: Before you can add a public key, you must first enable SSH smart card authentication with the `Enable` command described further below.
	`Configure PublicKey Remove <username>` removes a public key for a local user.

`Disable`	Disables smart card authentication for SSH user.
`Enable`	Enables smart card authentication for SSH users. If all the prerequisites for DNS and smart card configuration commands have been performed successfully, authentication with smart cards is enabled. **Note:** Before you can add a public key, you must first run this command to enable SSH smart card authentication.
`PWauth`	Enables or disables password authentication for SSH login.
`Show`	Shows the values of the mapping attribute and status of the smart card authentication.

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 Administrator's Guide*.

Configure authentication for a smart card or digital certificate for the NetBackup Web UI

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 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 single sign-on (SSO) authentication and authorization

You can configure SSO with a supported external identity provider (IDP) that uses the SAML 2.0 protocol for exchanging authentication and authorization information. Note that you can configure an IDP with more than one Veritas product. For example, the same IDP can be configured with NetBackup and with APTARE.

Note the following requirements and limitations:

- You must have a SAML 2.0 compliant identity provider configured in your environment.
- Only identity providers that use AD or LDAP directory services are supported. ADFS (Active Directory Federation Services) is currently the only supported IDP for the NetBackup Appliance.
- IDP configuration is managed by using the `Main > Settings > Security > Authentication > SingleSignOn` command. You can configure only one IDP for SSO.

- SAML users cannot use the APIs. API keys are used to authenticate a user and therefore cannot be used with SAML-authenticated users.
- SSO login is currently supported only to the NetBackup Appliance Web Console (web console).
- Global logout is not supported.

SSO configuration is supported from the NetBackup Appliance Shell Menu (shell menu). The following describes an overview on how to configure and enable SSO for an appliance.

Table 2-7 Process overview for SSO configuration

Step	Task	Description
1	Obtain the IDP metadata XML file.	The SAML metadata that is stored in XML files is used to share configuration information between the IDP and the appliance. The IDP metadata XML file is used to add the IDP configuration to the appliance. The following options are available: ■ Download the IDP metadata XML file from the service provider and upload it to the general share on the appliance. ■ Provide the URL address of the IDP metadata XML file for the appliance to download.
2	Configure SSO on the appliance.	Configure the appliance for SSO from the following shell menu view: `Main > Settings > Security > Authentication > SingleSignOn`
3	Authorize SSO users and user groups.	Configure appliance access for SSO users and user groups from the following shell menu view: `Main > Settings > Security > Authorization` You can grant administrator or AMS privileges to SSO users and user groups.

To perform the complete SSO configuration process, see the following topic:

See "Configure single sign-on (SSO) for a NetBackup Appliance" on page 35.

Configure single sign-on (SSO) for a NetBackup Appliance

The following procedure describes the complete process to configure an appliance for SSO.

To configure SSO on an appliance

1. Obtain the identity provider (IDP) metadata XML file by using one of the following methods:

   - Download
     Download and save the IDP metadata XML file from the IDP website. Then log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:
   - Log in to the NetBackup Appliance Shell Menu (shell menu) and upload the file to the appliance by opening the general share as follows:
     `Settings > Share > General Open`

     Note: You can also upload the file into the general share directory from the **File Manager** tab in the NetBackup Appliance Web Console.

   - URL
     Obtain the URL address of the IDP metadata XML file for the appliance to download. Make sure that it is a valid https address.

2. Configure SSO on the appliance as follows:

   Note: You can configure only one IDP for SSO.

   - Run the following command to add an IDP configuration to the appliance:
     `Settings > Security > Authentication > SingleSignOn Add`
   - `idpname` - enter the name that you want to use for this IDP configuration.
   - `metadata` - select how to associate the necessary metadata for the IDP configuration, as follows:
     Import: Import the IDP XML metadata file that you uploaded into the general share directory in the first step.
     URL: Enter the URL address of the IDP XML metadata file for the appliance to retrieve.
   - *`userFieldName [userPrincipalName]`*
     `groupFieldName [memberOf]`

These parameters are optional and are shown with their default values. You can change the default values as needed to retrieve the appropriate SAML assertion details.

After you have completed this step, the configuration is enabled by default.

3 Add authorized SSO user groups and users by running the `Settings > Security > Authorization` command. Use the following command options to authorize specific SSO user groups and users:

```
Grant Administrator SSO_Groups groups

Grant Administrator SSO_Users users

Grant AMS SSO_Groups groups

Grant AMS SSO_Users users
```

About multifactor authentication

Starting with NetBackup Appliance release 5.3, multifactor authentication is supported.

Multifactor authentication requires users to verify their appliance login identity by means of a system-generated code that is required in addition to the standard login password. When multifactor authentication is enabled, each time you log in to the appliance you enter your username and password as usual. Next, you are prompted through a remote device, such as a smartphone, to enter a second factor to verify your identity. When you open the app on your smartphone, it shows a unique 6-digit code that you must enter to complete the login.

Note: You cannot use multifactor authentication if Smart Card configuration is enabled.

An administrator must configure their user account for multifactor authentication before other users can con configure their user accounts. Configuration for the feature is done from the following NetBackup Appliance Shell Menu view:

```
Main > Settings > Security > Authentication > MFA
```

For complete details and descriptions of the command options for this feature, see the *NetBackup Appliance Commands Reference Guide*.

After the first administrator has configured their user account for multifactor authentication, all of the following appliance users can configure their user accounts:

- Active Directory (AD)

- LDAP
- Local users
- NetBackup CLI users
- No-role users

Note: NetBackupCLI and no-role users must log in to the appliance and run the `multifactor-authentication` command, then run the available submenu commands. For complete details, see the `Settings > Security > Authentication > MFA` description in the *NetBackup Appliance Commands Reference Guide*.

First-time configuration for multifactor authentication

This section describes how an administrator configures their user account for multifactor authentication to allow all other users to configure their user accounts later.

Requirements for administrator configuration:

- Minimum of two administrator accounts - The appliance must have at least two administrator accounts before they can configure multifactor authentication for their user accounts. If only one administrator user account exists when another user tries to configure the feature, an error message appears to inform them to add another administrator user account.
- Minimum of one NTP server - At least one NTP server must be configured and added before the first administrator can configure multifactor authentication for their user account. A message appears if an NTP server is needed.

  Note: The NTP server is typically configured when you perform the initial configuration on the appliance. If you did not configure an NTP server at that time, you must log in to the appliance shell menu and configure at least one NTP server with the `Main > Network > NTPServer` command. For details, see the *NetBackup Appliance Commands Reference Guide*.

- After the above configurations are completed, all other appliance users can configure their user accounts.

The following procedure describes the first-time configuration for an administrator to configure their user account for multifactor authentication.

For first-time administrator user account configuration for multifactor authentication

1. Log in to the shell menu as an administrator with the following command:

   ```
   Main > Settings > Security > Authentication > MFA Configure
   ```

2. Follow the prompts to configure multifactor authentication for your user account.
3. After completing the previous steps, have another administrator log in to the appliance with the following command to configure their user account to use multifactor configuration:

   ```
   Main > Settings > Security > Authentication > MFA Configure
   ```

4. To enforce multifactor authentication for all users of the appliance, run the following command:

   ```
   Main > Settings > Security > Authentication > MFA Enforce
   ```

   Note: You can run this command only after you have completed steps 1, 2, and 3.

Configure multifactor authentication for a user account

After the two required administrators have completed their user account configurations, all other appliance users can configure their user accounts.

Requirements for user configuration:

- If multifactor authentication is configured but not enforced for all users (global enforcement), a user can configure or unconfigure multifactor authentication for their account at any time.
- If multifactor authentication is configured and is also enforced for all users, a user can unconfigure multifactor authentication for their account only within a defined grace period. The grace period default is 90 days. After the grace period has expired, the user is forced to configure multifactor authentication during login, but they cannot unconfigure it.

To configure multifactor authentication for a user account

1. Log in to the appliance shell menu and run the following command to configure your user account for multifactor authentication:

   `Main > Settings > Security > Authentication > MFA Configure`

   For NetBackupCLI users and no-role users, log in to the appliance and run the `multifactor-authentication` command, then run the `Configure` submenu command.

2. Follow the prompts to configure multifactor authentication for your user account.

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 2-8 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 2-8 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.

Table 2-8 Appliance interfaces that support the login banner *(continued)*

Interface	Notes
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 2-9 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 2-9 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 or the AD policy
Minimum length	2 characters	2 characters	Determined by the LDAP or the AD policy

Table 2-9 User name specifications *(continued)*

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Restrictions	User names must not start with: ■ Number ■ Special character	User names must not start with: ■ Number ■ Special character	Determined by the LDAP or the AD policy
Space inclusion	User names must not include spaces.	User names must not include spaces.	Determined by the LDAP or the AD policy

Password specifications

The NetBackup appliance password policy has been updated to increase security on the appliance. All local users including NetBackupCLI users must meet STIG password policy rules. See "About STIG-compliant password policy rules" on page 42.

The password policy for registered remote users is determined by the LDAP or the AD policy.

Warning: Appliances do not support Maintenance account passwords such as `passwd`. These types of passwords are overwritten once the system is upgraded. 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.

Starting with appliance release 5.3, the STIG feature is enabled by default and cannot be disabled. All appliance user account passwords must meet STIG password policy rules. You can still modify some STIG configuration parameters as needed for your security requirements. For details, see "Appendix T" in the *NetBackup Appliance Commands Reference Guide* for version 5.3.

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

Note: The maximum days for password change can be modified based on local security requirements. For details, refer to the `Settings > Security > PasswordAge` command description in the *NetBackup Appliance Commands Reference Guide*.

- Dictionary words are not valid or accepted.
- The last seven passwords cannot be reused.

Note: The 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.

Password expiration

If you log in to the appliance with an expired password, a warning message appears that prompts you to change the password immediately, and then log in again with the new password.

Login lockout enforcement

Starting with appliance release 5.3, the STIG feature enforces a login lockout for any user that enters three consecutive incorrect passwords within 15 minutes. The locked out user has the following options:

- Wait 30 minutes for the lockout to expire, then log in with the correct credentials.
- Contact the system administrator to have them unlock the account.

Note: Any administrator that is locked out must contact another administrator user if they do not want to wait 30 minutes for the lockout to expire.

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 117.

Chapter 3

User authorization

This chapter includes the following topics:

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 50.
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 51.
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 42.

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 or AD users and user groups.	Use the `Settings > Security > Authentication` commands to add, delete, and view appliance users. See "About configuring user authentication" on page 19.

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 the NetBackup 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 the NetBackup Appliance Web Console. To list all of a group that has more than 2000 users, use the `List` command from the NetBackup 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 and Active Directory (AD) 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 51.
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 50.
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 Administrator SSO_Groups
Grant Administrator SSO_Users
Grant NetBackupCLI Group
Grant NetBackupCLI Users
Grant AMS Group
Grant AMS Users
Grant AMS SSO_Groups
Grant AMS SSO_Users
```

See "About configuring user authentication" on page 19.

See "About authorizing NetBackup appliance users" on page 47.

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.
- Local users and LDAP or Active Directory (AD) users and user groups assigned with an Administrator role can access the NetBackup Java console.

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 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.

Starting with appliance release 5.0, NetBackupCLI users can only run some commands as a superuser and are required to follow the NetBackup CLI authorization mechanism to authenticate and run such commands. Refer to the *NetBackup Commands Reference Guide* for more information on the exact permissions that are required by various NetBackup commands and command parameters.

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 the NetBackup 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: ■ `/opt/VRTSpbx/bin/*` ■ `/opt/VRTS/bin/*` ■ `/usr/openv/db/bin/*` ■ `/usr/openv/mqbroker/bin/goodies/*` ■ `/usr/openv/mqbroker/bin/install/*` ■ `/usr/openv/netbackup/bin/*` ■ `/usr/openv/netbackup/bin/admincmd/*` ■ `/usr/openv/netbackup/bin/goodies/*` ■ `/usr/openv/netbackup/bin/goodies/support/*` ■ `/usr/openv/netbackup/bin/support/*` ■ `/usr/openv/pdde/pdcr/bin/*` ■ `/usr/openv/pdde/vpfs/bin/*` ■ `/usr/openv/volmgr/bin/*` ■ `/usr/openv/volmgr/bin/goodies/*` ■ `/usr/openv/pdde/pdcr/bin/crcontrol` ■ `/usr/openv/pdde/pdag/bin/mtstrmd` ■ `/usr/openv/pdde/pdag/bin/pdcfg` ■ `/usr/openv/pdde/pdag/bin/pdusercfg` ■ `/usr/openv/pdde/pdconfigure/pdde`	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. ■ They cannot execute any command with an absolute path. All commands must be executed only with a short name. ■ They cannot run most of the system commands, except a few read-only system commands, such as `cat`, `date`, `whoami`, `ls`, `which`, `grep`, `sort`, `cut`, `jq` and `vi` commands that work in read-only mode.

How to run NetBackup commands as a NetBackupCLI user

Log in as a NetBackupCLI user and type `Command` at the command prompt to enter into a restrictive shell environment. You can then run the NetBackup commands from that shell. Using absolute paths to run NetBackup commands is not allowed. For example, you can run `bplist` but you cannot run `/usr/openv/netbackup/bin/admincmd/bplist` from the command shell.

With appliance release 5.3, the following command prefixes are enabled by default:

- `nbcmdrun`

This prefix is required to run most NetBackup commands. The following examples show how to enter commands with the prefix:

```
nbcliuser-!> nbcmdrun bpminlicense -list_keys
nbcliuser-!> nbcmdrun bpgetconfig -g localhost -L
nbcliuser-!> nbcmdrun bpps
```

For complete details about the `nbcmdrun` prefix, see the *NetBackup Commands Reference Guide*.

- `msdpcmdrun`

  This prefix is required to run all MSDP commands that reside in the `/usr/openv/pdde` directory. The following examples show how to enter commands with the prefix:

  ```
  nbcliuser-!> msdpcmdrun crstats
  nbcliuser-!> msdpcmdrun dcscan -a
  nbcliuser-!> msdpcmdrun spauser -l
  ```

  For complete details about the `msdpcmdrun` prefix, refer to the section "Running MSDP commands with the non-root user" in the *NetBackup Deduplication Guide*.

You may need additional authorization before you can run some of the NetBackup commands. You will see a different authorization prompt depending on the NetBackup command you are trying to run.

The following list describes the typical scenarios for successfully executing NetBackup commands:

- Authorization prompt: **web login is required**

  Some NetBackup commands may require a web login. You will see the following prompt:

  ```
  A web login is required. Run the 'bpnbat -login -loginType
  WEB|WEBUI|APIKEY' command to login.
  nbcmdrun: failed to run the command
  ```

  To authenticate such requests, you must log in to the NetBackup Web Management Service as a NetBackup administrator and run the following command:

  ```
  myappliance.NBCLIUSER> bpnbat -login -logintype WEB
  ```

  The following shows an example WEB login:

  ```
  Authentication Broker: ApplianceHostname
  Authentication Port: 0
  Authentication Type: unixpwd
  LoginName: Username
  Password: Password
  Operation completed successfully.
  ```

- Authorization prompt: **web ui login required**

  Some NetBackup commands may require an approval using an access token. To authenticate such requests, generate an access code by running the following command:

  ```
  # bpnbat -login -logintype webui
  ```

  Make a note of the access code that is displayed in the command window.

  Sign in to the NetBackup web UI as a NetBackup Command Line (CLI) Admin user and approve the CLI access request by entering the access code that you generated earlier. For more information about access key and approval requests, refer to the *NetBackup Security and Encryption Guide*.

General considerations:

- The authentication cases described earlier are typical scenarios. Some NetBackup commands may require other authentication methods. Refer to the *NetBackup Commands Reference Guide* for more information on the exact permissions that are required by various NetBackup commands and command parameters.
- Some NetBackup commands are run as root by default. You can verify whether a particular command requires root privileges by running the following command:

  ```
  nbucliuser-!> alias | grep NetBackup command
  ```

  For example, `msdpcmdrun` command runs as root by default:

  ```
  nbucliuser-!> alias | grep msdpcmdrun
  alias msdpcmdrun='sudo -n /usr/openv/netbackup/bin/msdpcmdrun'
  ```

- Some NetBackup commands are run by the current NetBackupCLI user by default. But there are some NetBackup command parameters that require root privileges. In such cases, you can use '`sudo <absolute path of command> <parameters>`' to run the command.

  If you see a prompt "sudo: a password is required", it means that the command cannot be run as root. Contact Veritas Technical Support for help with such scenarios.

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 allowed list`.
- Add the special directive commands to the `/home/nbusers` directory.

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

NetBackup Administrator's Guide, Volume 1

NetBackup Commands Reference Guide

About user authorization in NetBackup

You can use the **nbasecadmin** account to log in to the NetBackup web UI and assign NetBackup roles to local users on the appliance, or to users registered on an LDAP server or Active Directory (AD) server. The roles assigned in the NetBackup role-based access control (RBAC) allow appliance users to perform specific tasks in NetBackup, while restricting access to non-essential assets and features. For more information about RBAC and NetBackup user role management, see the *NetBackup Web UI Administrator's Guide*.

If you are upgrading an appliance running on versions 3.1.2 or 3.2, all non-administrative roles defined by the NetBackup RBAC are revoked after the upgrade. You must reconfigure the existing RBAC configuration by using the new RBAC model introduced in NetBackup 8.3.

You can migrate the existing backup administrator and security administrator roles to the NetBackup 8.3 RBAC model using the RBAC migration tool. The RBAC migration tool performs the following operations:

- Migrates the existing security administrator role along with its added principals.
- Removes the existing backup administrator role and reassigns its users to the administrator role.

For more information about the RBAC migration utility, seehttps://www.veritas.com/support/en_US/article.100047577.

Any currently configured workload administrator role and custom roles must be reconfigured after the upgrade. You can use the NetBackup 8.3 RBAC roles utility to add the latest role definitions. For details, see https://www.veritas.com/support/en_US/article.100047660

Chapter 4

Intrusion prevention and intrusion detection systems

This chapter includes the following topics:

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.

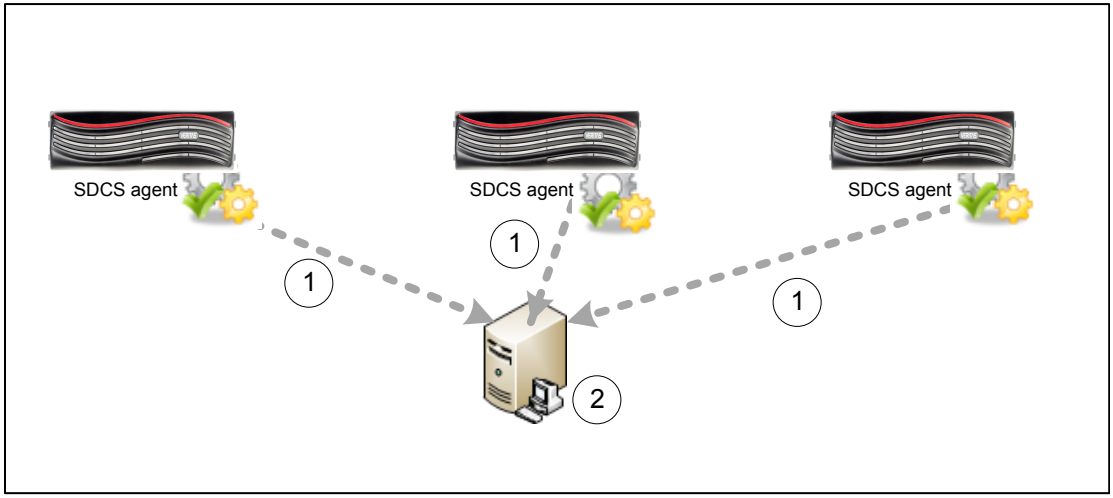
- Centralized managed mode operations
  Lets you use a central SDCS manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by SDCS.

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.

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 65.

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

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		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 67.	■ 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. See "Viewing log files using the Support command" on page 67.	Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedupTarget` ■ `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 69.	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 shell menu. The `LOGROOT/>` prompt appears.
2. To display the available log directories on your appliance, type `ls` at the `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 68.

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

1. You can view the 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 Log in to the log browser website with the `Main > Support > LogBrowser Start` command. Use the log browser 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.

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 65.

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`
Host change log	`<DIR> APPLIANCE hostchange.log`

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

Appliance log	Log file location
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`
	`messages`

Operating system (OS) audit log	`<DIR> APPLIANCE` `audit.log`
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	`/log/data-collect/sosreport*.tar.xz` You can download the `DataCollect.zip` file by logging into the log browser website with the `Main > Support > LogBrowser Start` command. Use the log browser desktop to map, share, and copy the logs.

See "About NetBackup appliance log files" on page 65.

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
- 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 one of the following commands to gather device logs:
   - `dataCollect`
   - `dataCollect advanced`
     Use this option to include detailed logs for a higher level of debugging.

   For appliance software versions 5.0 and later, the appliance generates the device log in the `/log/data-collect/sosreport*.tar.xz` file.
3. You can download the `DataCollect.zip` file by logging into the log browser website with the `Main > Support > LogBrowser Start` command. Use the log browser desktop to map, share, and copy the logs.
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 65.

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.

Starting with software version 5.0, both the appliance shell menu and appliance web console access logs are audited.

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 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/share`
  CIFS: `\\<appliance.name>\general_share`

  Note: You can also upload certificate files from the **Manage > File Manager** menu in the appliance web console.

- `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.
Forward logs	Select which types of logs to forward (OS, Appliance, AutoSupportClient, Infoscale). You can enter multiple log types with a comma-separated list.

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

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 software version 5.3

Software component	Version
Red Hat Enterprise Linux (RHEL)	8.8
Veritas InfoScale	8.0.2 **Note:** The Veritas InfoScale installation is modified and tuned for maximum performance on the appliance.
Symantec Data Center Security: Server 6.8 Advanced (SDCS)	6.9.3
OpenJDK Runtime Environment	17.0.8
Apache Tomcat	9.0.82-4
RabbitMQ	3.11.22-1
MongoDB	4.4.24-1
Intel IPMI Utils	1.8.18

Disable user access to the NetBackup appliance operating system

Depending on the security policies of your organization, you can choose to permanently disable user access to the NetBackup appliance operating system (VxOS). You can disable user access to the VxOS by configuring its security level to `High`. Note that the following restrictions are permanently enforced in the appliance:

- Users cannot access the maintenance shell. The `Support > Maintenance` menu is not available in the shell menu.

Note: Only Veritas support personnel can be granted access to the maintenance shell to troubleshoot issues and manage operating system-related tasks. See "Manage support access to the maintenance shell" on page 77.

To permanently disable user access to VxOS

1. To view the current security level of the VxOS, use the following command:

   `Main_Menu > Settings > Security > SecurityLevel Show`

   The VxOS can operate in either of the following security levels:

Security level	Description
`Optimal`	Access to VxOS is granted as per standard Veritas security policies. This is the default security configuration.
`High`	Access to VxOS is permanently disabled for all users.
`Maintenance`	Access to VxOS is temporarily granted to Veritas support personnel through the maintenance shell. The security level is automatically reverted to `High` after the maintenance activity is completed.

2. To permanently disable user access to VxOS, configure the security level to `High`. Use the following command:

   `Main_Menu > Settings > Security > SecurityLevel High`

Note: After switching to the `High` security level, you cannot revert to the default (`Optimal`) security level unless you perform a factory reset of the appliance.

Manage support access to the maintenance shell

The maintenance shell in the `Support > Maintenance` menu is disabled if you configure the security level of VxOS to `High`. However, to troubleshoot issues and manage OS tasks, you can allow Veritas support personnel to enable and access the maintenance shell.

Use the commands in the `Main_Menu > Support > System` menu to manage support access to the maintenance shell. For more information, see the *Veritas NetBackup Appliance Commands Reference Guide*.

Table 6-2 Commands for managing support access to the maintenance shell

Command	Description
`Support > System > Generate-otp`	Use this command to generate a ten digit one-time password (OTP), which will remain active for a period of two hours. The OTP can be shared with Veritas support personnel.
`Support > System > Show-otp`	Use this command to view the currently active OTP.
`Support > System > Unlock`	Veritas support personnel use this command to enable the maintenance shell (`Support > Maintenance`). In addition to an active OTP, Veritas support personnel require a customer case ID and support passphrase to run the `Unlock` command successfully and access the maintenance shell. **Note:** VxOS is temporarily configured to the `Maintenance` security level.
`Support > System > Lock`	Use this command to disable the maintenance shell. Veritas support personnel cannot access the maintenance shell and are logged out of any active session. **Note:** VxOS is reverted to the `High` security level.

Chapter 7

Data security

This chapter includes the following topics:

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) is 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 primary 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 82.

KMS support

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

The following describes the KMS key features:

- Does not require an additional license.
- Is a primary server-based symmetric key management service.
- Can be administered as a primary 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
Keystore file	The keystore file (`KMS_DATA`) contains all of the key group and key records, along with some metadata.

Table 7-1 KMS files *(continued)*

KMS files	Description
KPK file	The KPK file (`KMS_KPKF`) contains the KPK that is used to encrypt the ciphertext portions of the key records that are stored in the keystore file.
HMK file	The HMK file (`KMS_HMKF`) contains the HMK that is used to encrypt the entire contents of the keystore file. The keystore file header is an exception. It contains some metadata like the KPK ID and the HMK ID, which is not encrypted.

Configuring KMS

To configure KMS on an appliance primary server, you must log in as a NetBackupCLI user.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on managing role-based access control, see the *NetBackup Web UI Administrator's Guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user, See "About the NetBackupCLI user role" on page 51.

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 primary server as a NetBackupCLI user.
2. Enter into a restricted shell environment by using the `Command` command as follows:

   ```
   [nb-appliance.NBCLIUSER>]# Command
   ```

3. Authenticate your CLI access using the following steps:
   - Generate an access code by running the following command:

     ```
     #bpnbat -login -logintype webui -requestApproval
     ```

     Make a note of the access code that is displayed in the command window.
   - Sign in to the NetBackup web UI as a NetBackup Command Line (CLI) Admin user and approve the CLI access request by entering the access code that you generated earlier.

Once the request is approved, you will see a confirmation message in the restricted shell command window.

For more information about access key and approval requests, refer to the *NetBackup Security and Encryption Guide*.

4 Create an empty database using the `nbkms` command, as follows:

```
[nbucliuser-!>]# nbkms -createemptydb
```

5 Start `nbkms`. For example:

```
[nbucliuser-!>]# nbkms
```

6 Create a Key group. For example:

```
[nbucliuser-!>]# nbkmsutil -createkg -kgname KMSKeyGroupName
```

7 Create an active key. For example:

```
[nbucliuser-!>]# nbkmsutil -createkey -kgname KMSKeyGroupName
-keyname KMS KeyName
```

Enabling KMS encryption for MSDP

Verify that KMS is configured and running on the primary server. You can then enable KMS encryption for MSDP on all of the media servers that are associated with the primary server.

Before you proceed, ensure that the NetBackupCLI user is assigned the required RBAC permissions to configure and enable KMS. Use a NetBackup administrator account such as **nbasecadmin** to log in to the NetBackup Web UI and assign the Default Security Administrator role to the NetBackupCLI user.

For steps on how to manage role-based access control, see the *NetBackup Web UI Administrator's guide*.

Note: If required, you can create a new NetBackupCLI user for configuring and enabling KMS. For more information about the NetBackupCLI user, See "About the NetBackupCLI user role" on page 51.

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 NetBackupCLI user.

2 Change the following options in the order as shown:

- `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSType --value=0`
- `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSServerName --value=<primary server hostname`
- `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSKeyGroupName --value=msdp`
- `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KeyName --value=<KMS KeyName>`
- `nbucliuser-!> pdcfg --write=/msdp/data/dp1/pdvol/etc/puredisk/contentrouter.cfg --section=KMSOptions --option=KMSEnable --value=true`
- `nbucliuser-!> 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 primary server.

3 Identify yourself to the system by logging on to the NetBackup web application. Run the following command:

```
sudo /usr/openv/netbackup/bin/bpnbat -login -loginType WEB

Authentication Broker: ApplianceHostname

Authentication Port: 0

Authentication Type: unixpwd

LoginName: Username

Password: Password
```

4 Ensure that the KMS is registered with NetBackup Web Service.

```
sudo /usr/openv/netbackup/bin/nbkmscmd -discoverNbkms
```

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

- `bp.kill_all`

- `bp.start_all`

6 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
```

About antimalware protection

Starting with software release 5.3, antimalware protection lets you manage the detection and removal of malware on the appliance. Feature configuration is available using the `Settings > Security > Antimalware` command from the NetBackup Appliance Shell Menu (shell menu).

The following describes the general feature functionality:

- Enable full malware protection on the appliance, which includes automatic protection (**AutoProtect**) and on-demand protection. The feature is enabled by default.**AutoProtect** protection scans all incoming files to the appliance. On-demand protection scans files that already exist on the appliance. You must set a daily or a weekly schedule to use on-demand protection.
- Set up a server to receive malware reports from the appliance. The LiveUpdate server is set as the default server.
- Manually generate a report that identifies the type of malware that was detected, the affected files, the severity level, and whether any files have been quarantined.
- Restore quarantined files that are not malware.

For complete configuration details, see the *NetBackup Appliance Commands Reference Guide*.

Chapter 8

Web security

This chapter includes the following topics:

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.

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

Self-signed certificates

The appliance uses self-signed certificates for client and host validation. A host certificate issued by an internal CA is deployed on the primary and media servers during role configuration. The self-signed 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 protocols.

External certificates

NetBackup appliance also supports host certificates issued by an external certificates. You can use these as an alternative to the internal CA to provide host verification and security to meet your organization’s standards.

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

Table 8-1 Types of external certificate certificates

Certificate type	Description
Host certificate	The appliance's 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 **SubjectAlternativeName** certificate extension contains all the appliance host names and IP addresses by which the appliance is reached. Include the fully qualified host names and the short names.
Host private key (corresponding to the host certificate)	The appliance's host private key must be in PKCS#8 standard and encoded in PEM format.
(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 CAs, you must have all those intermediary and root CA certificates ready in a file called cacerts.pem.

About implementing external certificates

NetBackup appliance's web service uses the PKCS#12 standard and requires certificate files to be in the X.509 (`.pem`) format. If the certificate files are in the `.der`, `.DER`, or `.p7b` formats, NetBackup appliance automatically converts the files to an accepted format.

Certificate requirements

To prevent errors while importing certificates, ensure that the external certificate files meet the following requirements.

- Certificate files are in the `.pem` file format and begin with "`-----BEGIN CERTIFICATE-----`".

- Certificate files contain the host name and FQDN in the subject alternative name (SAN) field of the certificate. If the certificate is used in an HA environment, the SAN field must contain VIP, host name, and FQDN.
- Subject name and common name fields are not empty.
- Subject fields are unique for each host.
- Subject fields contain a maximum of 255 characters.
- Server and client authentication attributes are set in the certificate.
- Only ASCII 7 characters are used in the subject and SAN fields of the certificate.
- The private key file is in the PKCS#8 PEM format and begins with `-----BEGIN ENCRYPTED PRIVATE KEY-----` or `-----BEGIN PRIVATE KEY-----`.

Certificate Signing Request (CSR)

Although optional, you can use the `Settings > Security > Certificate > CertificateSigningRequest > Create` command to generate a CSR. Copy the CSR content from the command line to your external certificate portal to obtain the required external certificate files.

```
Example:
Enter specified value or use the default value.
Common Name (eg, your name or your server's hostname) [Default abc123]:
Organizational Unit Name (eg, section) []:Appliance
Organization Name (eg, company) [Default Company Ltd]:YourCompanyName
Locality Name (eg, city) [Default City]:YourCity
State or Province Name (full name) []:YourStateorProvince
Country Name (2 letter code) [XX]:YourCountryName
Email Address []:email@yourcompany.com
Please enter the following 'extra' attributes
to be sent with your certificate request.
-----
A challenge password []:123456
An optional company name []:ABCD
Subject Alternative Name (DNS Names and/or IP Addresses comma separated):
abc123,def456.yourcompany.com
Subject Alternative Name (email comma separated):
Certificate Signing Request Name [Default abc123.csr]:
Validity period (in days) [Default 365 days]:
Ensure that the Distinguished Name (DN) is specified as a string consisting
of a sequence of key=value pairs separated by a comma:
Then the generated certificate signing request will be shown on the screen.
```

Register the external certificate

Starting from version 4.1, you can register an external certificate on both NetBackup appliance and NetBackup using the `Settings > Security > Certificate > Import` command.

Perform the following steps to import the host certificate, host private key, and trust store to register the external certificate on NetBackup and NetBackup appliance. Both NetBackup and NetBackup appliance layers use the same host certificate, host private key, and trust store.

1. Log in to the appliance as an Administrator user.
2. From the NetBackup Appliance Shell Menu, run the `Settings > Security > Certificate > Import` command. The following NFS and CFS share locations are now accessible:
   - NFS: `/inst/share`
   - CFS: `\\<ApplianceName>\general_share`
3. Upload the certificate file, trust store file, and private key file to either of the share locations and enter the paths to the files.
4. Choose how to access the certificate revocation list (CRL). A CRL comprises a list of external certificates that have been revoked by the external certificate and should not be trusted. Select either of the following options:
   - Use the CRL location provided in the certificate file.
   - Provide the location of a CRL file (`.crl`) in the local network.
   - Do not use a CRL.
5. Confirm the location of the certificate files you want to register on the appliance.

A detailed example of how to import the certificates is provided here.

- Identify the certificate which should be imported.
- Import the certificate.

```
Enter the certificate:
Enter the following details for external certificate configuration:
Enter the certificate file path: cert_chain.pem
Enter the trust store file path: cacerts.pem
Enter the private key path: key.pem
Enter the password for the passphrase file path or skip security
configuration (default: NONE):
Should a CRL be honored for the external certificate?
1) Use the CRL defined in the certificate.
```

```
2) Use the specific CRL directory.
3) Do not use a CRL.
q) Skip security configuration.
CRL option (1): 2
Enter the CRL location path: crl
Then confirm input information and answer the subsequent questions.
```

Adding and removing certificates

You can manage external certificates on NetBackup appliance using the **Certificate** commands.

You can use the **Settings** > **Security** > **Certificate** > **Add CACertificate** command to add a server CA, HTTPS proxy CA, or LDAP CA certificate to the certificate authority list. Ensure that you paste the CA certificate content in the PEM or P7B format. The Appliance appends this CA certificate to the certificate authority list. Before appending the CA certificate, the appliance verifies whether the CA certificate is already being used on the appliance. If yes, the appliance quits with a message.

You can use the **Settings** > **Security** > **Certificate** > **Remove CACertificate** command to remove a server CA certificate from the certificate authority list. The available CA certificates are listed and you can select the certificate that you want to remove.

Chapter 9

Network security

This chapter includes the following topics:

About Network Access Control

The Network Access Control feature lets you control which IP addresses (IPv4 or IPv6) are allowed to access the appliance. This feature is available through the NetBackup Appliance Shell Menu as follows:

```
Main > Settings > Security > NetworkAccessControl
```

The available command options are *AddIP*, *DeleteIP*, and *Show*.

Appliance access is allowed through HTTPS for the NetBackup Appliance Web Console or rest APIs, and through SSH for the shell menu. To permit access to a specific appliance, add the necessary client IP addresses to the allowed list for that appliance. Any client IP addresses that are not included in the allowed list cannot access the appliance. Any interface level restrictions are managed separately and are also appliance-specific.

For high availability (HA) setups, you must configure the `NetworkAccessControl` options on both appliance nodes and the configurations must match.

If your appliance is configured as an Appliance Management Server (AMS) or is an agent for an AMS, make sure that you add those IP addresses to the allowed list. The AMS must include the IP addresses of the agents, and the agents must include the IP address of the AMS.

For complete details, see the *NetBackup Appliance Commands Reference Guide*.

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 primary servers, would be non-IPsec.

IPsec security works at IP level and allows securing IP traffic between two appliances. Device certificates are provisioned to the Primary and media appliances, these certificates are then enabled for configuring IPsec channels. This enables a secure interaction of the primary and media servers. The device certificates used are x509 certificates issued by DigiCert 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 appliances are detected after the device certificates are recognized. Only after this is the IPsec channel configured and enabled.

Contact Veritas Support to configure IPsec functionality on your appliance.

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 94.

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 9-1 lists the ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 9-1 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 109.

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 primary 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 9-2 shows the NetBackup Appliance ports that are open by default, before the appliance initial configuration has been completed.

Table 9-2 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`

Table 9-2 Factory default open NetBackup Appliance ports (before appliance initial configuration) *(continued)*

Port	Protocol	Usage
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 9-3 shows the NetBackup ports that are open by default, after the appliance initial configuration has been completed.

Table 9-3 Open NetBackup ports on NetBackup Appliances (after appliance initial configuration)

1025-5000	TCP	Veritas NDMP, `SERVER_PORT_WINDOW`
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`
13781	TCP	RabbitMQ
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 primary 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

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 https://netInsights.veritas.com portal is the unified address where 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.

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 the NetBackup 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
- Upgrade readiness status - upgrade readiness check results, downloaded upgrade package versions, appliance upgrade readiness analyzer package versions, AutoUpdate configuration for upgrade readiness check

See "Configuring Call Home from the NetBackup Appliance Shell Menu" on page 101.

See "About AutoSupport " on page 98.

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 99.

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. To register your appliance, sign in to the System Health Insights portal (https://systemhealth.netinsights.veritas.com) with your Veritas Account Manager credentials. For more information, see the *System Health Insights User Guide*.

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.

Note: Note: If you use the HTTPS protocol, you cannot upload DataCollect log files with the `Support > DataCollect Upload` command. To work around this issue, configure Call Home with the HTTP protocol before you upload the files.

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. By default, the HTTP protocol is used to communicate with the proxy server.

Note: If you want to use the HTTPS protocol, enter **https://** before the proxy server name. To ensure successful communication with the proxy server, add the latest CA certificate used by the proxy server by running the `Settings > Security > Certificate > AddCACertificate` command.

- 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 99.

See "About AutoSupport " on page 98.

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 versions 3.1 and later support SNMP V2.

NetBackup Appliance versions 4.0 and later support SNMP V2 and SNMP V3.

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

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

KCS Policy Control Mode

For NetBackup Appliance models 5250, 5340, and 5350 that are updated with BIOS version 2.01.0010 or later, the following message appears when you log in to the IPMI console:

```
KCS Policy Control Mode is Allow All.
This setting is intended for BMC provisioning and is
considered insecure for deployment.
```

You can safely ignore this message because the KCS policy setting only affects the in-band access of IPMI commands at the operating system level. These commands are accessible only to root level users. This default policy setting matches those from previous Veritas product releases.

LDAP Settings

Veritas recommends that you enable LDAP authentication with OpenLDAP. The IPMI sub-system is not compatible with Active Directory.

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	Stunnel **Note:** Support for AES and RC4 algorithms have been removed from KVM encryption in BMC Firmware: 01.51.11142.
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, 5250, and 5350
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
5124	RMM (Secured)	CDROM	Disabled	Enabled
22 or 66	SSH	CLI access	Disabled	Disabled
(UDP) 623	IPMI over LAN	Out-of-band management (ISM+ or RM*)	Disabled	Disabled
Ports specific to 5340, 5250, and 5350				
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

Table 11-3 RMM ports *(continued)*

Port	Service	Description	Default state on 5240	Default state on 5340, 5250, and 5350
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 you replace the default IPMI SSL certificate used to access the Veritas Remote Management (RMM) console. You can use a certificate signed by a trusted internal or external Certificate Authority (in PEM format), or by a self-signed certificate. Use the following procedure to create a minimal self-signed certificate on a Linux computer and import it into the IPMI web interface.

Note: Starting with BMC v2.86, the RMM console does not allow you to upload `.key` files. You can only upload `.pem` files for SSL certificates. When you generate a self-signed certificate, you must generate the private key with the `.pem` file extension.

To create a minimal self-signed certificate on a Linux computer and import it into the RMM console:

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 RMM console. You are about to enter 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 Copy the generated self-signed certificate and the private key files to a host that has access to the appliance RMM console.

5 Log in to the RMM console.

6 Click **Configuration > SSL Certification**.

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

7 From the **SSL Upload** page, do the following:

- Click **New SSL Certificate** and select the copied self-signed certificate file.
- Click **New Private Key** and select the copied key file.
- Click **Upload**.

8 A warning may appear that states an SSL certificate already exists. Press **OK** to continue.

9 A confirmation appears stating that the certificate and the key were uploaded successfully. Press **OK** to restart the web service.

10 Close and reopen the RMM console to verify that the new certificate is being presented.

Implementing an external IPMI SSL certificate

Use the following procedure to implement an external IPMI SSL certificate and import it into the IPMI web interface.

This procedure uses the following pass phrase and file names as examples. You can substitute this information as needed for your application.

- Pass phrase: 1234
- Private key file name: `privkey5250.pem`
- CSR file name: `ipmi5250.req`
- Certificate file name: `ipmi5250.cer`

To create and implement an external IPMI SSL certificate

1 Generate the private key.

Note: A pass phrase is required to generate the key. This example procedure uses “1234”. The pass phrase can be removed later.

Perform the following tasks to generate the private key:

- Log in to the NetBackup Appliance Shell Menu (shell menu) and enter the maintenance mode with the following command:
  `Support > Maintenance`
- Enter the name of the private key file with the following command, followed by the pass phrase when prompted:
  `openssl genrsa -out` *`privkey5250.pem`* `2048`
- Display the private key file content with the following command:
  `cat` *`privkey5250.pem`*
- Check the private key file with the following command, followed by the pass phrase when prompted:
  `openssl rsa -in` *`privkey5250.pem`* `-check -noout`

2 Generate the CSR for the IPMI.

The CSR file is created as a `.req` file and is uploaded to the CMP request.

- Enter the name of the CSR with the following command, followed by the pass phrase when prompted:
  `openssl req -new -key` *`privkey5250.pem`* `-sha256 -out` *`csr_ipmi.req`*
  `-subj` */CN=<HostFQDN>/OU=<>/O=<>/C=<>/L=<>/ST=<>*

Where *CN* is the server IPMI FQDN name, *OU* is the organizational unit, *O* is the organization, *C* is the country, *L* is the location, and *ST* is the state. The output file name result is `ipmi5250.req`.

- Verify the CSR with the following command:
  `openssl req -in ipmi5250.req -subject -verify -noout`
- Display the CSR file content with the following:
  `cat ipmi5250.req`
  Contact your security or network team to submit the CSR to the third-party certificate authority.
- You will receive the new certificate in an email. Save the certificates for IPMI and name the file as `ipmi5250.cer`.
- Display and view the certificate details with the following command:
  `openssl x509 -text -in certificate.cer`

3 Implement the IPMI certificate as follows:

- Remove the pass phrase from the private key with the following command, followed by the pass phrase when prompted:
  `openssl rsa -in privkey5250.pem -out privkey.pem`
- If the Remote Management Console (RMM) uses version BMC 2.86 or later, concatenate the CA root certificate, the CA intermediate certificate, and the server certificate into a single `.pem` file. For example:
  `cat ipmi5250.cer root-cacert.pem root-intermediatecert.pem > ipmi5250certificate.pem`
  If the RMM uses a BMC version earlier than 2.86, you must only use the server certificate that you received from the third-party certificate authority to upload.
- Copy the `ipmi5250certificate.pem` file to a Windows server where you can connect to the RMM console from the web browser.
- Log in to the RMM console and click **Configuration > SSL Certification** on the left screen menu.
- Click **Choose file**. When prompted for a new SSL certificate, select `ipmi5250certificate.pem` for **New SSL certificate** and `privkey.pem` for **New Private Key**.
- Click **Upload**. When a prompt appears to indicate that the certificate already exists, click **OK**. A message appears to indicate that the certificate was uploaded successfully.
- The RMM console reboots automatically. Wait a few minutes, then log in and reload the webpage to confirm that the certificate has been applied successfully.

Chapter 12

STIG and FIPS conformance

This chapter includes the following topics:

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.

Note the following about STIG functionality:

- Starting with software release 5.3, the STIG feature is enabled by default and you cannot disable it. These rules are based on the following profile from the Defense Information Systems Agency (DISA):
  STIG for Red Hat Enterprise Linux 8 Server - V1R10
- Upgrades to version 5.3 enable STIG automatically, even if it was not enabled before the upgrade.
- The `Settings > Security > STIG > Enable` command is available to manage the login banner and email addresses.

Starting with the 4.1 release, all STIG rule lists are available in separate documents on the Veritas Support site. Two checklists are currently available, one for the OS and one for Application Security STIG. For instructions about how to obtain these

documents, go to the **Latest releases** page on the Veritas Download Center, navigate to **NetBackup Appliance OS** and click **Learn more**.

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.

Note: 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

---

FIPS validation for Java

Starting with NetBackup appliance 4.1, the FIPS 140-2 standard is enabled by default for all Java-based services. The FIPS validation is achieved by using SafeLogic's CryptoComply modules.

FIPS validation for MSDP, NetBackup and VxOS

Starting with NetBackup appliance release 5.0, you can enable the FIPS 140-2 standard for MSDP, NetBackup and VxOS. The NetBackup Cryptographic Module, which is used by MSDP, NetBackup and VxOS, is FIPS validated.

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

- aes256-ctr
- aes256-gcm@openssh.com

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, NetBackup 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 NetBackup`, followed by the maintenance password.
  Enabling or disabling the `NetBackup` 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.
- `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*.

Limitations of FIPS mode

As FIPS security continues to increase, some older encryption methods can no longer be used.

When FIPS is enabled, appliance CIFS file share features work as follows: The appliance is added as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

CIFS shares opened by the following operations may not mount when using older authentication methods, like NTLM.

The following describes the impacted scenarios:

- For the general share:

  ```
  Settings> Share General Open
  Settings> LogForwarding > Share Open
  Manage> OpenStorage > Share Open
  Security> Certificate Import
  ```

- For incoming_patches:

  ```
  Manage> Software > Share Open
  ```

To work around these limitations, do one of the following:

- Disable the FIPS feature.
- Configure Active Directory authentication on the appliance. This adds the appliance as a domain member in Active Directory (AD) environments with Kerberos authentication that uses AES ciphers.

https://www.veritas.com/support/en_US/article.100054201

About FIPS compliant ciphers

The appliance restricts the use of FIPS compliant ciphers to communicate with Kerberos, AD and LDAP servers to strengthen the security of the appliance.

Appliance release 5.0

If you have configured the appliance to use the Kerberos server, only the following FIPS compliant ciphers are used for communicating with the Kerberos server.

- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha1-96

If you have configured the appliance to use the LDAP server, only TLS v1.2 and the following FIPS compliant ciphers are used for communicating with the LDAP server.

- ecdhe-rsa-aes128-gcm-sha256
- ecdhe-rsa-aes256-gcm-sha384
- dhe-rsa-aes128-gcm-sha256
- dhe-rsa-aes256-gcm-sha384

If you have configured the appliance to use the AD server, only the following FIPS compliant ciphers are used for communicating with the AD server.

- aes256-cts-hmac-sha1-96
- aes128-cts-hmac-sha1-96

Appliance release 5.1.1

When you run the `Main > Settings > Security > FIPS > Enable All` command, the following cipher policies are enforced:

- `cipher = AES-256-GCM AES-256-CCM AES-256-CTR AES-256-CBC AES-128-GCM AES-128-CCM AES-128-CTR AES-128-CBC`
- `group = SECP256R1 SECP384R1 SECP521R1 FFDHE-2048 FFDHE-3072 FFDHE-4096 FFDHE-6144 FFDHE-8192`
- `hash = SHA2-256 SHA2-384 SHA2-512 SHA2-224 SHA3-256 SHA3-384 SHA3-512`
- `key_exchange = ECDHE DHE DHE-RSA PSK DHE-PSK ECDHE-PSK`
- `mac = AEAD HMAC-SHA2-256 HMAC-SHA1 HMAC-SHA2-384 HMAC-SHA2-512`

Appliance release 5.3

The NGINX web server and the LDAP client support both TLS 1.3 and 1.2 protocols and only support the following strong FIPS compliant cipher suites:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384

If your browser and LDAP server support TLS 1.3 and these cipher suites, communication with the appliance is encrypted by default using the more secure TLS 1.3 protocol.

Index