Veritas NetBackup™ Appliance Security Guide

Release 3.0

VERITAS™

Veritas NetBackup Appliance Security Guide

Last updated: 2019-12-16

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

Documentation

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

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

Documentation feedback

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

APPL.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Contents

Chapter 1

About the NetBackup Appliance Security Guide

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 patch or provides a fix in a scheduled major release. To reduce the risk of unknown threats, Veritas regularly updates the third-party packages and modules in the product as part of regular maintenance release cycles.

The goal of this guide is to describe the security features implemented in NetBackup Appliance 3.0 and includes the following chapters and sub-sections:

NetBackup appliance user authentication

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

Table 1-1 Sections featuring authentication

Section name	Description	Link
About user authentication on the NetBackup appliance	This section describes the types of users, user accounts, and processes allowed to access the appliance.	See "About user authentication on the NetBackup appliance" on page 15.
About configuring user authentication	This section describes the configuration options for the various types of users that can authenticate on the appliance.	See "About configuring user authentication" on page 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 23.
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 24.
About authenticating Kerberos-NIS users	This section describes the prerequisites and process to configure the appliance to register and authenticate Kerberos-NIS users.	See "About authenticating Kerberos-NIS users" on page 25.
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 27.
About user name and password specifications	This section describes the user name and password credentials.	See "About user name and password specifications" on page 28.

NetBackup Appliance 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 32.
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 33.
About the Administrator user role	This section describes the Administrator user role.	See "About the Administrator user role" on page 36.
About the NetBackupCLI user role	This section describes the NetBackupCLI user role.	See "About the NetBackupCLI user role" on page 37.

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 41.
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 43.
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 44.

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

Section name	Description	Link
Reviewing SDCS events on the NetBackup appliance	This section describes the SDCS events based on their level of security.	See "Reviewing SDCS events on the NetBackup appliance" on page 45.
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 47.
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 47.
Overriding the NetBackup appliance intrusion prevention system policy	This section describes the procedure to override the IPS policy that is applied to the appliances.	
Re-enabling the NetBackup appliance intrusion prevention system policy	This section describes the procedure to re-enable the IPS policy that is applied to the appliances.	

NetBackup Appliance log files

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

Table 1-4 Working log sections

Section name	Description	Link
About working with log files	This chapter provides an overview on all the different types of logs that you can view for the NetBackup Appliance.	See "About NetBackup Appliance log files" on page 49.
About using the Collect Log files wizard	This chapter describes the usage of the Collect Log files wizard present on the NetBackup Appliance Web Console.	See "About the Collect Log files wizard" on page 51.

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

Section name	Description	Link
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 52.
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 53.
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 54.

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 58.
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 59.
Vulnerability scanning of the NetBackup appliance	This section lists some of the security scanners that Veritas uses to verify the security of the appliance.	See "Vulnerability scanning of the NetBackup Appliance" on page 60.

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 61.
About Data Integrity	This section lists the measures that are taken to improve data integrity.	See "About data integrity" on page 62.
About Data Classification	This section lists the measures that are taken to improve data classification.	See "About data classification" on page 63.
About Data Encryption	This section lists the measures that are taken to improve data encryption.	See "About data encryption " on page 63.

NetBackup Appliance web security

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

Table 1-7 Web security sections

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

NetBackup Appliance network security

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

Table 1-8 Network security sections

Section name	Description	Link
About IPsec Channel Configuration	This section describes the IPsec configuration for NetBackup Appliances.	See "About IPsec Channel Configuration" on page 70.
About NetBackup Appliance ports	This section describes the port information for NetBackup Appliances.	See "About NetBackup Appliance ports" on page 72.

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 75.
About Call Home	This section describes the Call Home feature in the NetBackup Appliance.	See "About Call Home" on page 76.
About SNMP	This section describes the SNMP feature in the NetBackup Appliance.	See "About SNMP" on page 81.

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 83.
Listing the Recommended IPMI settings	This section lists the recommended IPMI settings for a secure configuration.	See "Recommended IPMI settings" on page 83.

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. ■ Windows: The **admin** account and AD users with the Administrator role are 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.
AppComm	The `AppComm` account is used for internal process communication.

See "About authorizing NetBackup appliance users" on page 33.

User types that can authenticate on the NetBackup appliance

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

User type	Description	Notes
Local (native user)	A local user is added to the appliance database and is not referenced to an external directory-based server like an LDAP server. Once the user has been added, you can then grant or revoke the appropriate appliance access permissions.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage local users. ■ You can use the `Settings > Security > Authentication > LocalUser` command from the NetBackup Appliance Shell Menu to add and delete local users, as well as change their passwords. ■ You cannot add local user groups. ■ A local user can have the Administrator or NetBackupCLI role. **Note:** You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from the NetBackup Appliance Shell Menu.

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

User type	Description	Notes
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 23.	■ 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.
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 24.	■ 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.

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

User type	Description	Notes
Kerberos-NIS	A NIS (Network Information Service) user or user group exists on an external NIS server. Unlike the LDAP and AD implementations, configuring the appliance to communicate with the NIS domain requires Kerberos authentication. You must have an existing Kerberos service associated with your NIS server before you can configure the appliance to register the NIS users. After configuring the appliance to communicate with the NIS server and the Kerberos server, you can register the NIS users and user groups with the appliance. Once the user has been registered (added) to the appliance, you can then grant or revoke the appropriate appliance access permissions. See "About authenticating Kerberos-NIS users" on page 25.	■ You can use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to add, delete, and manage NIS users and user groups. ■ You can use the `Settings > Security > Authentication > Kerberos` command from the NetBackup Appliance Shell Menu to add and delete NIS users and user groups. ■ You can assign the Administrator or NetBackupCLI role to a NIS user or user group. **Note:** The NetBackupCLI role can be assigned to a maximum of nine (9) user groups at any given time.

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

About configuring user authentication

Table 2-3 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 2-3 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 33.	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 2-3 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 33.	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 2-3 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 33.	The following commands and options are available under `Settings > Security > Authentication > ActiveDirectory`: ■ `Configure` - Configure the appliance to allow AD users to register and authenticate with the appliance. ■ `Groups` - Add or remove one or more AD user groups. Only the user groups that already exist on the AD server can be added to the appliance. ■ `List` - List all of the AD users and user groups that have been added to the appliance. ■ `Status` - View the status of AD authentication on the appliance. ■ `Unconfigure` - Delete the AD configuration. ■ `Users` - Add or remove one or more AD users. Only the users that already exist on the AD server can be added to the appliance.
Kerberos-NIS	You can perform the following Kerberos-NIS configuration tasks under **Settings > Authentication > Kerberos-NIS** : ■ Configure a new Kerberos-NIS configuration. ■ Unconfigure an existing Kerberos-NIS configuration. Use the **Settings > Authentication > User Management** tab in the NetBackup Appliance Web Console to add Kerberos-NIS users and user groups. See "About authorizing NetBackup appliance users" on page 33.	The following commands and options are available under `Settings > Security > Authentication > Kerberos`: ■ `Configure` - Configure the appliance to allow NIS users to register and authenticate with the appliance. ■ `Groups` - Add or remove one or more NIS user groups. Only the user groups that already exist on the NIS server can be added to the appliance. ■ `List` - List all of the NIS users and user groups that have been added to the appliance. ■ `Status` - View the status of NIS and Kerberos authentication on the appliance. ■ `Unconfigure` - Delete the NIS and Kerberos configuration. ■ `Users` - Add or remove one or more NIS users. Only the users that already exist on the NIS server can be added to the appliance.

Generic user authentication guidelines

Use the following guidelines for authenticating users on the appliance:

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

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

See "About authorizing NetBackup appliance users" on page 33.

About authenticating LDAP users

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

Pre-requisites for using LDAP user authentication

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

- The LDAP schema must be RFC 2307 or RFC 2307bis compliant.
- The following firewall ports must be open:
  - LDAP 389

- LDAP OVER SSL/TLS 636
- HTTPS 443

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

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

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

Configuration methods for LDAP user authentication

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

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

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

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

About authenticating Active Directory users

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

Pre-requisites for using Active Directory user authentication

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

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

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

- Ensure that the authorized domain user credentials are used to configure the AD server with the appliance.
- Configure the appliance with a DNS server that can forward DNS requests to an AD DNS server. Alternatively, configure the appliance to use the AD DNS server as the name service data source.

Configuration methods for Active Directory user authentication

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

Configure AD authentication using one of the following methods:

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

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

F

About authenticating Kerberos-NIS users

The NetBackup Appliance uses the built-in Pluggable Authentication Module (PAM) plug-in to support the authentication of Network Information Service (NIS) users. This functionality allows users belonging to a NIS directory service to be added and

authorized to log on to a NetBackup Appliance. NIS is considered as another type of user directory with a schema installed on it by UNIX services.

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

Pre-requisites for using NIS user authentication with Kerberos

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

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

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

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

Configuration methods for NIS user authentication with Kerberos

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

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

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

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

About the appliance login banner

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

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

Table 2-4 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 2-4 Appliance interfaces that support the login banner

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

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

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

About user name and password specifications

The user name for the NetBackup Appliance user account must be in the format that the selected authentication system accepts. Table 2-5 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 2-5 User name specifications

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

Password specifications

The NetBackup Appliance password policy has been updated to increase security on the appliance. The password for the appliance user account must be in the

format that the selected authentication system accepts. Table 2-6 lists the password specifications for each user type.

Table 2-6 Password specifications

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Maximum length	No restrictions applied	No restrictions applied	Determined by the LDAP, AD, or NIS policy
Minimum length	Passwords must contain at least eight characters.	Passwords must contain at least eight characters.	Determined by the LDAP, AD, or NIS policy
Requirements	■ One uppercase letter ■ One lowercase letter (a-z) ■ One number (0-9) ■ Dictionary words are considered as weak passwords and are not accepted. ■ The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	■ One uppercase letter ■ One lowercase letter (a-z) ■ One number (0-9) ■ Dictionary words are considered as weak passwords and are not accepted. ■ The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP, AD, or NIS policy
Space inclusion	Passwords must not include spaces.	Passwords must not include spaces.	Determined by the LDAP, AD, or NIS policy

Table 2-6 Password specifications *(continued)*

Description	Administrator (local user)	NetBackupCLI (local user)	Registered remote user
Minimum password age	0 day	0 day **Note:** You can manage the user password age using the `Manage > NetBackupCLI > PasswordExpiry` command from the NetBackup Appliance Shell Menu. For more information, refer to the *NetBackup Appliance Command Reference Guide*.	Determined by the LDAP, AD, or NIS policy
Maximum password age	99999 days (doesn't expire)	99999 days (doesn't expire)	Determined by the LDAP, AD, or NIS policy
Password history	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	The last seven passwords cannot be reused and the new password cannot be similar to previous passwords.	Determined by the LDAP, AD, or NIS policy
Password expiry	Not applicable as the password does not expire	Use the `Manage > NetBackupCLI > PasswordExpiry` command to manage NetBackupCLI user passwords.	Determined by the LDAP, AD, or NIS policy
Password lockout	None	None	Determined by the LDAP, AD, or NIS policy
Lockout duration	None	None	Determined by the LDAP, AD, or NIS policy

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

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

Password protection

The NetBackup Appliance uses the following password protection measures:

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

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

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

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

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 36.

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

Role	Description
NetBackupCLI	A user account that is assigned the NetBackupCLI role is solely restricted to run a limited set of NetBackup CLI commands and does not have access outside the scope of NetBackup software directories. Once these users log on to the appliance, they are taken to a restricted shell menu from where they can manage NetBackup. The NetBackupCLI users do not have access to the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. See "About the NetBackupCLI user role" on page 37.

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

About authorizing NetBackup appliance users

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

Table 3-2 User authorization management

Task	NetBackup Appliance Web Console	NetBackup Appliance Shell Menu
Manage users	The following options are available under **Settings > Authentication > User Management** ■ View all of the users that have been added to the appliance. ■ Expand and view all belonging users to a single user group. ■ Add and delete local users. ■ Add and delete LDAP/AD/Kerberos-NIS users and user groups.	Use the `Settings > Security > Authentication` commands to add, delete, and view appliance users. See "About configuring user authentication" on page 19.
Manage user permissions (roles)	The following options are available under **Settings > Authentication > User Management**: ■ Grant and revoke the Administrator role for users and user groups. ■ Grant and revoke the NetBackupCLI role for users and user groups. ■ Synchronize members of registered user groups with Administrator role.	The following commands and options are available under `Main > Settings > Security > Authorization`: ■ `Grant` Grant the Administrator and NetBackupCLI roles to specific users and users groups that have been added to the appliance. ■ `List` List all of the users and user groups that have been added to the appliance, along with their designated roles. ■ `Revoke` Revoke the Administrator and NetBackupCLI roles from specific users and users groups that have been added to the appliance. ■ `SyncGroupMembers` Synchronize members of registered user groups.

Notes about user management

- You cannot grant the NetBackupCLI role to an existing local user. However, you can create a local NetBackupCLI user by using the `Manage > NetBackupCLI > Create` command from theNetBackup Appliance Shell Menu.
- The NetBackupCLI role can be assigned to a maximum of nine user groups at any given time.
- Active Directory (AD) user groups and user names support the use of a hyphen character in those names. The hyphen must appear between the first and the last character of a user name or a user group name. AD user names and user group names cannot begin or end with a hyphen.
- You can list all users of a group that has maximum to 2000 users from theNetBackup Appliance Web Console. To list all of a group that has more than 2000 users, use the `List` command from theNetBackup Appliance Shell Menu.

NetBackup Appliance user role privileges

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

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

Table 3-3 User roles and privileges

User role	Privileges
NetBackupCLI	Users can only access the NetBackup CLI. See "About the NetBackupCLI user role" on page 37.
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 36.

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

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

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

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

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

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

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

See "About configuring user authentication" on page 19.

See "About authorizing NetBackup appliance users" on page 33.

About the Administrator user role

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

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

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

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

- Perform appliance initial configuration.
- Monitor hardware, storage, and SDCS logs.
- Manage storage configuration, additional servers, licenses and so on.
- Update configuration settings like **Date and Time**, **Network**, **Notification**, etc.
- Restore the appliance.
- Decommission the appliance.
- Apply patches to the appliance.
- Mount or map shares. The following limitations apply:
  - Windows: Only the local **admin** user is authorized to mount or map Windows CIFS shares.
  - Linux: Only users with a root access account can issue the mount command directly to mount NFS shares.

A local, LDAP, Active Directory (AD), or NIS user needs to have the permissions of the Administrator user role to access and administer the appliance. After you have added a new user or a user group, use the **Settings > Authentication > User Management** page from the NetBackup Appliance Web Console to grant the Administrator user permissions.

About the NetBackupCLI user role

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

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

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

Privileges	Restrictions
The NetBackupCLI user can use the NetBackup Appliance Shell Menu to do the following: ■ Run the NetBackup CLI and access the NetBackup directories and files. ■ Modify or create NetBackup notify scripts using the `cp-nbu-notify` command. ■ Run the following NetBackup commands and for the following directories that contain the NetBackup CLI: ■ `/usr/openv/netbackup/bin/*` ■ `/usr/openv/netbackup/bin/admincmd/*` ■ `/usr/openv/netbackup/bin/goodies/*` ■ `/usr/openv/volmgr/bin/*` ■ `/usr/openv/volmgr/bin/goodies/*` ■ `/usr/openv/pdde/pdag/bin/mtstrmd` ■ `/usr/openv/pdde/pdag/bin/pdcfg` ■ `/usr/openv/pdde/pdag/bin/pdusercfg` ■ `/usr/openv/pdde/pdconfigure/pdde` ■ `/usr/openv/pdde/pdcr/bin/*`	The following restrictions are placed on NetBackupCLI users: ■ NetBackupCLI users do not have access outside of the NetBackup software directories. ■ They cannot edit the `bp.conf` file directly using an editor. Use the `bpsetconfig` command to set an attribute. ■ The `cp-nbu-config` command supports creating and editing NetBackup touch configuration files only in the `/usr/openv/netbackup/db/config` directory. ■ They cannot use the `man` or `-h` command to see the help of any other command.

How to run NetBackup commands as a NetBackupCLI user

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

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

How to run special directive operations

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

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

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

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

NetBackup Administrator's Guide, Volume 1

NetBackup Commands Reference Guide

Chapter 4

Intrusion prevention and intrusion detection systems

This chapter includes the following topics:

About Symantec Data Center Security on the NetBackup Appliance

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.

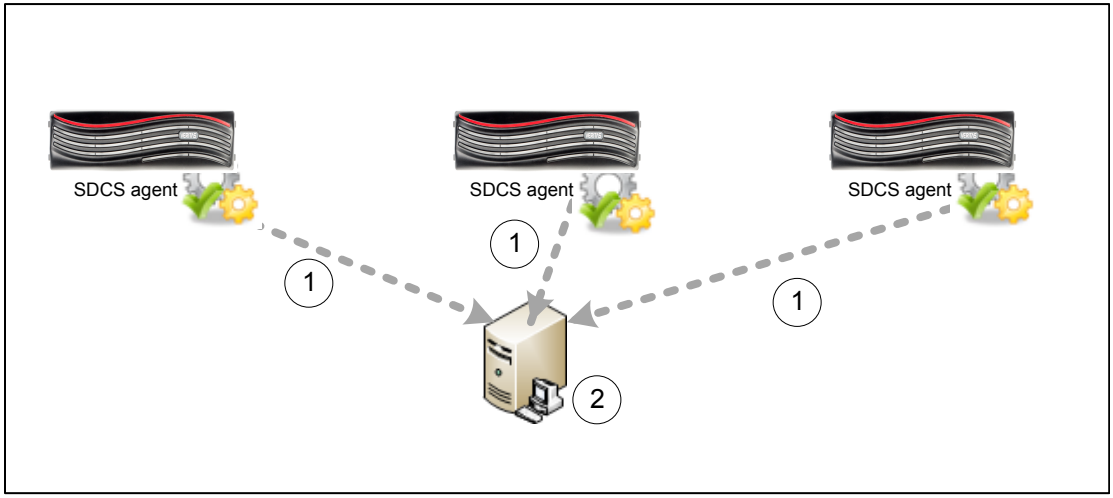
- Centralized managed mode operations
  Lets you use a central SDCS manager for an integrated view of security across multiple appliances as well as any other enterprise systems managed by SDCS.

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

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

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

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

About the NetBackup Appliance intrusion prevention system

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

The following list contains some of the IPS policy features:

- Real-time tight confinement of the appliance operating system processes and common applications, such as the following:
  - `nscd` - which caches DNS requests to cut down on remote DNS lookups.
  - `cron`
  - `syslog-ng`
  - `klogd`
  - `rpcd` for NFS
    - `rpc.idmapd`
    - `rpc.mountd`
    - `rpc.statd`
    - `rpcbind`

- Self-Protection for the SDCS agent itself to ensure that the security features and monitoring features of SDCS are not compromised.
- Lock-down of access to system binaries, except by identified and trusted applications, users, and user groups.
- Confinements that protect the system from the applications that try to install software, such as `sbin`) or change system configuration settings, such as `hosts` file.
- Prohibits applications from executing critical system calls such as `mknod`, `modctl`, `link`, `mount`, and so on.
- Prohibits unauthorized users or applications from accessing backup data, such as `/advanceddisk`, `/cat`, `/disk`, `/usr/openv/kms`, `/opt/NBUAppliance/db/config/data`, and so on.
- Restricted access to the root account by maintenance user.

About the NetBackup Appliance intrusion detection system

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

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

- User logons, logouts, and failed log on attempts
- Sudo commands
- User addition, deletion, and password changes
- User group addition, deletion, and member modifications
- System auto-start option changes
- Modifications to all system directories and files, including core system files, core system configuration files, installation programs, and common daemon files
- NetBackup services start and stop
- Detected system attacks from UNIX rootkit file/directory detection, UNIX worm file/directory detection, malicious module detection, suspicious permission change detection, and so on

- Audit of all the NetBackup Appliance Web Console and NetBackup Appliance Shell Menu activity, including shell operations for maintenance, root, and NetBackupCLI users.

Reviewing SDCS events on the NetBackup appliance

You can use the **Monitor > SDCS Events** page to view the Symantec Data Center Security (SDCS) logs. These audit logs can help in detecting security breaches and abnormal activity on the appliance. An event in the audit log includes the following details:

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

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

Table 4-1 SDCS event severity types

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

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

Severity types	Description	Events example

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

Warning	Events with a severity as Warning indicate unexpected activity or problems that have already been handled by SDCS. These Warning messages might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access to the specific resources if necessary.	For example, the following event helps to identify and unexpected activity, like the inbound connection from a local IP address. `Inbound connection allowed from <IPaddress> to local address.`

Major	Events with a severity as Major imply a more serious effect than Warning and less effect than Critical.	For example, the following event helps to identify unauthorized access.
		
		`General luser message`
		`Event source:SYSLOG Complete message:`
		`Feb 5 21:57 luser Unauthorized user by luser`
		`Denying access to system.`

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

Severity types	Description	Events example
Critical	Events with a severity as Critical indicate activity or problems that might require administrator intervention to correct.	For example, the following event can help to identify critical events that can affect the appliance in an unexpected manner. `Group Membership for "group1" CHANGED from 'admin1' to 'admin2'`

For more information about retrieving SDCS audit logs, refer to the *NetBackup Appliance Administrator's Guide*.

For information about the appliance operating system logs, such as syslogs and other appliance logs, See "About NetBackup Appliance log files" on page 49.

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. If you have not yet downloaded and installed SDCS in your environment, the server package and console package are available to download directly from the NetBackup Appliance Web Console under **Monitor > SDCS Events**. You need to make sure that the console is available to connect to the SDCS server and that the server is available to connect to the appliance.
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	You can use the **Collect Log files** wizard from the NetBackup Appliance Web Console to collect log files from an appliance. See "About the Collect Log files wizard" on page 51.	■ Logs created by the NetBackup Copy Logs tool (`nbcplogs`) ■ Appliance logs including high availability, hardware, and event logs ■ Operating system logs ■ All logs related to Media Server Deduplication Pool (MSDP) ■ All logs related to the NetBackup Appliance Web Console ■ Diagnostic information about NetBackup and the operating system ■ Hardware and storage device logs
NetBackup Appliance Web Console	You can use the **Monitor > SDCS Audit View** screen from the NetBackup Appliance Web Console to retrieve the audit logs of an appliance. See "Reviewing SDCS events on the NetBackup appliance" on page 45.	Appliance audit logs
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 52.	■ 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

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

From	Access methods	Log details
NetBackup Appliance Shell Menu	You can use the `Main > Support > Logs > VxLogView Module` *`ModuleName`* command to access the appliance VxUL (unified) logs. You can also use the `Main > Support > Share Open` command and use the desktop to map, share, and copy the VxUL logs. See "Viewing log files using the Support command" on page 52.	Appliance unified logs: ■ `All` ■ `CallHome` ■ `Checkpoint` ■ `Commands` ■ `Common` ■ `Config` ■ `CrossHost` ■ `Database` ■ `Hardware` ■ `HWMonitor` ■ `Network` ■ `RAID` ■ `Seeding` ■ `SelfTest` ■ `Storage` ■ `SWUpdate` ■ `Trace` ■ `FTMS` ■ `FTDedup` ■ `TaskService` ■ `AuthService`
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 54.	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

About the Collect Log files wizard

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

types of log files for NetBackup, the appliance, operating system, NBSU (NetBackup Support Utility), DataCollect, and others.

You can collect log files from any NetBackup appliance.

After you have generated the log files you can email them to recipients, download them to your computer, or upload them to Veritas Support.

Refer to the following for information about the Appliance Diagnostics Center:

See "About NetBackup Appliance log files" on page 49.

Viewing log files using the Support command

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

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

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

See "Where to find NetBackup Appliance log files using the Browse command" on page 53.

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

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

- `Logs VXLogView Module module_name`

  Use to display debug information for a specific module.

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

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

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

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

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

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

See "About NetBackup Appliance log files" on page 49.

Where to find NetBackup Appliance log files using the Browse command

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

Table 5-2 NetBackup Appliance log file locations

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

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

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

Operating system (OS) installation log	`<DIR> OS`
	`boot.log`
	`boot.msg`
	`boot.omsg`
	`messages`

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

See "About NetBackup Appliance log files" on page 49.

Gathering device logs on a NetBackup appliance

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

The DataCollect command collects the following logs:

- Release information

- Disk performance logs
- Command output logs
- iSCSI logs

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

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

To gather device logs with the DataCollect command

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

   `DataCollect`

   The appliance generates the device log in the `/tmp/DataCollect.zip` file.
3. Copy the `DataCollect.zip` to your local folders using the `Main > Support > Logs > Share Open` command.
4. You can send the `DataCollect.zip` file to the Veritas Support team to resolve your issues.

See "About NetBackup Appliance log files" on page 49.

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.

Secure log transmission

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

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

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

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

Configuration

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

- `LogForwarding Enable`
  Configures the feature functionality.

- `LogForwarding Disable`

  Deletes the configuration and disables the feature.

- `LogForwarding Interval`

  Sets how often logs are forwarded. Select from 0 (continuous), 15, 30, 45, or 60 minutes.

- `LogForwarding Share`

  Opens or closes an NFS or a CIFS share on the appliance for obtaining the required certificate and private key files. The share paths are the following:

  NFS: `<appliance.name>:/inst/logforwarding`.

  CIFS: `\\<appliance.name>\logforwarding`

- `LogForwarding Show`

  Shows the current configuration and status.

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

Table 5-3 `LogForwarding > Enable` command prompts

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

The NetBackup appliances run a customized Linux operating system (OS) provided by Veritas. Each NetBackup appliance software release includes the latest appliance OS and NetBackup software. In addition to regular security patches and updates, the appliance OS 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.
- Symantec Data Center Security: Server Advanced (SDCS) intrusion prevention and intrusion detection software that hardens the appliance OS and protects the backup data by isolating and sandboxing each process and all system files.
- Regular scan of the NetBackup 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.
- Nonusers and unused service accounts are removed or disabled.
- The appliance OS 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. The appliance OS 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`.
- TCP forwarding for SSH is disabled with the addition of `AllowTcpForwarding no` and `X11Forwarding no` to `/etc/ssh/sshd_config`.
- IP forwarding is disabled on the appliance OS 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.
- The NetBackup appliance does 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 which 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 the appliance OS are searched and fixed.
- The permissions of all the orphaned and unowned files and directories that are found in the appliance OS are searched and fixed.

Major components of the NetBackup Appliance OS

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

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

Software component	Version
Red Hat Enterprise Linux (RHEL)	6.8

Table 6-1 Major software components included in VxOS for appliance version 3.1.2. *(continued)*

Software component	Version
Veritas InfoScale	6.2 **Note:** The Veritas InfoScale installation is modified and tuned for maximum performance on the appliance.
Java Runtime Environment (JRE)	8.0_112
Apache Tomcat	8.0.33
RabbitMQ	3.5.0-1
MongoDB	
Intel IPMI Utils	

Vulnerability scanning of the NetBackup Appliance

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

Table 6-2 Vulnerability scanning software and versions

Security scanner	Version
Nessus™ Professional	6.8.1
QualysGuard™	8.7.24-1

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) are marked with Cyclic Redundancy Check (CRC) digital signatures when the backup takes place. A maintenance task continuously re-computes the CRC digital signatures and compares it with the original signature to detect if there has been any unwanted tampering or corruption in the Deduplication Pool.
- Unintended access to appliance storage is prevented by password protecting logins to the appliance.
- Access to shared data limited to authorized users only and NetBackup processes.

- Usage of HTTPS protocol and port 443 to connect to the Veritas AutoSupport server to upload hardware and software information using the Call Home feature. Veritas Technical Support uses this information to resolve any issues that you might report. This information is retained for 90 days and purged at the Veritas Secure Operations Center.
- Support “Checkpoints” that lets you easily roll back the entire system to a point in time to undo any misconfiguration. The checkpoint captures the following components:
  - Appliance operating system
  - Appliance software
  - NetBackup software
  - Tape media configuration on the master server
  - Networking configuration
  - LDAP configuration if it exists
  - Fiber channel configuration
  - Any previously applied patches

  Note: Critical components like the NetBackup Catalog and the KMS database may need additional configuration.

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

About data integrity

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

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

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

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

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

About data classification

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

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

NetBackup provides the following default data classifications:

- Platinum
- Gold
- Silver
- Bronze

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

About data encryption

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

- Transmits data in encrypted formats by using secure tunnels. These configurations can be made by client-side encryption and also replication. If these options are not used, once the data is transmitted from the appliance, the network infrastructure is used for securing data in flight.

- Starting with NetBackup Appliance version 3.0 (NetBackup version 8.0), MSDP provides AES encryption. If your environment uses encrypted MSDP, new incoming data gets encrypted with AES 128-bit (default) or AES 256-bit. For more information, see the following NetBackup documents:
  Veritas NetBackup Deduplication Guide
  Veritas NetBackup Security and Encryption Guide
- Supports encryption using NetBackup Key Management Service (KMS) which is integrated with NetBackup Enterprise Server 7.1. See "KMS support " on page 64.

KMS support

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

The following describes the KMS key features:

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

About the keys used under KMS

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

Table 7-1 KMS files

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

Configuring KMS

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

See "About the NetBackupCLI user role" on page 37.

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

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

To configure and enable KMS on an appliance

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

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

3. Start nbkms. For example:

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

4. Create a Key group. For example:

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

5. Create an active key. For example:

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

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.

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

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

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

Third-party certificates

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

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

See "Implementing third-party SSL certificates" on page 67.

Implementing third-party SSL certificates

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

Note: Contact Veritas Technical Support if you need assistance with this procedure.

To implement third-party SSL certificates:

1 Prepare the keystore file for web services.

This task varies with the type of PKCS (Public-key Cryptography Standards) you use. No matter which PKCS type you choose, the certificate must contain the following extension:

SubjectAlternativeName [

DNSName: localhost

IP addresses: 127.0.0.1

Ensure that the **SubjectAlternativeName** certificate extension contains all the appliance hostnames and IP addresses by which the appliance can be reached, including **localhost** and **127.0.0.1**. You must include the fully qualified hostnames and the short names.

The following describes the preparation required to use PKCS# 7 and PKCS# 12 standard formats:

- PKCS#7 (X.509) format
  Use the following link:
  convert certificate
- PKCS#12 format

  Do the following:

  - To convert a PEM formatted x509 Cert and Private Key to a PKCS# 12, type the following commands:

```
openssl pkcs12 -export -in server.crt -inkey server.key -out
server.p12 -name tomcat -CAfile ca.crt -caname root
```

For more information on `openssl` usage, refer to https://www.openssl.org/.

- At the bottom of the certificate file `server.crt`, make sure that you append the chain of intermediary certificate authority (CA) certificates, up to and including the root CA certificate.
- Make sure that you secure the PKCS #12 file with a password. When the password is not applied to the file, you may get a null reference exception when you try to import the file.
- To convert the PKCS #12 file to a Java Keystore, type the following commands:

```
keytool -importkeystore -deststorepass appliance -destkeypass
appliance -destkeystore keystore -srckeystore server.p12
-srcstoretype PKCS12 -srcstorepass yourpassword -alias tomcat
```

Note: Make sure to specify the same password for the `-deststorepass` and `-destkeypass` options. Otherwise, you may get an exception when the web server starts. For the password, only alphanumeric characters are supported. The default password is *appliance*. Also, make sure to specify **tomcat** for the `-alias` option. Otherwise, you may get an exception when the web server starts.

For more information on `keytool` usage, refer to the following link: http://docs.oracle.com/javase/8/docs/technotes/tools/solaris/keytool.html

2 Type the following command to shut down the database and relevant services:

```
/opt/IMAppliance/scripts/infraservices.sh database stop
```

```
/opt/IMAppliance/scripts/infraservices.sh webserver stop
```

3 Backup the existing web server keystore file with the following command:

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

4 Replace the existing keystore file from the `/opt/apache-tomcat/security/` directory with the new keystore file.

5. Set the permissions to the new keystore file:

   ```
   chmod 700 /opt/apache-tomcat/security

   chmod 600 /opt/apache-tomcat/security/keystore

   chown –R tomcat:tomcat /opt/apache-tomcat/security
   ```

6. Type the following command to update the web server configuration if you choose to use your own non-default password in the previous steps:

   ```
   /opt/apache-tomcat/vrts/scripts/tomcat_instance.py update
   --keystore --password <your password>
   ```

7. Update the **Tomcat_Keystore** and **Tomcat_Keystore_Passwd** settings in the `/etc/rc.d/init.d/as-functions` file.

8. The server-side and client-side certificates of the MongoDB are stored in `/config/mongodb_ssl_keycert.pem`. Import the certificates to the file as follows:

   ```
   /usr/bin/openssl pkcs12 -in server.p12 -out
   /config/mongodb_ssl_keycert.pem -passin pass: <keyPassword>
   -passout pass: <keyPassword>
   ```

9. Edit the line containing `sslPEMKeyPassword` in `/etc/mongod.conf` and specify the passphrase of the private key (typically **appliance**).

10. Type the following commands to restart the web service:

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

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

11. Type the following commands to restart the AutoSupport Service:

    ```
    service as-alertmanager stop

    service as-analyzer stop

    service as-transmission stop

    service as-alertmanager start

    service as-analyzer start

    service as-transmission start
    ```

Chapter 9

Network security

This chapter includes the following topics:

About IPsec Channel Configuration

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

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

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

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

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

Managing IPsec configuration

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

Table 9-1 IPsec commands

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

Table 9-1 IPsec commands *(continued)*

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

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

About NetBackup Appliance ports

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

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

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

Table 9-2 Inbound ports

Port	Service	Description
22	ssh	In-band management CLI **Note:** Port 22 is blocked for the Remote Management Module (RMM). You can enable SSH later. See "Enabling SSH on the Remote Management Module" on page 86.
443	HTTPS	In-band management GUI
2049	NFS	NFS
445		CIFS (for the Log/Install shares)

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

Table 9-3 Outbound ports

Port	Service	Description
443	HTTPS	Call Home notifications to Veritas Download SDCS certificate
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 85.

A complete list of all the applicable ports is available in the *NetBackup Network Ports 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 MyAppliance portal is the unified address that you register the appliance and edit registration details.

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

- Proactive monitoring lets Veritas support to automatically create cases, fix issues, and dispatch any appliance parts that might be at risk.
- The AutoSupport infrastructure within Veritas analyzes the Call Home data from appliance. This analysis provides proactive customer support for hardware failures, reducing the need for backup administrators to initiate support cases.
- With AutoSupport ability, Veritas support can begin to understand how customers configure and use their appliances, and where improvements would be most beneficial.
- Send and receive status and alert notifications for the appliance.
- Receive hardware and software status using Call Home.

- Provide more insight into the issues and identify any issues that might further occur as a result of the existing issue.
- View reports from the Call Home data to analyze patterns of hardware failure, and see usage trends. The appliance sends health data every 30 minutes.

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

Data security standards

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

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

About Call Home

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

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

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

To obtain the serial number of your appliance from theNetBackup Appliance Web Console, go to the **Monitor > Hardware > Health details** page. To determine the serial number of your appliance using the shell menu, go to the `Monitor > Hardware` commands. For more information about the `Monitor > Hardware` commands, refer to the *NetBackup Appliance Command Reference Guide*.

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

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

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

Monitoring status	Failure routine

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

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

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

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

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

See "Configuring Call Home from the NetBackup Appliance Shell Menu" on page 78.

See "About AutoSupport " on page 75.

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 76.

Enabling and disabling Call Home from the appliance shell menu

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

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

To enable or disable Call Home from the shell menu

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

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

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

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

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

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

- Further, you are required to answer the following:

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

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

  ```
  Successfully set proxy server
  ```

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

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

Understanding the Call Home workflow

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

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

The appliance initiates all communications. Your appliance needs access to https://receiver.appliance.veritas.com.

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

- Access a port to https://receiver.appliance.veritas.com every 24 hours.
- Perform a self-test operation to https://receiver.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 76.

See "About AutoSupport " on page 75.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It uses either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) for transport, depending on configuration. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

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

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

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

NetBackup Appliance 3.0 supports SNMP v2.

About the Management Information Base (MIB)

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) that is associated with it. Each OID consists of the numbers that are separated by decimal points (for example, 1.3.6.1.4.1.48328.1).

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

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

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

Chapter 11

Remote Management Module (RMM) security

This chapter includes the following topics:

Introduction to IPMI configuration

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.

Login

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

Table 11-1 Login security settings

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

LDAP Settings

Veritas recommends that you enable LDAP authentication.

SSL Upload

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

Remote Session

Table 11-2 Remote session security settings

Settings	Recommended values
KVM Encryption	AES
Media Encryption	Enable

Cipher recommendation

- Do NOT set cipher to zero on the IPMI channel

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

- Only use ciphers 3, 8, and 12.

Ethernet connection settings

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
80	HTTP	Out-of-band management (ISM+ or RM*)
443	HTTP	Out-of-band management (ISM+ or RM*)
5900	KVM	CLI access, ISO & CDROM redirection

Table 11-3 RMM ports *(continued)*

Port	Service	Description
623	KVM	
7578	RMM	CLI access
5120	RMM	ISO & CD-ROM redirection
5123	RMM	Floppy redirection
7582	RMM	KVM
5124	HTTPS	CDROM
22 or 66	SSH	Disabled by default
5127		USB or floppy

+ NetBackup Integrated storage manager

* Veritas Remote Management – Remote Console

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

Enabling SSH on the Remote Management Module

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

To enable SSH on the Remote Management Module

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

Replacing the default IPMI SSL certificate

Veritas recommends that the default IPMI SSL certificate used to access the IPMI web interface be replaced with either a certificate signed by a trusted internal or external Certificate Authority (in PEM format), or by a self-signed certificate. You

can use the following procedure to create a minimal self-signed certificate on a Linux computer and import it into the IPMI web interface:

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

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

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

Generating RSA private key, 2048 bit long modulus

.....+++

 .+++

 e is 65537 (0x10001)
```

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

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

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

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

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

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

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

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

-out ipmi.crt -signkey ipmi.key

-days 365

 Signature ok

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

/O=Veritas/OU=Your OU/

CN=hostname.your.company/

emailAddress=email@your.company


Getting Private key
```

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

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

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

6 Log in to your Veritas Remote Management (IPMI web interface).

7 Click **Configuration > SSL**.

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

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

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

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

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

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

13. A confirmation appears stating that the certificate and key were uploaded successfully, press **OK** to restart the Web service.
14. Close and reopen the Veritas Remote Management (IPMI web interface) interface to verify that the new certificate is being presented.

Chapter 12

STIG and FIPS conformance

Appendix A

Security release content

This appendix includes the following topics:

NetBackup Appliance security release content

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

- After you remove a user from the AD user group, the appliance requires up to 30 minutes to synchronize group members with the AD server. During this period, the deleted user still can access the appliance. This behaviour is caused by a dependency limitation of the 3rd Party software Samba 3.5.
- The appliance software is updated to the RHEL 6.8 Kernel to address the following security vulnerabilities:
  - CVE-2015-5157
  - CVE-2015-8767
  - CVE-2010-5313
  - CVE-2013-4312
  - CVE-2014-7842
  - CVE-2014-8134
  - CVE-2015-5156
  - CVE-2015-7509
  - CVE-2015-8215
  - CVE-2015-8324
  - CVE-2015-8543

- CVE-2016-4565

- The `libtiff-3.9.4-18.el6_8` package has been updated to address the following security vulnerabilities:
  - CVE-2014-9655
  - CVE-2015-1547
  - CVE-2015-8784
  - CVE-2015-8683
  - CVE-2015-8665
  - CVE-2015-8781
  - CVE-2015-8782
  - CVE-2015-8783
  - CVE-2016-3990
  - CVE-2016-5320
  - CVE-2014-8127
  - CVE-2014-8129
  - CVE-2014-8130
  - CVE-2014-9330
  - CVE-2015-7554
  - CVE-2015-8668
  - CVE-2016-3632
  - CVE-2016-3945
  - CVE-2016-3991
- The `libxml2-2.7.6-21.el6_8.1` and `libxml2-python-2.7.6-21.el6_8.1` packages have been updated to address the security vulnerability RHSA-2016:1292.
- The JRE version has been updated to 1.8.0_92 to address the security vulnerabilities:
  - CVE-2016-3458
  - CVE-2016-3485
  - CVE-2016-3498
  - CVE-2016-3500

- CVE-2016-3503
- CVE-2016-3508
- CVE-2016-3511
- CVE-2016-3550
- CVE-2016-3552
- CVE-2016-3587
- CVE-2016-3598
- CVE-2016-3606
- CVE-2016-3610
- CVE-2016-0686
- CVE-2016-0695

- The Kernel packages have been updated to `kernel-2.6.32-573.el6` to address the following security vulnerabilities:
  - CVE-2015-5157
  - CVE-2015-8767
- The `openssl-1.0.1e-48.el6_8.1` and `openssl-devel-1.0.1e-48.el6_8.1` packages have been updated to address the following security vulnerabilities:
  - CVE-2016-2108
  - CVE-2016-2105
  - CVE-2016-2106
  - CVE-2016-2107
  - CVE-2016-0799
  - CVE-2016-2842
  - CVE-2016-2109

Index