Veritas NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 8.2

VERITAS™

Veritas NetBackup™ Security and Encryption Guide

Document version: NetBackup 8.2

Legal Notice

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://sort.veritas.com/documents

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:

NB.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 9

Increasing NetBackup security

This chapter includes the following topics:

- About NetBackup security and encryption

- NetBackup security implementation levels

- World-level security

- Enterprise-level security

- Datacenter-level security overview

- NetBackup Access Control (NBAC)

- Combined world, enterprise, and data center levels

- NetBackup security implementation types

- Operating system security

- NetBackup security vulnerabilities

- Standard NetBackup security

- Client side encryption security

- NBAC on master, media server, and graphical user interface security

- NBAC complete security

About NetBackup security and encryption

NetBackup security and encryption provide protection for all parts of NetBackup operations on NetBackup master servers, media servers, and attached clients. Also made secure are the operating systems on which the servers and clients are running. The backup data is protected through encryption processes and vaulting. NetBackup data that is sent over the network is protected by dedicated and secure network ports.

The various level and implementation of NetBackup security and encryption are included in the following topics.

See "NetBackup security implementation levels" on page 16.

See "NetBackup Access Control (NBAC)" on page 20.

See "Operating system security" on page 27.

See "Standard NetBackup security" on page 28.

See "Client side encryption security" on page 29.

See "NBAC on master, media server, and graphical user interface security" on page 31.

See "NBAC complete security" on page 33.

NetBackup security implementation levels

The NetBackup security implementation perspective begins in a very broad sense at the world level and becomes more detailed at the enterprise level. Security becomes very specific at the data center level.

Table 1-1 shows how NetBackup security levels can be implemented.

Table 1-1   NetBackup security implementation levels

Security level	Description
World level	Specifies the web server access and the encrypted tapes that are transported and vaulted
Enterprise level	Specifies internal users and security administrators
Datacenter level	Specifies NetBackup operations

World-level security

World-level security lets external users access corporate web servers behind firewalls and allows encrypted tapes to be transported and vaulted off site. World-level security encompasses the enterprise level and the data center level.

Figure 1-1   World-level security scope

World Level

Transport

Vault off-site

External Users

Internet
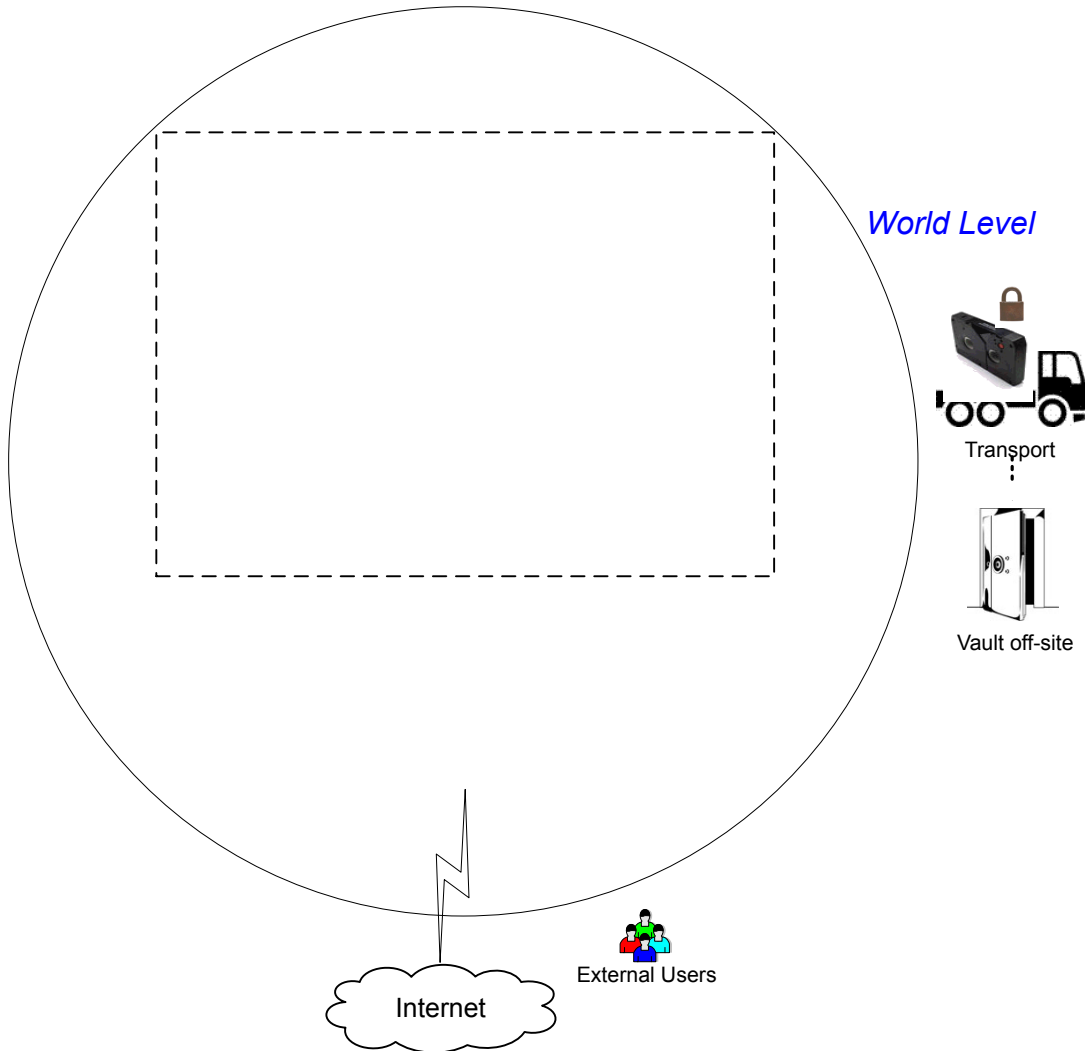
Table 1-2   Types of world-level security

Type	Description
World-level external users	Specifies that external users can access web servers behind firewalls. External users cannot access or use NetBackup functionality from the Internet, because the external firewall prevents NetBackup ports from being accessed.
World-level Internet	Specifies a collection of interconnected computer networks that are linked by copper wires, fiber cables, and wireless connections. Corporate web servers can be accessed from the Internet by using HTTP ports through firewalls.
World-level WAN	The Wide Area Network (WAN) is not shown in the security overview illustration. The WAN is a dedicated high-speed connection used to link NetBackup data centers that are geographically distributed.
World-level transport	Specifies that a transport truck can move encrypted client tapes off-site to secure vault facilities.
World-level vault off-site	Specifies that encrypted tape can be vaulted at secure storage facilities other than the current data center.

Enterprise-level security

Enterprise-level security contains more tangible parts of the NetBackup security implementation. It encompasses internal users, security administrators, and the data center level.

Figure 1-2   Enterprise-level security scope

Security Overview
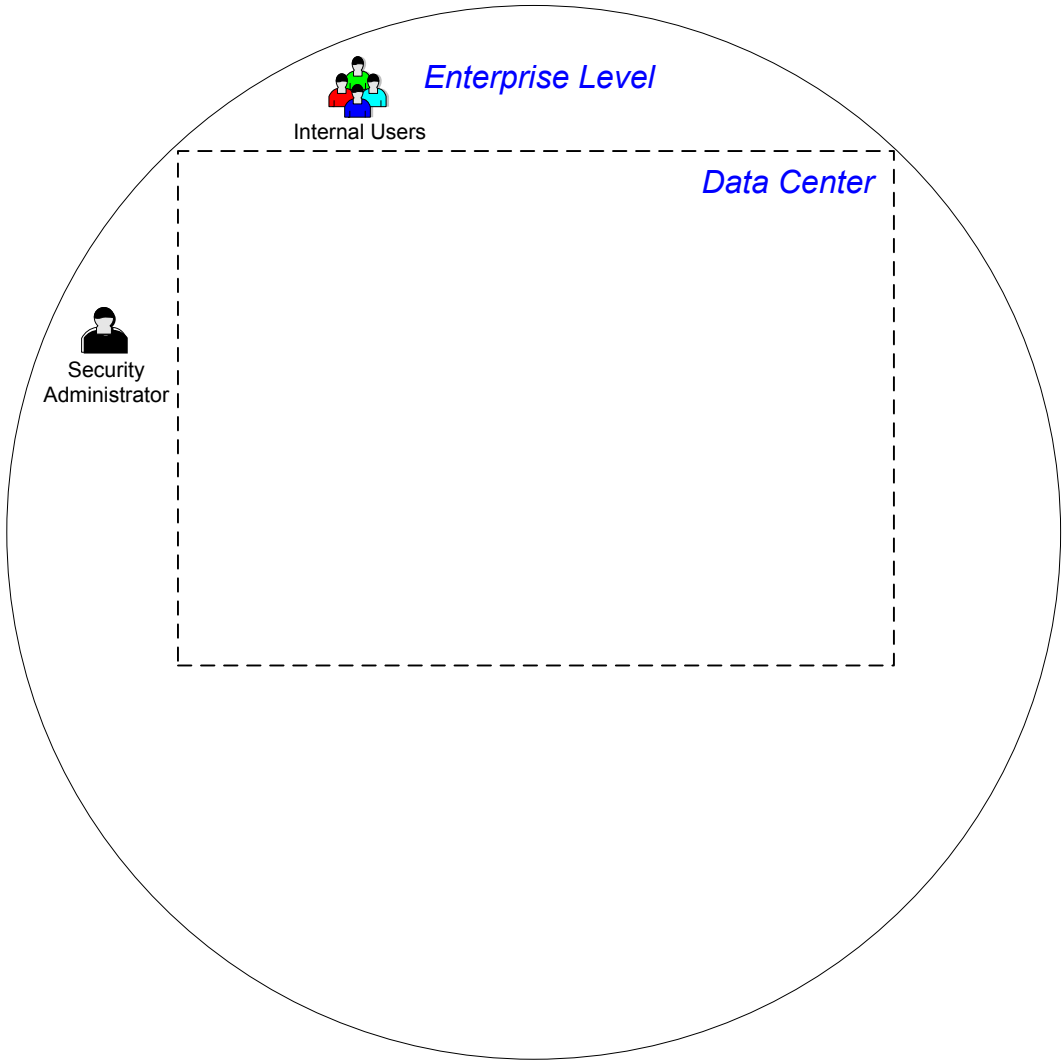
Table 1-3   Types of enterprise-level security

Type	Description
Internal users	Specifies the users who have permissions to access and use NetBackup functionality from within the data center. Internal users are typically a combination of individuals such as database administrators, backup administrators, operators, and general system users.
Security administrator	Specifies a user who has been granted administrator permissions to access and manage the NetBackup security functionality from within the data center.

Datacenter-level security overview

Datacenter-level security comprises the core of NetBackup security functionality. It can consist of a workgroup, a single data center, or a multi-datacenter.

Table 1-4 describes the deployment models unique to datacenter-level security.

Table 1-4   Deployment models for datacenter-level security

Type	Description
Workgroup	A small group of systems (less than 50) used with NetBackup in a wholly internal fashion.
Single datacenter	A medium-to-large group of hosts (greater than 50) and can back up hosts within the demilitarized zone (DMZ).
Multi-datacenter	Specifies a medium to large group of hosts (greater than 50) that span two or more geographic regions. They can connect by WAN. This configuration can also include hosts in the DMZ that are backed up.

See "NetBackup security implementation levels" on page 16.

NetBackup Access Control (NBAC)

The NetBackup Access Control (NBAC) functionality incorporates the NetBackup Product Authentication and Authorization into NetBackup, increasing security for the master servers, media servers, and clients.

See "About NetBackup security and encryption" on page 16.

Important points about NBAC include:

■ Authentication and Authorization are used together

- NBAC uses authentication identities from a trusted source to reliably identify involved parties. Access decisions can then be made for manipulation of NetBackup based on those identities. Note that NetBackup Security Services are now embedded.

- The NetBackup Product Authentication and Authorization consist of the root broker, authentication broker, authorization engine, and the graphical user interface.

- Oracle, Oracle Archiver, DB2, Informix, Sybase, SQL Server, SAP and EV Migrator are not supported with NBAC.

- NBAC is not supported on Appliances.

- The NetBackup catalog backup is supported with NBAC.

The following table describes the NetBackup components that are used in security.

Table 1-5   NetBackup components used in security

Component	Description
Root broker	The NetBackup master server is the root broker in a data center installation. There is no provision to use another root broker. The recommendation is to allow trust between root brokers. The root broker authenticates the authentication broker. The root broker does not authenticate clients.
Authentication broker	Authenticates the master server, media server, graphical user interface, and clients by establishing credentials with each one of them. The authentication broker also authenticates a user when operating a command prompt. There can be more than one authentication broker in a data center installation. The authentication broker can be combined with the root broker.
Authorization engine	Communicates with the master server and the media server to determine the permissions of an authenticated user. These permissions determine the functionality available to a given server. The authorization engine also stores user groups and permissions. Only one authorization engine is required in a data center installation. The authorization engine also communicates over the WAN to authorize other media servers in a multi-datacenter environment.
graphical user interface	Specifies a Remote Administration Console that receives credentials from the authentication brokers. The graphical user interface then may use the credentials to gain access to functionality on the clients, media, and master servers.
Master server	Communicates with the root broker and authentication broker, graphical user interface, authorization engine, media server, and clients.

Table 1-5   NetBackup components used in security *(continued)*

Component	Description
NetBackup administrator	Specifies a user who has been granted administrator permissions to access and manage the NetBackup functionality from within the data center.
Media server	Communicates with the master server, root broker and authentication broker, authorization engine, and clients 1 through 6. The media server writes unencrypted data to tape for client 5 and encrypted data to tape for client 6.
Clients	Specifies that clients 1 through 4 are standard NetBackup types. Client 5 is a web server type located in the DMZ. Client 6 is a client side encrypted type also located in the DMZ. All client types are managed by the master server and have their data backed up to tape through the media server. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.
Tapes	Specifies that the tape security in NetBackup can be increased by adding the following: ■ Client side encryption ■ Encryption of data at rest Unencrypted and encrypted data tapes are produced in the data center. The unencrypted tape data is written for clients 1 through 5 and stored on-site at the data center. The encrypted tapes are written for client 6 and are transported off-site to a vault for disaster recovery protection.
Encryption	Specifies that NetBackup encryption can increase security by providing the following: ■ Greater data confidentiality ■ The loss of physical tape is not as critical if all the data is effectively encrypted ■ The best risk mitigation strategy For more information about encryption: See "Encryption security questions to consider" on page 335.

Table 1-5   NetBackup components used in security *(continued)*

Component	Description
Data over the wire security	Includes the communication between master servers, media servers, clients, and communication using ports through firewalls and over WANs.
	For more information about ports:
	See "About NetBackup TCP/IP ports" on page 73.
	The data over the wire part of NetBackup can help increase security in the following ways:
	■ NetBackup Access Control (NBAC)
	■ Classic NetBackup daemons employ authentication when NBAC is enabled
	■ CORBA daemons use the fully encrypted channels that support confidentiality, and provide data integrity
	■ Firewalls
	■ Disabling the unused ports in NetBackup and in other products: See "Enabling or disabling random port assignments" on page 86.
	■ PBX and VNETD dedicated ports provide increased NetBackup security
	■ Central set of ports to monitor and open through firewalls
	Note: Communication between NetBackup 8.1 and later hosts is secure.
	See "About secure communication in NetBackup" on page 207.

Table 1-5   NetBackup components used in security *(continued)*

Component	Description

Firewall security	Specifies that the NetBackup firewall support can help increase security.
	
	Important points about firewall security include the following:
	
	■ Veritas recommends the use of firewall and intrusion detection protection for NetBackup
	■ Firewall protection relates to general network security from a NetBackup standpoint. It focuses on reducing the possible "door locks" for a thief to try to pick. It may be helpful to review the possibility of blocking NFS, telnet, FTP, email ports. They are not strictly needed for NetBackup use and can provide an "open door" for unwanted access.
	■ Secure the master server as much as possible
	■ Firewalls can include internal firewalls and external firewalls, as follows:
	  ■ Internal firewall - allows NetBackup to access web server client 5 and encrypted client 6 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. The HTTP ports are open in the External Firewall and are not allowed to pass through the internal firewall.
	  ■ External firewall - allows external users to access the web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of web server client 5 can pass through the external firewall to the Internet.

Demilitarized zone (DMZ)	Specifies that the demilitarized zone (DMZ) increases security as follows: ■ The DMZ is a restricted area in which the number of ports that are allowed for specific hosts is highly controlled ■ The DMZ exists between the external firewall and the internal firewall. The common area in this example is the web server. The external firewall blocks all ports except for the HTTP (standard) and HTTPS (secure) web ports. The internal firewall blocks all ports except for NetBackup and database ports. The DMZ eliminates the possibility of external Internet access to internal NetBackup server and database information. The DMZ provides a "safe" area of operation for the web server client 5 and encrypted client 6 between the internal firewall and external firewall. The web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports. Figure 1-3 shows an example internal and external firewall with DMZ.

The following figure shows an example of the internal and the external firewall with DMZ.

Figure 1-3   Example firewalls and DMZ

Minimum Firewall Configuration
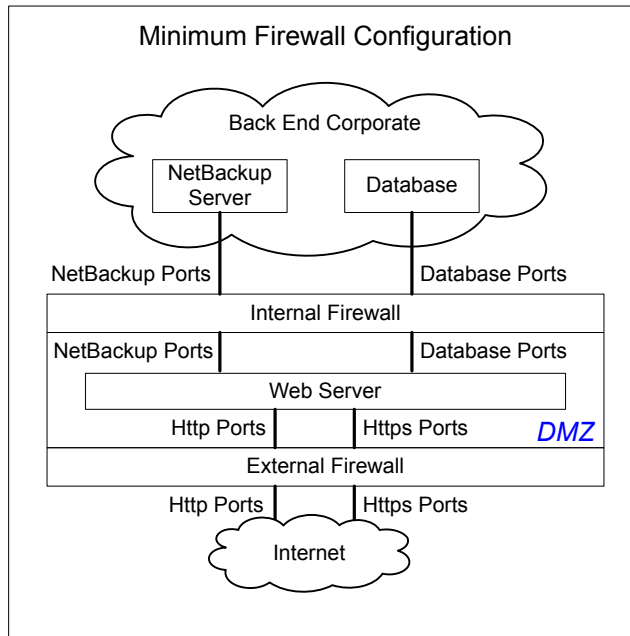
Combined world, enterprise, and data center levels

The combined world, enterprise, and data center levels model is the area where typical full-functioning NetBackup operations occur. Through the outermost world level, external users can access corporate web servers behind firewalls and encrypted tapes are transported and vaulted off-site. At the next level deeper, the enterprise level, functions related to internal users, security administrators, and the data center level occur. At the deepest level, the data center level, the core NetBackup security functionality occurs through a workgroup, single data center, or multi-datacenter.

The following figure shows the combined world, enterprise, and data center levels model.

Figure 1-4   Combined world, enterprise, and data level
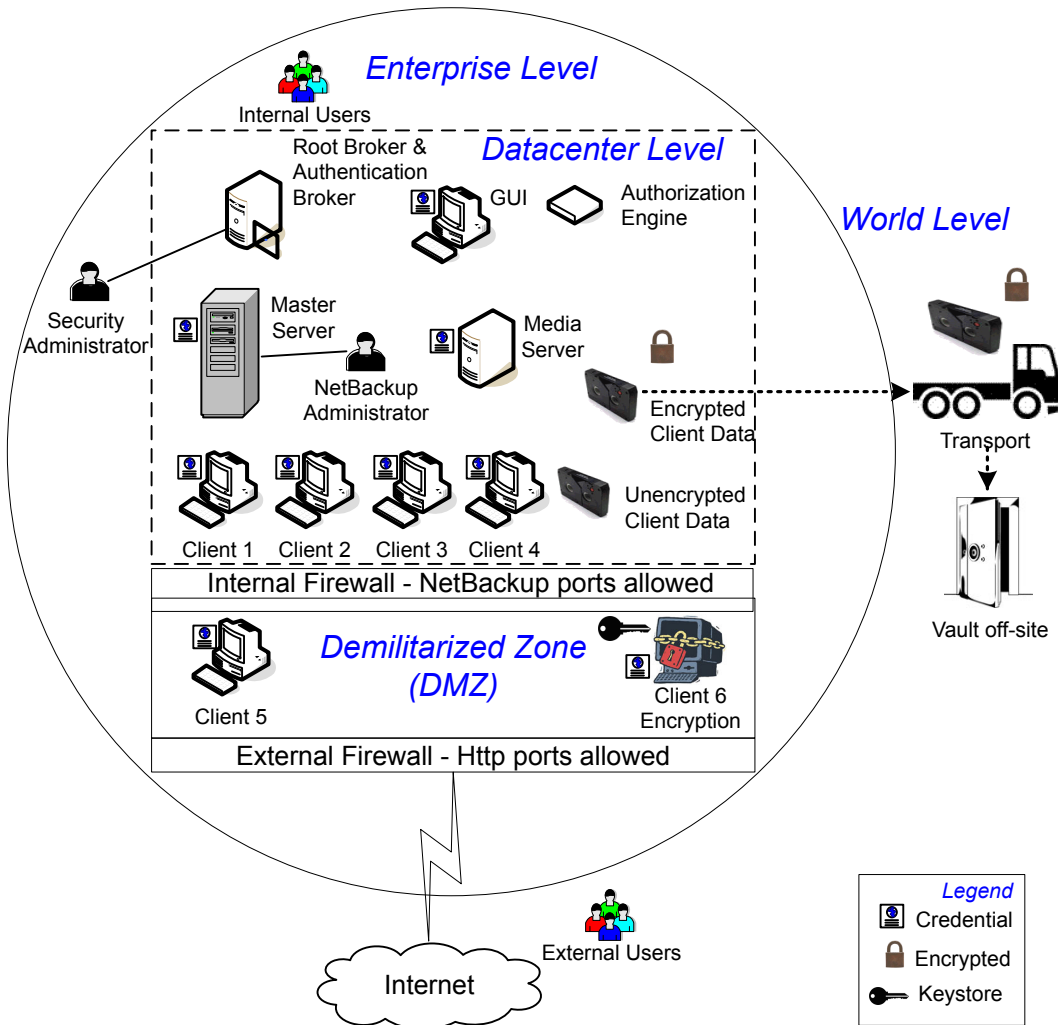
NetBackup security implementation types

The following table shows the NetBackup security implementation types, characteristics, complexity, and potential security deployment models.

Table 1-6   Security implementation types

Security implementation type	Characteristics	Complexity	Security deployment models
See "Operating system security" on page 27.	- Operating system dependent - Varies based on system components	Variable	Workgroup Single data center Multi-datacenter
See "Standard NetBackup security" on page 28.	- Manage as root or administrator - Data is not encrypted	Low	Workgroup with NetBackup Single data center with standard NetBackup Multi-datacenter with standard NetBackup
See "Client side encryption security" on page 29.	- Data is encrypted on the client - Encrypted data is sent over the wire - Can affect CPU performance on the client - Location of keys	Medium	Single data center with client side encryption Multi-datacenter with client side encryption
See "NBAC on master, media server, and graphical user interface security" on page 31.	- NBAC gives authorization to access master and media servers - Authenticates the system and users to access master and media servers	Medium	Single data center with NBAC on master and media servers Multi-datacenter with NBAC on master and media servers
See "NBAC complete security" on page 33.	- NBAC gives authorization throughout the system - NBAC gives authentication throughout the entire system (servers, clients, and users)	High	Single data center with NBAC complete Multi-datacenter with NBAC complete

Operating system security

Operating system security can be enhanced for master servers, media servers, and clients by doing the following:

- Installing operating system patches

Operating system patches include the upgrades applied to the operating system to keep it running at the highest level of system integrity. Upgrades and patches should be kept at the level that is specified by the vendor.

■ Following safe firewall procedures

■ Employing least privilege administration

■ Limiting root users

■ Applying the security protocol over IP (IPSEC) hardware

■ Turning off unused ports of the outward facing applications

■ Providing a secure base on which to run NetBackup

■ Adding a first line of intelligence in an investigation to determine if the operating system has been compromised

■ Making sure that security implementation is the same for all operating systems

■ Adding full interoperability between various systems using NBAC in a heterogenous environment

NetBackup security vulnerabilities

Veritas suggests that protective measures are in place to guard against the rare instance of a possible NetBackup security vulnerability as follows:

■ A full NetBackup update is provided with the next NetBackup maintenance patch

■ The importance of accumulative NetBackup updates

■ Use the Veritas website for information on possible security vulnerability issues: https://www.veritas.com/content/support/en_US/security.html, or http://www.veritas.com/security

■ Use email contacts for possible security vulnerability issues: secure@veritas.com

Standard NetBackup security

The standard NetBackup security only includes the security that is offered by the operating system and the hardware components of the data center. The authorized NetBackup users administer as root or administrator. Client data is not encrypted. The master server, media server, and client are all run within a local enterprise data center. Unencrypted data is usually stored on site, presenting a relatively high risk for no disaster recovery plan. Data that is sent off-site could be subject to a violation of confidentiality if it is intercepted.

The following figure shows an example of the standard NetBackup configuration.

Figure 1-5   Standard NetBackup
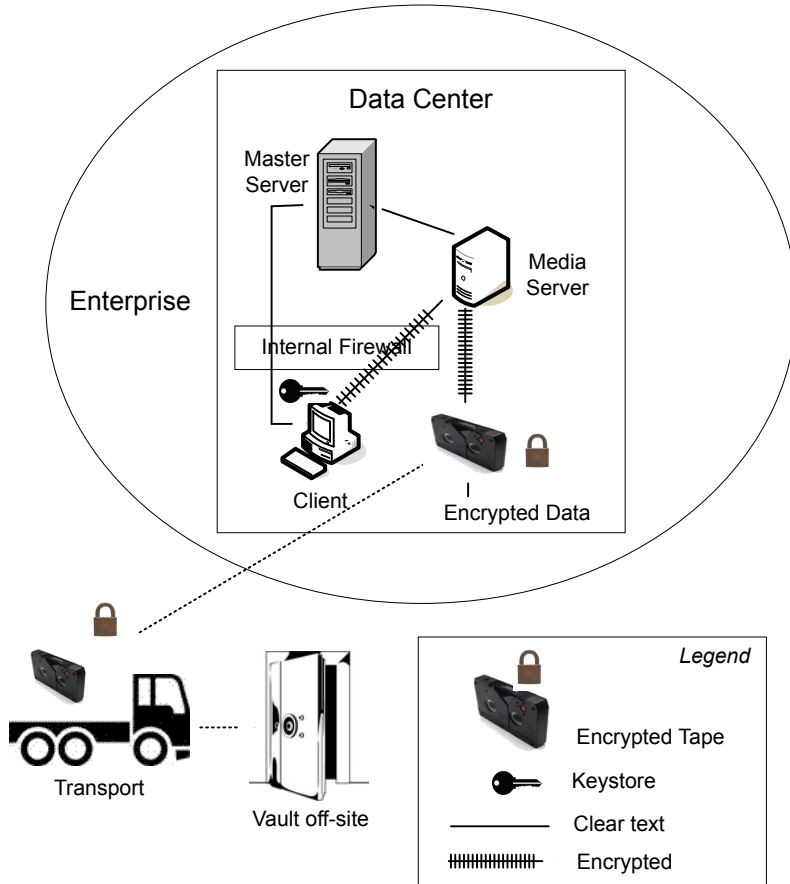
Client side encryption security

Client side encryption security is used to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. The risk of data exposure is reduced as the tapes are moved off site. The encryption key is located on the client. Data communication is encrypted over the wire between the client and the media server. Data encryption by the client can be CPU intensive.

The following backup policy types support the use of the client encryption option.

- AFS

- DB2

- DataStore

- DataTools-SQL-BackTrack

- Informix-On-BAR

- LOTUS_NOTES

- MS-Exchange

- MS-SharePoint

- MS-SQL-Server

- MS-Windows

- Oracle

- PureDisk-Export

- SAP

- Split-Mirror

- Standard

- Sybase

The following backup policy types do not support the Client Encryption Option. You cannot select the encryption check box in the policy attributes interface for these policy types.

- FlashBackup

- FlashBackup-Windows

- NDMP

- NetWare

- OS/2

- Vault

Note that VMS and OpenVMS clients do not support the client encryption option. These clients use the Standard policy type.

The following figure shows an example of the client side encryption configuration.

Figure 1-6   Client side encryption
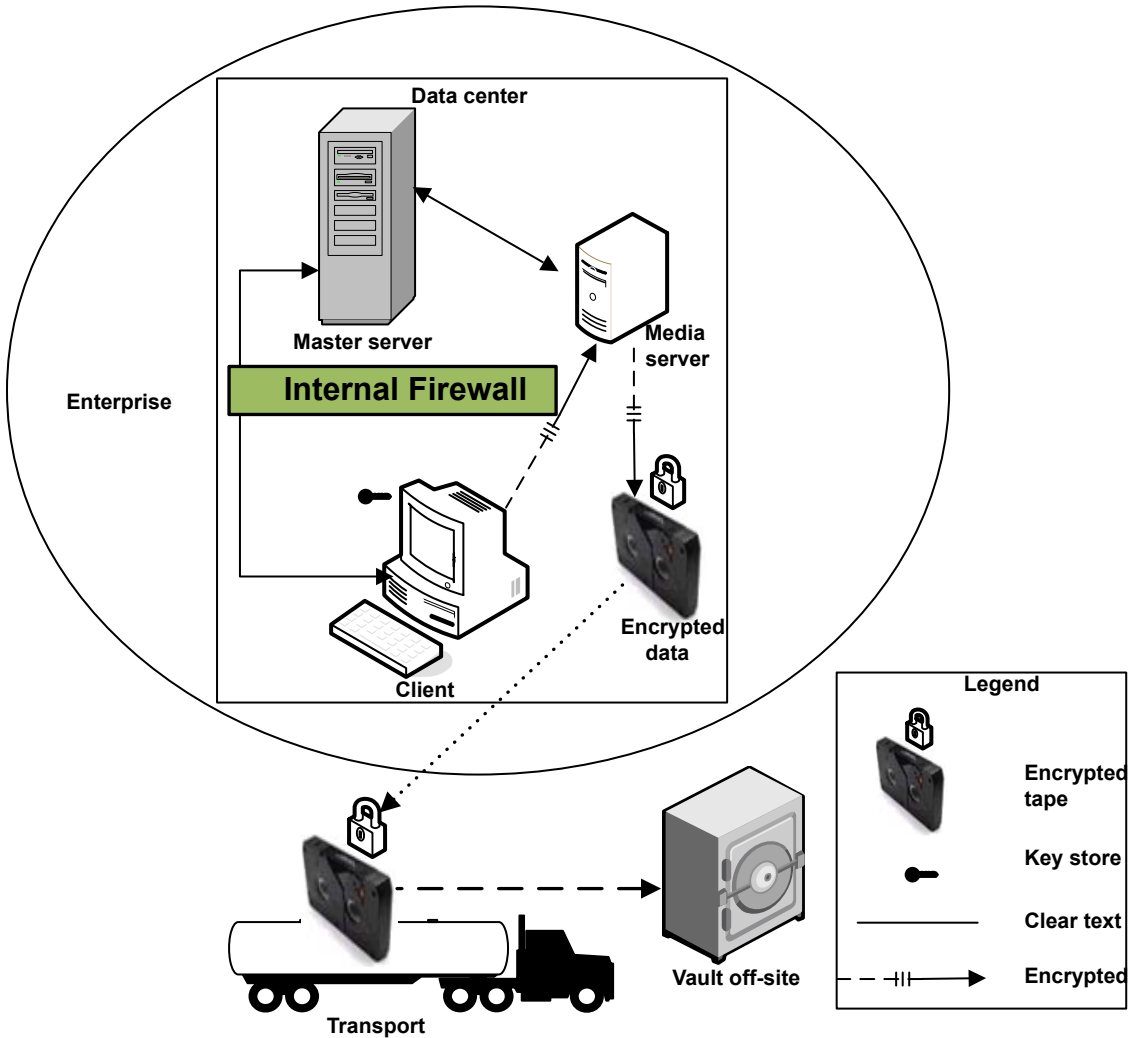
NBAC on master, media server, and graphical user interface security

The NBAC on master server, media server, and graphical user interface security method uses the authentication broker. The broker provides credentials to the master server, the media server, and the graphical user interface. This data center

example uses the NetBackup Access Control on the master and the media servers to limit access to portions of NetBackup. Non-root administration of NetBackup can also be done using this example. NBAC is configured for use between the servers and the graphical user interfaces. Non-root users can log on to NetBackup using the operating system. Use the UNIX password or the Windows local domain to administer NetBackup. The global user repositories (NIS/NIS+ or Active Directory) can also be used to administer NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

The following figure shows an example NBAC on master and media server configuration.

Figure 1-7   NBAC on master and media server
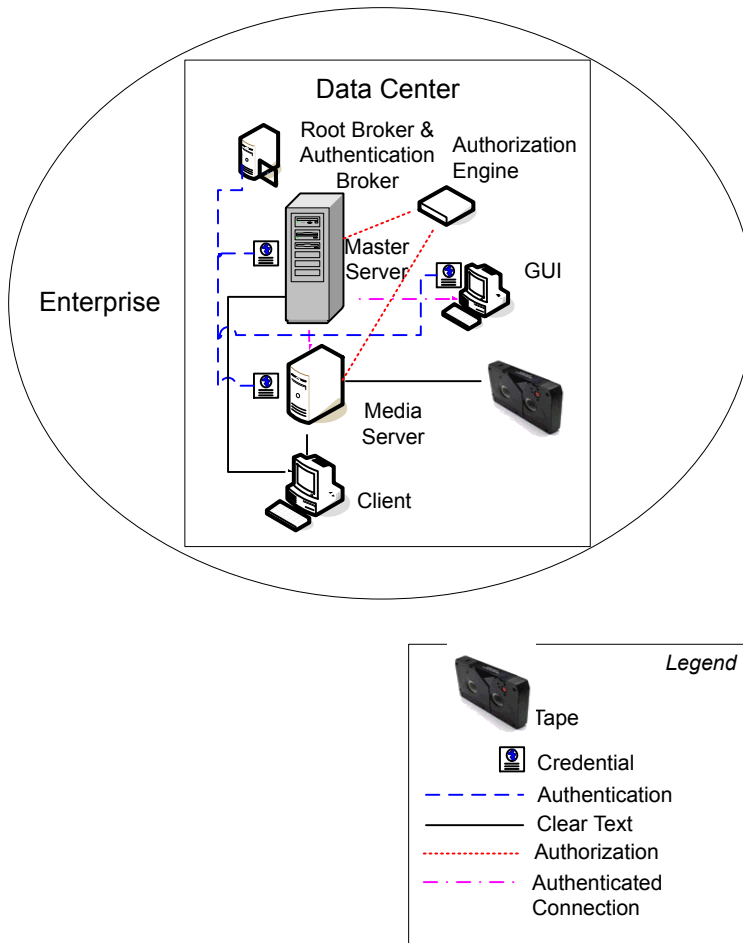
NBAC complete security

The NBAC complete security method uses the authentication broker to provide credentials to the master server, media server, and client. This environment is very similar to the NBAC master, media server, and graphical user interface model. The main differences are that all hosts participating in the NetBackup environment are reliably identified using credentials. And non-root administrators have the ability to manage the NetBackup clients based on configurable levels of access. Note that user identities can exist in global repositories such as Active Directory in Windows

or NIS in UNIX. Identities can also exist in local repositories (UNIX password, local Windows domain) on those hosts supporting an authentication broker.

The following figure shows an example of the NBAC complete configuration.

Figure 1-8   NBAC complete
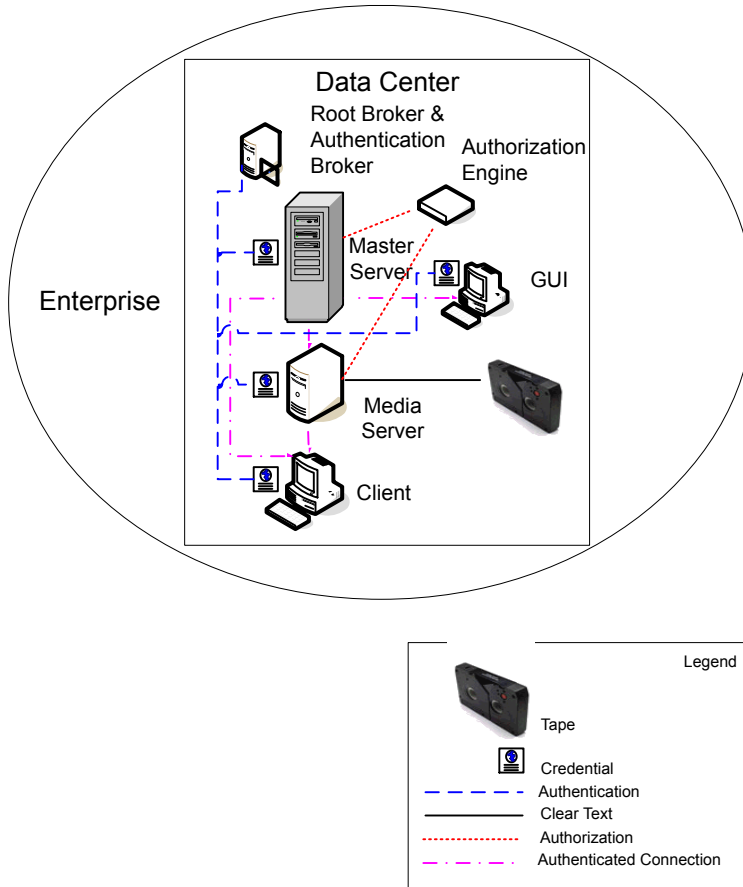
Security deployment models

This chapter includes the following topics:

- Workgroups

- Single datacenters

- Multi-datacenters

- Workgroup with NetBackup

- Single datacenter with standard NetBackup

- Single datacenter with client side encryption

- Single datacenter with NBAC on master and media servers

- Single datacenter with NBAC complete

- Multi-datacenter with standard NetBackup

- Multi-datacenter with client side encryption

- Multi-datacenter with NBAC on master and media servers

- Multi-datacenter with NBAC complete

Workgroups

A workgroup is a small group of systems (less than 50) that is used internally with NetBackup.

An example workgroup is shown as follows:

■ See "Workgroup with NetBackup" on page 36.

Single datacenters

A single datacenter is defined as a medium to large group of hosts (greater than 50).

Example single datacenters are shown in the following list:

■ See "Single datacenter with standard NetBackup" on page 39.

■ See "Single datacenter with client side encryption" on page 41.

■ See "Single datacenter with NBAC on master and media servers" on page 44.

■ See "Single datacenter with NBAC complete" on page 48.

Multi-datacenters

A multi-datacenter contains a medium to a large group of hosts (greater than 50). The hosts can span two or more geographic regions that are connected by a Wide Area Network (WAN).

Example multi-datacenters are shown in the following list:

■ See "Multi-datacenter with standard NetBackup" on page 51.

■ See "Multi-datacenter with client side encryption" on page 55.

■ See "Multi-datacenter with NBAC on master and media servers" on page 60.

■ See "Multi-datacenter with NBAC complete" on page 66.

Workgroup with NetBackup

A workgroup with NetBackup is classified as a small group of systems (less than 50). The workgroup is used with NetBackup internally. Typically, this configuration does not have a unified naming service such as NIS or Active Directory. It may not have an authoritative host naming service such as DNS or WINS. This configuration is typically found in the test labs of large corporations, or as environments in small corporations.

The workgroup with NetBackup includes the following highlights:

■ Very few NetBackup servers

■ Small computer environments

■ No externally facing equipment involved

Figure 2-1 shows an example workgroup with NetBackup.

Figure 2-1   Workgroup with NetBackup
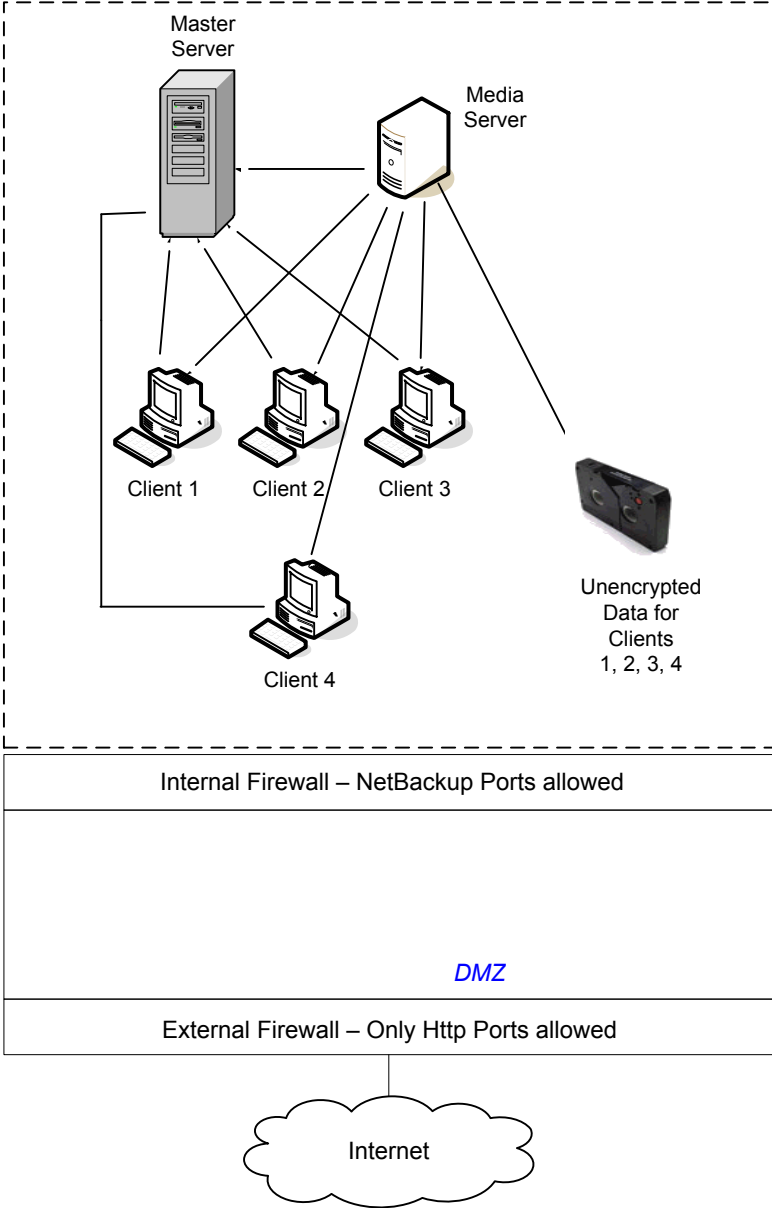
The following table describes the NetBackup parts that are used with the workgroup.

Table 2-1   NetBackup parts used with the workgroup

Part	Description
Master server	Communicates with the media server and clients 1, 2, 3, and 4.
Media server	Communicates with the master server and clients 1, 2, 3, and 4. The media server manages the writing of unencrypted data to tape for clients 1, 2, 3 and 4.
Tape	Contains unencrypted backup data that is written for clients 1, 2, 3, and 4.
Clients	Specifies that clients 1, 2, 3, and 4 are Standard NetBackup clients managed by the master server. They have their unencrypted data backed up to tape by the media server.
Internal firewall	Allows NetBackup to have access to clients in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall from the Internet. The internal firewall is not used with the Workgroup deployment model. In this example, no clients access the internal firewall so the NetBackup ports should not be opened through it. **Note:** In this example, there are no clients beyond the internal firewall. So the NetBackup ports should not be open through the internal firewall.
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for NetBackup clients existing between the internal firewall and external firewall. Possible clients operating in the DMZ include Web server NetBackup clients using either standard NetBackup clients or encrypted NetBackup clients. Clients in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. Web server NetBackup clients can receive connections from the external firewall to the Internet using typical HTTP ports. The DMZ is not accessible by clients in the Workgroup deployment model.
External firewall	Allows external users to access Web server NetBackup clients that are located in the DMZ from the Internet typically over HTTP ports. NetBackup ports open for clients to communicate through the internal firewall are not allowed to pass through the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks linked by copper wires, fiber-optic cables, and wireless connections. Clients do not use the Internet in the Workgroup deployment model. **Caution:** Customers should never put NetBackup clients outside the DMZ and directly in the Internet. You must use an external firewall to block the outside world from NetBackup ports at all times.

Single datacenter with standard NetBackup

A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

The single datacenter with standard NetBackup includes the following highlights:

- Externally facing hosts

- Centralized naming services typically exist

- Greater than 50 hosts in size

- Simplest to configure requiring only general NetBackup knowledge

- Typical configuration that is used for NetBackup customers

- Assumes no fear of passive data interception on the wire as the backup runs

Figure 2-2 shows an example single datacenter with standard NetBackup.

Figure 2-2   Single datacenter with standard NetBackup
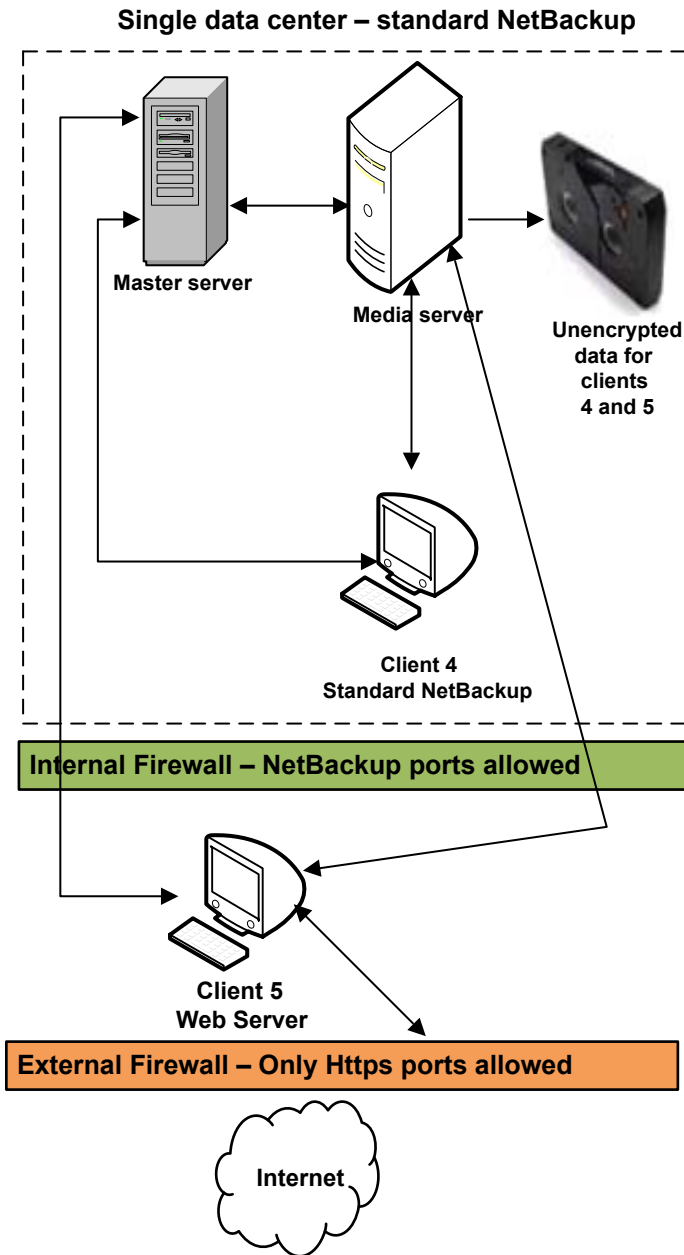
Single data center – standard NetBackup

The following table describes the NetBackup parts that are used for a single datacenter with standard NetBackup.

Table 2-2   NetBackup parts for a single datacenter with standard NetBackup

Part	Description
Master server	Communicates with the media server, standard NetBackup client 4 and Web server NetBackup client 5 in the DMZ.
Media server	Communicates with the master server, standard NetBackup client 4 and Web server NetBackup client 5 in the DMZ. The media server manages the writing of unencrypted data to tape for clients 4 and 5.
Tape	Contains unencrypted backup data that is written for clients 4 and 5.
Clients	Specifies that client 4 is a standard NetBackup type and client 5 is a Web server type. The master server manages both clients and have their unencrypted data backed up to tape by the media server. Client 4 exists in the datacenter. Client 5 exists in the DMZ. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall. Note that all NetBackup traffic for the lookup is sent unencrypted over the wire.
Internal firewall	Enables NetBackup to access Web server NetBackup client 5 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall cannot pass through the internal firewall from the Internet.
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for NetBackup client 5, Web server , that exists between the internal firewall and external firewall. Client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can communicate through the external firewall to the Internet using HTTP ports.
External firewall	Allows external users to access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for client 5 to communicate through the internal firewall. **Caution:** NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports to client 5 are open in the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. The Web server client 5 can receive connections over the Internet using HTTP ports through the external firewall.

Single datacenter with client side encryption

This single datacenter with client side encryption example uses the client side encryption to ensure data confidentiality across the wire as well as on tape. The

client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are moved off site. This datacenter model assures a medium to large number (greater than 50) of managed hosts. Clients inside the datacenter as well as the DMZ can use centralized naming services for hosts and user identities.

The single datacenter with client side encryption includes the following highlights:

- Useful for protecting off-site data

- Data from client is encrypted and eliminates passive interception of the data on the wire

- Key management is de-centralized on to the clients

- The original NetBackup encryption option

- Client CPU is used to perform encryption

- Must have the key to get data back. A lost key means lost data.

- Useful when you need to scan tapes off-site and/or you need confidentiality on the wire

Figure 2-3 shows an example single datacenter with client side encryption.

Figure 2-3   Single datacenter with client side encryption
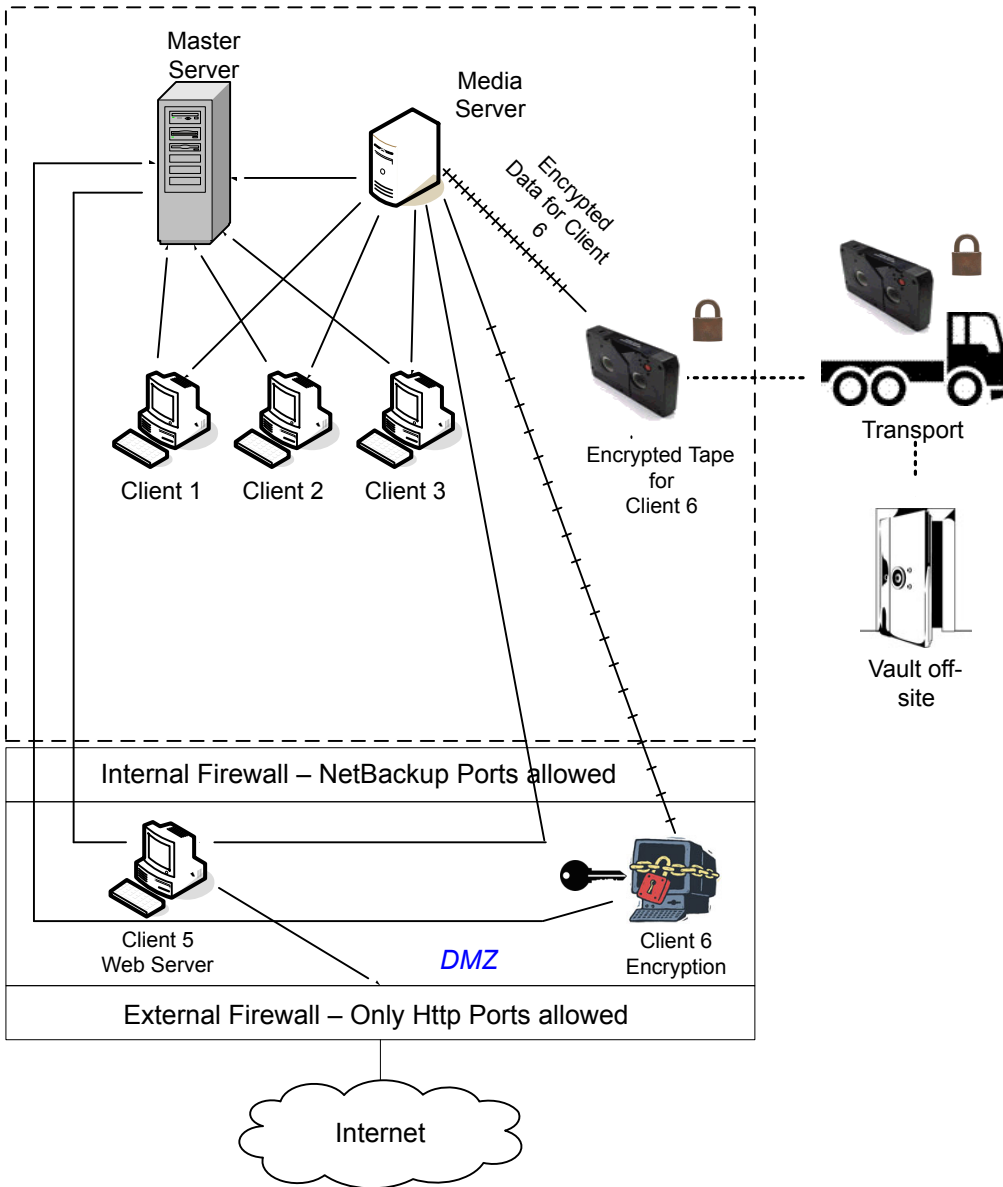
The following table describes the NetBackup parts that are used for a single datacenter with client side encryption.

| Table 2-3 | NetBackup parts for a single datacenter with client side encryption |

Part	Description
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for Web server client 5 and encrypted client 6. These clients exist between the internal firewall and external firewall. The Web server client 5 and encrypted client 6 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 and encrypted client 6 can communicate through the external firewall to the Internet using HTTP ports. The encrypted client 6 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports.
External firewall	Allows external users to access the Web server client 5 and encrypted client 6. These clients can be accessed in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 5 and encrypted client 6 to communicate through the internal firewall. However, NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 5 and encrypted client 6 can pass through the external firewall to the Internet. The external firewall limits client 5 and 6 from bidirectional communication over the Internet.
Internet	Specifies a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables, and wireless connections. The Web server client 5 can communicate over the Internet using HTTP ports through the external firewall.

Single datacenter with NBAC on master and media servers

The single datacenter with NBAC on master servers and media servers example uses the NetBackup Access Control on the master servers and media servers. This configuration limits access to portions of NetBackup and provides non-root administration of NetBackup. NBAC is configured for running between the servers and the GUIs. Non-root users can log in to NetBackup with operating system (UNIX password or Windows local domain) or global user repositories (NIS/NIS+ or Active Directory) to administer NetBackup. NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

The single datacenter with NBAC on master and media servers includes the following highlights:

- Administer non-root users

- Administer UNIX with a Windows User ID

- Administer Windows with a UNIX account

- Segregate and limit the actions of specific users

- Root or Administrator or client hosts can still do local client backups and restores

- Can be combined with other security-related options

- All servers must have the required NetBackup version

Figure 2-4 shows an example single datacenter with NBAC on master and media servers.

Figure 2-4   Single datacenter with NBAC on master and media servers
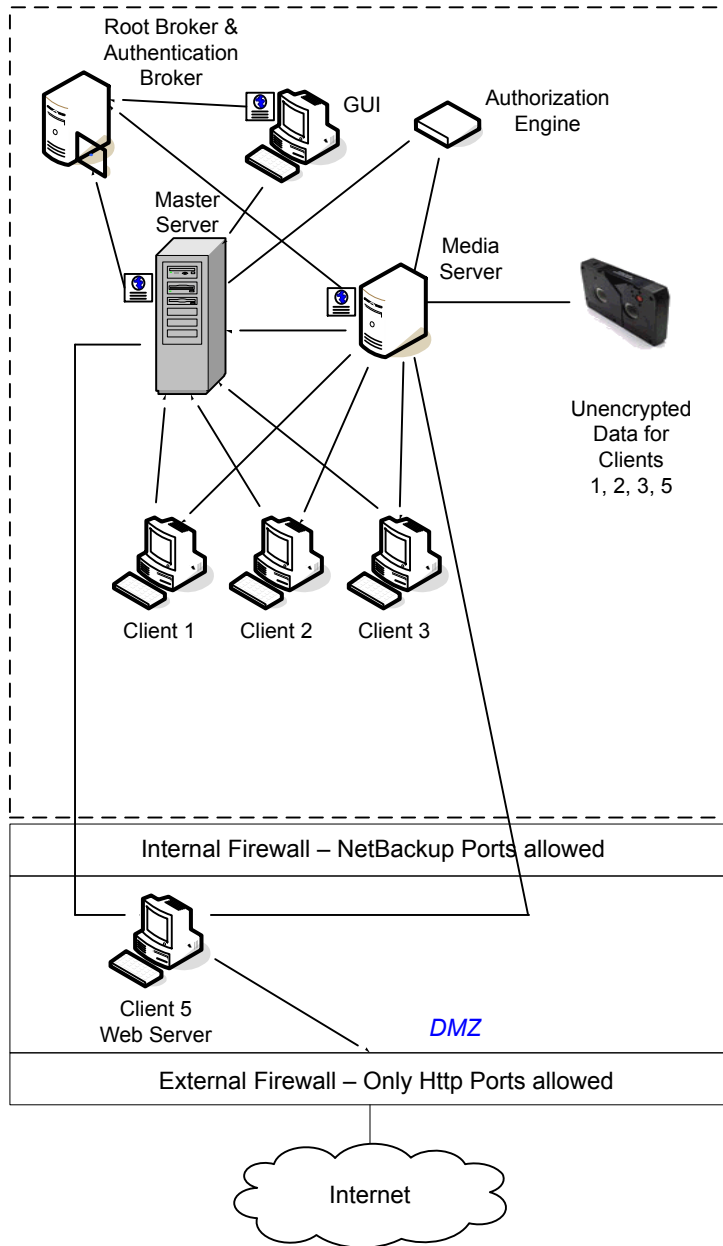
The following table describes the NetBackup parts that are used for a single datacenter with NBAC on the master and media servers.

| | Table 2-4 | NetBackup parts for a single datacenter with NBAC on the master and media servers |

Part	Description
Master server	Communicates with the media server, root, and authentication broker. It also communicates with the authorization engine, clients 1, 2, 3, and client 5, Web server, in the DMZ. The master server also communicates with and receives a credential from the authentication broker.
	When a CLI or GUI accesses a daemon on a master server, a credential is exchanged to identify the user. The authorization engine is then contacted to determine accessibility to the daemons functions.
Media server	Communicates with the master server, clients 1, 2, 3, and client 5, Web server, in the DMZ. The media server also communicates with the authorization engine and receives a credential from the authentication broker. The media server enables the writing of unencrypted data to tape for clients 1, 2, 3, and 5.
	When a CLI or GUI accesses a daemon on a media server, a credential is exchanged to identify the user. The authorization engine is then contacted to determine accessibility to the daemons functions.
GUI	Specifies that this remote administration console GUI receives a credential from the authentication broker. The GUI then uses this credential to gain access to functionality on the media servers and master servers.
Root broker	Authenticates the authentication broker but not the clients. In this example, the root broker and authentication broker are shown as the same component.
Authentication broker	Authenticates the master server, media server, and GUI by establishing credentials with each. If a command prompt is used, the authentication broker also authenticates a user.
Authorization engine	Communicates with the master server and media server to determine permissions of an authenticated user. These permissions determine the functionality available to the user. It also stores user groups and permissions. Only one authorization engine is needed.
	Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for the example only.
Tape	Contains unencrypted backup data that is written for clients 1, 2, 3, and 5.
Clients	Specifies that clients 1, 2, and 3 are standard NetBackup types and client 5 is a Web server type. Both types are managed by the master server and have their unencrypted data backed up to tape through the media server. Clients 1, 2, and 3 exist in the datacenter. Client 5 exists in the DMZ. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall.

	Table 2-4	NetBackup parts for a single datacenter with NBAC on the master and media servers *(continued)*

Part	Description
Internal firewall	Allows NetBackup to access Web server Client 5 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall.
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for Web server client 5 that exists between the internal firewall and external firewall. The Web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can communicate through the external firewall to the Internet using HTTP ports.
External firewall	Allows external users to access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for client 5 to communicate through the internal firewall. NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of client 5 can pass through the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks, linked by copper wires, fiber-optic cables, and wireless connections. Client 5 can communicate over the Internet using HTTP ports through the external firewall.

Single datacenter with NBAC complete

The single datacenter with NBAC complete environment is very similar to the single datacenter with NBAC master and media server. The main differences are that all of the hosts that participate in the NetBackup environment are reliably identified using credentials. And non-root administrators can manage the NetBackup clients based on configurable levels of access. Note that user identities may exist in global repositories, such as Active Directory in Windows or NIS in UNIX. Identities can also exist in local repositories (UNIX passwd, local Windows domain) on those hosts that support an authentication broker.

The single datacenter with NBAC complete includes the following highlights:

- Similar to highlights for single datacenter with NBAC master and media server, except for root or administrator on client

- On client systems, non-root / administrator users may be configured to do local backup and restores (setup by default)

- The environment facilitates trusted identification of all hosts participating in NetBackup

- All hosts should have the required NetBackup version

Figure 2-5 shows an example single datacenter with NBAC complete.

Figure 2-5   Single datacenter with NBAC complete
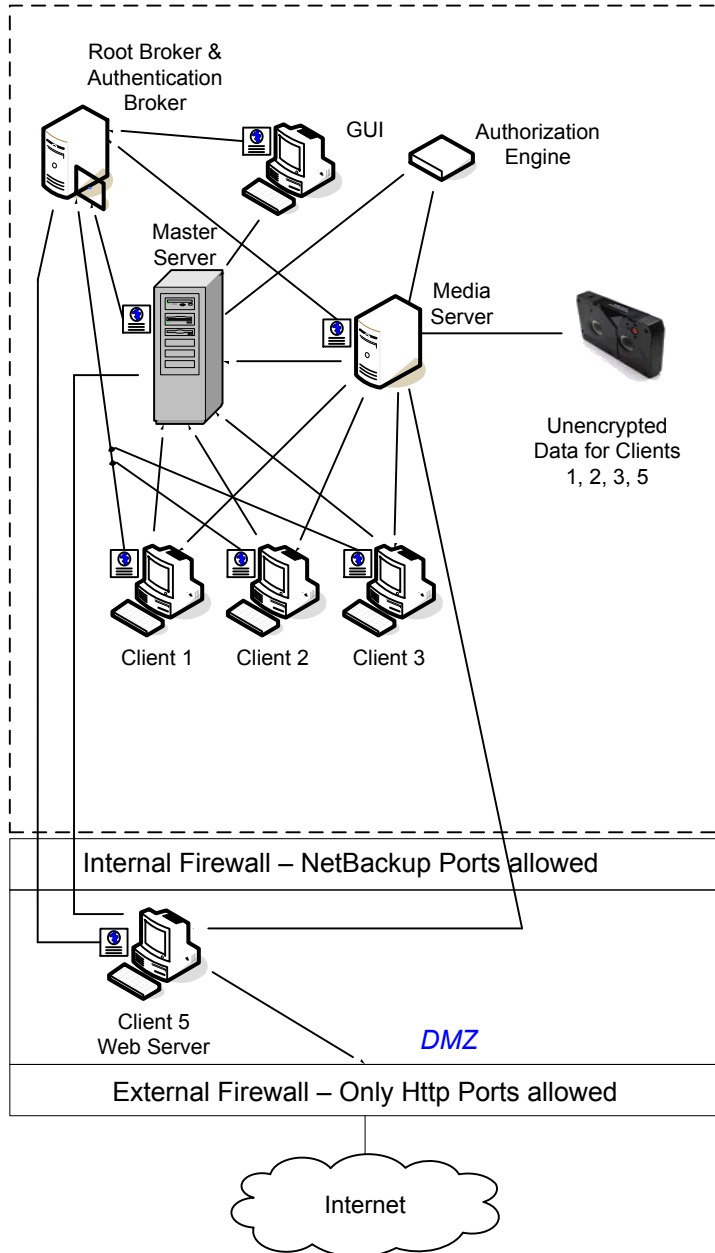
The following table describes the NetBackup parts that are used with a single datacenter with NBAC complete.

Table 2-5   NetBackup parts for a single datacenter with NBAC complete

Part	Description
Master server	Communicates with the media server, root broker, authentication broker. It also communicates with the authorization engine, clients 1, 2, 3, and client 5, Web server, in the DMZ. The master server further communicates with and receives a credential from the authentication broker.
	When a CLI or GUI accesses a daemon on a master server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.
Media server	Communicates with the master server, clients 1, 2, 3, and client 5, Web server, in the DMZ. The media server also communicates with the authorization engine and receives a credential from the authentication broker. The media server enables the writing of unencrypted data to tape for clients 1, 2, 3, and 5.
	When a CLI or GUI accesses a daemon on a media server, a credential is exchanged to identify the user. The authorization engine is contacted to determine accessibility to the daemons functions.
GUI	Specifies that the remote administration console, GUI, receives a credential from the authentication broker. The GUI then uses this credential to gain access to functionality on the media servers and master servers.
Root broker	Authenticates the authentication broker but not the clients. Figure 2-5, shows the root broker and the authentication broker as the same component.
Authentication broker	Authenticates the master server, media server, GUI, clients, and users by establishing credentials with each.
Authorization engine	Communicates with the master server and media server to determine permissions of an authenticated user. It also stores user groups and permissions. Only one authorization engine is needed.
	Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for the example only.
Tape	Contains unencrypted backup data that is written for clients 1, 2, 3, and 5.

Table 2-5   NetBackup parts for a single datacenter with NBAC complete
(continued)

Part	Description
Clients	Specifies that clients 1, 2, and 3 are standard NetBackup types and client 5 is a Web server type. When receiving credentials from the authentication broker, clients 1, 2, 3, and 5 are authenticated to the NetBackup Product Authentication Service domain. Both standard server and Web server types are managed by the master server and have their unencrypted data backed up to tape through the media server. Clients 1, 2, and 3 exist in the datacenter. Client 5 exists in the DMZ. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 receives connections from the Internet using HTTP only ports through the external firewall.
Internal firewall	Allows NetBackup to access Web server client 5 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall cannot pass through the internal firewall.
Demilitarized Zone (DMZ)	Provides a "safe" area of operation for Web server client 5 that exists between the internal firewall and external firewall. The Web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can communicate through the external firewall to the Internet using HTTP ports.
External firewall	Allows external users to access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for client 5 to communicate through the internal firewall. NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of client 5 can pass through the external firewall to the Internet.
Internet	Specifies a collection of interconnected computer networks, linked by copper wires, fiber-optic cables, and wireless connections. Client 5 can communicate over the Internet using HTTP ports through the external firewall.

Multi-datacenter with standard NetBackup

A multi-datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). These hosts can span two or more geographic regions and can be connected by a Wide Area Network (WAN). In this example one datacenter is located in London and the other datacenter is located in Tokyo. Both datacenters are connected through a dedicated WAN connection.

A multi-datacenter includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

The multi-datacenter with standard NetBackup includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN

- Centralized naming services typically exist

- Greater than 50 hosts in size

- Simplest to configure; requires only general NetBackup knowledge

- Assumes no fear of passive data interception on the wire as the backup runs

Figure 2-6 shows an example multi-datacenter with standard NetBackup.

Figure 2-6   Multi-datacenter with standard NetBackup
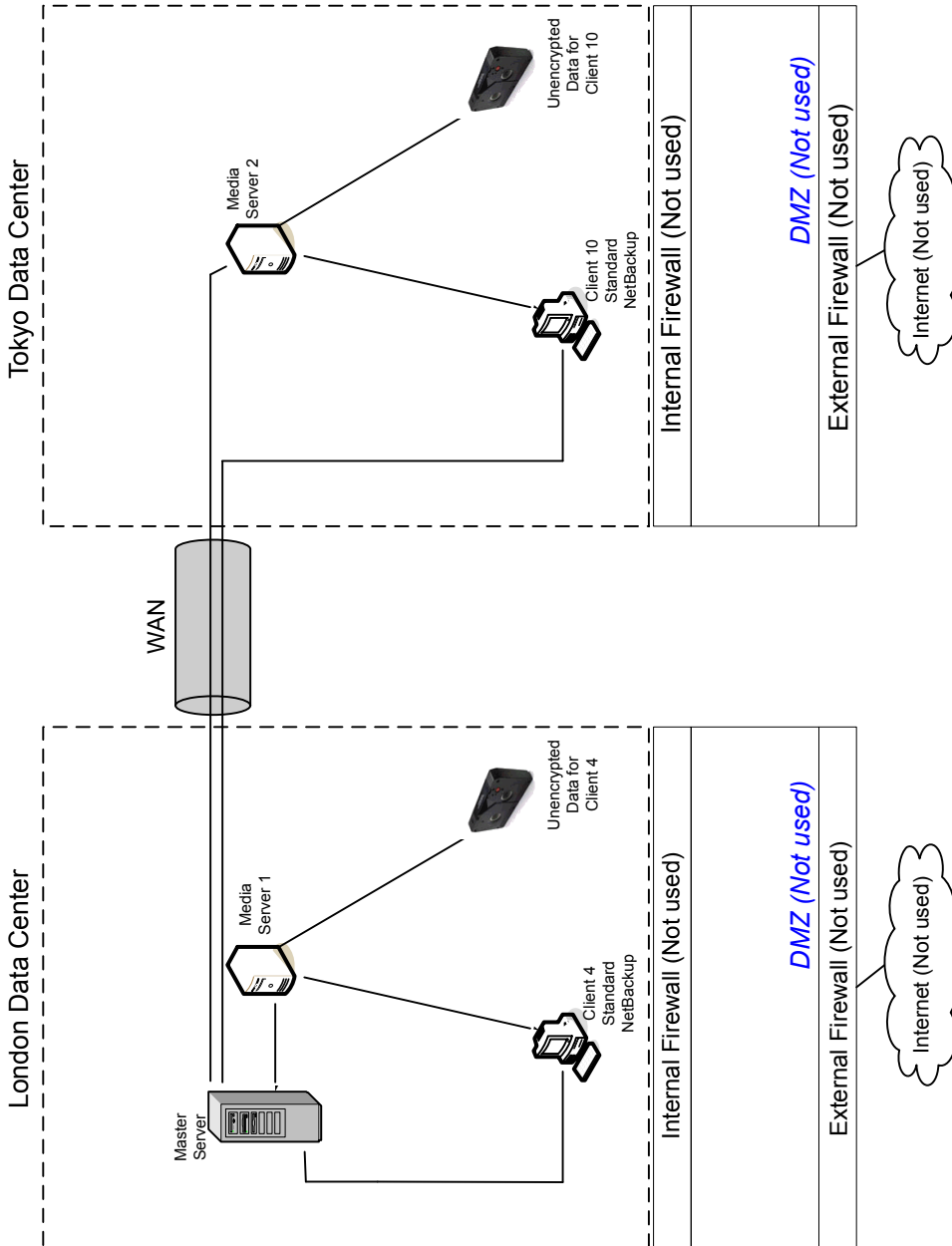
The following table describes the NetBackup parts that are used with a multi-datacenter that has implemented standard NetBackup.

Table 2-6   NetBackup parts for a multi-datacenter with standard NetBackup implemented

Part	Description
London datacenter	Contains the master server, media server 1, client 4 standard NetBackup, and the unencrypted data tape for client 4. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Contains the media server 2, client 10 standard NetBackup, and the unencrypted data tape for client 10. The Tokyo datacenter connects to the London datacenter through a dedicated WAN connection.
Wide Area Network (WAN)	Specifies the dedicated WAN link that connects the London datacenter to the Tokyo datacenter. The WAN provides connectivity between the master server and media server 2 and client 10.
Master server	Specifies that it is located in London and communicates with media server 1 in London. The master server also communicates over the WAN with the media server 2 in Tokyo. The master server communicates with standard NetBackup client 4 in London and client 10 over the WAN in Tokyo.
Media servers	Specifies that the multi-datacenter can have two media servers. One media server is in London and the other is in Tokyo. The media server 1 in London communicates with the master server and standard NetBackup client 4 also in London. Media server 1 manages the writing of unencrypted data to tape for client 4 in London.
	The media server 2 in Tokyo communicates with the master server in London and standard NetBackup client 10 in Tokyo. Media server 2 manages the writing of unencrypted data to tape for client 10 in Tokyo.
Tapes	Specifies that tapes are produced in both the London and Tokyo datacenters. The London tape contains unencrypted backup data that is written for client 4. The Tokyo tape contains unencrypted backup data that is written for client 10.
Clients	Specifies that the clients are located in both the London and Tokyo datacenters. Clients 4 and 10 are standard NetBackup types. Both clients can be managed by the master server that is located in London. Their unencrypted data is backed up to tape by the media server. Unencrypted data is written to both client 4 tape in London and client 10 tape in Tokyo. Note that all NetBackup traffic for client 10 lookup is sent unencrypted over the wire (WAN) from Tokyo to London.
Internal firewalls	Specifies that internal firewalls are not used at the London or Tokyo datacenter with standard NetBackup.
Demilitarized Zones (DMZs)	Specifies that DMZs are not used at the London or Tokyo datacenter with standard NetBackup.

Table 2-6	NetBackup parts for a multi-datacenter with standard NetBackup implemented *(continued)*

Part	Description
External firewalls	Specifies that external firewalls are not used at the London or Tokyo datacenter with standard NetBackup.
Internet	Specifies that the Internet is not used at the London or Tokyo datacenter with standard NetBackup.

Multi-datacenter with client side encryption

A multi-datacenter with client side encryption option is defined as a medium to large group of hosts (greater than 50). These hosts can span two or more geographic regions and can be connected by a Wide Area Network (WAN). In this example one datacenter is located in London and the other datacenter is located in Tokyo. Both datacenters are connected through a dedicated WAN connection.

The example multi-datacenter can use client side encryption to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. Risk of data exposure as the tapes are moved off site. This datacenter model assures a medium to large number (greater than 50) of managed hosts. Clients inside the datacenter as well as the DMZ, can have the potential for centralized naming services for hosts and user identities.

The multi-datacenter with client side encryption includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN

- Useful for protecting off-site data

- Data from client is encrypted and eliminates the passive interception of the data on the wire

- Key management is de-centralized on to the clients

- The original NetBackup encryption option

- Client CPU is used to perform encryption

- Must have the key to get data back. A lost key means lost data.

- Useful when you need to scan tapes off-site or you need confidentiality on the wire

Figure 2-7 shows an example multi-datacenter with client side encryption.

Figure 2-7 Multi-datacenter with client side encryption
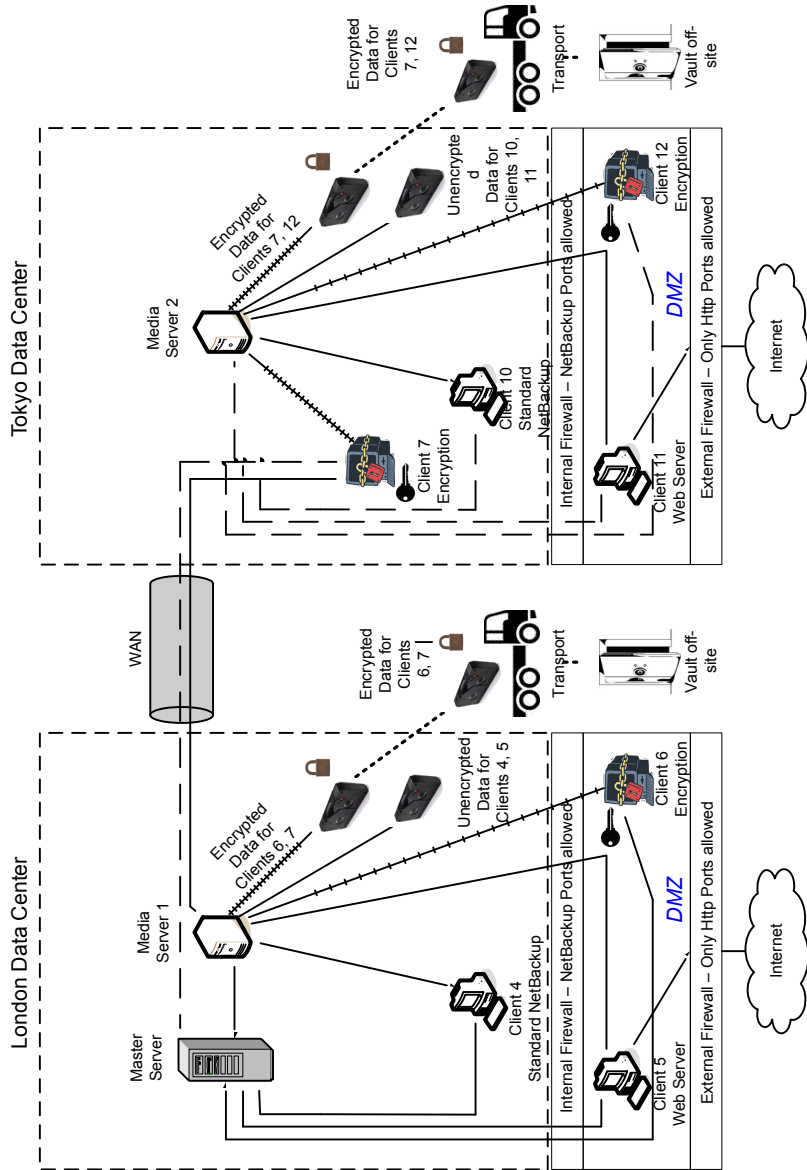
The following table describes the NetBackup parts that are used for a
multi-datacenter with client side encryption implemented.

| Table 2-7 | NetBackup parts for a multi-datacenter with client side encryption implemented |

Part	Description
London datacenter	Contains the master server, media server 1 and clients 4, 5, and 6. The London datacenter also contains the encrypted data tape for clients 6 and 7 and unencrypted data tape for clients 4 and 5. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Contains the media server 2 and clients 7, 10, 11, and 12. The Tokyo datacenter also contains the encrypted data tape for clients 7 and 12 and unencrypted data tape for clients 10 and 11. The Tokyo datacenter connects to the London datacenter through a dedicated WAN connection.
Wide Area Network (WAN)	Specifies that the dedicated WAN link connects the London datacenter with the Tokyo datacenter. The WAN provides connectivity between the master server in London to media server 2 with clients 7, 10, 11, and 12 in Tokyo. The WAN also provides connectivity between media server 1 in London to client 7 in London.
Master server	Specifies that the master server is located in the London datacenter and communicates with media server 1 and clients 4, 5, and 6. The master server also uses the WAN to communicate with media server 2, and clients 7, 10, 11, and 12 in Tokyo.
Media servers	Specifies that the multi-datacenter uses two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the master server and clients 4, 5, and 6. Media server 1 also communicates with client 7 in Tokyo. Media server 1 writes unencrypted data to tape for clients 4 and 5. Media server 1 writes encrypted data to tape for clients 6 and 7. Note that client 7 is located in Tokyo but its tape backup is located in London. The encrypted tape for clients 6 and 7 is transported off-site to a vault in London.
	In Tokyo, media server 2 communicates with the master server in London through the WAN and clients 7, 10, 11, and 12 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11. Media server 2 also writes encrypted data to tape for clients 7and 12. Note that even though client 7 is located in Tokyo and is backed up in London, client 7 is also backed up in Tokyo. The encrypted tape for clients 7 and 12 is transported off-site to a vault in Tokyo.
Client side encryption	Specifies that the client side encryption (not shown in the figure) ensures data confidentiality across the wire as well as on tape.

Table 2-7		NetBackup parts for a multi-datacenter with client side encryption implemented *(continued)*

Part	Description
Tapes	Specifies that both unencrypted and encrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. The encrypted tape contains client side encrypted backup data. In London, the unencrypted tape is written for clients 4 and 5 and stored on-site at the London datacenter. The encrypted tape is written for clients 6 and 7. The encrypted tape is transported off-site to a vault in London for disaster recovery protection.
	In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter. The encrypted tape is written for clients 7 and 12. Note that even though client 7 is located in Tokyo and is backed up in Tokyo, client 7 is also backed up in London. The encrypted tape is transported off-site to a vault in Tokyo for disaster recovery protection.
	Note: To decrypt the data, the key(s) used to encrypt the data must be made available.
Transports	Specifies that the multi-datacenter uses two transports. One transport is located in London and the other is located in Tokyo. The transport truck in London moves the encrypted tape for clients 6 and 7 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 7 and 12 off-site to a secure Tokyo vault facility. Note that a backup copy of client 7 is vaulted both in London and in Tokyo.
	Note: If in the remote case a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach. The breach is reduced through the use of client side data encryption.
Vaults off-site	Specifies that the multi-datacenter uses two vaults off-site. One vault is located in London and the other is located in Tokyo. Both vaults provide safe encrypted tape storage facilities off-site at different locations than the datacenters.
	Note: Storing the encrypted tapes at locations separate from the datacenters promotes good disaster recovery protection.

Table 2-7	NetBackup parts for a multi-datacenter with client side encryption implemented *(continued)*

Part	Description
Clients	Specifies that the clients are located in both the London and Tokyo datacenters. In London, client 4 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. Client 6 is client side encrypted and is also located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 1. Clients 5 and 6 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 6 receives connections from the Internet using HTTP only ports through the external firewall.
	In Tokyo, client 7 is a client side encrypted client but outside of the DMZ. Client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. Client 12 is client side encrypted also located in the DMZ. All client types can be managed by the master server in London. Client 7 data is backed up to tape through media server 1 and 2. Client 10, 11, and 12 data is backed up to tape through media server 2. Clients 11 and 12 communicate to NetBackup using NetBackup only ports through the internal firewall. Client 12 receives connections from the Internet using HTTP only ports through the external firewall.
Internal firewalls	Specifies that the multi-datacenter uses two internal firewalls. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall allows NetBackup to access Web server client 5 and client side encrypted client 6 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 and client side encrypted client 12 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. HTTP ports that are open in the external firewall cannot pass through the internal firewall.
Demilitarized Zones (DMZs)	Specifies that the multi-datacenter uses two DMZs. One DMZ is located in London and the other is located in Tokyo. In London, the DMZ provides a "safe" area of operation for the Web server client 5 and client side encrypted client 6. That client exists between the internal firewall and the external firewall. The Web server client 5 and client side encrypted client 6 in the DMZ can communicate to NetBackup. Both clients communicate through the internal firewall using designated NetBackup ports. The Web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports.
	In Tokyo, the DMZ provides a "safe" area of operation for the Web server client 11 and client side encrypted client 12. The client 12 exists between the internal firewall and external firewall. The Web server client 11 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 11 can also communicate through the external firewall to the Internet using only HTTP ports.

Table 2-7	NetBackup parts for a multi-datacenter with client side encryption implemented *(continued)*	

Part	Description
External firewalls	Specifies that the multi-datacenter can use two external firewalls. One external firewall is located in London and the other is located in Tokyo. In London, the external firewall lets external users access the Web server client 5 located in the DMZ from the Internet over HTTP ports. The NetBackup ports are open for Web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 5 can pass through the external firewall to the Internet. The client side encrypted client 6 cannot be accessed from the Internet.
	In Tokyo, the external firewall external users access the Web server client 11 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 11 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 11 can pass through the external firewall to the Internet. The client side encrypted client 12 cannot be accessed from the Internet.
Internet	Specifies that there is only one Internet but there are two Internet connections in this multi-datacenter example. One Internet connection is located in London and the other is located in Tokyo. The Internet is a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. In London, the Web server client 5 can communicate over the Internet using HTTP ports through the external firewall. In Tokyo, the Web server client 11 can communicate over the Internet using HTTP ports through the external firewall.

Multi-datacenter with NBAC on master and media servers

A multi-datacenter with NBAC on the master server and media server example is defined as a medium to large group of hosts (greater than 50). These hosts span two or more geographic regions and can be connected by a Wide Area Network (WAN). In this example one datacenter is located in London and the other datacenter is located in Tokyo. Both datacenters are connected through a dedicated WAN connection.

This datacenter example uses NetBackup Access Control on the master servers and media servers. The datacenter limits access to portions of NetBackup and can use non-root administration of NetBackup. Within this environment, NBAC is configured for use between the servers and the GUIs. Non-root users can log in to NetBackup using operating system (UNIX password or Windows local domain). Or global user repositories (NIS/NIS+ or Active Directory) can be used to administer

NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

The multi-datacenter with NBAC on master and media servers includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN

- Administer as non-root users

- Administer UNIX with a Windows User ID.

- Administer Windows with a UNIX account.

- Segregate and limit the actions of specific users.

- Root or Administrator or client hosts can still perform local client backups and restores

- Can be combined with other security-related options

- All servers must be NetBackup version 7.7 or later.

Figure 2-8 shows an example multi-datacenter with NBAC on the master servers and media servers.

Figure 2-8   Multi-datacenter with NBAC on the master servers and media servers
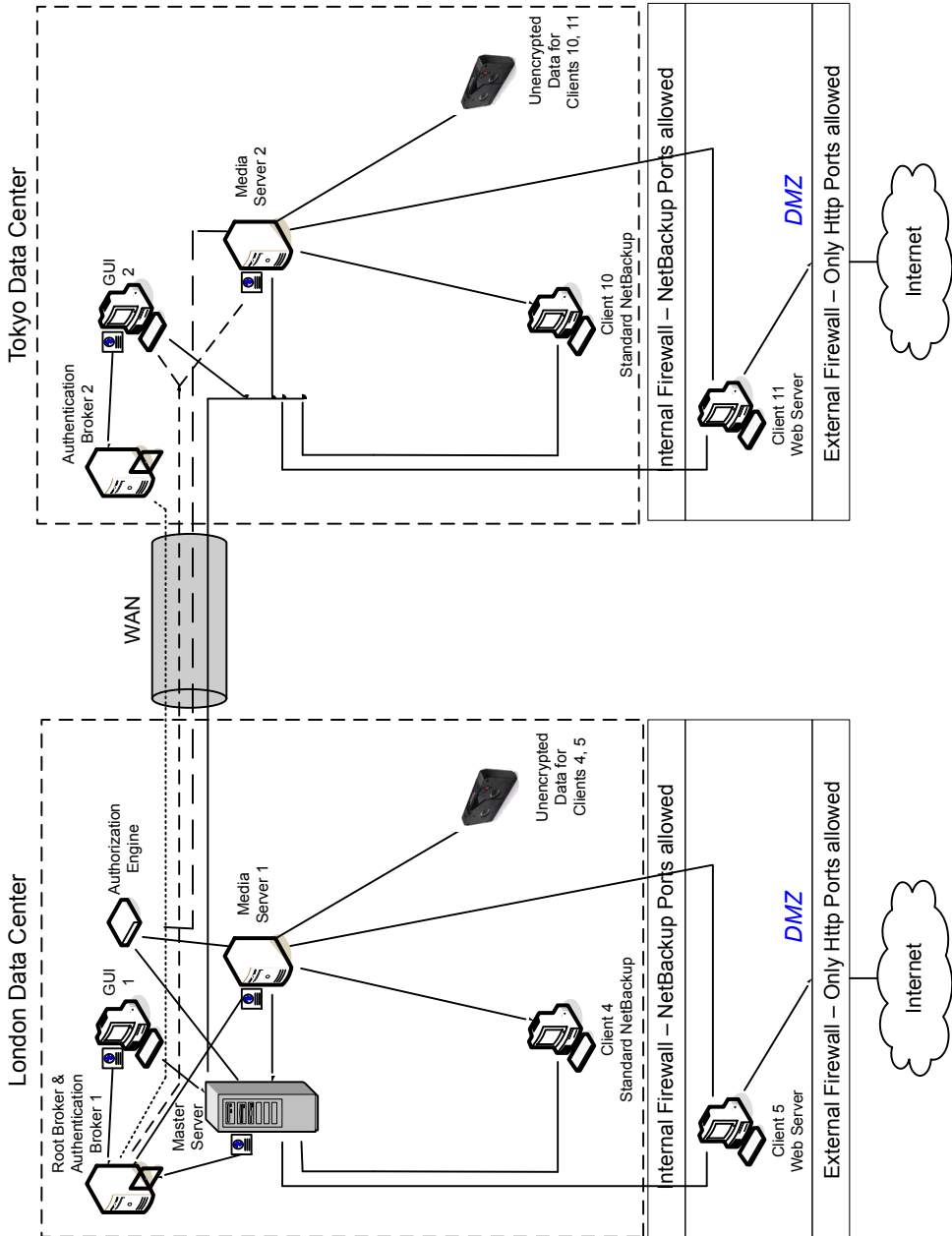
The following table describes the NetBackup parts that are used for a multi-datacenter with NBAC on the master and media servers.

Table 2-8   NetBackup parts used for a multi-datacenter with NBAC on the master and media servers

Part	Description
London datacenter	Specifies that the London datacenter contains the root broker, authentication broker 1, GUI 1, authorization engine, master server, media server 1, and clients 4 and 5. The London datacenter also contains the unencrypted data tape for clients 4 and 5. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Specifies that the Tokyo datacenter contains authentication broker 2, GUI 2, media server 2, and clients 10 and 11. The Tokyo datacenter also contains the unencrypted data tape for clients 10 and 11. The Tokyo datacenter connects to the London datacenter through a dedicated WAN connection.
Wide Area Network (WAN)	Specifies that the dedicated WAN link connects the London datacenter with the Tokyo datacenter. The WAN provides connectivity between the root broker and authentication broker 1 and authentication broker 2. In addition, the WAN provides connectivity between the root broker and authentication broker 1 and GUI 2 along with media server 2. The WAN also connects the authorization engine to media server 2. Finally, the WAN connects the master server with GUI 2, media server 2, and clients 10 and 11.
Master server	Specifies that the master server, located in the London datacenter, communicates with the root broker and authentication broker 1. It also communicates with GUI 1, authorization engine, and media server 1. The master server communicates with clients 4 and 5 in London. The master server also communicates with GUI 2, media server 2, and clients 10 and 11 in Tokyo.
Media servers	Specifies that in this multi-datacenter example, there are two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the master server, root broker and authentication broker 1, authorization engine, and clients 4 and 5. Media server 1 writes unencrypted data to tape for clients 4 and 5.
	In Tokyo, media server 2 communicates with the master server and authorization engine in London through the WAN. Media server 2 also communicates with GUI 2 and clients 10 and 11 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11.

Table 2-8 NetBackup parts used for a multi-datacenter with NBAC on the master and media servers *(continued)*

Part	Description
GUIs	Specifies that in this multi-datacenter example, there are two GUIs. The GUI 1 is in London and GUI 2 is in Tokyo. These remote administration console GUIs receive credentials from the authentication brokers. The GUIs then use the credentials to gain access to functionality on the media servers and master servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the master server and media servers 1 and 2. In Tokyo, GUI 2 receives a credential from the authentication broker 2. GUI 2 has access to functionality on the master server and media servers 1 and 2.
Root broker	Specifies that in a multi-datacenter installation there is only one root broker required. Sometimes, the root broker is combined with the authentication broker. In this example, the root broker and authentication broker are shown as the same component and are located in the London datacenter. In London, the root broker authenticates the authentication broker 1 also in London and the authentication broker 2 in Tokyo. The root broker does not authenticate clients.
Authentication brokers	Specifies that there can be more than one authentication broker in a multi-datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, two authentication brokers are used. The authentication broker authenticates the master server, media server, and GUI by establishing credentials with each. The authentication broker also authenticates a user who specifies a command prompt. In London, authentication broker 1 authenticates a credential with the master server, media server 1, and GUI 1. All NetBackup servers and clients in Tokyo and London authenticate to authentication broker 1 in London. GUI 1 authenticates to authentication broker 1 in London. GUI 2 authenticates to authentication broker 2 in Tokyo.
Authorization engine	Specifies that in a multi-datacenter installation there is only one authorization engine required. The authorization engine communicates with the master server and media server to determine permissions of an authenticated user. These permissions determine the functionality available to the user. The authorization engine also stores user groups and permissions. The authorization engine resides in London and communicates with the master server, and media server 1. The authorization engine also communicates over the WAN to authorize access to media server 2 in Tokyo. **Note:** The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for example only.
Tapes	Specifies that unencrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. In London, the unencrypted tape is written for clients 4 and 5 and stored on-site at the London datacenter. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter.

<table>
<tr><td align="center">**Table 2-8**</td><td>NetBackup parts used for a multi-datacenter with NBAC on the master and media servers *(continued)*</td></tr>
</table>

Part	Description
Clients	Specifies that clients are located in both the London and Tokyo datacenters. In London, client 4 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 1. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.
	In Tokyo, client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 2. Client 11 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 11 also receives connections from the Internet using HTTP only ports through the external firewall
Internal firewalls	Specifies that in this multi-datacenter example there are two internal firewalls. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall lets NetBackup access Web server client 5 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall.
Demilitarized Zones (DMZs)	Specifies that in this multi-datacenter example there are two DMZs. One DMZ is located in London and the other is located in Tokyo. In London, the DMZ provides a "safe" area of operation for the Web server client 5 that exists between the internal firewall and external firewall. The Web server client 5 and client side encrypted client 6 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports.
	In Tokyo, the DMZ provides a "safe" area of operation for the Web server client 11 that exists between the internal firewall and external firewall. The Web server client 11 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 11 can also communicate through the external firewall to the Internet using only HTTP ports.

	Table 2-8	NetBackup parts used for a multi-datacenter with NBAC on the master and media servers *(continued)*

Part	Description
External firewalls	Specifies that in this multi-datacenter example there are two external firewalls. One external firewall is located in London and the other is located in Tokyo. In London, the external firewall lets external users access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 5 can pass through the external firewall to the Internet.
	In Tokyo, the external firewall lets external users access the Web server client 11 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 11 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 11 can pass through the external firewall to the Internet.
Internet	Specifies that there is only one Internet but two Internet connections in this multi-datacenter example. One Internet connection is located in London and the other is located in Tokyo. The Internet is a collection of interconnected computer networks, tha are linked by copper wires, fiber-optic cables and wireless connections. In London, the Web server client 5 can communicate over the Internet using HTTP ports through the external firewall. In Tokyo, the Web server client 11 can communicate over the Internet using HTTP ports through the external firewall.

Multi-datacenter with NBAC complete

The multi-datacenter with NBAC complete example is defined as a medium to large group of hosts (greater than 50) that span two or more geographic regions and can be connected by a Wide Area Network (WAN). In this example, one datacenter is in London and the other datacenter is in Tokyo. Both datacenters are connected through a dedicated WAN connection.

This environment is very similar to the multi-datacenter with NBAC master and media server. The main differences are that all hosts participating in the NetBackup environment are reliably identified using credentials and non-root administrators can manage the NetBackup clients based on configurable levels of access. Note that user identities may exist in global repositories such as Active Directory in Windows or NIS in UNIX. Identities can also exist in local repositories (UNIX passwd, local Windows domain) on those hosts supporting an authentication broker.

The multi-datacenter with NBAC complete includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN

- Similar to highlights for multi-datacenter with NBAC master and media server except for root or administrator on client. The non-root administration of clients and servers is permitted in this configuration.

- On client systems, non-root / administrator users can be configured to perform local backup and restores (setup by default)

- The environment facilitates trusted identification of all hosts participating in NetBackup

- Requires all hosts to be at NetBackup version 7.7 or later.

Figure 2-9 shows an example multi-datacenter with NBAC complete.

Figure 2-9   Multi-datacenter with NBAC complete
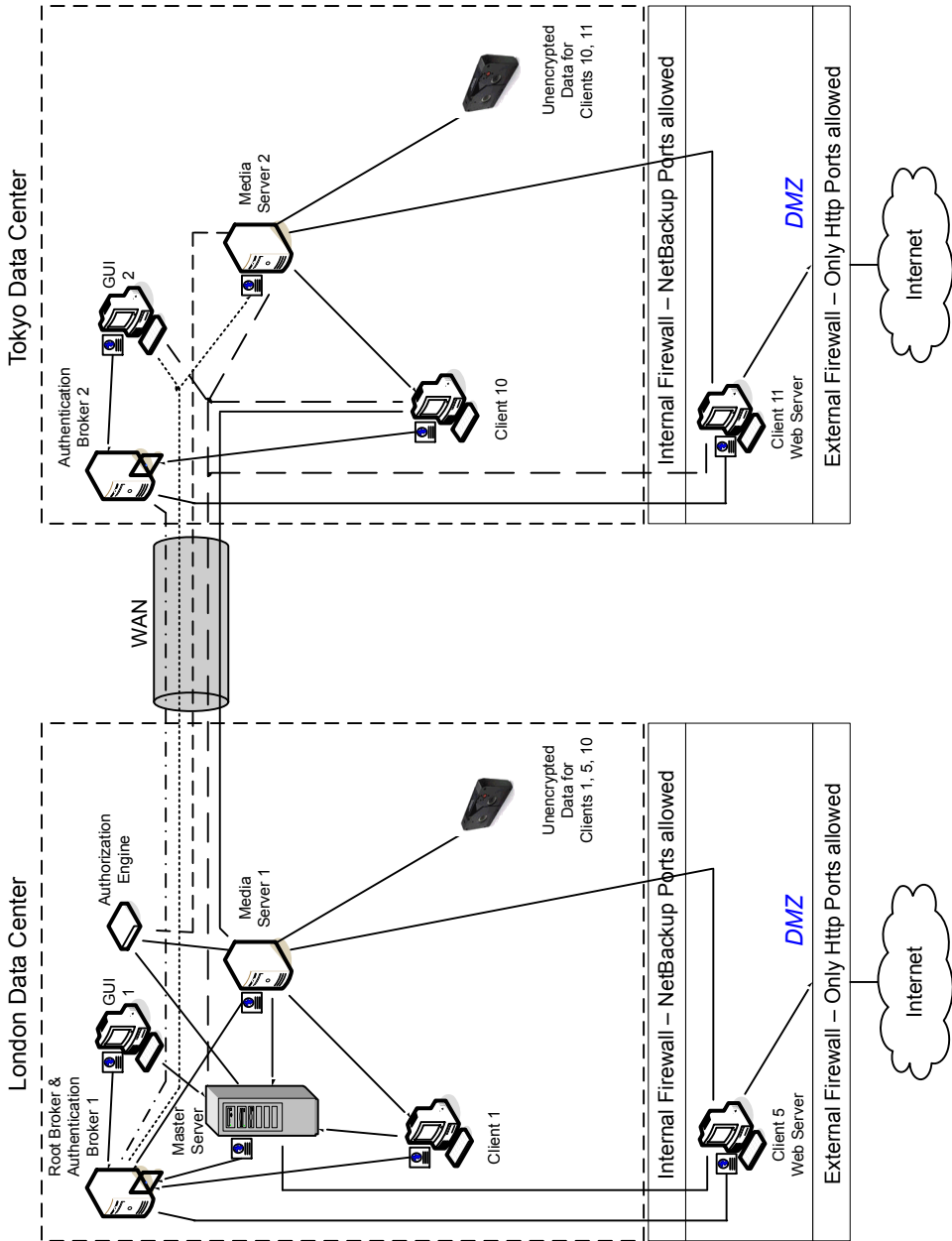
The following table describes the NetBackup parts that are used for a multi-datacenter with NBAC complete implemented.

Table 2-9   NetBackup parts used for a multi-datacenter with NBAC complete implemented

Part	Description
London datacenter	Specifies that the London datacenter contains the root broker, authentication broker 1, GUI 1, authorization engine, master server, media server 1, and clients 1 and 5. The London datacenter also contains the unencrypted data tape for clients 1, 5, and 10. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Specifies that the Tokyo datacenter contains the authentication broker 2, GUI 2, media server 2, and clients 10 and 11. The Tokyo datacenter also contains the unencrypted data tape for clients 10 and 11. The Tokyo datacenter connects to the London datacenter through a dedicated WAN connection.
Wide Area Network (WAN)	Specifies that the dedicated WAN link connects the London datacenter with the Tokyo datacenter. The WAN provides connectivity between the root broker and authentication broker 1 and authentication broker 2. In addition, the WAN provides connectivity between the root broker and authentication broker 1 and GUI 2 along with media server 2. The WAN connects the authorization engine to media server 2. The WAN connects the master server to GUI 2, media server 2, and clients 10 and 11. Finally the WAN connects media server 1 to client 10.
Master server	Specifies that the master server, located in the London datacenter, communicates with the root broker and authentication broker 1. It also communicates with GUI 1, authorization engine, and media server 1. The master server further communicates with GUI 2 and media server 2, and clients 10 and 11 in Tokyo.
Media servers	Specifies that in this multi-datacenter example there are two media servers. Media server 1 is located in the London datacenter and media server 2 is located in the Tokyo datacenter. In London, media server 1 communicates with the master server, root broker and authentication broker 1, authorization engine, and clients 1, 5, and 10. Media server 1 writes unencrypted data to tape for clients 1, 5, and 10. In Tokyo, media server 2 communicates with the master server, root broker, and authentication broker 1 and authorization engine in London through the WAN. Media server 2 also communicates with GUI 2, and clients 10 and 11 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11.
GUIs	Specifies that in this multi-datacenter example, there are two GUIs. GUI 1 is in London and GUI 2 is in Tokyo. These remote administration console GUIs receive credentials from the authentication brokers. The GUIs then use the credentials to gain access to functionality on the media servers and master servers. In London, GUI 1 receives a credential from authentication broker 1. GUI 1 has access to functionality on the master server and media servers 1 and 2. In Tokyo, GUI 2 receives a credential from the authentication broker 2. GUI 2 has access to functionality on the master server and media servers 1 and 2.

Table 2-9   NetBackup parts used for a multi-datacenter with NBAC complete
implemented *(continued)*

Part	Description
Root broker	Specifies that there is only one root broker required in a multi-datacenter installation. Sometimes the root broker is combined with the authentication broker. In this example the root broker and authentication broker are shown as the same component and are located in the London datacenter. In London, the root broker authenticates the authentication broker 1, also in London, and authentication broker 2 in Tokyo. The root broker does not authenticate clients.
Authentication brokers	Specifies that there can be more than one authentication broker in a datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, there are two authentication brokers. The authentication broker authenticates the master server, media server, GUI, and clients by establishing credentials with each. The authentication broker also authenticates a user through a command prompt. In London, authentication broker 1 authenticates a credential with the master server, media server 1, GUI 1, and clients 1 and 5. All NetBackup servers and clients in Tokyo and London authenticate to authentication broker 1 in London. GUI 1 authenticates to authentication broker 1 in London. GUI 2 authenticates to authentication broker 2 in Tokyo.
Authorization engine	Specifies that there is only one authorization engine required in a datacenter installation. The authorization engine communicates with the master server and media server to determine permissions of an authenticated user. These permissions determine the functionality available to the user. The authorization engine also stores user groups and permissions. The authorization engine resides in London and communicates with the master server, and media server 1. The authorization engine also communicates over the WAN to authorize access to media server 2 in Tokyo.
	Note: The authorization engine resides on the master server as a daemon process. It is shown in the figure as a separate image for example only.
Tapes	Specifies that the unencrypted data tapes are produced in both the London and Tokyo datacenters. In London, the unencrypted tape is written for clients 1, 5 and 10 and stored on-site at the London datacenter. In Tokyo, the unencrypted tape is written for clients 10 and 11 and stored on-site at the Tokyo datacenter. Note that even though client 10 is located in Tokyo and is backed up in Tokyo, client 10 is also backed up in London.

| | **Table 2-9** | NetBackup parts used for a multi-datacenter with NBAC complete implemented *(continued)* |

Part	Description
Clients	Specifies that the clients are located in both the London and Tokyo datacenters. In London, client 1 is a standard NetBackup type. Client 5 is a Web server type located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 1. Client 5 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 5 also receives connections from the Internet using HTTP only ports through the external firewall.
	In Tokyo, client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. All client types can be managed by the master server and have their data backed up to tape through media server 2. Client 11 communicates to NetBackup using NetBackup only ports through the internal firewall. Client 11 also receives connections from the Internet using HTTP only ports through the external firewall
Internal firewalls	Specifies that there can be two internal firewalls in this multi-datacenter example. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall lets NetBackup access Web server client 5 in the DMZ. In Tokyo, the internal firewall lets NetBackup access Web server client 11 in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication through the internal firewall and into and out of the DMZ. HTTP ports that are open in the external firewall are not allowed to pass through the internal firewall.
Demilitarized Zones (DMZs)	Specifies that there can be two DMZs in this multi-datacenter example. One DMZ is located in London and the other is located in Tokyo. In London, the DMZ provides a "safe" area of operation for the Web server client 5 that exists between the internal firewall and external firewall. The Web server client 5 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 5 can also communicate through the external firewall to the Internet using only HTTP ports.
	In Tokyo, the DMZ provides a "safe" area of operation for the Web server client 11 that exists between the internal firewall and external firewall. The Web server client 11 in the DMZ can communicate to NetBackup through the internal firewall using designated NetBackup ports. The Web server client 11 can also communicate through the external firewall to the Internet using only HTTP ports.

Table 2-9   NetBackup parts used for a multi-datacenter with NBAC complete implemented *(continued)*

Part	Description
External firewalls	Specifies that there can be two external firewalls in this multi-datacenter example. One external firewall is located in London and the other is located in Tokyo. In London, the external firewall lets external users access the Web server client 5 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 5 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 5 can pass through the external firewall to the Internet. In Tokyo, the external firewall lets external users access the Web server client 11 located in the DMZ from the Internet over HTTP ports. NetBackup ports are open for Web server client 11 to communicate through the internal firewall to NetBackup. The NetBackup ports are not allowed to pass through the external firewall to the Internet. Only the HTTP ports of Web server client 11 can pass through the external firewall to the Internet.
Internet	Specifies that there can be only one Internet but there are two Internet connections in this multi-datacenter example. One Internet connection is located in London and the other is located in Tokyo. The Internet is a collection of interconnected computer networks that are linked by copper wires, fiber-optic cables and wireless connections. In London, the Web server client 5 can communicate over the Internet using HTTP ports through the external firewall. In Tokyo, the Web server client 11 can communicate over the Internet using HTTP ports through the external firewall.

Port security

This chapter includes the following topics:

- About NetBackup TCP/IP ports
- About NetBackup daemons, ports, and communication
- About configuring ports
- Port requirements for NDMP backups
- Known firewall problems encountered when using NetBackup with third-party robotic products

About NetBackup TCP/IP ports

Like other application software, NetBackup sends data packets to the network and receives data packets from the network. The operating system organizes these data packets into queues, which are known in TCP/IP terminology as *ports*. All NetBackup data communication uses the TCP/IP protocol.

NetBackup uses two classes of ports: reserved ports and non-reserved ports. These ports are as follows:

- *Reserved ports* are numbered less than 1024 and typically are accessible only to operating system components.
  NetBackup master servers use reserved ports to communicate with older revisions of NetBackup software that reside on clients, media servers, and other NetBackup components on the network. These are sometimes called *back-rev connections*. Callback is used only for back-rev connections.

- *Nonreserved ports* are numbered at 1024 and above. User applications can access these ports.

Some NetBackup ports are registered with the Internet Assigned Numbers Authority (IANA) and other NetBackup ports are assigned dynamically. Table 3-1 explains these ports.

Table 3-1   Ports that NetBackup uses to enable TPC/IP connections

Port	Description
Registered ports	Specifies ports that are registered with the Internet Assigned Numbers Authority (IANA) and are assigned permanently to specific NetBackup services. For example, the port for the NetBackup client daemon, bpcd, is 13782. You can specify entries in the following files if you need to override the default port numbers: ■ On UNIX systems, you can specify ports in the /etc/services file. ■ On Windows systems, you can specify ports in the %systemroot%\System32\drivers\etc\services file.
Dynamically allocated ports	Specifies ports that are assigned from the ranges you specify on NetBackup clients and servers. You can configure NetBackup to select a port number at random from the allowed range, or you can configure NetBackup to start at the top of a range and use the first port available.

Caution: Veritas recommends that you use the default port number settings for NetBackup services and internet service ports.

If you modify the port number for a daemon, ensure that the daemon's port number is identical for all NetBackup master servers, media servers, and client systems that communicate with each other. If you ever need to contact Veritas Technical Services, inform the technical support representative of all nonstandard ports in your NetBackup environment.

The following other guides contain information about NetBackup ports:

■ NetBackup Administrator's Guide, Volume I

■ NetBackup Administrator's Guide, Volume II

The following topics contain information about NetBackup ports:

■ See "About NetBackup daemons, ports, and communication" on page 75.

■ See "About configuring ports" on page 86.

■ See "Port requirements for NDMP backups" on page 89.

■ See "Known firewall problems encountered when using NetBackup with third-party robotic products" on page 90.

About NetBackup daemons, ports, and communication

The following topics describe the ports that the NetBackup daemons use:

- See "Standard NetBackup ports" on page 75.

- See "NetBackup master server outgoing ports" on page 76.

- See "NetBackup media server outgoing ports" on page 77.

- See "NetBackup enterprise media management (EMM) server outgoing ports" on page 78.

- See "Client outgoing ports" on page 79.

- See "Java server outgoing ports" on page 79.

- See "Java console outgoing ports" on page 80.

- See "Additional port information for products that interoperate with NetBackup" on page 82.

Standard NetBackup ports

Table 3-2 shows the standard ports in a NetBackup environment. Some daemons are associated only with add-on products. The **Notes** column indicates the products that use the daemon.

Table 3-2   List of daemons and ports used in a standard NetBackup environment

Source	Port name and/or number	Destination	Notes
NetBackup master server	`VNETD` / 13724	NetBackup master server, media server, or client	Network daemon, `VNETD`.
NetBackup media server	`VNETD` / 13724	NetBackup master server, media server, or client	Network daemon, `VNETD`.
Client	`VNETD` / 13724	NetBackup master server	Network daemon, `VNETD`.
NetBackup master server	`veritas_pbx` 1556	NetBackup master server, media server, or client	Veritas private branch exchange service, VxPBX.
NetBackup media server	`veritas_pbx` 1556	NetBackup master server, media server, or client	Veritas private branch exchange service, VxPBX.

Table 3-2   List of daemons and ports used in a standard NetBackup
                   environment *(continued)*

Source	Port name and/or number	Destination	Notes
Client	`veritas_pbx` 1556	NetBackup master server	Veritas private branch exchange service, VxPBX.
NetBackup master server, media server, or client	13783	NetBackup master server	NetBackup authentication service, VxAT. NetBackup hosts connect using the PBX port.
NetBackup master server or media server	13722	NetBackup master server	NetBackup Authorization Service, VxAZ. NetBackup hosts connect using the PBX port.

In a NetBackup environment, the source port number for connections to the well-known destination port numbers (provided in the table) is always derived from the source component's client port window or the client reserved port window. A typical NetBackup environment uses additional daemons and ports as described in the following topics:

NetBackup master server outgoing ports

Table 3-3 shows the ports that the master server uses to connect to remote hosts.

Table 3-3   NetBackup master server outbound ports and destinations

Port name and number	Destination	Notes
`veritas_pbx` 1556	Media server	Connect-back for job information. Connect-back for resource information. Determines the NetBackup software release level on the media server. Starts `bpbrm` for backups and restores. Starts `bptm` to manage tape storage units. Starts `bpstsinfo` to manage disk storage units. Accesses or updates host properties for the media server.

Table 3-3   NetBackup master server outbound ports and destinations
(continued)

Port name and number	Destination	Notes
`veritas_pbx` 1556	Enterprise media management (EMM) server	Determines the NetBackup software release level on the client. Accesses or information about the device, media, and storage databases. Obtains the list of mount points for multistreamed backups. Accesses or updates host properties for the client.
`veritas_pbx` 1556	Administrative console or Java server	Connect-back for Activity Monitor.
`veritas_pbx` 1556	Java console	Connect-back for job monitor.
13783	Authentication server	Authenticates users and machines. Used only when the following are both true: ■ NetBackup access control (NBAC) is enabled. ■ Media servers and clients in the NetBackup environment host a NetBackup software release level that is lower than the release level on the master server.
13722	Authorization server	Authorizes a user for system administration. Used only when NBAC is enabled.

NetBackup media server outgoing ports

shows the ports that the media server uses to connect to remote hosts. The table shows the port name, port number, destination, and additional information.

| **Table 3-4** | | NetBackup media server outbound ports and destinations |

Port name and number	Destination	Notes
`veritas_pbx` 1556	Master server	Accesses legacy policy information from `bpdbm`. Accesses legacy job information from `bpjobd`. Updates image catalog information to `bpdbm`. Makes miscellaneous requests to `bprd`. Accesses job information. Accesses resource information.
`veritas_pbx` 1556	Media server	Establishes sockets to other media servers for duplication, disk staging, and synthetics.
`veritas_pbx` 1556	Enterprise media management (EMM) server	Accesses information about device, media, and storage databases.
`veritas_pbx` 1556	Client	Determines the NetBackup software release level on the client and is used to backup or restore the client files or data.
13783	Authentication server	Authenticates users and machines. Used only when NetBackup access control (NBAC) is enabled.
13722	Authorization server	Authenticates a user for system administration. Used only when NBAC is enabled.

NetBackup enterprise media management (EMM) server outgoing ports

This information applies to remote EMM servers in the NetBackup setups.

Table 3-5 shows the ports that the EMM server uses to connect to remote hosts.

| **Table 3-5** | | NetBackup EMM server outbound ports and destinations |

Port name and number	Destination	Notes
`veritas_pbx` 1556	Master server	Connect-back for information about device, media, and storage databases.

Table 3-5	NetBackup EMM server outbound ports and destinations *(continued)*

Port name and number	Destination	Notes
veritas_pbx 1556	Media server	Connect-back for information about device, media, and storage databases.
veritas_pbx 1556	Administrative console or Java server	Connect-back for information about device, media, and storage databases.
13783	Authentication server	Authenticates users and machines. Used only when the following are both true: ■ NetBackup access control (NBAC) is enabled. ■ Media servers and clients in the NetBackup environment host a NetBackup software release level that is lower than the release level on the master server.
13722	Authorization server	Authorizes a user for system administration.

Client outgoing ports

Table 3-6 shows the ports that clients use to connect to remote hosts.

Table 3-6	NetBackup client outbound ports and destinations

Port name and number	Destination	Notes
veritas_pbx 1556	Master server	Sends backup, restore, and other requests to bprd.
13783	Authentication server	Authenticates users or machines.

Java server outgoing ports

Table 3-7 shows the ports that the Java Server uses to connect to remote hosts.

The Java Server also uses outgoing ports to the NetBackup Product Authentication and Authorization Service (shown as VxSS Server).

| **Table 3-7** | | Java server outbound ports and destinations |

Port name and number	Destination	Notes
veritas_pbx 1556	Master server	Accesses the jobs manager, nbjm. Manages policies. Manages host properties. Starts manual backups and restores.
veritas_pbx 1556	Media server	Accesses devices.
veritas_pbx 1556	Enterprise media management (EMM) server	Accesses devices, media, and storage unit databases.
13783	Authentication server	Establishes user credentials for administration.

Java console outgoing ports

Table 3-8 shows the ports that the Administration Console uses to connect to remote hosts.

| **Table 3-8** | | Administration Console outbound ports and destinations |

Port name and number	Destination	Notes
veritas_pbx 1556	Master server	Establishes sockets with the job manager, nbjm.
vnetd 13724	Master server	Establishes sockets with the legacy job manager, bpjobd.
vnetd 13724	Java server	Establishes sockets with the legacy Java server, bpjava.

About MSDP port usage

The following table shows the ports that are used for NetBackup deduplication. If firewalls exist between the various deduplication hosts, open the indicated ports on the deduplication hosts. Deduplication hosts are the deduplication storage server, the load balancing servers, and the clients that deduplicate their own data.

If you have only a storage server and no load balancing servers or clients that deduplicate their own data, you do not have to open firewall ports.

Table 3-9   Deduplication ports

Port	Usage
10082	The NetBackup Deduplication Engine (`spoold`). Open this port between the hosts that deduplicate data. Hosts include load balancing servers and clients that deduplicate their own data.
10102	The NetBackup Deduplication Manager (`spad`). Open this port between the hosts that deduplicate data. Hosts include load balancing servers and clients that deduplicate their own data.
443	The PureDisk Storage Pool Authority. Open this port between the NetBackup clients that deduplicate their own data and the PureDisk Storage Pool.

About Cloud port usage

This is applicable for media server versions 7.7.x to 8.1.2 only.

Table 3-10 shows the port that is used by NetBackup Cloud.

Table 3-10   NetBackup Cloud port

Port	Usage
5637	The NetBackup Web Management Console (`nbwmc`) uses this port. Open this port between the master server and all the media servers that are configured for cloud storage. This port is used to provide back-level media server support. This is applicable for media server versions 7.7.x to 8.1.2 only. Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.

Even though legacy media servers are supported, Veritas recommends that you upgrade such cloud storage media servers to NetBackup 8.2 or later versions.

After the media servers are upgraded, port 5637 is no longer used. You can disable the service usage on that port using the following command:

UNIX:

```
# /usr/openv/wmc/bin/install/configurePorts -removeLegacyCloudService
```

Windows:

```
<install_path>\NetBackup\var\wmc\bin\install\configurePorts
-removeLegacyCloudService
```

This command removes the legacy cloud service connector from NetBackup web server's server.xml file.

Note: You must restart the NetBackup Web Management Console (nbwmc) service for the changes to take effect.

Additional port information for products that interoperate with NetBackup

The following topics describe port information that is specific to OpsCenter, Backup Exec, and other products that interoperate with NetBackup:

About communication ports and firewall considerations in OpsCenter

Figure 3-1 shows the key OpsCenter components and the communication ports that are used.

Figure 3-1   Key OpsCenter components and how they communicate
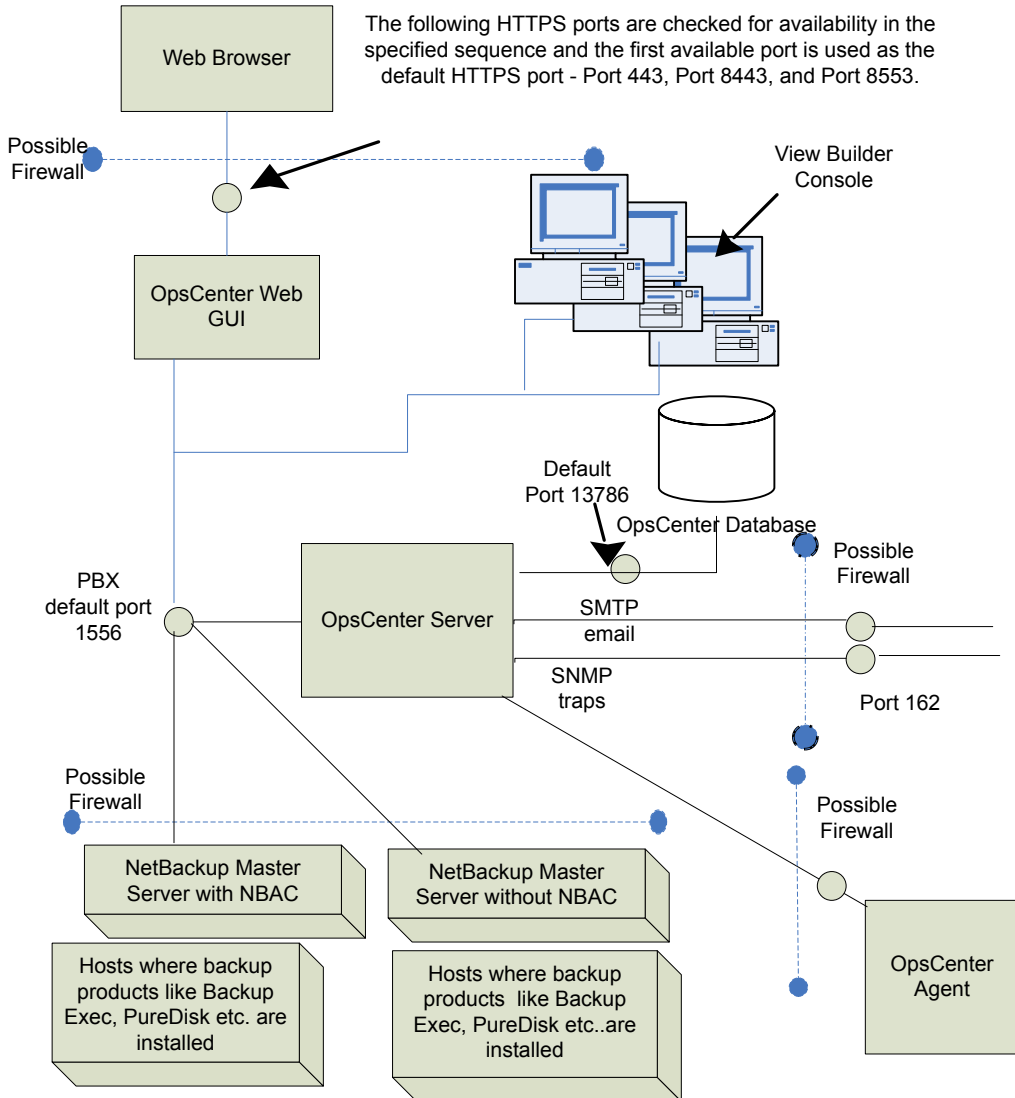
Ports required to communicate with backup products

This section provides information about the ports that OpsCenter Agent uses to communicate with backup products like Backup Exec and PureDisk.

Table 3-11 lists the ports that must be opened on OpsCenter Agent to collect data from various backup products.

Table 3-11   Ports required to communicate with backup products

Backup product	Communication	Port number
Backup Exec	OpsCenter (Backup Exec data collector) communicates with Backup Exec Server using Backup Exec API	6106
PureDisk	OpsCenter (PureDisk data collector) communicates with PureDisk SPA using `atssl`	443 (HTTPS) 2821 (AT)

Web browser to launch OpsCenter user interface

Web browsers use Secure hypertext transfer protocol (HTTPS) to communicate with the OpsCenter web graphical user interface. These protocols use TCP/IP.

Table 3-12 lists how the default HTTPS ports are selected.

Table 3-12   Default HTTPS ports

Sr. No.	HTTPS port number	Description
1.	443	Port 443 is checked for availability. ■ If port 443 is available, it is used as the default HTTPS port. ■ In case, some other application like a web server uses this port, then the next port is checked for availability.
2.	8443	Port 8443 is checked for availability. ■ If port 8443 is available, port 8443 is used as the default HTTPS port. ■ In case another application like VRTSWeb installed with VCS or any other product uses one or both ports, then the next port combination is checked for availability.
3.	8553	Port 8553 is checked for availability.

These HTTPS ports are opened only for input and are configurable using the command lines.

About OpsCenter user interface and OpsCenter server software communication

The OpsCenter web graphical user interface uses Veritas Private Branch Exchange (PBX) to communicate with the OpsCenter server software. The default port is 1556. The PBX port is opened for input and output traffic.

About OpsCenter server to NetBackup master server (NBSL) communication

OpsCenter requires the NetBackup Service Layer (NBSL) to be present on all managed master servers.

The OpsCenter server software collects data from NBSL in the following ways:

- Initial data load

- Listening for change notifications or events

Whenever OpsCenter server software starts, when data collection for a master server is enabled or when a master server is added in OpsCenter, the OpsCenter server starts collecting all the available data from NetBackup master server into the OpsCenter database using NBSL. The initial data load happens serially for each data type. As soon as the initial data load is complete, the OpsCenter server software listens to the notifications that are sent by NBSL for any change in NetBackup data. Then OpsCenter updates the OpsCenter database.

Veritas Private Branch Exchange (PBX) is used for communication and requires a port opened on the OpsCenter server and the NetBackup master server for input and output. The default PBX port is 1556.

About SNMP traps

SNMP trap protocol is used for outbound UDP traffic and requires a port that opens for output. The port number is 162.

About communication between OpsCenter and Sybase database

The OpsCenter web graphical user interface communicates with the OpsCenter Sybase SQL Anywhere database server by using the default port 13786.

The Sybase database server port is closed to all inbound connections. The database is available only to resident OpsCenter components on the OpsCenter server.

About email communication in OpsCenter

SMTP email server protocol is used for outgoing mail. The port number is defined when the user specifies the SMTP server port (see **Settings > Configuration > SMTP Server** in the OpsCenter console to specify this port). The port is opened for output only.

About configuring ports

NetBackup interfaces enable you to configure various nondefault ports in your environment to support firewalls and other network features.

The following topics explain how to set port configuration options:

- See "Enabling or disabling random port assignments" on page 86.
- See "Editing port information in configuration files" on page 87.
- See "Updating client connection options" on page 88.
- See "Updating port settings for the Media Manager in the vm.conf file" on page 88.

Enabling or disabling random port assignments

The **Use random port assignments** property specifies how the selected computer chooses a port when it communicates with NetBackup on other computers, as follows:

- When enabled, NetBackup chooses port numbers randomly from those that are free in the allowed range. For example, if the range is from 1023 through 5000, it chooses from the numbers in this range. This is the default behavior.

- When disabled, NetBackup chooses numbers sequentially, starting with the highest number that is available, in the allowed range. For example, if the range is from 1023 through 5000, NetBackup chooses 5000, assuming that it is free. If 5000 is used, NetBackup chooses port 4999.

The port selection scheme must be the same on the master server and on all media servers. By default, NetBackup assigns ports randomly. If you change one of your computers to use sequential port assignments, make sure to change *all* the computers in your environment to use sequential port assignments.

The following procedure explains how to specify port assignments.

To specify port assignments from the NetBackup Administration Console

1   In the **NetBackup Administration Console**, expand one of the following:

- To specify a master server's port assignments, expand **NetBackup Management > Host Properties > Master Servers**

- To specify a media server's port assignments, expand **NetBackup Management > Host Properties > Media Servers**

2 Double click the host you want to configure.

3 Click **Port Ranges**.

4 Check or clear **Use random port assignments**.

Make sure that the master server and the media servers in your environment are set identically. That is, make sure that **Use random port assignments**is cleared on both systems or that **Use random port assignments** is checked on both systems.

Editing port information in configuration files

NetBackup does not provide a graphical user interface for all port changes that you might need to make. For some settings, you need to edit the `bp.conf` file. The following are the `bp.conf` settings that you might want to change:

- `ALLOW_NON_RESERVED_PORTS`

- `CLIENT_PORT_WINDOW`

- `CLIENT_RESERVED_PORT_WINDOW`

- `CONNECT_OPTIONS`

- `DEFAULT_CONNECT_OPTIONS`

- `RANDOM_PORTS`

- `SERVER_RESERVED_PORT_WINDOW`

- `SERVER_PORT_WINDOW`

For information about the preceding settings, see the NetBackup Administrator's Guide, Volume I.

Veritas recommends that you do not change the `bp.conf` file directly. The following procedure uses general terms to explain how to use the `bpgetconfig` and `bpsetconfig` commands to change port information in the `bp.conf` file.

To change port settings in the bp.conf file

1 Type the `bpgetconfig` command from a NetBackup master server, NetBackup media server, or client.

```
bpgetconfig options > outputfile
```

For *options*, specify options from the `bpgetconfig` man page.

For *outputfile*, specify the name of a text file.

2 Edit the output file you created to update port information.

For example, on UNIX or Linux platform, you can use `vi`(1) to edit the file. On a Windows system, you can use Notepad to edit the file.

3 Type the `bpsetconfig` command to write the file back to NetBackup.

For more information about configuration settings and ports, see the following:

■ NetBackup Administrator's Guide, Volume I

■ NetBackup Commands Reference Guide

Updating client connection options

NetBackup provides the following ways to specify client connection options:

■ From the NetBackup administration console. Expand **Host Properties > Master Servers > Client Attributes > Connect Options**.

■ From the command line. You can use the `bpclient` command to update a variety of client attributes.
For example, you can use the `-connect_options` argument to the `bpclient` command to specify client port connection options.
For more information about the command, see the *NetBackup Commands* manual.

Updating port settings for the Media Manager in the vm.conf file

The `vm.conf` file specifies Media Manager connection options. If you want to override the default connection options, you need to edit the `vm.conf` file. The NetBackup administration console does not provide a way to change these settings. The path to the `vm.conf` is as follows:

■ On Linux or UNIX, the path is as follows:
`/usr/openv/volmgr/vm.conf`

■ On Windows systems, the path is as follows:
install_path`\volmgr\vm.conf`

Table 3-13 shows the `vm.conf` file settings that affect ports.

Table 3-13	Port usage-related Media Manager configuration settings

Setting	Description

CLIENT_PORT_WINDOW	Specifies the range of source ports that can be used on outgoing Media Manager connections. The format is as follows:
	
	`CLIENT_PORT_WINDOW = min max`
	
	The *min* argument defines the lowest source port number.
	
	The *max* argument defines the highest source port number.
	
	For *min* and *max*, specify `0` (zero) or specify integers from `1024` to `65535`. If *min* is `0` or if *max* is less than *min*, then the operating system determines the source port number.
	
	By default, `CLIENT_PORT_WINDOW = 0  0`.
	
	For example, the following setting defines a source port range from 3000 to 8000:
	
	`CLIENT_PORT_WINDOW = 3000 8000`

RANDOM_PORTS	Specifies whether NetBackup chooses ports randomly or sequentially when it communicates with other NetBackup servers. The format is as follows: `RANDOM_PORTS = YES	NO`  If `RANDOM_PORTS = YES`, or if there is no `RANDOM_PORT` entry, NetBackup selects a random port from the range specified by the `CLIENT_PORT_WINDOW` setting in the `vm.conf` file.  If `RANDOM_PORTS = NO`, the NetBackup attempts the connection with the highest source port number in the range. If the source port does not work, NetBackup tries the next highest source port number. The port number is chosen from the list until it finds a source port number that works.

Port requirements for NDMP backups

Network data management protocol (NDMP) storage unit backups require that specific ports be open in a firewall environment. The backup type determines the ports that need to be opened in the firewall.

The following table explains the ports requirements for NDMP backups.

Table 3-14   Ports requirements for NDMP backups

Backup type	Description
Local	For local operations, the Data Management Application (DMA) needs access to port 10000 on the NDMP server. In this case, the one NDMP server is both the NDMP tape server and the NDMP data server.
Three-way and remote NDMP	For three-way and remote NDMP, the DMA needs access to port 10000 on the NDMP tape server and the NDMP data server. There cannot be a firewall between the NDMP tape server and the NDMP data server. No firewall is needed because control is not required over the TCP/IP ports that are used for the data movement.

On UNIX systems, the NetBackup `avrd` process uses the Internet Control Message Protocol (ICMP) when it pings the NDMP hosts to verify network connectivity. If a ping fails, NetBackup skips this particular device, which leaves the status of the drive as up.

On Windows systems, NetBackup does not ping the NDMP device. It tries the connection. If the network experiences connectivity problems, this method can take longer as NetBackup waits for a timeout.

Known firewall problems encountered when using NetBackup with third-party robotic products

Communication between some third-party products and NetBackup occurs through undefined ports. NetBackup has no control over this communication, so there is no way to open firewall ports between a NetBackup media server and the following third-party servers:

- An automated cartridge system (ACS) server. A remote procedure call enables this communication. There is no common port.

- A Fujitsu library management facility (LMF) server.

- A tape library half-inch (TLH) IBM library manager server.

- A tape library multimedia (TLM) ADIC DAS/SDLC server.

Auditing NetBackup operations

This chapter includes the following topics:

- About NetBackup auditing

- Viewing the current audit settings

- Audit retention period and catalog backups of audit records

- Viewing the detailed NetBackup audit report

- User identity in the audit report

- Disabling auditing

- Audit alert notification for audit failures (NetBackup Administration Console)

- About Enhanced Auditing

About NetBackup auditing

Auditing is enabled by default in new installations. NetBackup auditing can be configured directly on a NetBackup master server or by using OpsCenter. See the *NetBackup OpsCenter Administrator's Guide* for more details.

Auditing of NetBackup operations provides the following benefits:

- Customers can gain insight from audit trails while they investigate unexpected changes in a NetBackup environment.

- Regulatory compliance.
  The record complies with guidelines such as those required by the Sarbanes-Oxley Act (SOX).

- A method for customers to adhere to internal change management policies.

- Help for NetBackup Support in troubleshooting problems for customers.

About the NetBackup Audit Manager

The NetBackup Audit Manager (`nbaudit`) runs on the master server and audit records are maintained in the Enterprise Media Manager (EMM) database.

An administrator can search specifically for:

- When an action occurred

- Failed actions in certain situations

- The actions that a specific user performed

- The actions that were performed in a specific content area

- Changes to the audit configuration

Note the following:

- The audit record truncates any entries greater than 4096 characters. (For example, policy name.)

- The audit record truncates any restore image IDs greater than 1024 characters.

Actions that NetBackup audits

NetBackup records the following user-initiated actions.

Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
Alerts and email notifications	If an alert cannot be generated or an email notification cannot be sent for NetBackup configuration settings. For example, SMTP server configuration and the list of excluded status codes for alerts.
Asset actions	Deleting an asset, such as a vCenter server, as part of the asset cleanup process with the Asset Database API is audited and logged. Creating, modifying, or deleting an asset group as well any action on an asset group for which a user is not authorized is audited and logged.
Authorization failure	Authorization failure is audited when you use the NetBackup web UI, the NetBackup APIs, or Enhanced Auditing. See "About Enhanced Auditing" on page 100.
Catalog information	This information includes: ■ Verifying and expiring images. ■ Read the requests that are sent for the front-end usage data.

Certificate management	Creating, revoking, renewing, and deploying of NetBackup certificates and specific NetBackup certificate failures.
Certificate Verification Failures (CVFs)	Any failed connection attempts that involve SSL handshake errors, revoked certificates, or host name validation failures.
	For certificate verification failures (CVFs) that involve SSL handshakes and revoked certificates, the timestamp indicates when the audit record is posted to the master server. (Rather than when an individual certificate verification fails.) A CVF audit record represents a group of CVF events over a time period. The record details provide the start and the end times of the time period as well as the total number of CVFs that occurred in that period.
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools.
Hold operations	Creating, modifying, and deleting hold operations.
Host database	NetBackup host database-related operations.
Logon attempts	Any successful or any failed logon attempts for the NetBackup Administration Console, the NetBackup web UI or the NetBackup APIs.
Policies actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
Restore and browse image user actions	All the restore and browse image content (`bplist`) operations that a user performs are audited with the user identity.
Security configuration	Information that is related to changes that are made to the security configuration settings.
Starting a restore job	NetBackup does not audit when other types of jobs begin. For example, NetBackup does not audit when a backup job begins.
Starting and stopping the NetBackup Audit Manager (`nbaudit`).	Starting and stopping of the `nbaudit` manager is always audited, even if auditing is disabled.
Storage lifecycle policy actions	Attempts to create, modify, or delete a storage lifecycle policy (SLP) are audited and logged. However, activating and suspending an SLP using the command `nbstlutil` are not audited. These operations are audited only when they are initiated from a NetBackup graphical user interface or API.
Storage servers actions	Adding, deleting, or updating storage servers.
Storage units actions	Adding, deleting, or updating storage units.
	Note: Actions that are related to storage lifecycle policies are not audited.
Token management	Creating, deleting, and cleanup of tokens and specific token issuing failures.

User management

Adding and deleting Enhanced Auditing users in the Enhanced Auditing mode.

User action that fails to create an audit record

If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the `nbaudit` log. NetBackup status code 108 is returned (`Action succeeded but auditing failed`). The **NetBackup Administration Console** does not return an exit status code 108 when auditing fails.

Actions that NetBackup does not audit

The following actions are not audited and do not display in the audit report:

Any failed actions.

NetBackup logs failed actions in NetBackup error logs. Failed actions do not display in audit reports because a failed attempt does not bring about a change in the NetBackup system state.

The effect of a configuration change

The results of a change to the NetBackup configuration are not audited. For example, the creation of a policy is audited, but the jobs that result from its creation are not.

The completion status of a manually initiated restore job

While the act of initiating a restore job is audited, the completion status of the job is not audited. Nor is the completion status of any other job type, whether initiated manually or not. The completion status is displayed in the Activity Monitor (Administration Console) and in the Jobs (web UI).

Internally initiated actions

NetBackup-initiated internal actions are not audited. For example, the scheduled deletion of expired images, scheduled backups, or periodic image database cleanup is not audited.

Rollback operations

Some operations are carried out as multiple steps. For example, creating an MSDP-based storage server consists of multiple steps. Every successful step is audited. Failure in any of the steps results in a rollback, or rather, the successful steps may need to be undone. The audit record does not contain details about rollback operations.

Host properties actions

Changes made using the `bpsetconfig` or the `nbsetconfig` commands, or the equivalent property in the Host Properties utility, are not audited. Changes that are made directly to the `bp.conf` file or to the registry are not audited.

Viewing the current audit settings

To view the current audit configuration, use either the `nbemmcmd` command on a NetBackup master server or view the settings using OpsCenter.

For directions about how to use OpsCenter to configure auditing, see the NetBackup OpsCenter Administrator's Guide.

To view the current audit settings

1   Log on to the master server.

2   Open the following directory:

Windows: *install_path*\NetBackup\bin\admincmd

UNIX: /usr/openv/netbackup/bin/admincmd

3   Run the following command:

nbemmcmd -listsettings -machinename *masterserver*

Where *masterserver* is the master server in question.

4   The following configuration settings are listed:

■   AUDIT="ENABLED"
Indicates that auditing is turned on.

■   AUDIT="DISABLED"
Indicates that auditing is turned off.

■   AUDIT_RETENTION_PERIOD="90"
Indicates that if auditing is enabled, the records are retained for this length of time (in days) and then deleted. The default audit retention period is 90 days. A value of 0 (zero) indicates that the records are never deleted.

Audit retention period and catalog backups of audit records

The audit records are kept as part of the NetBackup database, for as long as the retention period indicates. The records are backed up as part of the NetBackup catalog backup. The NetBackup Audit Service (nbaudit) deletes expired audit records once every 24 hours at 12:00 A.M. (local time).

By default, audit records are kept for 90 days. Use an audit retention period value of 0 (zero) if you do not want to delete the audit records.

To configure the audit retention period

1 Log on to the master server.

2 Open the following directory:

Windows: *install_path*\NetBackup\bin\admincmd

UNIX: /usr/openv/netbackup/bin/admincmd

3 Enter the following command:

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
number_of_days -machinename masterserver
```

Where *number_of_days* indicates (in days) how long audit records are to be retained for the audit report.

In the following example, the records of user actions are retained for 30 days and then deleted.

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
-machinename server1
```

To ensure that audit records are not missed from a catalog backup, configure the catalog backup frequency to be less frequent or equal to the -AUDIT_RETENTION_PERIOD.

Viewing the detailed NetBackup audit report

You can view the actions NetBackup audits from a master server using the NetBackup web user interface or the NetBackup Administration Console. You can see full audit event details with the nbauditreport command or in NetBackup OpsCenter.

See the NetBackup OpsCenter Administrator's Guide for more details.

To view the full audit report

1 Log on to the master server.

2 Enter the following command to display the audit report in the summary format.

Windows: *install_path*\NetBackup\bin\admincmd\nbauditreport

UNIX: /usr/openv/netbackup/bin/admincmd\nbauditreport

Or, run the command with the following options.

`-sdate`
 	
`<"MM/DD/YY`
`[HH:[MM[:SS]]]">`
	The start date and time of the report data you want to view.

`-edate`
 	
`<"MM/DD/YY`
`[HH:[MM[:SS]]]">`
	The end date and time of the report data you want to view.

`-ctgy` *category*	The category of user action that was performed. Categories such as `POLICY` may contain several sub-categories such as schedules or backup selections. Any modifications to a sub-category are listed as a modification to the primary category. See the NetBackup Commands Guide for `-ctgy` options.

`-user`
 	
`<`*username*`[:`*domainname*`]>`
	Use to indicate the name of the user for whom you'd like to display audit information.

`-fmt DETAIL`	The `-fmt DETAIL` option displays a comprehensive list of audit information. For example, when a policy is changed, this view lists the name of the attribute, the old value, and the new value. This option has the following sub-options: ■ `[-notruncate]` . Display the old and new values of a changed attribute on separate lines in the details section of the report. ■ `[-pagewidth <NNN>]` . Set the page width for the details section of the report.
`-fmt PARSABLE`	The `-fmt PARSABLE` option displays the same set of information as the `DETAIL` report but in a parsable format. The report uses the pipe character (`|`) as the parsing token between the audit report data. This option has the following sub-options: ■ `[-order <DTU|DUT|TDU|TUD|UDT|UTD>]`. Indicate the order in which the information appears. `D` (Description) `T` (Timestamp) `U` (User)

3 The audit report contains the following details:

DESCRIPTION	The details of the action that was performed.
USER	The identity of the user who performed the action. See "User identity in the audit report" on page 99.
TIMESTAMP	The time that the action was performed.

The following information only displays if you use the -fmt DETAIL or the -fmt PARSABLE options.

CATEGORY	The category of user action that was performed.
ACTION	The action that was performed.
REASON	The reason that the action was performed. A reason displays if a reason was specified for the operation that created the change.
DETAILS	An account of all of the changes, listing the old values and the new values.

Example of the audit report:

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP          USER          DESCRIPTION
04/20/2018 11:52:43  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:42  root@server1   Schedule 'full' was added to Policy 'test_pol_1'
04/20/2018 11:52:41  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:08  root@server1   Policy 'test_pol_1' was created
04/20/2018 11:17:00  root@server1   Audit setting(s) of master server 'server1' were modified

Audit records fetched: 5
```

User identity in the audit report

The audit report indicates the identity of the user who performed a specific action. The full identity of the user includes the user name and the domain or the host name that is associated with the authenticated user. A user's identity appears in the audit report as follows:

- Audit events always include the full user identity. Root users and administrators are logged as "root@hostname" or "administrator@hostname".

- In NetBackup 8.1.2 and later, image browse and image restore events always include the user ID in the audit event. NetBackup 8.1.1 and earlier log these events as "root@hostname" or "administrator@hostname".

- For any operations that do not require credentials or require the user to sign in, operations are logged without a user identity.

Disabling auditing

NetBackup auditing is enabled by default. To disable Enhanced Auditing, see the following:

See "Disabling Enhanced Auditing" on page 106.

To disable auditing

1 Log on to the master server.

2 Open the following directory:

   Windows: *install_path*\NetBackup\bin\admincmd

   UNIX: /usr/openv/netbackup/bin/admincmd

3 Enter the following command:

   nbemmcmd -changesetting -AUDIT DISABLED -machinename *masterserver*

   In the following example, auditing has been turned off for server1.

   nbemmcmd -changesetting -AUDIT DISABLED -machinename server1

Audit alert notification for audit failures (NetBackup Administration Console)

Use the alert notification option to choose if you want to be notified when an auditable action fails to create an audit record. This option is located in the status bar of the NetBackup Administration Console.
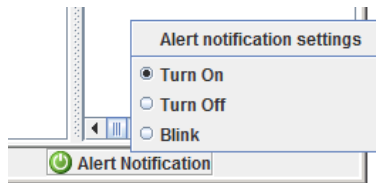
Table 4-1   Audit alert notification options

Turn on	A pop-up message appears to alert the administrator about the failure.
Blink	The icon blinks in the event of an auditing failure. Click the icon to display the failure message.
Turn off	An auditing failure does not display a notification. The icon appears gray.

About Enhanced Auditing

With Enhanced Auditing, NetBackup administrators can delegate NetBackup administrator privileges to other designated users. The feature thus allows non-root users to administer NetBackup. The audit logs capture information about the actual user who makes changes to the NetBackup environment. Enhanced Auditing helps organizations track key information about the user activity that is important for audit compliance requirements. In particular, it is a feature that customers in highly regulated industries find useful.

Note: Any authorization failure is also audited with Enhanced Auditing.

By default, only a root or administrator can perform NetBackup operations through the command-line interface. However, with NetBackup configured for Enhanced Auditing and with the right NetBackup Administrator privileges, users can perform NetBackup operations through the command-line interface. Enhanced Auditing provides coarse access control where the user is either an administrator or not one.

Enhanced Auditing is not supported on the NetBackup Appliances.

Note: NBAC and Enhanced Auditing are mutually exclusive features.

Note: For now, Enhanced Auditing support is available for user operations such as NetBackup Policies, Jobs, Storage Units, Disk Pools, Storage Servers, Catalogs, and Host Properties, certificate deployment, and token generation.

The following table lists the commands where user actions are audited with Enhanced Auditing:

Table 4-2   Commands and categories supported for Enhanced Auditing

Category	Commands
Policy	`bpplcatdrinfo, bpplclients, bppldelete, bpplinclude, bpplinfo, bppllist, bpplsched, bpplschedrep, bpplschedwin, bpplvalid, bppolicynew`
Jobs	`bpdbjobs`
Storage Unit	`bpstuadd, bpstuddel, bpsturep, bpstulist`
Disk Pool	`nbdevconfig and nbdevquery`
Storage Servers	`nbdevconfig and nbdevquery`
Catalogs	`bpexpdate, bpcatlist, bpimmedia, bpimagelist, bpverify, and nbdeployutil`
Host Properties	`bpconfig, bpsetconfig, bpgetconfig, nbsetconfig, nbgetconfig, and nbemmcmd`
Security tokens	`createToken, deleteToken, and cleanupToken`
Certificates	`getCertificate, revokeCertificate, signCertificate, and renewCertificate`

Enabling Enhanced Auditing

Use the following procedure to enable Enhanced Auditing.

To configure NetBackup for Enhanced Auditing

1 Run the `bpnbaz -SetupExAudit` command on the master server.

Note: In a clustered NetBackup setup, while you configure NetBackup to enable Enhanced Auditing, you need to run the `bpnbaz -SetupExAudit` command only on the active node.

---

2 Restart the NetBackup services.

See "Disabling Enhanced Auditing" on page 106.

See "Configuring Enhanced Auditing" on page 102.

Configuring Enhanced Auditing

You must perform a few additional configuration steps for certain scenarios for Enhanced Auditing. These steps are applicable when you perform a change server operation.

- A security certificate is mandatory when you connect to a media server through the **NetBackup Administration Console**.
  See "Connecting to a media server with Enhanced Auditing" on page 102.
- When you do a change server from a master server to another master server, you have to execute additional steps on the master server.
  See "Changing a server across NetBackup domains" on page 103.

Connecting to a media server with Enhanced Auditing

For Enhanced Auditing, a security certificate is mandatory when a user wants to connect to a media server through the NetBackup Administration Console. Additional steps must be executed on the master server to get the certificate for each media server. Refer to the following procedure for details:

To generate a security certificate for a server

1 Run the `bpnbaz -ProvisionCert target.server.com` command on the master server. Here the `target.server.com` is the media server name.

Sample usage: `acme.domain.mycompany.com` is a media server to which a user wants to do a change server

Run the command `bpnbaz -ProvisionCert acme.domain.mycompany.com` on the master server.

The following is the output:

```
bpnbaz -ProvisionCert acme.domain.mycompany.com

Setting up security on target host: acme.domain.mycompany.com

Certificate deployed successfully

Operation completed successfully.
```

2 Always restart the services on the media servers after generating a certificate.

Note: Generating a security certificate is a one-time activity.

Changing a server across NetBackup domains

For Enhanced Auditing, when you perform a Change Server operation from a master or media server in one NetBackup domain to a host (master or media server or client) in another NetBackup domain, you must execute additional steps on each NetBackup server. You must also set up a trust on both master servers.

Note: Executing these steps is a one-time activity.

The following steps help you to change the server and set up the trust on both master servers.

To change server from a master to master server

1 We have two NetBackup domains, `NetBackup Domain 1` and `NetBackup Domain 2`.

Consider two master servers, `Master_nbu_dom1` and `Master_nbu_dom2`. `Master_nbu_dom1` has media servers `Media1_nbu_dom1`, `Media2_nbu_dom1`, `MediaN_nbu_dom1`, and a set of clients. Similarly, `Master_nbu_dom2` has media servers `Media1_nbu_dom2`, `Media2_nbu_dom2`, `MediaM_nbu_dom2`, and a set of clients as shown in the image:

NetBackup Domain 1

Master_nbu_dom1

Media1_nbu_dom1	Media2_nbu_dom1	MediaN_nbu_dom1

Client Client Client Client Client Client

NetBackup Domain 2

Master_nbu_dom2

Media1_nbu_dom1	Media2_nbu_dom2	MediaM_nbu_dom2

Client Client Client Client Client Client
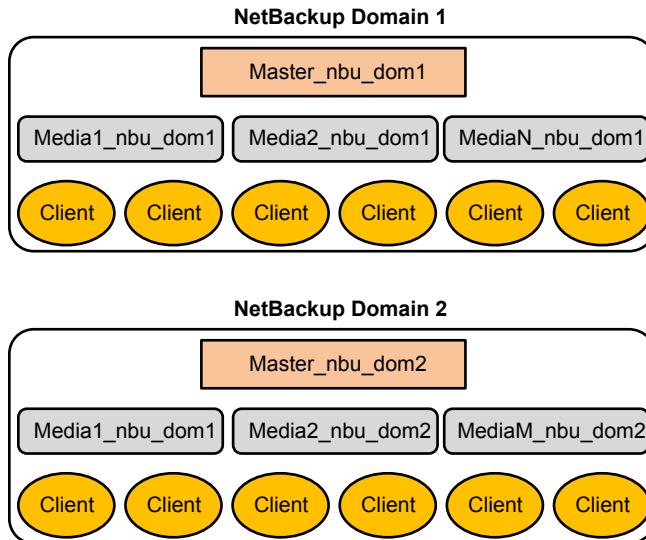
The user is connected to one of the servers in `NetBackup Domain 1` (either master or media), for example, `Master_server_nbu_dom1`, and wants to do a change server to one of the hosts on NetBackup Domain 2, for example `Host_nbu_dom2`. It is mandatory that both the master servers (`Master_nbu_dom1` and `Master_nbu_dom2` here) establish a trust. `Host_nbu_dom2` must set up a trust with `Master_server_nbu_dom1`.

2 To set up the trust, you must invoke a set of commands on UNIX and Windows:

On UNIX and Linux:

```
/usr/openv/netbackup/sec/at/bin/vssat setuptrust -b
```

```
Master_server_nbu_dom1:1556:nbatd -s high on Host_nbu_dom2.
```

On Windows:

```
InstallPath\Veritas\NetBackup\sec\at\bin\vssat.bat
```

3 You must add an additional server entry in Host_nbu_dom2 for the Master_server_nbu_dom1 in the bp.conf file. Run the following command:

```
SERVER = Master_server_nbu_dom1 /*this should __not__ be the first
SERVER entry*/
```

You can also add the additional server entry by connecting to the target master server through the NetBackup Administration Console.

4 The host that has the NetBackup Administration Console or the remote Java Administration console is also required to trust the X.509 NBATD certificate on the `Master_server_nbu_dom2`.

The trust can be set up by directly connecting to the `Master_server_nbu_dom2`master server through the GUI.

You can also invoke `/usr/openv/java/sec/at/bin/vssat setuptrust -b`

`Master_server_nbu_dom2:1556:nbatd -s high` on the NetBackup Administration Console host.

Configuration requirements if using Change Server with NBAC or Enhanced Auditing

Additional configuration is required to perform the Change Server operation if NetBackup Access Control or Enhanced Auditing is used.

The following steps assume that NBAC or Enhanced Auditing is already configured.

Configuration to support the Change Server operation: *fromServer -> toServer*

- Add *fromServer* to the host properties Additional Servers list on *toServer*.

- If *fromServer* and *toServer* are from different NetBackup domains (media servers of different master servers):

  - Use the `vssat` command to set up trust between the master servers of *fromServer* and *toServer*. (See "Changing a server across NetBackup domains" on page 103. Refer to step 2 in the procedure.)

  - Add the master server of *fromServer* to the host properties Additional Servers list on *toServer*.

- If *fromServer* or *toServer* are media servers:

  - Use the `bpnbaz -ProvisionCert` command to deploy the security (Machine) certificate if needed. (See "Connecting to a media server with Enhanced Auditing" on page 102.)

Additional configuration steps

To use the auth.conf file:

- Add the `USER` entry to the auth.conf file on each server.

- If NBAC is enabled, run the `nbsetconfig` on each server to add the entry:

  `USE_AUTH_CONF_NBAC = YES`

To use the Remote Administration Console:

- Set up trust with each master server by using either the `vssat` command or explicitly log on to each server at least once. (See "Changing a server across NetBackup domains" on page 103. Refer to step 2 in the procedure.)

To troubleshoot the configuration after setup, use `nslookup` and `bptestnetconn` `-a -s` to check server communications.

Disabling Enhanced Auditing

When you enable Enhanced Auditing, the `USE_AUTHENTICATION` option is set to ON. To disable Enhanced Auditing, you must set the `USE_AUTHENTICATION` option to OFF. The following steps help you:

To disable Enhanced Auditing

1   Run the `bpnbaz -DisableExAudit` command.

2   Restart the NetBackup services.

Access control security

This chapter includes the following topics:

- About access control in NetBackup

- Managing users with Enhanced Auditing

- User authentication with Enhanced Auditing

- Impact of Enhanced Auditing on NetBackup Administration Console authorization

About access control in NetBackup

NetBackup provides the following types of access control:

- The NetBackup Administration Console (default)
  NetBackup administrators can control who can view the various applications in
  NetBackup. Root users and administrators have full access to the NetBackup
  Administration Console. A non-root or non-administrator user can access the
  Backup, Archive, and Restore application. This user can also access additional
  applications, as defined for that user in the `auth.conf` file.
  Access control is view-based, not role-based. The administrator can control the
  applications that a user can view and manage, but cannot control which tasks
  a user can perform based on their role in the organization. Access control is
  limited to the NetBackup Administration Console. (Interfaces like the Backup,
  Archive, and Restore client and the NetBackup MS SQL Client are not affected.)
  For detailed information about access control with the NetBackup Administration
  Console, refer to the NetBackup Administrator's Guide, Volume I.

- Role Based Access Control (RBAC)
  Beginning with the NetBackup 8.1.2 release, the NetBackup web user interface
  provides role-based access control for a limited number of security settings and
  workloads. Refer to the NetBackup Web UI Security Administrator's Guide for
  more information.

- Enhanced Auditing

  This feature allows a non-root user or a non-administrator to perform all the NetBackup operations through a command-line interface or the NetBackup Administration Console. The user is authorized to either perform all operations or no operations. This feature does not offer role-based access control.

  See "About Enhanced Auditing" on page 100.

- NetBackup Access Control (NBAC)

  NBAC is the original role-based access control provided with NetBackup for the NetBackup Administration Console and the CLIs. Veritas recommends that you use one of the other methods of access control to manage your NetBackup environment.

Access control methods for NetBackup Administration Console and the CLIs

Refer to the following table for key differences between the access control methods available for the NetBackup Administration Console and CLIs. (The RBAC feature in the NetBackup web UI only provides access control for the web UI and for the NetBackup APIs.) For information on NBAC, refer to the NetBackup documentation for 8.1.2 and earlier releases.

Table 5-1

Access and auditing	NetBackup Admin Console and auth.conf	Enhanced Auditing
Who can use the NetBackup Administration Console?	Root users and administrators have full access to the Admin Console. Non-root users or non-administrators are limited to the Backup, Archive, and Restore application by default. Otherwise, these users can access the applications that are defined for them in the `auth.conf` file.	Root users, administrators, and NetBackup administrators have full access to the Admin Console. Non-root users or non-administrators are limited to the Backup, Archive, and Restore application by default.
Who can use the CLI?	Root users and administrators have full access to the CLI.	Root users, administrators, and NetBackup administrators have full access to the CLI.
How is a user audited?	As root or administrator	With the real user name
Compatibility with other features	Enhanced Auditing	NBAC works independently.

Refer to the following flowcharts for details about the access control methods for the NetBackup Administration Console and the CLIs.

Figure 5-1   Access control for CLI users with Enhanced Auditing
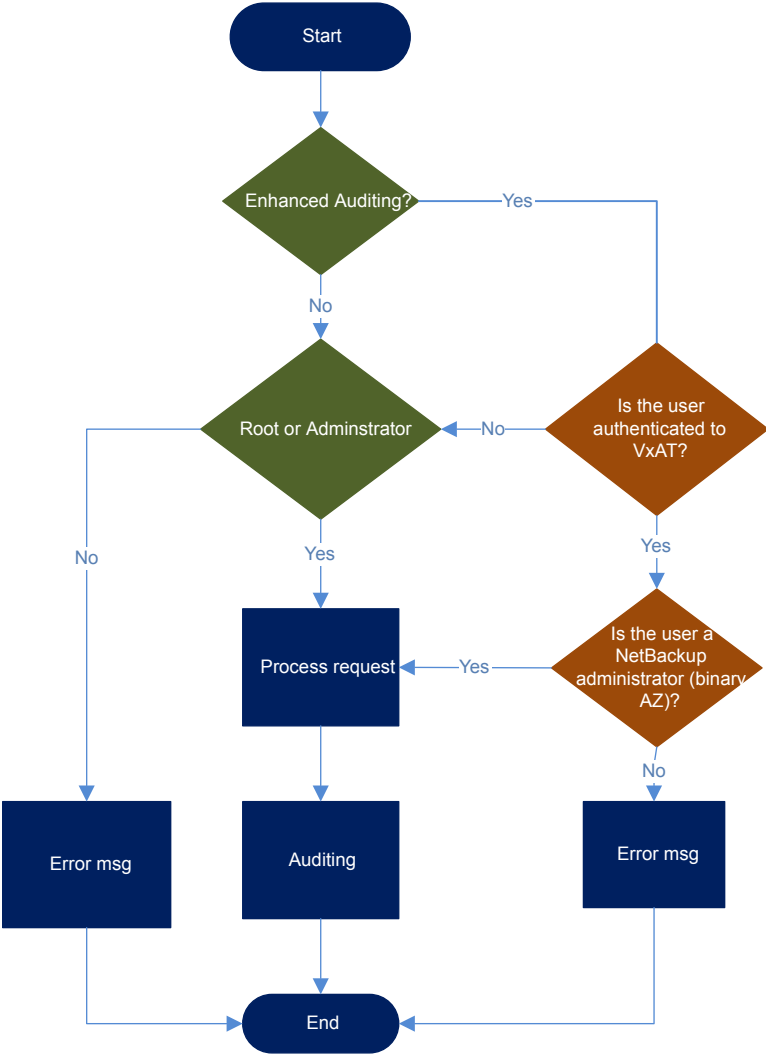
Figure 5-2   Access control for NetBackup Administration Console users with
Enhanced Auditing enabled
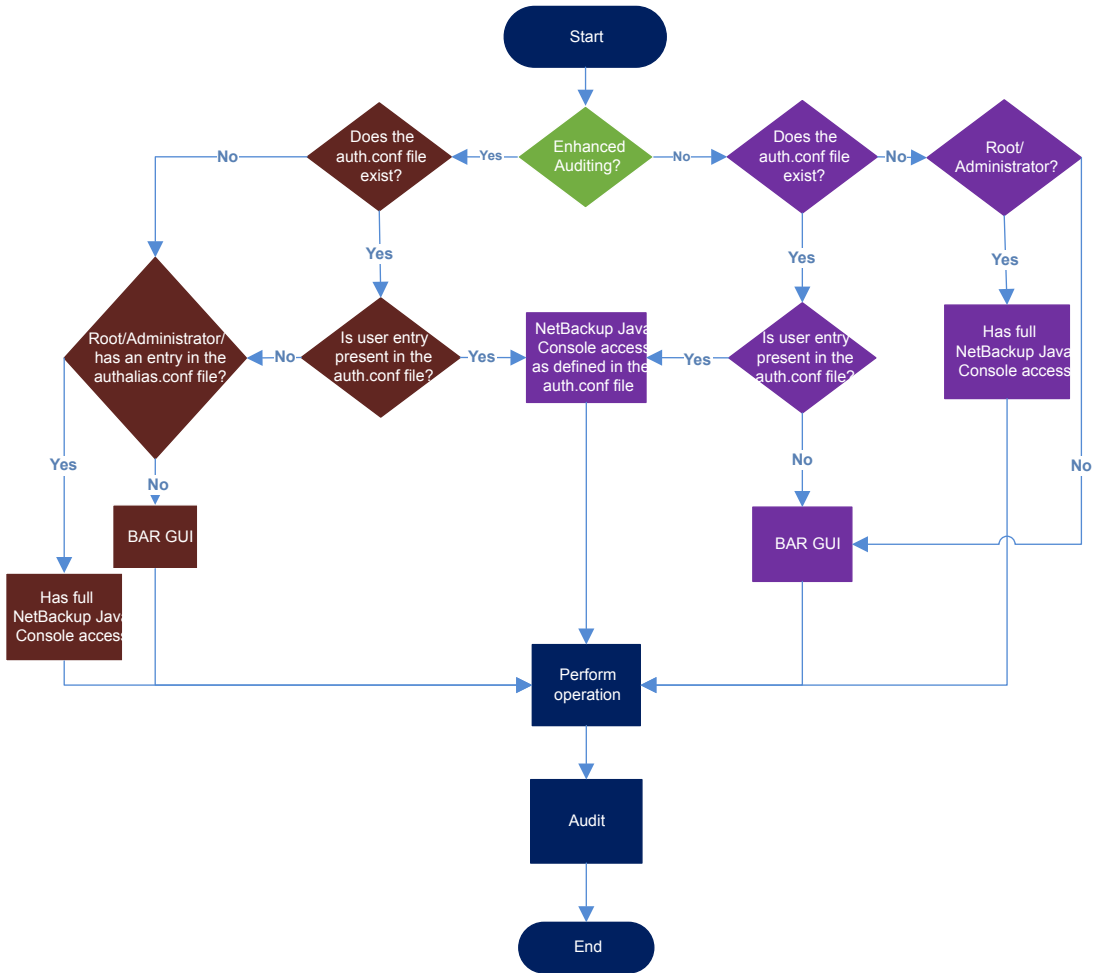
Managing users with Enhanced Auditing

With NetBackup configured for Enhanced Auditing, the administrator can:

- Grant and revoke NetBackup administrator privileges to users.

- Look up a user who has NetBackup administrator privileges.

- List users with NetBackup administrator privileges.

Note: Only a user with NetBackup administrator privileges can perform user management tasks.

Use the `bpnbaz` command to perform user management tasks. The add, delete, lookup, and lists users commands must be run with the following options:

```
bpnbaz -[AddUser | DelUser] Domain_Type:Domain_Name:User_Name [-M
server] [-credfile][-reason]
```

```
bpnbaz -LookupUser Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]
```

```
bpnbaz -ListUsers Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]
```

The following table lists information about each command:

Table 5-2

Command	Description	Example usage
-AddUser	Helps the user to grant NetBackup administrator privileges.	`bpnbaz -AddUser` `unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-DelUser	Helps the user to revoke NetBackup administrator privileges.	`bpnbaz -DelUser` `unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-LookupUser	Helps the user to search for user or to look up users who have administrative privileges.	`bpnbaz -LookupUser` `unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-ListUsers	Helps the user to list the users with NetBackup administrator privileges.	`bpnbaz -ListUsers`

For more information about the `bpnbaz` command, see the NetBackup Commands Reference Guide.

User authentication with Enhanced Auditing

By default, NetBackup does not mandate user authentication. However, when NetBackup is configured for Enhanced Auditing, user authentication from master server is mandatory.

The user should use the `bpnbat -login` command for authentication.

The log in process for UNIX and Windows users varies.

UNIX

- Running the `bpnbat -login` command is mandatory for all users except the root user.

Windows

- The administrator logs in automatically through the Single Sign On (SSO) option.

- A standard user also logs in through the SSO option. But if the SSO fails, the user must run the `bpnbat -login` command. The user can also run the `bpnbat -GetBrokerCert` command to establish a trust with the server.

Impact of Enhanced Auditing on NetBackup Administration Console authorization

Access to the command-line and NetBackup Administration Console works differently when you configure Enhanced Auditing. Entries in the `auth.conf` file supersede the access control for the NetBackup Administration Console.

See "Managing users with Enhanced Auditing " on page 110.

If a user is assigned administrator privileges, the user can perform all auditable NetBackup operations through the command line. Refer to the following table for information about user access:

Table 5-3   User access

auth.conf entry	CLI access	Java interface access
Debbie has an entry in the auth.conf file.	No access	Access as specified in the `auth.conf` file
Debbie has NetBackup administrator privileges, but has no entry in the `auth.conf` file.	Complete access	Complete access

Table 5-3   User access *(continued)*

auth.conf entry	CLI access	Java interface access
Debbie has NetBackup administrator privileges and also has entry in the `auth.conf` file.	Complete access	Access as specified in the `auth.conf` file
Debbie does not have an entry in the `auth.conf` file and also does not have NetBackup administrator privileges.	No access	No access

NetBackup Access Control Security (NBAC)

This chapter includes the following topics:

About using NetBackup Access Control (NBAC)

NetBackup Access Control (NBAC) is the legacy access control method for NetBackup and is no longer being updated. Veritas recommends that you use role-based access control (RBAC) with the web UI.

Note: You cannot use the NetBackup web UI and the web APIs if you have NetBackup Access Control (NBAC) enabled.

The NetBackup Access Control (NBAC) is the role-based access control that is used for master servers, media servers, and clients. NBAC can be used in situations where you want to:

- Use a set of permissions for different levels of administrators for an application. A backup application can have operators (perhaps load and unload tapes). It can have local administrators (manage the application within one facility). It can also have overall administrators who may have responsibility for multiple sites and determine backup policy. Note that this feature is very useful in preventing user errors. If junior level administrators are restricted from certain operations, they are prevented from making inadvertent mistakes.

- Separate administrators so that root permission to the system is not required to administer the system. You can then separate the administrators for the systems themselves from the ones who administer the applications.

The following table lists the NBAC considerations.

Table 6-1   NBAC considerations

Consideration or issue	Description or resolution
Prerequisites before you configure NBAC	This prerequisites list can help you before you start to configure NBAC. These items ensure an easier installation. The following list contains the information for this installation: - User name or password for master server (root or administrator permission). - Name of master server - Name of all media servers that are connected to the master server - Name of all clients to be backed up - Host name or IP address **Note:** Host names should be resolvable to a valid IP address. - Use the `ping` or `traceroute` command as one of the tools to ensure that you can see the hosts. Using these commands ensures that you have not configured a firewall or other obstruction to block access.

Table 6-1   NBAC considerations *(continued)*

Consideration or issue	Description or resolution
Determine if the master server, media server, or client is to be upgraded	Determine if the master server, media server, or client is to be upgraded as follows: ■ Some features are provided by upgrading master servers, some by media servers, and some from upgrading clients. ■ NetBackup works with a higher revision master server and lower revision clients and media servers. ■ Feature content determines what is deployed. ■ Deployment can be step wise if required.
Information about roles	Determine the roles in the configuration as follows: ■ Who administers the hosts (root permission on master server equals head administrator). ■ Determine roles to start and then add on the roles as required.
NBAC license requirements	No license is required to turn on the access controls.
NBAC and KMS permissions	Typically when using NBAC and when the `Setupmaster` command is run, the NetBackup related group permissions (for example, NBU_Admin and KMS_Admin) are created. The default root and administrator users are also added to those groups. In some cases the root and administrator users are not added to the KMS group when NetBackup is upgraded. The solution is to grant the root and the administrator users NBU_Admin and KMS_Admin permissions manually.
Windows Server Failover Clustering (WSFC) error messages while unhooking shared security services from PBX	In WSFC environments running the `bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname>` command can trigger error messages. However the shared Authentication and Authorization services are successfully unhooked from PBX and the errors can be ignored.
Possible cluster node errors	In a clustered environment when the command `bpnbaz -setupmaster` is run in the context of local Administrator the `AUTHENTICATION_DOMAIN` entries may not contain the other cluster node entries. In such case these entries must be manually added from Host Properties into the `bp.conf` file.
Catalog recovery fails when NBAC is set to **REQUIRED** mode	If NBAC is running in **REQUIRED** mode and a catalog recovery was performed, NBAC needs to be reset back from **PROHIBTED** mode to **REQUIRED** mode.

	Table 6-1	NBAC considerations *(continued)*

Consideration or issue	Description or resolution
Policy validation fails in NBAC mode (USE_VXSS = REQUIRED)	Back up, restore, and verification of policy for snapshot can fail in NBAC enabled mode if one of the following has been done. ■ Authenticated Principle is removed from the NBAC group: NBU_Users group ■ Back up and restore permissions of NBU_User group have been removed
The bpnbaz -setupmaster command fails with an error "Unable to contact Authorization Service"	If a user other than an Administrator tries to modify NetBackup security, the bpnbaz –setupmaster fails. Only a user 'Administrator' who is a part of the Administrator's group has permissions to modify the NetBackup security and enable NBAC.
Failure of authentication broker configuration during installation.	Invalid domain name configuration of the system causes failure during configuration of authentication broker. To correct this problem, use the bpnbaz -configureauth command to configure the authentication broker. For information about the bpnbaz command, see the NetBackup Commands Reference Guide.
NetBackup GUI errors may occur if NBAC is enabled on a system that previously had Enhanced Auditing enabled.	When switching the NetBackup server from Enhanced Auditing to NBAC, make sure that all directories that are named after users are deleted in the following directory: Windows: *install_path*\NetBackup\logs\user_ops UNIX, Linux: /usr/openv/netbackup/logs/user_ops The following topic contains more details: See "Troubleshooting NBAC issues" on page 134.

NetBackup access management administration

The access to NetBackup can be controlled by defining the user groups and granting explicit permissions to these groups. You can configure the user groups and assign permissions. Select **Access Management** in the **NetBackup Administration Console**.

Note: In order for the **NetBackup Administration Console** to function, the user must have permission to log on to the system remotely.

Note: If some media servers are not configured with access control, non-root/non-administrator users cannot manage those servers.

About NetBackup Access Control (NBAC) configuration

Note: NBAC is already installed as part of the NetBackup installation. Only the NBAC configuration is required for this release.

The NBAC configuration instructions are for an NBAC configuration in non-HA environments. NetBackup supports a wide variety of HA environments across Linux, Solaris, and Windows environments. The NBAC configuration is as follows:

- If required, build a cluster for the master server. HA information is described in the NetBackup in Highly Available Environments Administrator's Guide for replication and disaster recovery. Clustering information is described in the NetBackup Clustered Master Server Administrator's Guide.

- Configure NBAC for operation by using the instructions provided.
  See "Configuring NetBackup Access Control (NBAC)" on page 118.

Configuring NetBackup Access Control (NBAC)

Note: The manual authentication and authorization client installs need to be done for older media servers and client hosts. NetBackup has the authentication clients and authorization clients that are embedded in them. No authentication servers and authorization servers are needed on media servers and clients.

For information on the NBAC configuration sequence, see the following procedure.

Configuring NetBackup Access Control (NBAC)

1 Configure the master server for NetBackup Access Control (NBAC).

See "Configuring NetBackup Access Control (NBAC) on standalone master servers" on page 120.

Note: The master server can be installed in a standalone mode or in a highly available configuration on a cluster.

---

2 Configure media servers for NBAC.

See "Configuring NetBackup Access Control (NBAC) on media servers" on page 122.

3 Configure clients for NBAC.

See "Installing and configuring access control on clients" on page 124.

NBAC configuration overview

This topic contains recommendations for configuring NetBackup Access Control (NBAC) using the bpnbaz command. This command is available under the NETBACKUP_INSTALL_PATH/bin/admincmd directory.

The bpnbaz utility is required to configure NBAC on the master servers, media servers, and clients. This tool also configures NBAC for all the back revision media's and client's hosts. See the following topic for a summary of the bpnbaz command: See "NBAC configure commands summary" on page 124. This topic provides an example of how to use these commands with specific details on recommended usage. Note that the services should be restarted on each of the servers and clients after configuration.

Since the configuration is done from the master server, ensure that operational communications links exist between the master server, the media servers, and the clients. To review the prerequisites list: See "About using NetBackup Access Control (NBAC)" on page 114. Review the list to ensure that you have noted all the associated media servers, clients, and the addresses to communicate with them.

See the following topic for troubleshooting information: See "Configuration and troubleshooting topics for NetBackup Authentication and Authorization" on page 136. A set of OS commands and one NetBackup command is useful for the first level of troubleshooting. The OS commands are ping, traceroute, and telnet. The NetBackup command is bpclntcmd. Use these commands to establish that the hosts can communicate with each other.

Configuring NetBackup Access Control (NBAC) on standalone master servers

The following procedures describe how to configure NetBackup Access Control (NBAC) on the master servers that are installed on a single computer. A master server requires an authentication server and authorization server.

The following table describes the host names for the NBAC configuration examples.

Table 6-2 Example host names

Host name	Windows	UNIX
Master servers	win_master	unix_master
Media servers	win_media	unix_media
Clients	win_client	unix_client

The following procedure describes how to configure NBAC on standalone master servers.

Note: Use `-setupmaster` and set `USE_VXSS = AUTOMATIC` on the master server. If `USE_VXSS = REQUIRED` is set on the master server and an attempt is made to configure NBAC on media server, the following error can occur: NetBackup master server is configured in `REQUIRED` Mode. Please change the mode to `AUTOMATIC` to complete configuration of the media server.

Configuring NBAC on standalone master servers

1 Complete all of the NetBackup master server installations or upgrades.

2 Run the `bpnbaz -setupmaster` command.

Enter **y**. The system begins to gather configuration information. Then, the system begins to set up the authorization information.

3 Restart the NetBackup services on this computer after the `bpnbaz -setupmaster` command completes successfully.

4 Proceed to set up the media servers. See "Configuring NetBackup Access Control (NBAC) on media servers" on page 122.

Installing the NetBackup master server highly available on a cluster

You can use the following procedure to install the NetBackup master server highly available on a cluster.

Installing NetBackup with clustering

1 Configure the cluster system on which the NetBackup master server is to be installed.

2 Install the NetBackup master server on all nodes of the cluster.

3 Cluster the NetBackup master server.

HA information for replication and disaster recovery is described in the NetBackup in Highly Available Environments Administrator's Guide

Clustering information is described in the NetBackup Clustered Master Server Administrator's Guide.

4 Do a test backup to ensure that it works within the NetBackup domain without having NBAC enabled.

Configuring NetBackup Access Control (NBAC) on a clustered master server

Note: In a Windows clustered environment, after setup master is run, the `AUTHENTICATION_DOMAIN` entry in the passive nodes can be the same as the active node name. This is not acceptable. After a failover on a passive node, when `MFC UI` is launched (using <[local machine name] > \[Administrator user]), an authentication-related pop-up error message is displayed. The work-around for this issue is to add the local node name as authentication domain into the `AUTHENTICATION_DOMAIN` on passive nodes after setup master (before failover). Before updating the value of `AUTHENTICATION_DOMAIN`, get the current value using the `C:\Program Files\Veritas\NetBackup\bin\admincmd\bpgetconfig` command. Then add the local node name as authentication domain in the existing domain list using the `C:\Program Files\Veritas\NetBackup\bin\admincmd\bpsetconfig` command. To exit and save from the `bpsetconfig` command prompt press `Ctrl + Z` and then press the `Enter` key.

Note: Reverting the NBAC mode from REQUIRED to PROHIBITED on the active node of a cluster, can lead the cluster into a faulted state. The workaround for this issue is to do the following. On an active node run the bpclusterutil -disableSvc nbazd command followed by the bpclusterutil -disableSvc nbatd command. Change the bp.conf USE_VXSS=AUTOMATIC or REQUIRED value to PROHIBITED using the bpsetconfig command. Run the bpclusterutil -enableSvc nbazd command followed by the bpclusterutil -enableSvc nbatd command on the active node while turning NBAC to REQUIRED mode to monitor the security services.

You can use the following procedure to configure NetBackup Access Control (NBAC) on a clustered master server.

Configuring NetBackup Access Control (NBAC) on a clustered master server

1   Log on to the primary cluster node.

2   If you use Windows, open a command console.

3   For UNIX, change the directory to /usr/openv/netbackup/bin/admincmd. For Windows, change the directory to C:\Program Files\Veritas\NetBackup\bin\admincmd.

4   Run bpnbaz -setupmaster on the active node.

5   Log on to the master server console GUI.

6   Restart the NetBackup services to ensure that the NBAC settings take place.

Configuring NetBackup Access Control (NBAC) on media servers

The following procedure describes how to configure NetBackup Access Control (NBAC) on media servers in a NetBackup configuration. These steps are needed for the media servers that are not co-located with the master server.

Note: Use -setupmedia set USE_VXSS = AUTOMATIC on the master server. If USE_VXSS = REQUIRED is set on the master server and an attempt is made to configure NBAC on media server, the following error can occur: NetBackup master server is configured in REQUIRED Mode. Please change the mode to AUTOMATIC to complete configuration of the media server.

Configuring access control on media servers

1   Log on to the master server computer.

2   Run the `bpnbat -login` command.

Make sure that you run the `bpnbat -login` command before the `bpnbaz -setupmedia` command to avoid a command failure.

The `bpnbaz -setupmedia` command has a number of options.

This command does not work without an extension for either the individual host, or the `-all` option.

It is recommended to do a dry run of the configuration first, with the `-dryrun` option. It can be used with both `-all` and a single-server configuration. By default, the discovered host list is written to the file `SetupMedia.nbac`. You can also provide your own output file name using the `-out <output file>` option. If you use your own output file, then it should be passed for the subsequent runs with the `-file` option. The dry-run command would look something like the following:

```
bpnbaz -SetupMedia -all -dryrun [-out <outfile>]
```
 or

```
bpnbaz -SetupMedia <media.server.com> -dryrun [-out <outfile>].
```

If all of the media servers that you want to update are in the log file, use the `-dryrun` option. You can proceed with the `-all` command to do them all at once. For example, you can use:

```
bpnbaz -SetupMedia -all
```
 or

```
bpnbaz -SetupMedia -file <progress file>.
```

Note that the `-all` option updates all of the media servers seen each time it runs. If you want to run it for a selected set of media servers, can you do it. Keep only the media server host names that you wanted to configure in a file, and pass that file using the `-file` option. This input file would either be `SetupMedia.nbac` or the custom file name you provided with the `-out` option in the previous dry run. For example, you may have used: - `bpnbaz -SetupMedia -file SetupMedia.nbac`.

To configure a single media server, specify the media server host name as the option. For example, use:

```
bpnbaz -SetupMedia <media.server.com>.
```

3 Restart the NetBackup services on the target media servers after the command completes successfully.

It sets up NBAC on the target hosts. If the configuration of some target hosts did not complete, you can check the output file.

Proceed to the access control configuration for the client hosts after this step.

See "Installing and configuring access control on clients" on page 124.

Installing and configuring access control on clients

The following steps describe installing and configuring NetBackup Access Control on clients in a NetBackup configuration. A client requires authentication client software.

Use the following procedure to install and configure access control on clients.

1 Make sure that no backups are currently running.

2 To set up the client, run the following command on the master server:

```
bpnbaz -setupClient
```

About including authentication and authorization databases in the NetBackup hot catalog backups

If you have a NetBackup environment that uses the online hot catalog backup method, no additional configuration is needed to include the NetBackup Authentication and Authorization databases in the catalog backup.

NBAC configure commands summary

The following table summarizes the commands that are used in the NBAC quick configure sequences.

The following conventions are frequently used in the synopsis of command usage.

Brackets [ ] indicate that the enclosed command-line component is optional.

Vertical bar or pipe (|) -indicate separates optional arguments to choose from. For example, when a command has the format: command arg1|arg2 you can select either the arg1 or arg2 variable.

| **Table 6-3** | NBAC configure commands summary |

Command	Description
`bpnbaz -GetConfiguredHosts [target.server.com [-out file]	-all [-outfile]	-file progress.file]`	The `bpnbaz -GetConfiguredHosts` command is used to obtain NBAC status on the host. Either the `-all` or `target.server.com` options are required for this command. The syntax is: ■ *target.server.com* is the name of a single target host. If for example you want to find out NBAC status on single host, then use this option. ■ `-out` option is used to specify a custom output file name. By default, the output is written to the `SetupMedia.nbac` file. This option can be used with `-all` and the single host configuration options. ■ `-all` is an option that goes through all the policies and collects all unique host names. These host names are found in the policies. It also collects all configured media server(s) and captures the NBAC status of each host in `ConfiguredHosts.nbac` file. ■ `-file progress.file` is an option used to specify host name(s) to be read from `progress_file`. This option expects one host name per line in the progress_file.CLI updates the `progress_file` with the host's NBAC status. It appends `#` after `hostname` followed by the NBAC status. ■ When used with `target.server.com` or `-all` option, status of the host(s) is captured in the `ConfiguredHosts.nbac` file.

	Table 6-3	NBAC configure commands summary *(continued)*

Command	Description

`bpnbaz -SetupMaster [-fsa`
`[<domain type>:<domain`
`name>:]<user name>]`
	The `bpnbaz -SetupMaster` command is run to set up the master server for using NBAC. The authorization server and authentication broker are expected to be installed and running on the master server.
	
	Use the `bpnbaz -SetupMaster -fsa` command with the First Security Administrator option to provision a particular OS user as NBU Administrator.
	
	The syntax is:
	
	■ `-fsa` option is used for provisioning a specific OS user as NBU Administrator. When using this option you are asked for the password for your current OS user identity.
	■ *domain type* is the type of network domain you are using. For example the `bpnbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe` command provisions the Windows enterprise domain user `jdoe` as NBU Administer.
	■ *domain name* is the name of the particular domain you are using. For example the `bpnbaz -SetupMaster -fsa jdoe`command takes the current logged on user domain type (Windows/UNIXPWD), domain name, and provisions `jdoe` user in that domain.
	■ *user name* is the particular OS user name you are designating as an NBU Administrator.
	
	Note: The user is verified for the existence in the specified domain. Existing behavior of provisioning the logged-on Administrator or root as NBU Admin is preserved.

Table 6-3　　　　NBAC configure commands summary *(continued)*

Command	Description
`bpnbaz -SetupMedia [` `media.server.com [-out file] |` `-all [-out file]	-file` `progress.file] [-dryrun]` `[-disable]`	The `bpnbaz -SetupMedia` command is run by an NBU_Administrator group member on the master server. It should not be run until a `bpnbaz -SetupMaster` has been completed successfully. It expects connectivity between the master server and target media server systems. Either the `-all` or `target.server.com` options are required for this command. The syntax is: ■ *media.server.com* is the name of a single target host. Use this option to add a single additional host for use with NBAC. ■ `-out` option is used to specify a custom output file name. By default, the output is written to the `SetupMedia.nbac` file. This option can be used with `-all` and the single host configuration options. ■ `-all` goes through all the storage units and collect all unique host names that are found in the storage unites. These can be tried in a sorted order. The results are written to the progress file. ■ `-file` *progress_file* option is used to specify an input file with a specific set of media server host names. After the run, status for each media server is updated in the progress file. Successfully completed ones are commented out for the subsequent runs. This command can be repeated until all the media servers in the input file are successfully configured. ■ `-dryrun` can generate the list of media server names and write them to the log. This option can work with media.server.com but it is intended to be used with the `-all` option. ■ `-disable` option can disable NBAC (USE_VXSS = PROHIBITED) on targeted hosts.

Table 6-3		NBAC configure commands summary *(continued)*

Command	Description
`bpnbaz -SetupClient [ client.server.com [-out file] | -all [-images] [-out file] | -file progress.file ] [-dryrun] [-disable]`	The `bpnbaz -SetupClient` command is used for setting up NBAC on the clients. It should not be run until the `bpnbaz -SetupMaster` command has been completed successfully. The `bpnbaz -SetupClient` needs to run from the master server. It expects connectivity between the master server and target client systems. Either the `-all` or `target.server.com` options are required for this command. The syntax is: ■ *client.server.com* is the name of a single target host. If for example you wished to add a single additional host for use with NBAC, then this name is the option for you. ■ `-out` is an option that is used to specify a custom output file name. By default, the output is written to the `SetupClient.nbac` file. This option can be used with `-all` and the single host configuration options. The `-out` option is used to specify a custom output file name. By default, the output is written to the `SetupClient.nbac` file. This option can be used with `-all` and the single host configuration options. ■ `-all` is an option that goes through all the policies and collects all unique host names that are found within the policies. The policies are tried in a sorted order. The results are written to the progress file. ■ `-images` is an option that searches all images for unique host names. This option cannot be recommended for customers with large catalogs unless they add the -dryrun option. This option yields all unique clients that are contained in the image catalog. Older catalogs can contain a larger number of decommissioned hosts, hosts that are moved to new masters, or are renamed. Run time of the command can increase as attempts are made to contact unreachable hosts. ■ `-dryrun` is an option that generates the list of client names and writes them to the log. It does not result in actual configuration of the target systems. ■ `-disable` is an option that disables NBAC (USE_VXSS = PROHIBITED) on targeted hosts. ■ `-file progress.file` is an option used to specify a different file name for the progress log. The CLI reads the host names from the progress_file. The status is appended next to each host name with a [# separated value]. Successfully completed ones are commented out. This command can be run multiple times until all the clients in the `progress_file` are successfully configured.

Unifying NetBackup Management infrastructures with the setuptrust command

Note: This is done automatically when the OpsCenter server name is provided during install time. If not, there is a command that adds OpsCenter server name to the NetBackup master server. That establishes the trust from the NetBackup side.

The Veritas products management servers need to communicate so that an administrator for one product has permission to administer another product. This communication ensures that application processes in one management server work with another server. One way of ensuring that communication is to use a common independent security server called a root broker. If all of the management servers point to a common root broker, the permission for each server is based on a common certificate. Another way of ensuring communication is to use the `setuptrust` command. This command is used to establish trust between the two management servers. The command is issued from the management server that needs to trust another management server. The security information is transferred from that host to the one requesting the trust establishment. A one-way trust is established. Setting up two way (mutual) trust is performed by issuing the `setuptrust` command from each of the two servers involved. For example, a NetBackup configuration may consist of one OpsCenter server (OPS) and three master servers (A, B, and C). Each of the master servers has connected to them the NBAC policies and management for the clients and the media servers.

The first step is to have the OpsCenter server (OPS) setup trust with each of the master servers (A, B, and C). This trust ensures that the Veritas OpsCenter server receives secure communications from each of the master servers, the clients and the media servers connected to each of the master servers. A sequence of these events is as follows:

- The OPS sets up trust with master server A.

- The OPS sets up trust with master server B.

- The OPS sets up trust with master server C.

If Veritas OpsCenter is set up to perform actions on the individual master servers, a trust relationship needs to be set up from each of the master servers to the OpsCenter server (OPS). A sequence of these events is as follows. In this case, the `setuptrust` command is run six times.

- The master server A sets up trust with Veritas OpsCenter server (OPS).

- The master server B sets up trust with Veritas OpsCenter server (OPS).

- The master server C sets up trust with Veritas OpsCenter server (OPS).

- The Veritas OpsCenter server OPS sets up trust with master server A.

- The Veritas OpsCenter server OPS sets up trust with master server B.

- The Veritas OpsCenter server OPS sets up trust with master server C.

Note: NetBackup and OpsCenter establish trust automatically. You may need to do these setuptrust operations manually with older NetBackup master servers. At the end of the NetBackup master server installation, there is a question on the OpsCenter host name. With that, the master server can initiate a two-way trust setup.

Details on the setuptrust command are described in the NetBackup Commands Reference Guide. See "Using the setuptrust command" on page 130.

Using the setuptrust command

You can use the setuptrust command to contact the broker to be trusted, obtain its certificate or details over the wire, and add to the trust repository if the furnished details are trustworthy. The security administrator can configure one of the following levels of security for distributing root certificates:

- High security (2): If a previously untrusted root is acquired from the peer (that is, if no certificate with the same signature exists in our trust store), the user is prompted to verify the hash.

- Medium security (1): The first authentication broker is trusted without prompting. Any attempts to trust subsequent authentication brokers causes the user to be prompted for a hash verification before the certificate is added to the trusted store.

- Low security (0): The authentication broker certificate is always trusted without any prompting. The vssat CLI is located in the authentication service 'bin' directory.

The setuptrust command uses the following syntax:

```
vssat setuptrust --broker <host[:port]> --securitylevel high
```

The setuptrust command uses the following arguments:

The broker, host, and port arguments are first. The host and port of the broker to be trusted. The registered port for Authentication is 2821. If the broker has been configured with another port number, consult your security administrator for information.

Configuring Access Control host properties for the master and media server

To configure the access control host properties for the master server or media server, expand **NetBackup Management > Host Properties > Master Servers** *or* **Media Servers >** *server name* **> Access Control**.

Set **NetBackup Product Authentication and Authorization** to either **Required** or **Automatic**. A setting of **Automatic** takes into account that there may be hosts within the configuration that are not yet configured for NBAC. The server attempts to negotiate the most secure connection possible when it communicates to other NetBackup systems. The **Automatic** setting should be used until all of the clients and servers are configured for NBAC.

When **Automatic** is selected, you can specify computers or the domains required to use **NetBackup Product Authentication and Authorization**. Otherwise, you can specify the computers that are prohibited from using the **NetBackup Product Authentication and Authorization**.

Authentication Domain tab

The **Authentication Domain** tab is used to define the following:

- Which authentication servers support which authentication mechanisms
- What each domain supports.

Add the domain that you want users to authenticate against.

The following examples contain six authentication domains.

Note: When a UNIX authentication domain is used, enter the fully qualified domain name of the host that performed the authentication.

Note: The authentication types that are supported are `NIS`, `NISPLUS`, `WINDOWS`, `vx`, and `unixpwd` (`unixpwd` is default).

Authorization Service tab

Note: No changes are allowed from this tab. It is read only.

Within the **Access Control** host properties, on the **Authorization Service** tab, you can see the host name. All of this information is grayed out because it is read only. You cannot make any changes to this screen.

Network Attributes tab

View the **Access Control** host properties on the **Network Attributes** tab. Add the master server to the **Networks** list. Then, set the **NetBackup Product Authentication and Authorization** to **Required**.

Each new NetBackup client or media server that is added to the NetBackup master needs to have the **Access Control** properties configured. These properties are configured on both itself and the master. This configuration can be done through the host properties on the master server.

Access Control host properties dialog for the client

Select the NetBackup client in the host properties. (On the master server, in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Clients > *Selected clients* > Access Control**.)

Set the **NetBackup Product Authentication and Authorization** to **Required** or **Automatic**. In this example, **Automatic** is selected.

Authentication Domain tab for the client

Select the NetBackup client in the host properties. It can be used to control which systems require or prohibit the use of NetBackup Product Authentication and Authorization on a per-machine basis. Note that both systems must have matching settings to communicate.

Within the **Access Control** host properties, on the **Authentication Domain** tab, add the list of domains a client can use to authenticate. You can click **Find** to get a list of available authentication domains. Then, click **Add** to create a list of selected authentication domains.

Network Attributes tab for the client

Within the **Access Control** host properties, on the **Network Attributes** tab, add the list of networks that the client can use to authenticate.

Using NetBackup Access Control (NBAC) with Auto Image Replication

If Auto Image Replication is configured for two domains and NetBackup Access Control (NBAC) is used, it must be used in both the source domain and the target domain. The configuration for the master servers must be either `USE_VXSS = REQUIRED` or `USE_VXSS = AUTOMATIC`. (However, the setting may be `REQUIRED` in one domain and `AUTOMATIC` in the other.

Auto Image Replication is not supported between master server domains where one master server is configured to use NBAC and NBAC is disabled on the other master server. That is, the configuration for one master server is `USE_VXSS = AUTOMATIC` or `USE_VXSS = REQUIRED` and on the other master server it is `USE_VXSS = PROHIBITED` (disabled).

The following configuration is necessary if NBAC is used in the master server domains:

- In the source master server domain:
  The administrator should make sure that the target master server has the permissions set correctly before configuration for the operation begins.

- In the target master server domain:
  The security administrator in the target domain must give the administrator in the source domain the correct set of permissions. The source domain administrator needs Browse, Read, and Configure permissions on the following objects: **HostProperties**, **DiskPool**, and **DevHost**.
  The source domain administrator can be added as a member to any existing group which has all three permissions.

Consider the following example:

Two NBAC domains each contain a master server:

- Replication source NBAC domain: *DomainA* contains *Master-A*

- Replication target NBAC domain: *DomainB* contains *Master-B*

NBAC is enabled in both the domains. (If NBAC is used in one domain, it must be used in the other domain.)

For *UserA* to create an Auto Image Replication SLP with *Master-B* as the target, *UserA* needs permission on *Master-B* to do so.

A security administrator (*UserB*) in *DomainB* must create a user group (*NB_InterDomainUsers*, for example) and give Browse, Read, and Configure permissions in the following areas:

- **HostProperties**

- **DiskPool**

- **DevHost**

The security administrator in *DomainB* (*UserB*) then assigns *NB_InterDomainUsers* to `DomainA\UserA` using the `bpnbaz -AddUser` command.

Troubleshooting Access Management

To troubleshoot access management and to determine if certain processes and functionality are operating correctly:

See "Configuration and troubleshooting topics for NetBackup Authentication and Authorization" on page 136.

These verification points include:

- Windows verification points
  See "Windows verification points" on page 143.

- UNIX verification points
  See "UNIX verification points" on page 152.

- Verification points in a mixed environment with a UNIX master server
  See "Verification points in a mixed environment with a UNIX master server" on page 159.

- Verification points in a mixed environment with a Windows master server
  See "Verification points in a mixed environment with a Windows master server" on page 165.

Troubleshooting NBAC issues

The following table lists the issues and solutions that are related to NBAC:

Table 6-4   NBAC issues

Issue and Cause	Solution
A user directed backup or restore fails A user-directed backup or restore fails with NBAC in the automated mode. The Backup, Archive, and Restore interface shows some errors in the Windows interface when NBAC is configured. A backup or restore failure can happen when a NetBackup setup on a UNIX master server is configured with NBAC and you try to use the Windows interface without first configuring the interface for such a setup. Another reason may be that there is an expired certificate in the home directory.	Configure the Windows interface to support the setup. There should be at least one Microsoft Windows system that acts as an Authentication Broker to authenticate users from the Active Directory domain. Refer to the TECH199281 for steps to configure the Windows interface to make use of existing users from Active Directory to manage or operate or use a NetBackup environment that is primarily on UNIX/Linux platforms. After you correctly configure the setup run the `bpnbat -logout` command to log out from the setup before you restart the interface.
Authentication failure with error 116 The authentication fails with '`error 116-VxSS authentication`' when you try to set up NBAC on a target host.	Check whether NBAC authentication is configured correctly and also if you have a valid usable credential for the target host.
Error when a non-admin user from the NBU_Operator group tries to use Access Management A non-admin user is added to the NBU_Operator group. Read, Browse, and Configure permissions are assigned along with the permission to configure the Host Properties. However, when the user tries to open the Access Management utility, an error displays.	The users from the NBU_Operator group have limited permissions. The user would require a different set of permissions to use the Access Management utility. For the required permissions, add the user to the NBU_Security_Admin group. For more information about user groups: See "NetBackup default user groups" on page 176.
The authorization file (auth.conf) functionality does not work in an NBAC-enabled environment. By default, the auth.conf file is supported by the Java interface in non-NBAC environments only.	For the auth.conf file to work in an NBAC-enabled environment, use the `nbgetconfig` and `nbsetconfig` commands to add the `USE_AUTH_CONF_NBAC` entry to the Windows registry or the bp.conf file on UNIX. The entry must be set to `YES`, as follows: `USE_AUTH_CONF_NBAC = YES` For more details about the auth.conf file, refer to the NetBackup Administrators Guide, Volume I.

	Table 6-4	NBAC issues *(continued)*

Issue and Cause	Solution
Error when switching NetBackup server from Enhanced Auditing to NBAC The NetBackup Administration Console creates user directories with *user name* as directory name, in `netbackup/logs/user_ops`. For Enhanced Auditing, these directories are used by NetBackup processes that run with root privileges. For NBAC, these directories are used by NetBackup processes that run without root privileges. NetBackup GUI errors may occur in the following case: ■ The user directories that were created when Enhanced Auditing was enabled still exist when NBAC is enabled, and ■ Any of those users do not have root privileges. Some examples of errors: ■ In the Backup, Archive, and Restore interface, no jobs appear on the **Task Progress** tab. ■ For a VMware VM restore, the pre-recovery check reports error 12.	**1** On each NetBackup server that the users log on to by means of the GUI, delete the user directories in the following directory: Windows: *install_path*`\NetBackup\logs\user_ops` UNIX, Linux: `/usr/openv/netbackup/logs/user_ops` **2** When the directories are deleted, restart the NetBackup GUI.

Configuration and troubleshooting topics for NetBackup Authentication and Authorization

The following table lists helpful configuration and troubleshooting topics and tips for **NetBackup Authentication and Authorization**. In addition, the table also contains information about a few known issues and tips to resolve them:

Table 6-5   Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization

Topic	Configuration tips
Verifying master server settings	Running `bpnbat -whoami` and specifying the computer credentials, tells in what domain a host is registered and the name of the computer the certificate represents. ```bpnbat -whoami -cf "c:\program Files\veritas\netbackup\var\vxss\credentials\ master.company.com "Name: master.company.com Domain: NBU_Machines@master.company.com Issued by: /CN=broker/OU=root@master.company.com/O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.``` If the domain listed is not NBU_Machines@master.company.com, consider running `bpnbat -addmachine` for the name in question (master). The command is run on the computer that serves the NBU_Machines domain (master). Then, on the computer where you want to place the credentials, run: `bpnbat -loginmachine`

Establishing root credentials	If you have problems setting up either the authentication server or authorization server, and the application complains about your credentials as `root`: ensure that the `$HOME` environmental variable is correct for `root`.
	
	 Use the following command to detect the current value:
	
	 `echo $HOME`
	
	 This value should agree with root's home directory, which can be typically found in the `/etc/passwd` file.
	
	 Note that when switching to `root`, you may need to use:
	
	 `su -`
	
	 instead of only `su` to correctly condition the `root` environment variables.

Expired credentials message	If your credential has expired or is incorrect, you may receive the following message while running a `bpnbaz` or `bpnbat` command: `Supplied credential is expired or incorrect. Please reauthenticate and try again.` Run `bpnbat -Login` to update an expired credential.

Table 6-5	Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*
Topic	**Configuration tips**
Useful debug logs	The following logs are useful to debug NetBackup Access Control: On the master: `admin`, `bpcd`, `bprd`, `bpdbm`, `bpjobd`, `bpsched` On the client: `admin`, `bpcd` Access control: `nbatd`, `nbazd`. If the master server uses NetBackup Access Control (NBAC) in the REQUIRED mode and the EMM database is remote, the logging information appears in the `bpdbm` log. See the NetBackup Troubleshooting Guide for instructions on proper logging.
Uninstalling NetBackup Authentication and Authorization Shared Services	On UNIX: Using `installics`, select the option for uninstalling authentication and authorization. The following directories should be empty after uninstalling: /opt/VRTSat and /opt/VRTSaz `/etc/vx/vss` `/var/VRTSat and /var/VRTSaz` On Windows: Use the Windows Add/Remove Programs panel from the Control Menu to uninstall authentication and authorization. The `\Veritas\Security` directory should be empty after uninstalling.
Unhooking Shared AT from PBX	When NetBackup is upgraded and NBAC was already enabled in a previous setup, the old Shared AT should be unhooked from PBX. To unhook shared AT, run following command. On UNIX platforms, run `/opt/VRTSat/bin/vssat setispbxexchflag --disable`. On Windows x86, run `C:\Program Files\VERITAS\Security\Authentication\bin\vssat setispbxexchflag --disable`. On Windows x64 , run `C:\Program Files(x86)\VERITAS\Security\Authentication\bin\vssat setispbxexchflag --disable`.

Table 6-5   Configuration and troubleshooting topics and tips for NetBackup
                        Authentication and Authorization *(continued)*

Topic	Configuration tips
Where credentials are stored	The NetBackup Authentication and Authorization credentials are stored in the following directories: UNIX: User credentials: `$HOME/.vxss` Computer credentials: `/usr/openv/var/vxss/credentials/` Windows: <user_home_dir>\Application Data\VERITAS\VSS
How system time affects access control	Credentials have a birth time and death time. Computers with large discrepancies in system clock time view credentials as being created in the future or prematurely expired. Consider synchronizing system time if you have trouble communicating between systems.

NetBackup Authentication and Authorization ports	The NetBackup Authentication and Authorization daemon services use ports 13783 and 13722 for back-level media server and clients. The services use PBX connections.
	
	You can verify that the processes are listening with the following commands:
	
	Authentication:
	
	UNIX
	
	`netstat -an | grep 13783`
	
	Windows
	
	`netstat -a -n | find "13783"`
	
	Authorization:
	
	UNIX
	
	`netstat -an | grep 13722`
	
	Windows
	
	`netstat -a -n | find "13722"`

Table 6-5   Configuration and troubleshooting topics and tips for NetBackup
Authentication and Authorization *(continued)*

Topic	Configuration tips

Stopping NetBackup Authentication and Authorization daemons for Shared Services	When the NetBackup Authentication and Authorization services are stopped, stop authorization first, then stop authentication.
	
	UNIX -Use the following commands.
	
	To stop authorization use the term signal as shown in the example:
	
	``
	# ps -fed |grep nbazd
	   root 17018 1 4 08:47:35 ? 0:01 ./nbazd
	   root 17019 16011 0 08:47:39 pts/2 0:00 grep nbazd
	 # kill 17018
	``
	
	To stop authentication use the term signal as shown in the example:
	
	``
	# ps -fed |grep nbatd
	   root 16018 1 4 08:47:35 ? 0:01 ./nbatd
	   root 16019 16011 0 08:47:39 pts/2 0:00 grep nbatd
	 # kill 16018
	``
	
	Windows
	
	Use the Services utility that Windows provides, since these services do not appear in the NetBackup Activity Monitor.

If you lock yourself out of NetBackup	You can lock yourself out of the **NetBackup Administration Console** if access control is incorrectly configured. If this lockout occurs, use `vi` to read the bp.conf entries (UNIX) or `regedit` (Windows) to view the Windows registry in the following location: `HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\ CurrentVersion\config` You can look to see if the following entries are set correctly: AUTHORIZATION_SERVICE, AUTHENTICATION_DOMAIN, and USE_VXSS. The administrator may not want to use NetBackup Access Control or does not have the authorization libraries installed. Make certain that the `USE_VXSS` entry is set to `Prohibited`, or is deleted entirely.
Backups of storage units on media servers might not work in an NBAC environment	The host name of a system in NetBackup domain (master server, media server, or client) and host name that is specified in the `bp.conf` file should be the same.

Table 6-5 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips
Using the nbac_cron utility	Use the `nbac_cron.exe` utility to create identities under which to run cron or at jobs.
	For more information about the `nbac_cron` utility:
	See "About the nbac_cron utility" on page 172.
	`nbac_cron.exe` is found in the following location:
	UNIX - `/opt/openv/netbackup/bin/goodies/nbac_cron`
	Windows - `Install_path\Veritas\netbackup\bin\goodies\nbac_cron.exe`
	For detailed information about using the `nbac_cron` utility:
	See "Using the nbac_cron utility" on page 172.
Enabling NBAC after a recovery on Windows	Use the following procedure to manually enable NBAC after a recovery on Windows.
	- Add `AUTHENTICATION_DOMAIN`, `AUTHORIZATION_SERVICE`, and `USE_VXSS` entries in Registry. - Change the service type of NetBackup Authentication and Authorization services to `AUTOMATIC`. - Restart the NetBackup services. - Verify that the `nbatd` and `nbazd` services are running.
	Note: On a cluster run the `bpclusterutil -enableSvc nbatd` and `bpclusterutil -enable nbazd` commands.
In cluster installations the `setupmaster` might fail	A known issue exists in the case of cluster installations, where the configuration file is on a shared disk, the `setupmaster` might fail.
Known issue on a cluster if shared security services (`vxatd` or `vxazd`) are clustered along with the master server	A known issue exists on a cluster if shared security services (`vxatd` or `vxazd`) are clustered along with the master server. When executing the `bpnbaz -SetupMaster` command and setting up security (NBAC), freeze the shared security services service groups persistently where applicable or offline the services (but make sure their shared disk is online), and run the `setupmaster` command.

Table 6-5   Configuration and troubleshooting topics and tips for NetBackup
Authentication and Authorization *(continued)*

Topic	Configuration tips
Known issue in a clustered master server upgrade with NBAC, that all the AUTHENTICATION_DOMAIN entries in the bp.conf file are updated with the master server virtual name as the authentication broker	A known issue exists where in a clustered master server upgrade with NBAC, all the AUTHENTICATION_DOMAIN entries in the bp.conf file are updated with the master server virtual name as the authentication broker. If any domain entry is present that refers to a different authentication broker other than the master server (and the master server does not service that domain), that entry needs to be manually removed from the bp.conf file.
Known issue on Windows 2003 dual stack computers	A known issue exists on Windows 2003 dual stack computers. You need Microsoft patch kb/928646 from http://support.microsoft.com/.
Known issue relating to access control failures and short and long host names	A known issue exists that includes failures with respect to access control. Determine if the short and long host names are properly resolvable and are resolving to the same IP address.
Known issue in a cluster upgrade with NBAC when the broker profile has ClusterName set to the virtual name of AT	A known issue exists in a cluster upgrade with NBAC when the broker profile has ClusterName set to the virtual name of AT. This is migrated as-is to the embedded broker. The embedded broker has UseClusterNameAsBrokerName set to 1 in its profile. When a request is sent for broker domain maps, it uses the virtual name of the shared AT as the broker name. The bpnbaz -GetDomainInfosFromAuthBroker returns none. In upgrades, the bp.conf file is updated to have the NetBackup virtual name.
Known issue of multiple instances of bpcd causing a possible error	A known issue exists where the bpnbaz -SetupMedia command, bprd uses the AT_LOGINMACHINE_RQST protocol to talk with bpcd on the destination box. A new instance of bpcd is spawned. After the command completes it tries to free a char array as a regular pointer possibly causing bpcd to core dump on the client side. Functionality should not be lost as this bpcd instance is only created temporarily and exits normally. The parent bpcd is unaffected.
Known issue with clusters using shared AT with configuration files on the shared drive	A known issue exists with clusters that use a shared AT with configuration files on the shared drive. Unhooking shared services only works on the node where this shared drive is accessible. Unhook fails on the remaining nodes. The implication of this is that while doing a bpnbaz -SetupMaster to manage remote broker parts fail. You will have to manually configure passive nodes. Run bpnbaz -SetupMedia for each passive node.
Known issue relating to database utilities supporting NBAZDB	A known issue exists in which some database utilities support NBAZDB and other database utilities do not. The following database utilities support NBAZDB: nbdb_backup, nbdb_move, nbdb_ping, nbdb_restore, and nbdb_admin. The following utilities do not support NBAZDB: nbdb_unload and dbadm.

Windows verification points

The following configuration procedures can help you verify that the master server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See "Master server verification points for Windows" on page 144.

- See "Media server verification points for Windows" on page 148.

- See "Client verification points for Windows" on page 150.

Figure 6-1 shows an example configuration containing Windows systems only.

Figure 6-1   Example configuration containing Windows systems only

authentication
server   NBU master server (Windows) win_server.min.com

▪ Root Broker
authorization Authentication Broker
server   ▫ Authorization Service

Private Veritas Product Authentication and Authorization domain called:

NBU_Machines@win_server.min.com

contains the following host accounts:

win_server.min.com
win_media.min.com
win_client.min.com

Media server (Windows) win_media.min.com

authentication client, authorization client

win_media.min.com

Windows User accounts authenticate
via Windows authentication Broker

Client (Windows) win_client.min.com

authentication client

win_client.min.com

Note:
Each machine has a private domain account that is created for it. Using these accounts allows NetBackup to more reliably identify machines as they communicate with each other.

Master server verification points for Windows

The following topics describe procedures to:

- Verify Windows master server settings.

- Verify which computers are permitted to perform authorization lookups.

- Verify that the database is configured correctly.

- Verify that the `nbatd` and `nbazd` processes are running.

- Verify that the host properties are configured correctly.

The following table describes the master server verification procedures for Windows.

	Table 6-6	Master server verification procedures for Windows

Procedure	Description
Verify Windows master server settings	You can determine the domain in which a host is registered (where the primary authentication broker resides). Or you can determine the name of the computer the certificate represents. Run `bpnbat` with `-whoami` and specify the host credential file. The server credentials are located in the `c:\Program Files\Veritas\Netbackup\var\vxss\credentials\...` directory.

For example:

```
bpnbat -whoami -cf
"c:\Program
Files\Veritas\Netbackup\var\vxss\credentials\
 win_master"
Name: win_master.company.com
Domain: NBU_Machines@win_master.company.com
Issued by: /CN=broker/OU=root@win_master.company.com/
 O=vx
Expiry Date: Oct 31 20:17:51 2007 GMT
Authentication method: Veritas Private Security
Operation completed successfully.
```

If the domain listed is not NBU_Machines@win_master.company.com, consider running `bpnbat -addmachine` for the name in question (win_master). This command is run on the computer with the authentication broker that serves the NBU_Machines domain (win_master).

Then, on the computer where we want to place the certificate (win_master), run:

```
bpnbat -loginmachine
```

Note: As you determine when a user's credentials expire, keep in mind that the output displays the expiration time in GMT, not local time.

Note: For the remaining procedures in this verification section, assume that the commands are performed from a console window. And that the user identity in question has run `bpnbat -login` from that window. The user is an identity that is a member of NBU_Security Admin. This identity is usually the first identity with which the security was set up.

	Table 6-6	Master server verification procedures for Windows *(continued)*

Procedure	Description
Verify which computers are present in the authentication broker	To verify which computers are present in the authentication broker, log on as a member of the Administrators group and run the following command: `bpnbat -ShowMachines` This command shows the computers for which you have run `bpnbat -AddMachine`. **Note:** If a host is not on the list, run `bpnbat -AddMachine` from the master. Then run `bpnbat -loginMachine` from the host in question.

Verify which computers are permitted to perform authorization lookups	To verify which computers are permitted to perform authorization lookups, log on as a member of the Administrators group and run the following command:
	
	`bpnbaz -ShowAuthorizers`
	
	This command shows that win_master and win_media (master and media servers) are permitted to perform authorization lookups. Note that both servers are authenticated against the same Private Domain (domain type vx), NBU_Machines@win_master.company.com.
	
	Note: Run this command by local administrator or by `root`. The local administrator must be a member of the NBU_Security Admin user group.
	
	<pre>bpnbaz -ShowAuthorizers
	==========
	Type: User
	Domain Type: vx
	Domain:NBU_Machines@win_master.company.com
	Name: win_master.company.com
	==========
	Type: User
	Domain Type: vx
	Domain:NBU_Machines@win_master.company.com
	Name: win_media.company.com
	Operation completed successfully.</pre>
	If a master server or media server is not on the list of authorized computers, run `bpnbaz -allowauthorization server_name` to add the missing computer.

| | Table 6-6 | Master server verification procedures for Windows *(continued)* |

Procedure	Description

Verify that the database is configured correctly	To make sure that the database is configured correctly, run `bpnbaz -listgroups`:
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	If the groups do not appear, or if `bpnbaz -listmainobjects` does not return data, you may need to run `bpnbaz -SetupSecurity`.

Verify that the `nbatd` and `nbazd` processes are running	Use the Windows Task Manager to make sure that `nbatd.exe` and `nbazd.exe` are running on the designated host. If necessary, start them.

Verify that the host properties are configured correctly	In the access control host properties, verify that the NetBackup Authentication and Authorization property is set correctly. (The setting should be either Automatic or Required, depending on whether all computers use NetBackup Authentication and Authorization or not. If all computers do not use NetBackup Authentication and Authorization, set it to Automatic.)
	
	The host properties can also be verified by looking at USE_VXSS in the registry at:
	
	`HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\`
	`CurrentVersion\config.`
	
	Figure 6-2 shows an example of the host properties settings on the **Authentication** domain tab.
	
	In the **Access Control** host properties, verify that the listed authentication domains are spelled correctly and point to the proper servers (valid authentication brokers). If all of the domains are Windows-based, they should point to a Windows computer that runs the authentication broker.

The following figure shows the host properties settings on the **Authentication** domain tab.

Figure 6-2   Host properties settings

Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHENTICATION_DOMAIN	REG_MULTI_SZ	CORE7 "ADDED AUTOMATICALLY" WINDOWS core7 0 NBU_HOSTS@core7
AUTHORIZATION_SERVICE	REG_SZ	core7 0
Browser	REG_SZ	core7
Client_Name	REG_SZ	core7
CONNECT_OPTIONS	REG_SZ	localhost 1 0 2
EMMPORT	REG_DWORD	0x00000614 (1556)
EMMSERVER	REG_SZ	core7
Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin*.lock C:\Program Files\Veritas\···
HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	core7
TELEMETRY_UPLOAD	REG_SZ	NO
USE_AUTHENTICATION	REG_SZ	OFF
USE_VXSS	REG_SZ	AUTOMATIC
UUID_core7	REG_SZ	c771edff-aca9-438d-9523-d8280270caf0
VERBOSE	REG_DWORD	0x00000005 (5)
VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetbackupDB\conf
VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetbackupDB\data
VXSS_SERVICE_TYPE	REG_SZ	INTEGRITYANDCONFIDENTIALITY

Media server verification points for Windows

The following topics describe the media server verification procedures for Windows:

- Verify the media server.

- Verify that the server has access to the authorization database.

- Unable to load library message

The following table describes the media server verification procedures for Windows.

	Table 6-7	Media server verification procedures for Windows

Procedure	Description
Verify the media server	To determine which authentication broker the media server is authenticated against, run `bpnbat -whoami` with `-cf` for the media server's credential file. The server credentials are located in the `c:\Program Files\Veritas\Netbackup\var\vxss\credentials\...` directory.
	For example:

	<pre>bpnbat -whoami -cf "c:\Program
	Files\Veritas\Netbackup\var\vxss\credentials\
	 win_media.company.com"
	Name: win_media.company.com
	Domain: NBU_Machines@win_master.company.com
	Issued by: /CN=broker/OU=root@win_master.company.com/
	 O=vx
	Expiry Date: Oct 31 20:11:40 2007 GMT
	Authentication method: Veritas Private Security
	Operation completed successfully.</pre>

	If the domain listed is not NBU_Machines@win_master.company.com, consider running `bpnbat -addmachine` for the name in question (win_media). This command is run on the computer with the authentication broker that serves the NBU_Machines domain (win_master).
	Then, on the computer where we want to place the certificate (win_media), run:
	`bpnbat -loginmachine`

| | Table 6-7 | Media server verification procedures for Windows *(continued)* |

Procedure	Description

Verify that the server has access to the authorization database	To make sure that the media server is able to access the authorization database as it needs, run `bpnbaz -ListGroups -CredFile "machine_credential_file"`
	
	For example:
	
	<pre>bpnbaz -ListGroups -CredFile "C:\Program
	Files\Veritas\NetBackup\var\vxss\credentials\
	 win_media.company.com"
	NBU_Operator
	NBU_Admin
	NBU_SAN Admin
	NBU_User
	NBU_Security Admin
	Vault_Operator
	Operation completed successfully.</pre>
	If this command fails, run `bpnbaz -AllowAuthorization` on the master server that is the authorization server (win_master.company.com).

Unable to load library message	Verify the media server and that it has access to the proper database. This verification indirectly informs you that the **NetBackup Authentication and Authorization** client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries": Check to make certain the authentication client libraries and authorization client libraries are installed. You may also verify that the authentication domains are correct by viewing the access control host properties for this media server.

Client verification points for Windows

The following topics describe the client verification procedures for Windows:

- Verify the credential for the client.

- Verify that the authentication client libraries are installed.

- Verify correct authentication domains.

The following table describes the client verification procedures for Windows.

	Table 6-8	Client verification procedures for Windows

Procedure	Description
Verify the credential for the client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run `bpnbat -whoami` with -cf for the client's credential file.
	For example:

	<pre>bpnbat -whoami -cf "c:\Program
	Files\Veritas\Netbackup\var\vxss\credentials\
	 win_client.company.com
	"
	Name: win_client.company.com
	Domain: NBU_Machines@win_master.company.com
	Issued by: /CN=broker/OU=root@win_master.company.com/
	 O=vx
	Expiry Date: Oct 31 20:11:45 2007 GMT
	Authentication method: Veritas Private Security
	Operation completed successfully.</pre>

	If the domain listed is not NBU_Machines@win_master.company.com, consider running `bpnbat -addmachine` for the name in question (win_client). This command is run on the computer with the authentication broker that serves the NBU_Machines domain (win_master).
	Then, on the computer where we want to place the certificate (win_client), run: `bpnbat -loginmachine`
Verify that the authentication client libraries are installed	**Note:**
	Run `bpnbat -login` on the client to verify that the authentication client libraries are installed.

	<pre>bpnbat -login
	Authentication Broker: win_master
	Authentication port [Enter = default]:
	Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)
	 : WINDOWS
	Domain: ENTERPRISE
	Name: Smith
	Password:Operation completed successfully.</pre>

	If the libraries are not installed, a message displays: The NetBackup Authentication and Authorization libraries are not installed. This verification can also be done by looking at the Windows Add/Remove Programs.

	Table 6-8	Client verification procedures for Windows *(continued)*

Procedure	Description
Verify correct authentication domains	Check that any defined authentication domains for the client are correct either in the **Access Control** host properties or by using regedit. Ensure that the domains are spelled correctly. Ensure that the authentication brokers that are listed for each of the domains is valid for that domain type.

UNIX verification points

Use the following procedures (and the following figure) to verify that the UNIX master server, media server, and client are configured correctly for access control:

- UNIX master server verification
  See "UNIX master server verification" on page 153.

- UNIX media server verification
  See "UNIX media server verification" on page 156.

- UNIX client verification
  See "UNIX client verification" on page 158.

The following example shows an example configuration that contains UNIX systems only.

Figure 6-3   Example configuration containing UNIX systems only
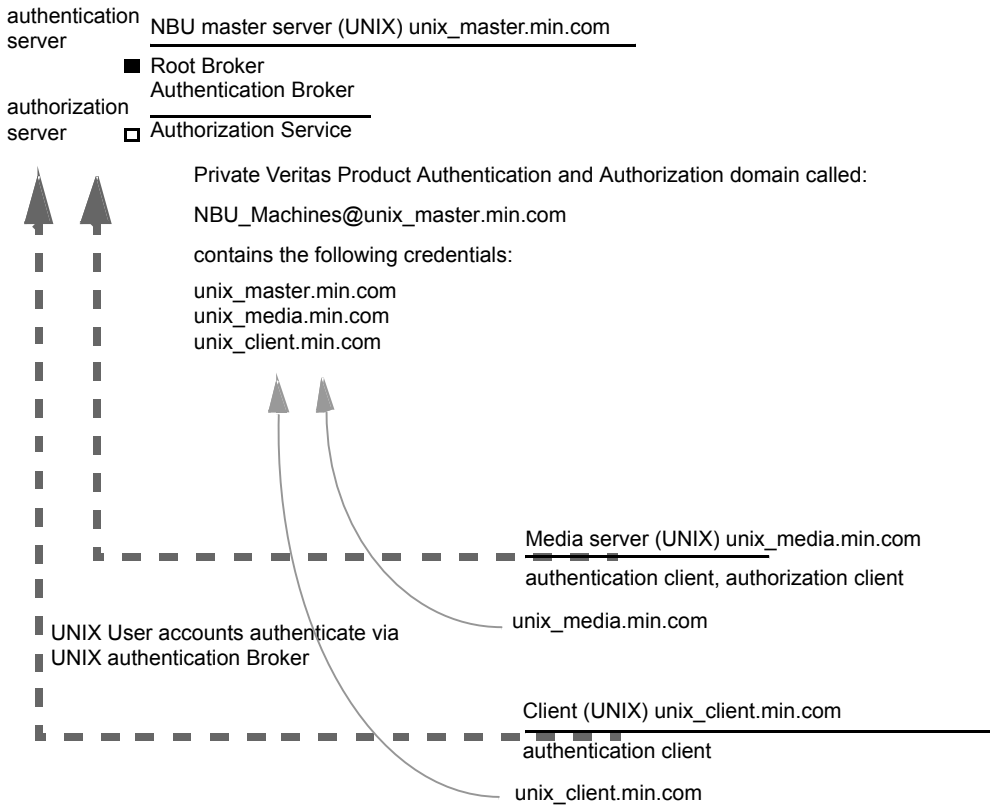
Note:
Each machine has a private domain account that are created for it. Using these accounts
allows NetBackup to more reliably identify machines as they communicate with each other.

UNIX master server verification

Use the following procedures to verify the UNIX master server:

- Verify UNIX master server settings.

- Verify which computers are permitted to perform authorization lookups.

- Verify that the database is configured correctly.

- Verify that the nbatd and nbazd processes are running.

- Verify that the host properties are configured correctly.

The following table describes the verification process for the UNIX master server.

Table 6-9   Verification process for the UNIX master server

Process	Description

Verify UNIX master server settings	Determine in what domain a host is registered (where the primary authentication broker resides), and determine the name of the computer the certificate represents. Run `bpnbat` with `-whoami` with `-cf` for the master server's credential file. The server credentials are located in the `/usr/openv/var/vxss/credentials/` directory.
	
	For example:
	
	<pre>bpnbat -whoami -cf
	/usr/openv/var/vxss/credentials/unix_master.company.com
	Name: unix_master.company.com
	Domain: NBU_Machines@unix_master.company.com
	Issued by: /CN=broker/OU=root@unix_master/O=vx
	Expiry Date: Oct 31 15:44:30 2007 GMT
	Authentication method: Veritas Private Security
	Operation completed successfully.</pre>
	If the domain listed is not NBU_Machines@unix_master.company.com, or the file does not exist, consider running `bpnbat -addmachine` for the name in question (unix_master). Run this command on the computer that serves the NBU_Machines domain (unix_master).
	
	Then, on the computer where we want to place the certificate (unix_master), run: `bpnbat -loginmachine`
	
	Note: When determining if a credential has expired, remember that the output displays the expiration time in GMT, not local time.
	
	Note: For the remaining procedures in this verification topic, assume that the commands are performed from a console window. The window in which the user identity is in question has run `bpnbat -login` using an identity that is a member of NBU_Security Admin. This identity is usually the first identity with which the security was set up.

Verify which computers are present in the authentication broker	To verify which computers are present in the authentication broker, log on as a member of the Administrators group and run the following command:
	
	`bpnbat -ShowMachines`
	
	The following command shows which computers you have run:
	
	`bpnbat -AddMachine`

| Table 6-9 | Verification process for the UNIX master server *(continued)* |

Process	Description

Verify which computers are permitted to perform authorization lookups	To verify which computers can perform authorization lookups, log on as root on the authorization broker and run the following command:
	
	`bpnbaz -ShowAuthorizers`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_master.company.com`
	
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_media.company.com`
	
	`Operation completed successfully.`
	
	This command shows that unix_master and unix_media are permitted to perform authorization lookups. Note that both servers are authenticated against the same vx (Veritas Private Domain) Domain, NBU_Machines@unix_master.company.com.
	
	If a master server or media server is not part of the list of authorized computers, run `bpnbaz -allowauthorization <server_name>` to add the missing computer.

Verify that the database is configured correctly	To make sure that the database is configured correctly, run `bpnbaz -listgroups`:
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	If the groups do not appear, or if `bpnbaz -listmainobjects` does not return data, run `bpnbaz -SetupSecurity`.

Table 6-9   Verification process for the UNIX master server *(continued)*

Process	Description
Verify that the nbatd and nbazd processes are running	Run the `ps` command to ensure that the `nbatd` and `nbazd` processes are running on the designated host. If necessary, start them. For example: ``` ps -fed |grep vx root 10716 1 0 Dec 14 ? 0:02 /usr/openv/netbackup/bin/private/nbatd root 10721 1 0 Dec 14 ? 4:17 /usr/openv/netbackup/bin/private/nbazd ```
Verify that the host properties are configured correctly	In the **Access Control** host properties, verify that the **NetBackup Authentication and Authorization** property is set correctly. (The setting should be either **Automatic** or **Required**, depending on whether all of the computers use **NetBackup Authentication and Authorization** or not. If all computers do not use **NetBackup Authentication and Authorization**, set it to **Automatic**. In the **Access Control** host properties, verify that the authentication domains on the list are spelled correctly. Also make sure that they point to the proper servers (valid authentication brokers). If all domains are UNIX-based, they should point to a UNIX machine that is running the authentication broker. This process can also be verified in `bp.conf` using `cat`. ``` cat bp.conf SERVER = unix_master SERVER = unix_media CLIENT_NAME = unix_master AUTHENTICATION_DOMAIN = company.com "default company NIS namespace" NIS unix_master 0 AUTHENTICATION_DOMAIN = unix_master "unix_master password file" PASSWD unix_master 0 AUTHORIZATION_SERVICE = unix_master.company.com 0 USE_VXSS = AUTOMATIC # ```

UNIX media server verification

Perform the following to verify the UNIX media server:

- Verify the media server.

- Verify that the server has access to the authorization database.

- Understand the unable to load library message.

The following table describes the verification procedures for the UNIX media server.

	Table 6-10	Verification process for the UNIX media server

Process	Description

Verify the media server	To determine which authentication broker the media server is authenticated against, run `bpnbat -whoami` with -cf for the media server's credential file. The server credentials are located in the `/usr/openv/var/vxss/credentials/` directory.
	
	For example:
	
	<pre>bpnbat -whoami -cf
	/usr/openv/var/vxss/credentials/unix_media.company.com
	Name: unix_media.company.com
	Domain: NBU_Machines@unix_master.company.com
	Issued by: /CN=broker/OU=root@unix_master.company.com/
	  O=vx
	Expiry Date: Oct 31 14:48:08 2007 GMT
	Authentication method: Veritas Private Security
	Operation completed successfully.</pre>
	If the domain listed is not NBU_Machines@unix_master.company.com, consider running `bpnbat -addmachine` for the name in question (unix_media). This command is run on the computer with the authentication broker that serves the NBU_Machines domain (unix_master).
	
	Then, on the computer where we want to place the certificate, run (unix_master): `bpnbat -loginmachine`

Verify that the server has access to the authorization database	To make sure that the media server is able to access the authorization database as it needs, run `bpnbaz -ListGroups`
	
	"machine_credential_file"
	
	For example:
	
	<pre>bpnbaz -ListGroups -CredFile
	/usr/openv/var/vxss/credentials/unix_media.company.com
	NBU_User
	NBU_Operator
	NBU_Admin
	NBU_Security Admin
	Vault_Operator
	Operation completed successfully.</pre>
	If this command fails, run `bpnbaz -AllowAuthorization` on the master server that is the authorization server (unix_master). Note that you need to run as root or administrator.

Process	Description
Unable to load library message	Verify the media server and that it has access to the proper database. This verification indirectly informs us that the NetBackup Authentication and Authorization client libraries for both authentication and authorization are properly installed. If either of these procedures fail with the message "unable to load libraries," check to make certain the Authentication and Authorization client libraries are installed. You may also verify that the authentication domains are correct. Do this verification viewing the access control host properties for this media server, or by `cat(1)ing` the `bp.conf` file.

UNIX client verification

The following procedures are used to verify the UNIX client:

- Verify the credential for the UNIX client.

- Verify that the authentication client libraries are installed.

- Verify correct authentication domains.

The following table describes the verification procedures for the UNIX client.

Table 6-11   Verification procedures for the UNIX client

Procedures	Description
Verify the credential for the UNIX client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run `bpnbat -whoami` with -cf for the client's credential file. For example: ``` bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_client.company.com Name: unix_client.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master.company.com/O=vx Expiry Date: Oct 31 14:49:00 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. ``` If the domain listed is not NBU_Machines@unix_master.company.com, consider running `bpnbat -addmachine` for the name in question (unix_client). This command is run on the computer with the authentication broker that serves the NBU_Machines domain (unix_master). Then, on the computer where we want to place the certificate (unix_client), run: `bpnbat -loginmachine`

Table 6-11   Verification procedures for the UNIX client *(continued)*

Procedures	Description
Verify that the authentication client libraries are installed	Run `bpnbat -login` on the client to verify that the authentication client libraries are installed. ```bpnbat -login Authentication Broker: unix_master.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd): NIS Domain: min.com Name: Smith Password: Operation completed successfully.```
Verify correct authentication domains	Check that any defined authentication domains for the client are correct in the **Access Control** host properties or by using `cat(1)`. Ensure that the domains are spelled correctly. Also ensure that the authentication brokers on the list for each of the domains are valid for that domain type. This process can also be verified in `bp.conf` using `cat(1)`. ```cat bp.conf SERVER = unix_master SERVER = unix_media CLIENT_NAME = unix_master AUTHENTICATION_DOMAIN = min.com "default company NIS namespace" NIS unix_master 0 AUTHENTICATION_DOMAIN = unix_master.company.com "unix_master password file" PASSWD unix_master 0 AUTHORIZATION_SERVICE = unix_master.company.com 0 USE_VXSS = AUTOMATIC```

Verification points in a mixed environment with a UNIX master server

The following procedures can help you verify that the master server, media server, and client are configured correctly. These should be configured for a heterogeneous NetBackup Access Control environment. The master server is a UNIX machine.

- Master server verification points for mixed UNIX master
- Media server verification points for mixed UNIX master
- Client verification points for mixed UNIX master

Figure 6-4 is an example of a mixed configuration that contains a UNIX master server.

Figure 6-4   Example mixed configuration containing a UNIX master server

NBU master server (UNIX) unix_master.min.com

authentication ■ Root Broker
server   Authentication Broker
authorization
server   □ Authorization Service

Private Veritas Product Authentication and Authorization domain
called NBU_Machines@unix_master.min.com
contains the following credentials: Host (Windows)
                                                             win_server.min.com
unix_master.min.com
win_media.min.com   authentication ■ Authentication Broker
win_client.min.com   server
unix_media.min.com   win_server.min.com
unix_client.min.com

                                                                    Windows hosts
                                                                    authenticate via
                                                                    Windows
                                                                    Authentication
                                                                    Broker

                              Media server (Windows) win_media.min.com

                              authentication client, authorization client
           See note.
                              win_media.min.com

                              Client (Windows) win_client.min.com

                              authentication client

                              win_client.min.com

                              Media server (UNIX) unix_media.min.com

                              authentication client, authorization client

                              unix_media.min.com

■ UNIX hosts authenticate via
■ UNIX authentication Broker
                              Client (UNIX) unix_client.min.com

                              authentication client

                              unix_client.min.com

Note:
Each machine has a private domain account. Using these accounts allows NetBackup to more reliably
identify machines as they communicate with each other.

Master server verification points for a mixed UNIX master server

See the following topic for the verification procedure for a UNIX master server:

See "UNIX master server verification" on page 153.

Media server verification points for a mixed UNIX master server

The following table describes the media server verification procedures for a mixed UNIX master server.

Table 6-12   Verification procedures for a mixed UNIX master server

Procedure	Description
Verify the UNIX media server	See the following topic for the verification procedure for a UNIX media server:
	See "UNIX media server verification" on page 156.
Verify the Windows media server	Check that the computer certificate comes from the root authentication broker, which is found on the UNIX master server (unix_master).
	If there is a missing certificate, run the following commands to correct the problem:
	■ `bpnbat -addmachine` on the root authentication broker (in this example, unix_master)
	■ `bpnbat -loginmachine` (in this example, win_media)
	For example:
	<pre>bpnbat -whoami -cf "C:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@ unix_master.company.com/O=vx Expiry Date: Oct 31 20:11:04 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>

Table 6-12   Verification procedures for a mixed UNIX master server
(continued)

Procedure	Description

Verify that a media server is permitted to perform authorization lookups	Ensure that the media server is allowed to perform authorization checks by running `bpnbaz -listgroups -CredFile`.
	
	For example:
	
	`bpnbaz -listgroups -CredFile "C:\Program`
	`Files\Veritas\Netbackup\var\vxss\credentials\`
	` win_media.company.com"`
	`NBU_User`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	If the media server is not allowed to perform authorization checks, run `bpnbaz -allowauthorization` on the master server for the media server name in question.

Unable to load library message	Verify the Windows media server and that it can perform authorization checks indirectly. This verification informs us that the **NetBackup Authentication and Authorization** client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries," make certain the authentication client libraries and authorization client libraries are installed.

Verify authentication domains	Verify that the authentication domains are correct by viewing the access control host properties for this media server.
	
	You can also use `regedit` (or `regedit32`) directly on the media server in the following location:
	
	`HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\`
	`CurrentVersion\config\AUTHENTICATION_DOMAIN`

Table 6-12   Verification procedures for a mixed UNIX master server
(continued)

Procedure	Description
Cross platform authentication domains	Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers.
	The example Authentication domain tab shows available authentication Windows domains that can be added to the Windows broker. In this case, it is not a mixed environment as both systems are Windows based. If there were a combination of Windows and UNIX domains it is important to match the brokers to the most useful authentication domains.
	Figure 6-5 for a display on how to match the platform to the most useful authentication domains.

Figure 6-5 Cross platform authentication domains
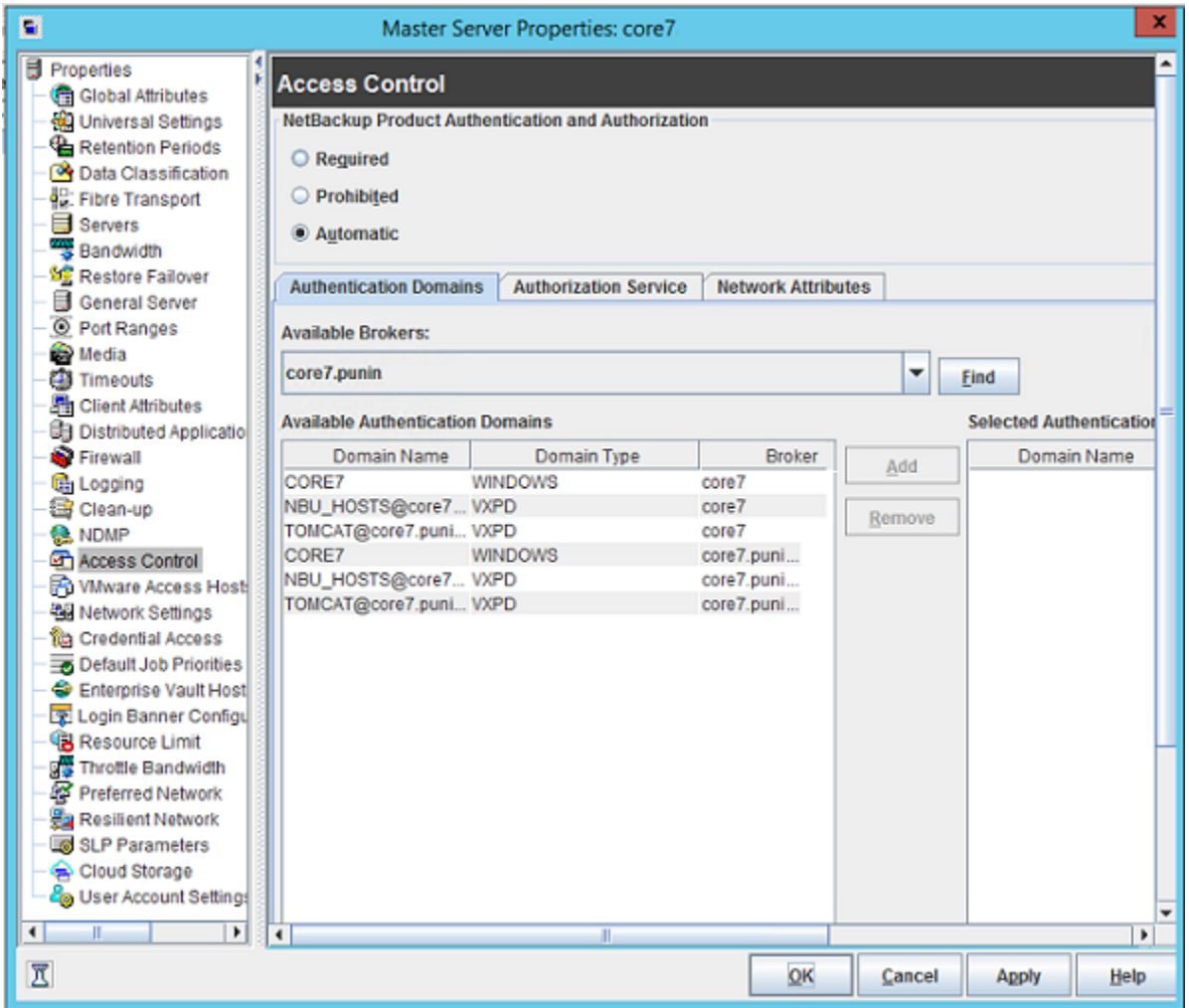
Client verification points for a mixed UNIX master server

See the following topic for procedures to verify the UNIX client computers:

See "UNIX client verification" on page 158.

The following table describes the procedures to verify Windows clients.

| Table 6-13 | Procedures to verify Windows clients |

Procedures	Description
Verify the credential for the Windows client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run `bpnbat -whoami` with -cf for the client's credential file.
	For example:
| | ```
bpnbat -whoami -cf "c:\Program
Files\Veritas\Netbackup\var\vxss\credentials\
 win_client.company.com
Name: win_client.company.com
Domain: NBU_Machines@unix_master.company.com
Issued by: /CN=broker/OU=root@unix_master.company.com/
 O=vx
Expiry Date: Oct 31 19:50:50 2007 GMT
Authentication method: Veritas Private Security
Operation completed successfully.
``` |
| Verify that the authentication client libraries are installed | Run `bpnbat -login` on the client to verify that the authentication client libraries are installed. |
| | For example: |
| | ```
bpnbat -login
Authentication Broker: unix_master.company.com
Authentication port [Enter = default]:
Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)
 : NIS
Domain: min.com
Name: Smith
Password:
Operation completed successfully.
``` |
| Verify the Windows authentication broker | Ensure that the Windows authentication broker has mutual trust with the main UNIX authentication broker. Also, make sure that the broker uses the UNIX broker as its root broker. |

Verification points in a mixed environment with a Windows master server

The following procedures can help you verify that the master server, media server, and client are configured correctly. They should be configured for a heterogeneous NetBackup Access Control environment. The master server is a Windows computer.

- Master server verification points for mixed Windows master
  See "Master server verification points for a mixed Windows master server" on page 168.

- Media server verification points for mixed Windows master
  See "Media server verification points for a mixed Windows master server" on page 168.

- Client verification points for mixed Windows master

See "Client verification points for a mixed Windows master server" on page 170.

Figure 6-6 is an example configuration that contains a Windows master server.

Figure 6-6   Example mixed configuration containing a Windows master server

authentication NBU master server (Windows) win_master.min.com
server
■ Root Broker
Authentication Broker

authorization
server □ Authorization Service

Private Veritas Product Authentication and Authorization
domain called NBU_Machines@win_server.min.com
contains the following credentials:

MediaServer (UNIX)
unix.media2min.com

win_master.min.com
unix_media2.min.com   authentication ■Authentication Broker
unix_media.min.com   server
unix_client.min.com   unix_media2min.com
win_media.min.com
win_client.min.com

UNIX user accounts
authenticate via UNIX
Authentication Broker

Media server (UNIX) unix_media.min.com

authentication client, authorization client

See note.   unix_media.min.com

Client (UNIX) unix_client.min.com

authentication client

unix_clientmin.com

Media server (Windows) win_media.min.com

authentication client, authorization client

win_media.min.com

Windows user accounts
authenticate via Windows
authentication broker

Client (Windows) win_client.min.com

authentication client

win_client.min.com

Note:
Each machine has a private domain account. Using these accounts allows NetBackup to more
reliably identify machines as they communicate with each other.

Master server verification points for a mixed Windows master server

See the following topic for the verification procedures for a mixed Windows master:

See "Master server verification points for Windows" on page 144.

Media server verification points for a mixed Windows master server

The following table describes the media server verification procedures for a mixed Windows master server.

Table 6-14   Media server verification procedures for a mixed Windows master server

Procedure	Description
Verify the Windows media server for a mixed Windows master server	See the following topic for the verification procedures for a Windows media server:
	See "Media server verification points for Windows" on page 148.
Verify the UNIX media server	Check that the computer certificate is issued from the root authentication broker, found on the Windows master server (win_master). To determine which authentication broker the media server is authenticated against, run `bpnbat -whoami` with -cf for the media server's credential file.
	For example:
	``` bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com Name: unix_media.company.comDomain: NBU_Machines@ win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 14:48:08 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. ```

	Table 6-14	Media server verification procedures for a mixed Windows master server *(continued)*

Procedure	Description
Verify that the server has access to the authorization database	To make sure that the media server is able to access the authorization database it needs to perform authorization checks. Run `bpnbaz -ListGroups -CredFile "/usr/openv/var/vxss/credentials/<hostname>"` For example: <pre>bpnbaz -ListGroups -CredFile\\ /usr/openv/var/vxss/credentials/unix_media.company.com NBU_Operator NBU_AdminNBU_SAN Admin NBU_UserNBU_Security Admin Vault_Operator Operation completed successfully.</pre> If the media server is not allowed to perform authorization checks, run `bpnbaz -allowauthorization` on the master server for the media server name in question.
Unable to load library message	Verify the media server and that it has access to the proper database indirectly. This verification informs us that the NetBackup Authentication and Authorization client libraries for both authentication and authorization are properly installed. If either of these procedures fail with a message "unable to load libraries": Check to make certain the authentication client libraries and authorization client libraries are installed.

Table 6-14   Media server verification procedures for a mixed Windows master
server *(continued)*

Procedure	Description
Cross platform authentication domains	You may also verify that the authentication domains are correct by viewing the access control host properties for this media server. Or, you may also verify by `cat(1)ing` the `bp.conf` file.
	Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers.
	In the example, note that the PASSWD domains and NIS domains point to unix_media2.company.com, which, in this example, is the UNIX authentication broker:
	``
	cat bp.conf
	SERVER = win_master.company.com
	MEDIA_SERVER = unix_media.company.com
	MEDIA_SERVER = unix_media2.company.com
	CLIENT_NAME = unix_media
	AUTHENTICATION_DOMAIN = win_master "win_master domain"
	WINDOWS win_master.company.com
	0
	AUTHENTICATION_DOMAIN = enterprise "enterprise domain"
	WINDOWS win_master.company.com 0
	AUTHENTICATION_DOMAIN = unix_media2.company.com "local
	unix_media2 domain" PASSWD unix_media2.company.com 0
	AUTHENTICATION_DOMAIN = min.com "NIS domain" NIS
	unix_media.company.com 0
	AUTHORIZATION_SERVICE = win_master.company.com 0
	USE_VXSS = AUTOMATIC
	``

Client verification points for a mixed Windows master server

The following table describes the client verification procedures for a mixed Windows master server.

Table 6-15   Verification procedures for a mixed Windows master server

Procedure	Description
Verify the credential for the Windows client	See the following topic for the verification procedures for Windows clients:

Table 6-15   Verification procedures for a mixed Windows master server
(continued)

Procedure	Description

Verify the credential for the UNIX client	Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run `bpnbat -whoami` with -cf for the client's credential file.
	
	For example:
	
	<pre>bpnbat -whoami -cf \
	 "/usr/openv/var/vxss/credentials/
	  unix_client.company.com"
	 Name: unix_client.company.com
	 Domain: NBU_Machines@win_master.company.com
	 Issued by: /CN=broker/OU=root@
	  win_master.company.com/O=vx
	 Expiry Date: Oct 31 21:16:01 2007 GMT
	 Authentication method: Veritas Private Security
	 Operation completed successfully.</pre>

Verify that the authentication client libraries are installed	Run `bpnbat -login` on the client to verify that the authentication client libraries are installed.
	
	<pre>bpnbat -login
	 Authentication Broker: unix_media2.company.com
	 Authentication port [Enter = default]:
	 Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)
	  : NIS
	 Domain: min.com
	 Name: Smith
	 Password:
	 You do not currently trust the server:
	  unix_media.company.com, do
	you wish to tr
	ust it? (y/n):
	y
	 Operation completed successfully.</pre>

Verify the UNIX authentication broker	Ensure that the UNIX authentication broker has mutual trust with the main windows authentication broker or ensure that it uses the Windows broker as its root broker.

About the nbac_cron utility

NetBackup operations can be performed as scheduled jobs by using the cron utility. When NBAC is enabled, these jobs can be run in the context of an OS user who has the privileges to run the required commands. You can use the nbac_cron.exe utility to create the credentials that are needed to run cron or AT jobs. These credentials are valid for a longer period of time as compared to the credentials that are obtained when a user performs a `bpnbat` logon. Here the validity is a year.

The utility is found in the following location:

```
-/opt/openv/netbackup/bin/goodies/nbac_cron
```

For detailed steps to configure the nbac_cron utility and run a cron job, see the following topic:

See "Using the nbac_cron utility" on page 172.

Using the nbac_cron utility

The following steps help you to create credentials to execute cron jobs.

Using the nbac_cron utility to run cron jobs

1 Run the command `nbac_cron-addCron` as root or administrator on the master server.

```
root@amp# /usr/openv/netbackup/bin/goodies/nbac_cron -AddCron

# nbac_cron -AddCron

This application will generate a Veritas private domain identity
that can be used in order to run unattended cron and/or at jobs.

User name to create account for (e.g. root, JSmith etc.): Dan

Password:*****

Password:*****

Access control group to add this account to [NBU_Admin]:

Do you with to register this account locally for root(Y/N) ? N

In order to use the account created please login as the OS
identity that will run the at or cron jobs. Then run nbac_cron
-setupcron or nbac_cron -setupat. When nbac_cron -setupcron or
nbac_cron -setupat is run the user name, password and
authentication broker will need to be supplied. Please make note
of the user name, password, and authentication broker. You may
```

```
rerun this command at a later date to change the password for an
account.
```

```
Operation completed successfully.
```

If you do not explicitly specify an access control group (for example, NBU_Operator or Vault_Operator) to add the user to, the cron user (Dan here), is added to the NBU_Admin group.

If you respond with a 'Yes' to register the account locally for root, the `nbac_cron -SetupCron` command is automatically executed for the cron_user as root. If you plan to run the cron jobs as a non-root OS user then you should say 'No' here and manually run the `nbac_cron -SetupCron` command as that non-root OS user.

An identity is generated in the Veritas private domain. This identity can be used to run the cron jobs.

2   Now, run the `nbac_cron-SetupCron` command as the OS user who wants to execute the cron jobs to obtain credentials for this identity.

```
[dan@amp ~]$ /usr/openv/netbackup/bin/goodies/nbac_cron -SetupCron

This application will now create your cron and/or at identity.

Authentication Broker: amp.sec.punin.sen.veritas.com

Name: Dan

Password:*****

You do not currently trust the server:
amp.sec.punin.sen.veritas.com, do you wish to trust it? (Y/N): Y

Created cron and/or at account information. To use this account
in your own cron or at jobs make sure that the environment
variable VXSS_CREDENTIAL_PATH is set to
"/home/dan/.vxss/credentials.crat"

Operation completed successfully.
```

The 'You do not currently trust' the server message is only shown once if you have not already trusted the broker.

The credential is created in the user's home directory at`user/.vxss/credentials.crat`. The credential is valid for a year from the time when it is generated.

If required, you can check the credential details as shown:

```
dan@amp~]$ /usr/openv/netbackup/bin/bpnbat -whoami -cf
~dan/.vxss/credentials.crat
```

```
Name: CronAt_dan

Domain: CronAtUsers@amp.sec.punin.sen.veritas.com

Issued by: /CN=broker/OU=amp.sec.punin.sen.veritas.com

Expiry Date: Feb 4 13:36:08 2016 GMT

Authentication method: Veritas Private Domain

Operation completed successfully.
```

You must re-run the `SetupCron` operation (Step 2) to renew the credential before it expires.

3   You can now create your own cron jobs. Ensure that the `VXSS_CREDENTIAL_PATH` path is set to point to the credentials you created above before you schedule any new job.

Using the Access Management utility

The users that are assigned to the **NetBackup Security Administrator** user group have access to the **Access Management** node in the NetBackup Administration Console. The users and the NetBackup Administrators who are assigned to any other user group can see the **Access Management** node. This node is visible in the **NetBackup Administration Console**, but you cannot expand it.

If a user other than a Security Administrator tries to select **Access Management**, an error message displays. The toolbar options and menu items that are specific to **Access Management** are not displayed.

Upon successful completion, the default NetBackup user groups should display in the **NetBackup Administration Console > Access Management > NBU user groups** window.

To list the groups on the command line, run the `bpnbaz -ListGroups` command on the computer where the authorization server software is installed.

UNIX

`bpnbaz` is located in directory `/usr/openv/netbackup/bin/admincmd`

Windows

`bpnbaz` is located in directory `Install_path\Veritas\NetBackup\bin\admincmd`

(You must be logged on as the Security Administrator by using `bpnbat -login`)

```
bpnbaz -ListGroups
 NBU_User
 NBU_Operator
```

```
NBU_Admin
NBU_Security Admin
Vault_Operator
NBU_SAN Admin
NBU_KMS Admin
Operation completed successfully.
```

The NetBackup user groups are listed. This process verifies that the Security Administrator can access the user groups.

About determining who can access NetBackup

The **Access Management** utility allows only one user group. By default, the NBU_Security Admin user group defines the following aspects of NetBackup Access Management:

- The permissions of individual users.
  See "Individual users" on page 176.

- The creation of user groups.
  See "User groups" on page 176.

First, determine which NetBackup resources your users need to access. For resources and associated permissions:

See "Viewing specific user permissions for NetBackup user groups" on page 182.

The Security Administrator may want to first consider what different users have in common, then create user groups with the permissions that these users require. User groups generally correspond to a role, such as administrators, operators, or end users.

Consider basing user groups on one or more of the following criteria:

- Functional units in your organization (UNIX administration, for example)

- NetBackup resources (drives, policies, for example)

- Location (East Coast or West coast, for example)

- Individual responsibilities (tape operator, for example)

Note that permissions are granted to individuals in user groups, not to individuals on a per-host basis. They can only operate to the extent that they are authorized to do so. No restrictions are based on computer names.

Individual users

The NetBackup **Access Management** utility uses your existing OS-defined users, groups, and domains. The **Access Management** utility maintains no list of users and passwords. When members of groups are defined, the Security Administrator specifies existing OS users as members of user groups.

Every authenticated user belongs to at least one authorization user group. By default, every user belongs to the user group NBU_Users, which contains all of the authenticated users.

All authenticated users are implicit members of the NBU_Users user group. All other groups must have members defined explicitly. The NetBackup Security Administrator can delete a manually added member to other groups. However, the Security Administrator may not delete the predefined implicit members of the NBU_Security Admin groups. The OS groups and OS users can be added to an authorization group.

User groups

NetBackup **Access Management** can be configured by assigning permissions to user groups and then assigning users to the user groups. Assigning permissions to groups is done rather than assigning permissions directly to individual users.

Upon successful installation, NetBackup provides default user groups that complement how sites often manage the duties of NetBackup operation. The user groups are listed under `Access Management > NBU User Groups`. The contents of **Access Management** are only visible to members of the NBU_Security Admin group.

The Security Administrator can use the default NetBackup user groups or create custom user groups.

NetBackup default user groups

The users that are granted permissions in each of the default user groups relate directly to the group name. Essentially, an authorization object correlates to a node in the **NetBackup Administration Console** tree.

The following table describes each NetBackup default user group.

	Table 6-16	NetBackup default user groups

Default user group	Description
Operator (NBU_Operator)	The main task of the NBU_Operator user group is to monitor jobs. For example, members of the NBU_Operator user group might monitor jobs and notify a NetBackup administrator if there is a problem. Then, the administrator can address the problem. Using the default permissions, a member of the NBU_Operator user group would probably not have enough access to address larger problems.
	Members of the NBU_Operator user group have the permissions that allow them to perform tasks such as moving tapes, operating drives, and inventorying robots.
Administrator (NBU_Admin)	Members of the NBU_Admin user group have full permission to access, configure, and operate any NetBackup authorization object. Some exceptions exist for SAN Administrators. In other words, members have all of the capabilities that are currently available to administrators without Access Management in place. However, as members of this group, you do not necessary log on as root or administrator in the OS.
	Note: Members of the NBU_Admin user group cannot see the contents of Access Management, and therefore, cannot ascribe permissions to other user groups.
SAN Administrator (NBU_SAN Admin)	By default, members of the NBU_SAN Admin user group have full permissions to browse, read, operate, and configure disk pools and host properties. These permissions let you configure the SAN environment and NetBackup's interaction with it.
User (NBU_User)	The NBU_User user group is the default NetBackup user group with the fewest permissions. Members of the NBU_User user group can only back up, restore, and archive files on their local host. NBU_User user group members have access to the functionality of the NetBackup client interface (BAR).
Security administrator (NBU_Security Admin)	Usually very few members exist in the NBU_Security Admin user group.
	The only permission that the Security Administrator has, by default, is to configure access control within **Access Management**. Configuring access control includes the following abilities:
	■ To see the contents of **Access Management** in the **NetBackup Administration Console** ■ To create, modify, and delete users and user groups ■ To assign users to user groups ■ To assign permissions to user groups

Table 6-16	NetBackup default user groups *(continued)*

Default user group	Description
Vault operator (Vault_Operator)	The Vault_Operator user group is the default user group that contains permissions to perform the operator actions necessary for the Vault process.
KMS Administrator (NBU_KMS Admin)	By default, members of the NBU_KMS Admin user group have full permissions to browse, read, operate and configure encryption key management properties. These permissions make sure that you can configure the KMS environment and NetBackup's interaction with it.
Additional user groups	The Security Administrator (member of NBU_Security Admin or equivalent) can create user groups as needed. The default user groups can be selected, changed, and saved. Veritas recommends that the groups be copied, renamed, and then saved to retain the default settings for future reference.

Configuring user groups

The Security Administrator can create new user groups. Expand **Access Management > Actions > New Group** or select an existing user group and expand **Access Management > Actions > Copy to New Group**.

Creating a new user group

You can use the following procedure to create a new user group.

To create a new user group

1   As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.

2   Select **Actions > New User Group**. The Add New user group dialog displays, opened to the **General** tab.

3   Type the name of the new group in the **Name** field, then click the **Users** tab.

4   Select the defined users that you want to assign to this new user group. Then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.

5   Click the **Permissions** tab.

6   Select a resource from the Resources list and an Authorization Object. Then select the permissions for the object.

7   Click **OK** to save the user group and the group permissions.

Creating a new user group by copying an existing user group

You can use the following procedure to create a new user group by copying an existing user group.

To create a new user group by copying an existing user group

1 As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.

2 Select an existing user group in the **Details** pane. (The pane on the left side of the **NetBackup Administration Console**.)

3 Select **Actions > Copy to New User Group**. A dialog that is based on the selected user group displays, opened to the **General** tab.

4 Type the name of the new group in the **Name** field, then click the **Users** tab.

5 Select the defined users that you want to assign to this new user group. Then click **Assign**. Or, to include all the defined users in the group, click **Assign All**. To remove users from the assigned users list, select the user name, then click **Remove**.

6 Click the **Permissions** tab.

7 Select a resource from the Resources list and Authorization Object, then select the permissions for the object.

8 Click **OK** to save the user group and the group permissions. The new name for the user group appears in the **Details** pane.

Renaming a user group

Once a NetBackup user group has been created, the user group cannot be renamed. The alternative to directly renaming a user group is to follow these steps: copy the user group, give the copy a new name, ensure the same membership as the original, then delete the original NetBackup user group.

Adding a new user to the user group

Click **New User** to add a user to the **Defined Users** list. After you add a user, the name appears in the **Defined Users** list and the Security Administrator can assign the user to the user group.

See "Assigning a user to a user group" on page 181.

About defining a user group and users

NetBackup authenticates existing users of the operating system instead of requiring that NetBackup users be created with a NetBackup password and profile.

Users can belong to more than one user group and have the combined access of both groups.

Figure 6-7 shows defining a user group.

Figure 6-7   Defining a user group

Users can be members of multiple user groups simultaneously, but NetBackup does not allow user groups to be nested. For example, members of a user group can belong to more than one user group, but a user group cannot belong to another user group.

The following figure shows that nested user groups are not allowed.

Figure 6-8   Nested user groups are not allowed

Logging on as a new user

You can use the following procedure to log on as a new user.

To log on as a new user

◆ Expand **File > Login as New User** (Windows). This option is only available on computers that are configured for access control. It is useful to employ the concept of operating with least privileges and an individual needs to switch to using an account with greater privilege.

Assigning a user to a user group

You can use the following procedure to assign a user to a user group. A user is assigned from a pre-existing name space (NIS, Windows, etc.) to an NBU user group. No new user accounts are created in this procedure.

To add a user to a user group

1   As a member of the NBU_Security Admin user group (or equivalent), expand **Access Management > NBU User Groups**.

2   Double-click on the user group to which you want to add a user.

3   Select the **Users** tab and click **Add User**.

4   Enter the user name and the authentication domain. Select the domain type of the user: NIS, NIS+, PASSWD, Windows, or Vx.

5   Select the **Domain Type** of the user:

   ■ NIS
      Network Information Services

   ■ NIS+
      Network Information Services Plus

   ■ PASSWD
      UNIX password file on the authentication server

   ■ Windows
      Primary domain controller or Active Directory

   ■ Vx
      Veritas private database

6   For the **User Type**, select whether the user is an individual user or an OS domain.

7   Click **OK**. The name is added to the **Assigned Users** list.

About authorization objects and permissions

In general, an authorization object correlates to a node in the **NetBackup Administration Console** tree.

The **Authorization Objects** pane contains the NetBackup objects to which permissions can be granted.

The **Permissions for "DevHost"** pane indicates the permission sets for which the selected user group is configured.

An authorization object may be granted one of these permission sets:

- **Browse/Read**

- **Operate**

- **Configure**

A lowercase letter in the **Permissions for "DevHost"** column indicates some (but not all) of the permissions in a permission set. Permissions have been granted for the object.

Viewing specific user permissions for NetBackup user groups

The permissions that are granted to each of the NBU user groups correlate to the name of the authorization object. The NBU default user groups include the NBU_Operator, NBU_Admin, NBU_SAN Admin, NBU_User, NBU_Security Admin, and Vault_Operator.

Due to the complexities of interdependencies between resources, in some places it is not possible to map access to a resource or to a single permission. There might be multiple underlying permissions across resources that need to be evaluated to make an access check decision. This mix of permissions can cause some discrepancies between resource permissions and resource access. This possible discrepancy is mostly limited to read access. For example, a Security_Admin might not have permissions to list or browse policies. The administrator needs access to policies as they contain client information that is required to configure security for clients.

Note: There can be a permissions anomaly. The NBU_User, NBU_KMS_Admin, NBU_SAN Admin, and Vault_Operator users are not able to access host properties from the Java GUI. To fetch data for host properties reference is made to the policy object as well. This anomaly means that to access the host properties the user requires Read/Browse access on the policy object. Manually giving read access to the policy object resolves the issue.

> **Note:** More information on this subject can be found by referring to the Veritas technical support site.

To View specific user permissions

1 In the **NetBackup Administration Console**, expand **Access Management > NBU User Groups**.

2 Double click on the appropriate NBU_Operator, NBU_Admin, NBU_SAN Admin, NBU_User, NBU_Security Admin, or Vault_Operator in the **Security** window.

3 In the **NBU_Operator** window, select the **Permissions** tab.

4 In the **Authorization Objects** pane, select the desired authorization object. The **Permissions** pane displays the permissions for that authorization object.

Granting permissions

You can use the following procedure to grant a permission to the members of a user group.

To grant a permission to the members of a user group

1 Select an authorization object.

2 Then place a check in front of a permission that you want to grant the members of the user group currently selected.

When a user group is copied to create a new user group, the permission settings are also copied.

Authorization objects

The following tables show the authorization objects in the order that they appear in the **NetBackup Administration Console**, **NBU_Operator** window.

The tables also show the relationships between the authorization objects and default permissions for each of the NBU user groups as follows:

- The "X" indicates that the specified user group has permission to perform the activity.

- The "---" indicates that the specified user group does not have permission to perform the activity.

Media authorization object permissions

The following table shows the permissions that are associated with the Media authorization object.

Table 6-17 Media authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Update barcodes	X	X	---	---	---	X	---
	Eject	X	X	---	---	---	X	---
	Move	X	X	---	---	---	X	---
	Assign	X	X	---	---	---	X	---
	Deassign	X	X	---	---	---	X	---
	Update Database	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	X	---
	Delete	---	X	---	---	---	X	---
	Expire	---	X	---	---	---	X	---

Policy authorization object permissions

The following table shows the permissions that are associated with the Policy authorization object.

Table 6-18 Policy authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	---	---
Read	Read	X	X	---	---	---	---	---
Operate	Back up	X	X	---	---	---	---	---
Configure	Activate	---	X	---	---	---	---	---
	Deactivate	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

Drive authorization object permissions

The following table shows the permissions that are associated with the Drive authorization object.

Table 6-19   Drive authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Up	X	X	---	---	---	---	---
	Down	X	X	---	---	---	---	---
	Reset	X	X	---	---	---	---	---
	Assign	X	---	---	---	---	---	---
	Deassign	X	---	---	---	---	---	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

Report authorization object permissions

The following table shows the permissions that are associated with the Report authorization object. Reports include only the Access permission set, and do not include a Configure or Operate permission set.

Table 6-20   Report authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---

NBU_Catalog authorization object permissions

The following table shows the permissions that are associated with the NetBackup catalog authorization object.

Table 6-21   NBU_Catalog authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---
Operate	Back up	---	X	---	---	---	---	---
	Restore	---	X	---	---	---	---	---
	Verify	---	X	---	---	---	---	---
	Duplicate	---	X	---	---	---	---	---
	Import	---	X	---	---	---	---	---
	Expire	---	X	---	---	---	---	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---
	Read Configuration	---	X	---	---	---	---	---
	Set Configuration	---	X	---	---	---	---	---

Robot authorization object permissions

The following table shows the permissions that are associated with the robot authorization object.

Table 6-22   Robot authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Inventory	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	X	---
	Delete	---	X	---	---	---	X	--

Storage unit authorization object permissions

The following table shows the permissions that are associated with the storage unit authorization object.

Table 6-23　　　　Storage unit authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	---	---
Read	Read	X	X	---	---	---	---	---
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

DiskPool authorization object permissions

The following table shows the permissions that are associated with the disk pool authorization object.

Table 6-24　　　　DiskPool authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	---
Operate	New	---	X	X	---	---	---	---
	Delete	---	X	X	---	---	---	---
	Modify	---	X	X	---	---	---	---
	Mount	---	X	X	---	---	---	---
	Unmount	---	X	X	---	---	---	---
Configure	Read Configuration	---	X	X	---	---	---	---
	Set Configuration	---	---	X	---	---	---	---

BUAndRest authorization object permissions

The following table shows the permissions that are associated with the backup and restore authorization object.

Table 6-25   BUAndRest authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	---	---	X
Read	Read	X	X	X	X	---	---	X
Operate	Back up	X	X	X	X	---	---	X
	Restore	X	X	X	X	---	---	X
	Alternate Client	X	X	---	---	---	---	---
	Alternate Server	X	X	---	---	---	---	---
	Admin Access	X	X	---	---	---	---	---
		---	---	---	---	---	---	---
	Database Agent	---	---	X	X	---	---	X
	List							

Job authorization object permissions

The following table shows the permissions that are associated with the Job authorization object.

Table 6-26   Job authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---

Table 6-26   Job authorization object permissions *(continued)*

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Operate	Suspend	X	X	---	---	---	X	---
	Resume	X	X	---	---	---	X	---
	Cancel	X	X	---	---	---	X	---
	Delete	X	X	---	---	---	X	---
	Restart	X	X	---	---	---	X	---
	New	X	X	---	---	---	X	---

Service authorization object permissions

The following table shows the permissions that are associated with the Service authorization object.

Table 6-27   Service authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Operate	Stop	X	X	---	---	---	---	---

The Read and Browse permissions do not have an effect on the Daemons tab. This information is harvested from the server using user level calls. The calls are used to access the process task list and is displayed to all users for informational purposes.

If a user is not a member of the NBU_Admin user group, but is logged on as an OS administrator (Administrator or root), then:

- The user is able to restart a service from within the **NetBackup Administration Console** or from the command line.

- The user is able to stop a service from within the **NetBackup Administration Console** but not from the command line.

If a user is not a member of the NBU_Admin user group, but is logged on as an OS administrator (`root`). That user is able to restart a daemon from the command line only:

```
/etc/init.d/netbackup start
```

If a user is a member of the NBU_Admin user group, but is not logged on as an OS administrator (Administrator), then:

- The user is not able to restart a service from within the **NetBackup Administration Console** or from the command line.

- The user is not able to stop a service from within the **NetBackup Administration Console** but the user can use the command line.
  (For example, `bprdreq -terminate`, `bpdbm -terminate`, or `stopltid`.)

If a user is a member of the NBU_Admin user group, but is not logged on as an OS administrator (`root`). That user is not able to restart a daemon from the **NetBackup Administration Console** or from the command line.

HostProperties authorization object permissions

The following table shows the permissions that are associated with the host properties authorization object.

Table 6-28   HostProperties authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	X	X	X
Read	Read	X	X	X	X	X	X	X
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	--

License authorization object permissions

The following table shows the permissions that are associated with the License authorization object.

Table 6-29   License authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	X	X	X
Read	Read	X	X	X	X	X	X	X
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

Volume group authorization object permissions

The following table shows the permissions that are associated with the volume group authorization object.

Table 6-30   Volume group authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

VolumePool authorization object permissions

The following table shows the permissions that are associated with the volume pool authorization object.

Table 6-31   VolumePool authorization object permissions

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---

		Table 6-31		VolumePool authorization object permissions *(continued)*				

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	Assign	---	X	---	---	---	---	---
	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

DevHost authorization object permissions

The following table shows the permissions that are associated with the device host authorization object.

Note: The DevHost object controls access to the **Media and Device Management > Credentials** node.

		Table 6-32		DevHost authorization object permissions				

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	X	---	---	X	---
Read	Read	X	X	X	---	---	X	---
Operate	Stop	X	X	---	---	---	---	---
	Synchronize	X	X	---	---	---	---	---
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---

Security authorization object permissions

The following table shows the permissions that are associated with the security authorization object.

	Table 6-33			Security authorization object permissions				
Set	**Activity**	**NBU_ Operator**	**NBU_ Admin**	**NBU_ SAN Admin**	**NBU_ User**	**NBU_ Security Admin**	**Vault_ Operator**	**NBU_KMS Admin**
Browse	Browse	---	---	---	---	X	---	---
Read	Read	---	---	---	---	X	---	---
Configure	Security	---	---	---	---	X	---	---

Fat server authorization object permissions

The following table shows the permissions that are associated with the Fat server authorization object.

	Table 6-34			Fat server authorization object permissions				
Set	**Activity**	**NBU_ Operator**	**NBU_ Admin**	**NBU_ SAN Admin**	**NBU_ User**	**NBU_ Security Admin**	**Vault_ Operator**	**NBU_KMS Admin**
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	---
Configure	Modify	---	X	X	---	---	---	---
	Modify SAN Configuration	---	---	X	---	---	---	---

Fat client authorization object permissions

The following table shows the permissions that are associated with the Fat client authorization object.

	Table 6-35			Fat client authorization object permissions				
Set	**Activity**	**NBU_ Operator**	**NBU_ Admin**	**NBU_ SAN Admin**	**NBU_ User**	**NBU_ Security Admin**	**Vault_ Operator**	**NBU_KMS Admin**
Browse	Browse	X	X	X	---	---	---	---
Read	Read	X	X	X	---	---	---	--
Operate	Discover	---	X	X	---	---	---	---

	Table 6-35		Fat client authorization object permissions *(continued)*					
Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	Modify	---	X	X	---	---	---	---

Vault authorization object permissions

The following table shows the permissions that are associated with the vault authorization object.

	Table 6-36		Vault authorization object permissions					
Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	X	---
Read	Read	---	X	---	---	---	X	---
Operate	Manage Containers	---	X	---	---	---	X	---
	Run Reports	---	X	---	---	---	X	---
Configure	Modify	---	X	---	---	---	---	---
	Run Sessions	---	X	---	---	---	---	---

Server group authorization object permissions

The following table shows the permissions that are associated with the server group authorization object.

	Table 6-37		Server group authorization object permissions					
Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	X	X	---	---	---	X	---
Read	Read	X	X	---	---	---	X	---

	Table 6-37			Server group authorization object permissions *(continued)*				

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Configure	New	---	X	---	---	---	---	---
	Delete	---	X	---	---	---	---	---
	Modify	---	X	---	---	---	---	---

Key management system (kms) group authorization object permissions

The following table shows the permissions that are associated with the Key management system group authorization object.

	Table 6-38			Key management system group authorization object permissions				

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_ SAN Admin	NBU_ User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
Browse	Browse	---	X	---	---	---	---	X
Read	Read	---	X	---	---	---	---	X
Configure	New	---	---	---	---	---	---	X
	Delete	---	---	---	---	---	---	X
	Modify	---	---	---	---	---	---	X

Upgrading NetBackup Access Control (NBAC)

Note: If NBAC is enabled, it is upgraded as part of the NetBackup upgrade. Refer to the NetBackup Upgrade Guide for instructions about how to upgrade NetBackup. Make sure that current AT and AZ services are running when the upgrade is performed. If NetBackup is running in a cluster server, make sure that both services are running in the active node where NetBackup is running and the upgrade is performed.

The following procedure describes how to upgrade NetBackup Access Control (NBAC).

Upgrading NetBackup Access Control (NBAC)

1   On the master server, stop NetBackup.

2   Upgrade NetBackup.

On the media servers and client computers, first stop NetBackup and then upgrade NetBackup. Note that the shared authentication and authorization packages are no longer used on media servers and client computers. These products can be removed if no other Veritas product uses them.

About AD and LDAP domains

This chapter includes the following topics:

- Adding AD or LDAP domains in NetBackup

- Troubleshooting AD or LDAP domain configuration issues

- Certificate authorities trusted by the NetBackup Authentication Service

Adding AD or LDAP domains in NetBackup

NetBackup supports Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain users.

If an AD domain or an LDAP domain is added in NetBackup, the respective domain users can logon to a NetBackup master server and Security Administrator can assign role-based access control (RBAC) roles to these domain users.

For more information on RBAC, see the *NetBackup Web UI Security Administrator's Guide*.

http://www.veritas.com/docs/DOC5332

The following procedure describes how to add an existing AD or LDAP domain in NetBackup and authenticate the domain users to access NetBackup.

To add an AD domain or an LDAP domain in NetBackup

1 Run the following command to add an AD domain or an LDAP domain in the NetBackup master server:

```
vssat addldapdomain -d DomainName -s server_URL
-u user_base_DN -g group_base_DN [-f trusted_CA_file_name] [-t rfc2307 | msad |
{-c user_object_class -a user_attribute -q user_GID_attribute
-un user_display_name_attribute -ui user_ID_attribute[:value_type]
-ud user_description_attribute -x group_object_class -y group_attribute
-z group_GID_attribute -gn group_display_name_attribute
-gi group_ID_attribute[:value_type] -gd group_description_attribute
[-k DN | UID]]} [-b FLAT | BOB] -m admin_user_DN [-w admin_user_password]
[-p SUB | ONE | BASE]
```

> **Note:** Ensure that the user that is specified in the -m option has the required rights to query the AD or LDAP server.
>
> Use the -f to add the CA certificate in the Authentication Service (nbatd) trust store.
>
> In case of LDAPS, if the Authentication Service (nbatd) does not trust the certificate authority (CA) that has signed the server's certificate, use the -f option to add the CA certificate in the nbatd trust store.
>
> See "Certificate authorities trusted by the NetBackup Authentication Service" on page 204.

For more information on the vssat command, see the *NetBackup Commands Reference Guide*.

http://www.veritas.com/docs/DOC5332

An example to add an LDAP domain:

```
vssat addldapdomain -d nbudomain -s ldap://example.com -u "OU=Users,DC=example,DC=com"
-g "OU=Groups,DC=example,DC=com" -m "CN=TestUser,OU=Users,DC=example,DC=com" -t msad
```

2 Run the `vssat validateprpl` command to verify whether the specified AD or LDAP domain is successfully added or not.

For more information on the command, see the *NetBackup Commands Reference Guide*.

http://www.veritas.com/docs/DOC5332

If the AD or LDAP domain is added and the `vssat validateprpl` or `vssat validategroup` command fails, you need to carry out certain troubleshooting steps to resolve the issue.

See "Troubleshooting AD or LDAP domain configuration issues " on page 199.

Troubleshooting AD or LDAP domain configuration issues

After you added an AD or LDAP domain configuration, verify the configuration using the `vssat validateprpl` and `vssat validategroup` commands. The commands validate the existing AD / LDAP user and group respectively.

A successful execution of the `vssat validateprpl` and the `vssat validategroup` commands implies that the associated AD or LDAP domain is successfully added.

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

If the commands fail, the following error message is displayed:

```
The principal or group does not exist.
```

Validation of AD or LDAP domain can fail because of any of the following reasons:

- Connection cannot be established with the AD or LDAP server

- Invalid user credentials

- Invalid user base DN or group base DN

- Multiple users or groups exist with the same name under the user base DN or the group base DN

- User or group does not exist

Connection cannot be established with the AD or LDAP server

To troubleshoot the issue

1 Check if the `nbatd` logs contain the following error:

```
(authldap.cpp) CAuthLDAP::validatePrpl - ldap_simple_bind_s()
failed for user 'CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com', error
= -1, errmsg = Can't contact LDAP server,9:debugmsgs,1
```

2 Check if any of the following scenarios is true and carry out the steps provided for that scenario.

The LDAP server URL (-s option) that is provided with the vssat addldapdomain may be wrong

Run the following command to validate:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Example:

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

The server certificate issuer is not a trusted CA

This is applicable if the ldaps option is used and can be validated using the ldapsearch command:

```
set env var LDAPTLS_CACERT to cacert.pem
```

```
ldapsearch -H <LDAPS_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

File path for cacert.pem:

On Windows:

<Install_path>\NetBackup\var\global\vxss\eab\data\systemprofile\certstore\trusted\pluggins\ldap\cacert.pem

On Unix:

/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/certstore/trusted/pluggins/ldap/cacert.pem

Example:

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized.. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

The NetBackup Authentication Service (`nbatd`) does not trust the certificate authority that has signed the LDAP server's security certificate

See "Certificate authorities trusted by the NetBackup Authentication Service" on page 204.

Use the `-f` option of the `vssat addldapdomain` command to add the CA certificate in the Authentication Service (`nbatd`) trust store.

Invalid user credentials

To troubleshoot the issue

1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - ldap_simple_bind_s() failed for user
'CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com', error = 49, errmsg =
Invalid credentials,9:debugmsgs,1
```

2 Check if the following scenario is true and carry out the steps provided for the scenario.

Invalid admin user DN or password provided while adding an LDAP domain using the `vssat addldapdomain` command

Run the following command to validate:

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Example:

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o
nettimeout=60 ldap_bind: Invalid credentials (49)
```

Invalid user base DN or group base DN

To troubleshoot the issue

1   Check if the `nbatd` logs contain the following error:

    ```
    CAuthLDAP::validatePrpl - ldap_search_s() error = 10, errmsg =
    Referral,9:debugmsgs,1 CAuthLDAP::validatePrpl - ldap_search_s()
    error = 34, errmsg = Invalid DN syntax,9:debugmsgs,1
    ```

2   You may see the errors in the logs if user base DN (the `-u` option) or group
    base DN (the `-g` option) values are incorrect.

    Run the following command to validate:

    Example:

    ```
    ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
    User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b
    "OU=VRTSUsers,DC=VRTS,DC=con" "(&(cn=test
    user)(objectClass=user))"
    ```

    ```
    ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
    User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b "VRTS" "(&(cn=test
    user)(objectClass=user))"
    ```

Multiple users or groups exist with the same name under user base DN or group base DN

To troubleshoot the issue

1   Check if the `nbatd` logs contain the following error:

    ```
    CAuthLDAP::validateGroup - search returned '2' entries for group
    name 'team_noone', even with referrals set to OFF,9:debugmsgs,1
    ```

2   This is applicable if user search attribute (`-a` option) and group search attribute
    (`-y` option) do not have unique values for the existing user base DN and group
    base DN respectively.

    Validate the number of matching entries for the existing base DN using the
    `ldapsearch` command.

    ```
    ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
    <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
    ```

    Example:

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b "DC=VRTS,DC=com"
"(&(cn=test user)(objectClass=user))" # LDAPv3 # base <DC=VRTS,DC=com>
```

```
with scope subtree # filter: (cn=Test User) # requesting: ALL # Test
User, VRTSUsers, VRTS.com dn: CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com
# Test User, RsvUsers, VRTS.com dn: CN=Test
User,OU=RsvUsers,DC=VRTS,DC=com # numEntries: 2
```

User or group does not exist

To troubleshoot the issue

1 Check if the `nbatd` logs contain the following error:

```
CAuthLDAP::validatePrpl - user 'test user' NOT found,9:debugmsgs,4
CAuthLDAP::validateGroup - group 'test group' NOT
found,9:debugmsgs,4
```

2 If a user or group exists in the LDAP domain, but the `vssat validateprpl` or the `vssat validategroup` command fails with this error, validate if the user or the group exists in the current base DNs (-u and -g options) using the following command.

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
```

Certificate authorities trusted by the NetBackup Authentication Service

The NetBackup Authentication Service (`nbatd`) trusts the following certificate authorities:

- CyberTrust
- DigiCert GeoTrust
- Certification Services Division
- VeriSign Trust Network
- RSA Security Inc.
- GlobalSign
- Symantec Corporation

Security management using NetBackup CA and NetBackup certificates

This chapter includes the following topics:

- Overview of security certificates in NetBackup

- About secure communication in NetBackup

- About the Security Management utilities

- About audit events

- About host management

- About global security settings

- About host name-based certificates

- About host ID-based certificates

- About Token Management for host ID-based certificates

- About the host ID-based certificate revocation list

- About revoking host ID-based certificates

- Deleting host ID-based certificates

- Host ID-based certificate deployment in a clustered setup

- About the communication between a NetBackup client located in a demilitarized zone and a master server through an HTTP tunnel

■   Adding a NetBackup host manually

Overview of security certificates in NetBackup

NetBackup uses security certificates to authenticate NetBackup hosts. The security certificates conform to the X.509 Public Key Infrastructure (PKI) standard. A master server acts as the Certificate Authority (CA) and issues digital certificates to hosts.

Any security certificates that were generated before NetBackup 8.0 are referred to as host name-based certificates. NetBackup is in the process of replacing these older certificates with newer host ID-based certificates. The transition will be completed in future releases and the use of host name-based certificates will be eliminated.

However, the transition is on-going and NetBackup continues to require the older host name-based certificates for some operations. The following table lists various operations where host name-based certificate is required.

Note: All NetBackup 8.1 hosts must have a host ID-based certificate.

Table 8-1   Host name-based certificate requirements for NetBackup 8.1 hosts

Operation or component	Type of certificate required
NetBackup Access Control (NBAC)	If NBAC is enabled on a NetBackup host, the host requires a host name-based certificate. These are automatically deployed when NBAC is enabled.
Enhanced Auditing operations	Enhanced Auditing operations require that the hosts have host name-based certificates. See "Deploying host name-based certificates" on page 237.
Cloud storage	This is applicable to NetBackup media server versions 8.0 to 8.1.2 only. The NetBackup CloudStore Service Container requires that the host name-based certificate be installed on the media server. If the certificate is not installed, the Service Container cannot start. See "Deploying host name-based certificates" on page 237. For more information, see the NetBackup Cloud Administrator's Guide.

About secure communication in NetBackup

NetBackup 8.1 and later hosts can communicate with each other only in a secure mode. NetBackup 8.1 hosts must have a Certificate Authority (CA) certificate and a host ID-based certificate for successful communication.

NetBackup uses Transport Layer Security (TLS) protocol for host communication where each host needs to present its security certificate and validate the peer host's certificate against the Certificate Authority (CA) certificate.

Two nodes on the **NetBackup Administration Console** provide secure communication settings: **Host Management** and **Global Security Settings**.

See "About host management" on page 213.

See "Adding host ID to host name mappings" on page 214.

See "About global security settings" on page 228.

See "About secure communication settings" on page 228.

See "About disaster recovery settings" on page 233.

Two commands, nbhostmgmt and nbhostidentity, along with enhancements to nbcertcmd and nbseccmd, provide options to manage certificate deployment and other security settings.

About the Security Management utilities

The **NetBackup Administration Console > Security Management** node is visible only to administrators on the NetBackup master server.

Security Management contains the utilities to view login activity, manage host ID-based certificates, and configure secure communications in the domain.

- Use **Security Events** to view the login details about the current administrator and the user-initiated changes that are made to certificates, tokens, hosts, and security configurations. You can also view details about host connections.

- Use the **Host Management** node to carry out NetBackup host operations, such as adding or approving host ID to host name mappings, resetting host, or adding comments for a host.
  See "Hosts tab" on page 213.

- Use the **Certificate Management** node to carry out operations specific to certificates such as viewing, revoking, or reissuing.
  See "Using the Certificate Management utility to issue and deploy host ID-based certificates" on page 240.

- Use the **Global Security Settings** node to configure security settings like enable insecure communication, disaster recovery package passphrase, certificate deployment level and so on.

About login activity

NetBackup captures information about the access history of users and keeps a track of when a user's password will expire. The information is displayed in the **My Recent Login Activity** window at the top right corner of the **NetBackup Administration Console**.

My Recent Login Activity

Last successful login to NetBackup:
Date: 06/07/2016 14:45:50
From: V-12365A.company.acme.com

Last failed login to NetBackup:
Date: 06/02/2016 18:29:41
From: V-12365A.company.acme.com

Password expires in:
33 days 20 hours 14 minutes

Close

The **My Recent Login Activity** window closes after you begin to use the **NetBackup Administration Console**.

The password expiration information is not available in the following scenarios:

- If you have remotely logged in to the master server using the Single Sign-on (SSO) feature of the **NetBackup Administration Console**
- If you have logged in to the UNIX or Linux master server using the **NetBackup Administration Console**

Note: The login and the password expiration details are displayed only after the first successful login and logout from the **NetBackup Administration Console**.

The login details are not automatically refreshed. You must log off from the **NetBackup Administration Console** and log in again to view the latest information about the last login details.

This information is also displayed in **Security Events** on the **Access History** tab.

About audit events

Events specific to the following security parameters are audited in the **NetBackup Administration Console**:

- Certificate

- Connection

- Host

- Login

- Security Configuration

- Token

See "Viewing the detailed NetBackup audit report" on page 96.

Viewing audit events

NetBackup records a number of events that occur while you work with the product. For example, a security certificate is issued to a host, an authorization token is deleted, connection between hosts is established and so on.

See "Viewing audit event details" on page 210.

See "Audit Events Details dialog box" on page 211.

See "Viewing audit event status" on page 212.

To view audit events

1   In the **NetBackup Administration Console**, expand **Security Management > Security Events**.

2   In the details pane, click the **Audit Events** tab.

See "Audit Events tab" on page 209.

Audit Events tab

The Audit Events tab displays NetBackup events according to the audit categories that you select. NetBackup records a number of events that occur while you work with the product. For example, a security certificate is issued to a host, an authorization token is deleted, connection between hosts is established and so on.

The following information is displayed on the tab:

Select Date/Time	Select the date range - **From** and **To** dates - for which you want to view audit events.
	Alternatively, you can select the **Current Time** check box instead of selecting the **To** date. Audit events that have occurred from the specified date until the current time are displayed.
Select Audit Categories	Select the audit categories like Certificate, Connection, Host and so on to view the respective events in the report pane.
	Alternatively, you can select the **All** check box, select all audit categories at once.
Show Status	Click the link to open the **Status of Selected Audit Categories** pop-up screen. The pop-up screen displays the audit events that are fetched per selected categories.
	See "Viewing audit event status" on page 212.
Defaults	Click the button to set the default settings for the date and audit categories.
Fetch Audit Events	Click the button to display audit events according to the categories that are selected.
	To view additional information about a specific event, select it from the table in the report pane and double-click. The **Details** dialog box opens.
	See "Audit Events Details dialog box" on page 211.
	Initially, the **Audit Events** tab displays audit events for all categories that are recorded so far. You can select the required audit categories and then click the **Fetch Audit Events** button (or refresh the screen) to fetch the recent events for the selected categories.
Date	Date and time when the audit event was recorded.
User	User who triggered the event.
Category	Audit category, for example Certificate (CERT), Login (LOGIN), Security Configuration (SEC_CONFIG), or Token (TOKEN).
Action	Action that the user has taken, for example CREATE (created a certificate) or MODIFY (modified a security configuration)
Description	Details about the event and the user action.

Viewing audit event details

This section provides the procedure on how to view details of NetBackup audit events.

See "Audit Events tab" on page 209.

See "Viewing audit events" on page 209.

To view audit event details

1   In the **NetBackup Administration Console**, expand **Security Management**
> **Security Events**.

2   In the details pane, click the **Audit Events** tab.

3   On the report pane, on the table, double-click the audit event for which you
want to view the details. The **Details** dialog box is displayed.

See "Audit Events Details dialog box" on page 211.

Audit Events Details dialog box

The **Details** dialog box displays the information specific to the audit event that you
have selected on the **Audit Events** tab.

See "Audit Events tab" on page 209.

The dialog box displays the following details:

Description	Description of the audit event that you have selected.
User	User who triggered the event.
Date	Date and time when the audit event was recorded.
Category	Audit category, for example Certificate (CERT), Login (LOGIN), Security Configuration (SEC_CONFIG), or Token (TOKEN).
Action	Action that the user has taken, for example CREATE (created a certificate) or MODIFY (modified a security configuration)
Reason	Reason for the audit event.

Note: If you see audit records in the CONNECTION category, make sure to review
the record details. For certain records in this category, the **Date** field that is displayed
on the dialog box indicates when the audit record was posted to the master server.
It does not necessarily indicate when an individual event occurred. This type of
audit record (for example, a certificate verification failure (CVF) record) represents
a group of events that have occurred over a time period. The audit record details
provide the **Beginning Event Time** and **Ending Event Time** of the time period as
well as the **Event Count** (the total number of events that occurred in that time
period).

Following are the audit trail details for the events that are displayed on the dialog box:

Attribute	Attribute of the associated audit event. For example: If a host ID-to host name mapping is modified, in the audit trail details, the following attributes are displayed: isApproved, isAddedManually, ApprovalState
Old Value	Old value of the attribute that is associated with the audit event.
New Value	New value of the attribute.

Viewing audit event status

This section provides the procedure on how to view status of the audit events that you want to fetch and view.

See "Audit Events tab" on page 209.

See "Viewing audit events" on page 209.

To view status of audit events

1 In the **NetBackup Administration Console**, expand **Security Management** > **Security Events**.

2 In the details pane, click the **Audit Events** tab.

3 On the **Audit Events** tab, click the **Show Status** link. The **Status of Selected Audit Categories** pop-up screen is displayed with the following information:

Category	Audit category for example, Certificate, Connection, Host and so on.
Status	Status of the events that are fetched and displayed per audit category. For example: 10 audit events are fetched.
	Note: The **Audit Events** tab displays maximum of 10000 events per audit category. If the number of records exceeds the maximum allowed limit for a given date and time, the **Status of Selected Audit Categories** pop-up screen shows the data truncated message. To view the previous records, change the **Show Date/Time** filter on the **Audit Events** tab or use the nbauditreport command.
	For information about the nbauditreport command, see the *NetBackup Commands Reference Guide*.
	http://www.veritas.com/docs/DOC5332

Troubleshooting auditing issues related to the Access History tab

The **NetBackup Administration Console** > **Security Management** > **Security Events** > **Access History** tab displays details about the login activities that the current user has performed.

The **Accessed from** field on the **Access History** tab displays the component that the user has used to login: **NetBackup Administration Console** or **NetBackup API**.

NetBackup requires the bprd service to be running to display the audit details of the users who are logged in using the **NetBackup Administration Console**.

If you observe that the required audit records are not being displayed on the **Access History** tab, ensure that the bprd service is running on the master server.

About host management

The **Security Management > Host Management** node lets you map host names to their respective host IDs. Appropriate mapping between host ID-to-host names is important for secure host communication.

See "About secure communication in NetBackup" on page 207.

See "Adding host ID to host name mappings" on page 214.

See "Resetting NetBackup host attributes" on page 224.

Hosts tab

The **Hosts** tab provides the following information:

Host	The name of the host.
	Note: The **Host Management** node shows only those hosts that have a host ID.
Mapped Host Names / IP Addresses	Host names or IP addresses that are mapped to the host ID of the selected client.
	See "Add or Remove Host Mappings dialog box" on page 216.
Version	The NetBackup version that is installed on the host.

Allow Auto Reissue Certificate Validity	The time until which certificate can be reissued on the host without requiring a reissue token.
	By default, the **Allow Auto Reissue Certificate** option has a validity of 48 hours.
	See "Allowing or disallowing automatic certificate reissue" on page 225.
Operating System	The operating system version that is installed on the host.
OS Type	The type of operating system (Windows or UNIX) that is installed on the host.
CPU Architecture	The architecture of the central processing unit that is used on the host.
Secure	States whether the communication status of the host is secure or not.
	If the host is 8.1, the communication status is secure and it can communicate securely.
Comment	Comment or additional information that you have added for the host.
Hardware Description	The hardware that is used on the host.
NetBackup Host ID	A unique identifier for the host.
NetBackup EEBs	States whether the NetBackup EEBs (Emergency Engineering Binary) are installed or not.
Servers	Additional servers that are associated with the host.
Master Server	Master server host that is associated with the host.
Issued On	Date when the host ID-based certificate was issued to the host.
Last Updated On	Date when the host ID-based certificate was updated.

Adding host ID to host name mappings

Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs.

During communication, NetBackup may detect new host names or IP addresses with respect to a host ID. These host names or IP addresses can be automatically or manually mapped to the respective host ID for successful communication.

Host names or IP addresses that are detected by the system are automatically mapped to the respective host ID, if the **Automatically map host ID to host names** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected.

See "Automatically mapping host ID to host names and IP addresses" on page 232.

Important notes

Review the following notes specific to host ID to host name mappings:

- In the case of DHCP (Dynamic Host Configuration Protocol) hosts, dynamic IP addresses may be detected by the system during communication and added as host ID to host name mappings. You should delete such mappings.

- In the case of a cluster setup, host name, and FQDN (Fully Qualified Domain Name) of virtual name are discovered during host communication.

- If you redeploy a certificate on a host using a host name that is not mapped with the existing host ID, a new certificate is deployed and a new host ID is issued to the host. This is because, NetBackup considers it as a different host. To avoid this situation, you should map all available host names with the existing host ID.

Use the following procedure to manually map a specific host ID to the corresponding host names or IP addresses.

See "Add or Remove Host Mappings dialog box" on page 216.

See "Removing host ID to host name mappings" on page 217.

To add host ID to host name mappings

1 In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2 On the **Hosts** tab, in the details pane, right-click the host that you want to modify.

3 Click the **Add or Remove Host Mappings** option.

4   On the **Add or Remove Host Mappings** screen, host ID of the selected client host is displayed along with the existing mappings.

Click **Add**.

5   On the **Add Mapping** dialog box, provide the following details:

Mapping Name	Specify host ID-to-host name mapping.
	Note: Host ID-to-host name mappings are not case-sensitive.
Audit Reason	Specify the reason or additional information for adding this mapping for auditing purpose.
Save	Click to save the mapping that you have added and to continue to add more mappings for the same host ID.
Cancel	Click to close the dialog box without saving any changes.

To add host ID to host name mapping using the command-line interface

1   Run the following command to authenticate your web services login:

    bpnbat -login -loginType WEB

2   Run the following command to add a host ID to host name mapping:

    nbhostmgmt -add -hostid *host_ID* -mappingname *mapping_name*

Add or Remove Host Mappings dialog box

Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs.

On the **Security Management > Host Management > Hosts** tab, right-click the host that you want to modify, and click the **Add or Remove Host Mappings** option to open the dialog box.

Only System Administrator can access the **Add or Remove Host Mappings** properties for a NetBackup host.

See "Adding host ID to host name mappings" on page 214.

See "Removing host ID to host name mappings" on page 217.

The **Add or Remove Host Mappings** dialog box contains the following properties.

NetBackup Host ID	Displays the host ID of the selected host.

Mapped Host Names / IP Addresses	Lists host names and IP addresses that are mapped to the host ID of the client host.
Auto-discovered	States whether the mapped host name or IP address was automatically discovered by the system or not.
Created On	Date and time when the mapping was created.
Last Updated On	Date and time when the mapping was last updated.
Add	Click to add new host ID to host name mappings for the client host.
	The **Add Mapping** dialog box is displayed.
	See "Adding host ID to host name mappings" on page 214.
Remove	Click to remove the selected host ID to host name mapping for the client host.
	The **Remove Mapping** dialog box is displayed.
	See "Removing host ID to host name mappings" on page 217.
	Note: The operations that you carry out on the **Add Mapping** and **Remove Mapping** dialog boxes directly update the NetBackup database.
Close	Click to close the **Add or Remove Host Mappings** dialog box.
Help	Click to see help.

Removing host ID to host name mappings

Use the following procedure to remove host ID to host name mappings.

See "Add or Remove Host Mappings dialog box" on page 216.

See "Adding host ID to host name mappings" on page 214.

To remove host ID to host name mappings

1   In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2   In the details pane, on the **Hosts** tab, right-click the client host that you want to modify.

3   Click the **Add or Remove Host Mappings** option.

4   On the **Add or Remove Host Mappings** screen, host ID of the selected client host is displayed along with the existing mappings.

5   Select the mapping that you want to remove.

6 Click **Remove**.

7 On the **Remove Mapping** dialog box, specify the audit reason for removing the selected mapping for auditing purpose.

8 Click **Yes**.

To remove host ID to host name mapping using the command-line interface

1 Run the following command to authenticate your web services login:

```
bpnbat -login -loginType WEB
```

2 Run the following command to remove a host ID to host name mapping:

```
nbhostmgmt -delete -hostid host_ID-mappingname mapping_name
```

Mappings for Approval tab

Use the **Security Management > Host Management > Mappings for Approval** tab to view host ID-to-host name mappings that are pending for approval.

The following options are available on the **Mappings for Approval** tab:

Host	Name of the selected host.
Auto-discovered Mapping	Host ID-to-host name mapping that was discovered with respect to the host during communication.
Conflict	States if there is any conflict in the mappings. For example, in a cluster setup, a mapping can be shared across host IDs.
Discovered On	Date and time when the mapping was discovered by the system.
NetBackup Host ID	Host ID of the host.

See "Viewing auto-discovered mappings" on page 219.

See "Add or Remove Host Mappings dialog box" on page 216.

Note: If the **Automatically map host ID to host names** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected, the **Mappings for Approval** tab shows only conflicting mappings.

See "Automatically mapping host ID to host names and IP addresses" on page 232.

Viewing auto-discovered mappings

During communication, NetBackup may detect new host names or IP addresses with respect to a host ID. You can view the host ID-to-host name mappings that are automatically discovered.

See "Add or Remove Host Mappings dialog box" on page 216.

To view auto-discovered host ID-to-host name mappings

1 In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2 In the details pane, click the **Mappings for Approval** tab.

See "Mappings for Approval tab" on page 218.

Note: If the **Automatically map host ID to host names** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected, the **Mappings for Approval** tab shows only conflicting mappings.

See "Automatically mapping host ID to host names and IP addresses" on page 232.

Mapping Details dialog box

Use the **Mapping Details** dialog box to approve or reject the pending host ID-to-host name mappings.

On the **Security Management > Host Management > Mappings for Approval** tab, right-click the host ID-to-host name mapping that you want to approve or reject, and click **Mapping Details** to open the dialog box.

See "Add or Remove Host Mappings dialog box" on page 216.

See "Approving host ID to host name mappings" on page 220.

See "Rejecting host ID to host name mappings" on page 221.

See "Mappings for Approval tab" on page 218.

The following options are available on the dialog box:

Host	Displays name of the host for which you want to approve or reject the mapping.
Mapped Host Names / IP Addresses	Lists the existing mappings that are associated with the host.

NetBackup Host ID	Displays the host ID of the host.
Conflict in mapping - Shared with hosts	**Note:** This information is displayed if the selected mapping is already associated with other hosts.
	This table lists information of all hosts across which the selected mapping is shared.
	For example, in a cluster set up, multiple host IDs share the same virtual name.
	If a mapping is added for a host ID and if the same mapping is discovered against a different host ID, it is listed on the **Mappings for Approval** tab. You can either approve this mapping or reject it using the **Mapping Details** dialog box.
	■ Host - Displays the name of the host with which the selected mapping is already associated.
	■ NetBackup Host ID - Displays host ID of the host with which the selected mapping is already associated.
	See "About shared or cluster mapping scenarios" on page 222.
Reason	Provide the reason for approving or rejecting the mapping.
Approve	Click to approve the pending mapping.
Reject	Click to reject the pending mapping.
Close	Click to close the dialog box without saving the changes.
Help	Click to see help.

Approving host ID to host name mappings

This section provides a procedure for approving host ID to host name mappings that are pending for approval.

See "Add or Remove Host Mappings dialog box" on page 216.

See "Rejecting host ID to host name mappings" on page 221.

To approve host ID to host name mapping

1   In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2   In the details pane, click the **Mappings for Approval** tab.

3   Select the mapping that you want to approve and right-click.

4   On the right-click options, click **Approve**. The selected mappings are approved.

Alternatively, click **Mapping Details** on the right-click options. Use the **Mapping Details** dialog box to approve the selected mapping.

See "Mapping Details dialog box" on page 219.

Rejecting host ID to host name mappings

This section provides a procedure for rejecting host ID to host name mappings that are pending for approval.

See "Add or Remove Host Mappings dialog box" on page 216.

See "Approving host ID to host name mappings" on page 220.

To reject host ID to host name mapping

1   In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2   In the details pane, click the **Mappings for Approval** tab.

3   Select the mapping that you want to reject and right-click.

4   On the right-click options, click **Reject**. The selected mappings are rejected.

Alternatively, click **Mapping Details** on the right-click options. Use the **Mapping Details** dialog box to reject the selected mapping.

Adding shared or cluster mappings

In certain scenarios, host ID to host name mappings are shared across host IDs. For example, in a cluster setup, virtual name is shared across all nodes. You need to add these shared mappings using the **NetBackup Administration Console** so that the master server can successfully communicate with the nodes.

See "Add or Remove Host Mappings dialog box" on page 216.

To add shared mappings

1   In the **NetBackup Administration Console**, expand **Security Management > Host Management**.

2   On the **Hosts** tab, in the details pane, right-click to view the options.

3   On the right-click options, select **Add Shared or Cluster Mappings**.

4   On the **Add Shared or Cluster Mappings** dialog box, specify the shared mapping name.

See "Add Shared or Cluster Mappings dialog box" on page 223.

5   Select host IDs to be mapped with the specified shared mapping name.

6   Click **Save**.

About shared or cluster mapping scenarios

Host ID to host name mappings can be shared across multiple hosts in the following scenarios:

- If multiple hosts from different domains use the same host name

- In a cluster setup where the same virtual name is used by multiple cluster nodes

However, in a scenario where the associated hosts do not have the same communication status (some are 8.0 or earlier and can communicate insecurely and some are 8.1 or later and communicate securely), communication may fail.

See "Add or Remove Host Mappings dialog box" on page 216.

Scenario 1 - If multiple hosts from different domains use the same host name

Consider the following example:

- Host1 – abc.secure.domain1.com, version – 8.1, policy – P1

- Host2 – abc.insecure.domain2.com, version – 7.7.3, policy – P2

- Host1 and Host 2 use the same name – abc – as their host name. Security Administrator adds abc as a shared mapping for Host2.
  See "Adding shared or cluster mappings" on page 221.

- Insecure communication with 8.0 and earlier hosts is enabled.
  See "About insecure communication with 8.0 and earlier hosts" on page 231.

- When Host2 initiates communication with another host, the master server validates the communication status of host2 (which is insecure), which is different than Host1 (which is secure). Because both hosts use the same host name, but their communication status do not match, the communication with Host2 fails.

- Recommendation – Host2 should be upgraded to 8.1 or later.

Scenario 2 - In a cluster setup where the same virtual name is used by multiple cluster nodes

Consider the following example:

- Host1 – abc.secure.domain1.com, active cluster node, version – 8.1

- Host2 – abc.secure.domain1.com, inactive cluster node, version – 8.0

- Host1 and Host2 use the same virtual name that is abc. Security Administrator adds abc as a shared or cluster mapping for Host2.

- Insecure communication with 8.0 and earlier hosts is enabled.

- Host1 fails over to Host2. The master server validates the communication status of host2 (that is insecure), which is different than Host1 (that is secure). Because communication status for both hosts do not match, the communication with Host2 fails.

- Recommendation – Host2 should be upgraded to 8.1.

- Workaround – Delete the host ID-to-host name mapping abc for Host1. In case of shared mapping, if the associated hosts do not have the same communication status (secure), communication fails for the host that has insecure communication status.

Add Shared or Cluster Mappings dialog box

Use this option to add shared or cluster mappings. On the **Security Management > Host Management > Hosts** tab, on the right-click options, click **Add Shared or Cluster Mappings** to open the dialog box.

The following options are available on the **Add Shared or Cluster Mappings** dialog box:

Shared mapping name or virtual name of cluster	Enter the mapping name that needs to be shared by multiple host IDs.
Select Hosts	Click the button to list all hosts and select the ones that you want to map with the specified mapping name.
	The **Select Hosts** pop-up screen lists all available hosts. Select the required hosts and click **Add to list**.
	The selected hosts appear in the list on the **Add Shared or Cluster Mappings** dialog box.
Host	Name of the host that you want to map with the specified shared name.
NetBackup Host ID	Host ID of the host that you want to map with the specified shared name.
Save	Click to save the mapping.
Cancel	Click to close the dialog box without saving the changes.
Help	Click to see help.

Resetting NetBackup host attributes

In certain scenarios, you may need to clean up or reset host attributes: For example, you have downgraded the host.

In such cases, you need to reset host ID to host name mapping information, communication status and so on for successful communication.

Review the following notes before resetting host attributes

- You must reset the host attributes of the downgraded host if you want the master server to communicate with the host in an insecure mode.

- Resetting host attributes resets host ID to host name mapping information, communication status and so on. It does not reset the host ID, host name, or security certificates of the host.

- After you reset the host attributes, the connection status (is secure flag) is set to insecure state. At the time of the next host communication, the connection status is updated appropriately.

- If you have inadvertently used the **Reset Host Attributes** option, you can undo the changes by restarting the bpcd service. Else the host attributes are automatically updated with the appropriate values after 24 hours.

About resetting host attributes

NetBackup 8.1 master server can communicate securely with all 8.1 hosts. However, it communicates insecurely with 8.0 and earlier hosts.

In certain scenarios, you may need to downgrade a NetBackup client from 8.1 version to 8.0 or earlier. After the downgrade, the master server cannot communicate with the client, because the communication status for the client is still set to secure mode. The communication status is not automatically updated to insecure mode after the downgrade.

Use one of the following options to reset a host:

To reset a host using the NetBackup Administration Console

1   Expand **Security Management > Host Management**.

2   On the **Hosts** tab, in the details pane, right-click the host that you have downgraded and which you want to reset, and click **Reset Host Attributes**.

Note: To resume insecure communication with downgraded hosts, ensure that the **Enable insecure communication with 8.0 and earlier hosts** option on the **Security Management > Global Security Settings > Secure Communication** tab is selected.

To reset host attributes using the command-line interface

1   Run the following command to authenticate your web services login:

    bpnbat -login -loginType WEB

2   Run the following command to reset the host:

    nbemmcmd -resethost

Allowing or disallowing automatic certificate reissue

This section provides the procedures for allowing and disallowing automatic certificate reissue.

The **Allow Auto Reissue Certificate** option enables the autoreissue parameter of a host that in turn allows you to deploy a certificate on the host without requiring a reissue token.

See "Deploying host ID-based certificates" on page 247.

By default, the autoreissue parameter is enabled for 2880 minutes (or 48 hours or 2 days). After this duration, the parameter is disabled and the certificate reissue operation requires a reissue token.

See "Configuring validity of the autoreissue parameter for a host" on page 227.

To manually disable the autoreissue parameter, use the **Disallow Auto Reissue Certificate** option.

Note: During the Bare Metal Restore (BMR) process, the `autoreissue` flag is automatically set.

For more information on Bare Metal Restore, refer to the *NetBackup Bare Metal Restore Administrator's Guide*.

https://www.veritas.com/support/en_US/article.DOC5332

To allow automatic certificate reissue using the NetBackup Administration Console

1   Expand **Security Management** > **Host Management**.

2   In the right pane, select the host for which you want to allow automatic certificate reissue.

3   Right-click the host and select the **Allow Auto Reissue Certificate** option.

To allow automatic certificate reissue using the command-line interface

1   Run the following command to authenticate your web services login:

    bpnbat -login -loginType WEB

2   Run the following command to enable the `autoreissue` parameter, which in turn allows automatic certificate reissue:

    nbhostmgmt -allowautoreissuecert -hostid *host_ID* -autoreissue 1

To disallow automatic certificate reissue using the NetBackup Administration Console

1   Expand **Security Management** > **Host Management**.

2   In the right pane, select the host for which you want to disallow automatic certificate reissue.

3   Right-click the host and select the **Disallow Auto Reissue Certificate** option.

To disallow automatic certificate reissue using the command-line interface

1   Run the following command to authenticate your web services login:

    bpnbat -login -loginType WEB

2   Run the following command to disable the `autoreissue` parameter, which in turn disallows automatic certificate reissue:

    nbhostmgmt -allowautoreissuecert -hostid *host_ID* -autoreissue 0

Configuring validity of the `autoreissue` **parameter for a host**

When you allow automatic reissue of a host ID-based certificate, the `autoreissue` parameter is by default enabled for 2880 minutes (or 48 hours or 2 days). After this duration, the parameter is reset and the certificate reissue operation requires a reissue token.

You can configure the duration for automatic reissue of certificate or the time-to-live (TTL) setting for the `autoreissue` parameter by updating the `web.conf` file.

To configure validity of the `autoreissue` parameter or the TTL setting

1   Open the `web.conf` file. Location for the file is as follows:

On Windows: `Install_Path\var\global\wsl\config\web.conf`

On Linux: `/usr/openv/var/global/wsl/config/web.conf`

2   Configure the TTL setting for the `autorissue` parameter in minutes. For example:

`ttl.autoReissue.minutes = 1440`

Note: Valid range for the `autoreissue` TTL setting is 0 min to 43200 min (or 30 days).

If the TTL value that you have configured is not within the valid range, the server continues using the last configured TTL value.

---

3   For the new `autoreissue` TTL value to take effect, do one of the following:

   ■   Restart the NetBackup Web Management Console (WMC) service.

   ■   Run the following command:
       On Windows: `Install_Path/bin/nbhostdbcmd -reloadconfig -host`
       On UNIX: `NETBACKUP_INSTALL_DIR\bin\nbhostdbcmd -reloadconfig -host`

Adding or deleting comment for a host

You can provide additional information about a NetBackup host using the **Add or Edit Comment** dialog box. For example, if a host is decommissioned, you can add a comment to explain why and when it was decommissioned.

To add or edit a comment for a host

1 Expand **Security Management > Host Management**.

2 On the **Hosts** tab, in the details pane, right-click the host for which you want to provide additional information, and click **Add or Edit Comment**.

3 On the **Add or Edit Comment** dialog box, in the **Comment** pane, enter the required information or comments.

Click **Save**.

To delete a comment for a host

1 Expand **NetBackup Management > Security Management > Host Management**.

2 On the **Hosts** tab, in the details pane, right-click the host for which you want to delete comment, and click **Delete Comment**.

About global security settings

The **Security Management > Global Security Settings** node lets you configure the settings that are crucial for secure communication in NetBackup.

See "About secure communication in NetBackup" on page 207.

See "About disaster recovery settings" on page 233.

See "About secure communication settings" on page 228.

About secure communication settings

NetBackup provides settings that you can configure for secure communication between hosts.

Table 8-2   Secure communication settings

Setting	Description
Certificate authority	Displays the certificate authorities that your NetBackup domain supports.
	The NetBackup web server can be configured to enable the NetBackup domain to use:
	■ NetBackup CA-signed certificates only
	■ External CA-signed certificates only
	■ NetBackup CA-signed certificates and external CA-signed certificates
	Use the -configureWebServerCerts command for certificate configuration for the web server.
	For more information, refer to the *NetBackup Commands Reference Guide*.
Enable insecure communication with NetBackup 8.0 and earlier hosts	NetBackup communicates insecurely with 8.0 and earlier hosts.
	For increased security, upgrade all your hosts to the current version and disable this setting. This ensures that only secure communication is possible between NetBackup hosts.
	By default, the option is selected, which allows NetBackup to communicate with hosts including 8.0 and earlier hosts that may be present in the existing NetBackup environment.
	This option also allows communication between NetBackup 8.1 or later master server and OpsCenter server.
	See "Disabling insecure communication" on page 230.
	See "About insecure communication with 8.0 and earlier hosts" on page 231.
	If you have configured Auto Image Replication, ensure the following before you clear the option:
	The trusted master server that you have specified for image replication is of the version that is later than NetBackup 8.0.
	For more information, refer to the NetBackup Administrator's Guide, Volume I.

Table 8-2   Secure communication settings *(continued)*

Setting	Description
Automatically map NetBackup host ID to host names	Hosts may have multiple host names or IP addresses associated with them. For successful communication between hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs.
	During communication, NetBackup may detect new host names or IP addresses with respect to a host ID.
	Select this option to automatically map the host ID to host names or IP addresses that are detected by the system.
	By default, the option is selected.
	For increased security, clear this option so that the NetBackup Administrator can manually verify the mappings and approve them.
	See "Automatically mapping host ID to host names and IP addresses" on page 232.
Security level for certificate deployment	Based on the security level that is configured on the NetBackup master server, the certificate deployment approach is determined.
	For example, if the security level is set to **Very High**, an authorization token is a must for certificate deployment.
	Note: Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, this option cannot be accessed.
	See "About NetBackup certificate deployment security levels" on page 244.
	See "Configuring the certificate deployment security levels" on page 246.

Disabling insecure communication

By default, NetBackup can communicate with 8.0 and earlier hosts. For increased security, you should upgrade all hosts to the current version and disable communication with 8.0 and earlier hosts.

See "About secure communication settings" on page 228.

To disable insecure communication

1   In the **NetBackup Administration Console**, expand **Security Management > Global Security Settings**.

2   In the details pane, click the **Secure Communication** tab.

3   Clear the **Enable insecure communication with 8.0 and earlier hosts** option.

4   Click **Save**.

Note: If you are disabling insecure communications, it is recommended that you restart services to ensure that already established insecure connections are terminated.

About insecure communication with 8.0 and earlier hosts

NetBackup communicates insecurely with 8.0 or earlier hosts.

If you have NetBackup 8.0 or earlier hosts in your environment, you can allow insecure communication with them using the **Enable insecure communication with 8.0 and earlier hosts** option in the **NetBackup Administration Console**.

The option is available on the **Security Management > Global Security Settings > Secure Communication** tab.

This option also allows communication between NetBackup 8.1 or later master server and OpsCenter server.

By default, insecure communication is enabled. However, for increased security, you should upgrade all hosts to the current version and disable communication with 8.0 and earlier hosts.

See "Disabling insecure communication" on page 230.

See "About communication with 8.0 or earlier host in multiple NetBackup domains" on page 232.

Note: If you have configured Auto Image Replication, ensure the following before you disable insecure communication: The trusted master server that you have specified for image replication is of the version that is later than NetBackup 8.0.

See "About secure communication in NetBackup" on page 207.

About communication with 8.0 or earlier host in multiple NetBackup domains

This section provides information on what is the impact of the **Enable insecure communication with 8.0 and earlier hosts** option on the host communication when one of the NetBackup hosts is in multiple domains.

Consider the following scenario:

- Host A is of version 8.1, which is present in multiple NetBackup domains called M1 and M2.

- Host B is of version 8.0, which is present in a NetBackup domain called M3.

- The **Enable insecure communication with 8.0 and earlier hosts** option is cleared on master server M1, which means hosts that are associated with M1 cannot communicate with hosts that are 8.0 or earlier.

- The **Enable insecure communication with 8.0 and earlier hosts** option is selected on master server M2, which means hosts that are associated with M2 can communicate with hosts that are 8.0 or earlier.

- The configuration file (`bp.conf` file on UNIX or registry keys on Windows) for Host A contains 'M2' as the first entry in the master server list.

When Host A initiates communication with Host B, the status of the **Enable insecure communication with 8.0 and earlier hosts** option is verified for the first master server that appears in the configuration file of Host A, which is M2. As per the option set for M2, communication with 8.0 or earlier hosts is allowed. Therefore, communication between Host A and Host B is successful.

Automatically mapping host ID to host names and IP addresses

For successful communication between NetBackup hosts, all relevant host names and IP addresses need to be mapped to the respective host IDs. You can choose to automatically map the host ID to the respective host names (and IP addresses) or allow the NetBackup Administrator to verify the mappings before approving them.

See "Add or Remove Host Mappings dialog box" on page 216.

Note: For increased security, clear this option so that the NetBackup Administrator can manually verify the mappings and approve them.

To automatically map host ID to host names or IP addresses

1   In the **NetBackup Administration Console**, expand **Security Management**
     > **Global Security Settings**.

2   In the details pane, click the **Secure Communication** tab.

3   Select the **Automatically map host ID to host names** option.

4   Click **Save**.

See "About secure communication settings" on page 228.

About disaster recovery settings

For increased security, a disaster recovery package is created during each catalog
backup.

See "Disaster recovery packages" on page 236.

During each catalog backup, a disaster recovery package is created and encrypted
with the passphrase that you set. You need to provide this encryption passphrase
while you install NetBackup on the master server in a disaster recovery mode after
a disaster.

The following options are displayed on the **Disaster Recovery** tab:

Table 8-3   Disaster recovery settings

Setting	Description
Passphrase	Enter the passphrase to encrypt disaster recovery packages. ■ The passphrase must contain a minimum of 8 and a maximum of 1024 characters. ■ The existing passphrase and the new passphrase must be different. ■ Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > " See "Setting a passphrase to encrypt disaster recovery packages" on page 234.
Confirm Passphrase	Re-enter the passphrase for confirmation.

Caution: Ensure that the passphrase contains only the supported characters. If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

Note the following before you modify the passphrase for the disaster recovery packages:

- Subsequent disaster recovery packages are encrypted with the new passphrase that you set.

- If you change the passphrase anytime, it is not changed for the previous disaster recovery packages. Only new disaster recovery packages are associated with the new passphrase.

- Passphrase that you provide while you install NetBackup on the master server in a disaster recovery mode after a disaster must correspond to the disaster recovery package from which you want to recover the master server host identity.

Setting a passphrase to encrypt disaster recovery packages

During each catalog backup, a disaster recovery package is created and encrypted with the passphrase that you set.

See "Disaster recovery packages" on page 236.

Workflow to set a passphrase to encrypt disaster recovery packages and use it after a disaster:

Review the following workflow to learn about disaster recovery package restore:

1. Set an encryption passphrase for disaster recovery packages.

2. Create a catalog policy.

   Consider the following scenarios:

   - If you have not set the passphrase earlier, NetBackup prevents you from configuring a new catalog backup policy.

   - If the catalog backup policy is upgraded from a previous version, catalog backups continue to fail until the passphrase is set.

   Note: Catalog backups may fail with status code 144 even though the passphrase is set. This is because the passphrase may be corrupted. To resolve this issue, you must reset the passphrase.

3. After a disaster, when you install NetBackup on the master server in a disaster recovery mode, provide the passphrase that you have set earlier. NetBackup decrypts the disaster recovery package using this passphrase and gets the identity of the master server back during installation.

Caution: If you fail to provide the appropriate passphrase while you install NetBackup on the master server after a disaster, you may need to redeploy the security certificates on all NetBackup hosts. For more details, refer to the following article:

http://www.veritas.com/docs/000125933

---

4. Once the master server identity is back in place, the secure communication between the master server and the media server is established and you can perform catalog recovery.

5. After successful catalog recovery, you must set the disaster recovery package passphrase again, because the passphrase is not recovered during the catalog recovery. Catalog backups that you configure in a new NetBackup instance continue to fail until you set the passphrase.

To set or modify a passphrase

1 In the **NetBackup Administration Console**, expand **Security Management** > **Global Security Settings**.

2 In the details pane, click the **Disaster Recovery** tab.

See "About disaster recovery settings" on page 233.

3 Provide **Passphrase** and **Confirm Passphrase**.

Review the following password rules:

- The existing passphrase and the new passphrase must be different.

- The passphrase must contain a minimum of 8 and a maximum of 20 characters.
  The passphrase must contain a minimum of 8 and a maximum of 1024 characters.

- Only the following characters are supported for the passphrase: White spaces, uppercase characters (A to Z), lowercase characters (a to z), numbers (0 to 9), and special characters. Special characters include: ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > "

> **Caution:** If you enter a character that is not supported, you may face problems during disaster recovery package restore. The passphrase may not be validated and you may not be able to restore the disaster recovery package.

4 Click **Save**. If the passphrase already exists, it is overwritten.

To set or modify a passphrase using the command-line interface

1 The NetBackup administrator must be logged on to the NetBackup Web Management Service to perform this task. Use the following command to log on:

```
bpnbat -login -loginType WEB
```

2 Run the following command to set a passphrase to encrypt disaster recovery packages:

```
nbseccmd -drpkgpassphrase
```

3 Enter the passphrase.

If a passphrase already exists, it is overwritten.

Disaster recovery packages

For increased security, a disaster recovery package is created during each catalog backup. The disaster recovery package file has `.drpkg` extension.

The disaster recovery package stores the identity of the master server host. NetBackup requires this package to get the identity of the master server back after a disaster. Once you have recovered the host identity, you can perform the catalog recovery.

The disaster recovery package contains the following information:

- NetBackup CA-signed certificates and private keys of the master server certificate and the NetBackup certificate authority (CA) certificate

- Information about the hosts in the domain

- Security settings

- External CA-signed certificates
  External CA-signed certificates from Windows certificate store, if applicable

- NetBackup configuration options that are specific to external CA-signed certificates

Note: You must set a passphrase for the disaster recovery package for the catalog backups to be successful.

See "About disaster recovery settings" on page 233.

See "Setting a passphrase to encrypt disaster recovery packages" on page 234.

About host name-based certificates

By default, individual NetBackup master servers are provisioned with a host name-based certificate during installation. To provision a host name-based certificate on a media server or client, the NetBackup administrator runs the `bpnbaz` command on the master server to push the certificate to other hosts.

See "Overview of security certificates in NetBackup" on page 206.

Deploying host name-based certificates

Choose one of the following procedures to deploy a host name-based security certificate on NetBackup hosts. Only a NetBackup administrator can deploy certificates.

Table 8-4   Deploying host name-based certificates

Procedure	Description and link to procedure
Deploying a host name-based security certificate for a master server in a cluster	Use this procedure to deploy the host name-based security certificates on all of the nodes in a NetBackup master server cluster. Deploying a host name-based certificate for a master server in a cluster
Deploying a host name-based security certificate for media servers or clients	This procedure uses IP address verification to identify the target NetBackup host and then deploy the certificate. With this procedure, you can deploy a host name-based certificate for an individual host, for all media servers, or for all clients. Deploying a host name-based certificate on media servers or clients

Note: Deploying a host name-based certificate is a one-time activity for a host. If a host name-based certificate was deployed for an earlier release or for a hotfix, it does not need to be done again.

Deploying a host name-based certificate for a master server in a cluster

Use this procedure to deploy host name-based certificates on all cluster nodes.

Ensure the following before you deploy a host-name based certificate:

- All nodes of the cluster have a host ID-based certificate.
- All Fully Qualified Domain Names (FQHN) and short names for the cluster nodes are mapped to their respective host IDs.
  See "Adding host ID to host name mappings" on page 214.

To deploy a host name-based security certificate for a NetBackup master server in a cluster

1 Run the following command on the active node of the master server cluster:

On Windows: *Install_path*\NetBackup\bin\admincmd\bpnbaz -setupat

On UNIX: /usr/openv/netbackup/bin/admincmd/bpnbaz -setupat

2 Restart the NetBackup Service Layer (nbsl) service and the NetBackup Vault Manager (nbvault) service on the active node of the master server.

Deploying a host name-based certificate on media servers or clients

This procedure works well when you deploy host name-based security certificates to many hosts at one time. As with NetBackup deployment in general, this method assumes that the network is secure.

To deploy a host name-based security certificate for media servers or clients

1 Run the following command on the master server, depending on your environment. Either specify a host name, or deploy to all media servers or clients.

On Windows: *Install_path*\NetBackup\bin\admincmd\bpnbaz -ProvisionCert *host_name*|-AllMediaServers|-AllClients

On UNIX: /usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert *host_name*|-AllMediaServers|-AllClients

2 Restart the NetBackup Service Layer (nbsl) service on the media server.

No services need to be restarted if the target host is a NetBackup client.

Note: In you use dynamic IPs on the hosts (DHCP), ensure that the host name and the IP address are correctly listed on the master server. To do so, run the following NetBackup `bpclient` command on the master server:

On Windows: *Install_path*`\NetBackup\bin\admincmd\bpclient -L -All`

On UNIX: `/usr/openv/netbackup/bin/admincmd/bpclient -L -All`

About host ID-based certificates

Each host in a NetBackup domain has a unique identity, which is referred to as a host ID or a Universally Unique Identifier (UUID). The master server is the Certificate Authority (CA). It assigns host ID-based certificates to hosts and stores the host information in the `nbdb` database. The CA maintains a list of all of the host IDs that have certificates (or revoked certificates). The host ID is used in many certificate management operations to identify the host.

Host IDs are randomly generated by the system and are not tied to any property of the hardware.

NetBackup provides a list of host ID-based certificates that you have revoked.

See "About the host ID-based certificate revocation list" on page 270.

See "Overview of security certificates in NetBackup" on page 206.

Only a NetBackup administrator can control the settings that are related to certificate deployment and revocation.

The host ID remains the same even when the host name changes.

If a host obtains certificates from multiple NetBackup domains, it has multiple host IDs that correspond to each NetBackup domain.

When the master server is configured as part of a cluster, each node in the cluster receives a unique host ID. An additional host ID is assigned for the virtual name. For example, if the master server cluster is comprised of *N* nodes, the number of host IDs that are allocated for the master server cluster is *N* + 1.

Web login requirements for nbcertcmd command options

The `nbcertcmd` command can be used to perform all of the operations that are associated with host-ID based certificates. However, some of the `nbcertcmd` options require that the user first logs in to the NetBackup Web Management Service (`nbwmc`).

- To log in to the NetBackup Web Management Service, run the following command:

```
bpnbat -login -logintype WEB
```
The account must have NetBackup administrator privileges.
The following shows an example `WEB` login:

```
bpnbat -login -LoginType WEB
Authentication Broker: server.domain.com
Authentication port [0 is default]: 0
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
Domain: server.domain.com
Login Name: root
Password: ********
Operation completed successfully.
```

- The `bpnbat -login -logintype AT` command creates a session with the NetBackup Authentication Broker (`nbatd`). (The NetBackup Authentication Broker may not always be the master server.)

Note: An `nbatd` session is not necessary to run the `nbcertcmd` commands.

- If neither `WEB` nor `AT` is indicated, `bpnbat -login` creates a login session for both `nbatd` and `nbwmc`. (This is true if the Authentication Broker is located on the master server.)

Note: The authentication broker for a WEB login is the master server as the `nbwmc` service runs only on the master server.

The NetBackup Commands Reference Guide lists the privilege details that each `nbcertcmd` option requires. This guide also contains detailed information about running the `bpnbat` command.

Using the Certificate Management utility to issue and deploy host ID-based certificates

The process for host ID-based certificate deployment varies based on the certificate deployment security level configured on the master server. The levels are **Medium**, **High**, and **Very High**. By default, the security level is **High**.

A host ID-based certificate is automatically deployed on the master server during upgrade or installation.

Host ID-based certificates are deployed on hosts after confirming the fingerprint. Whether an authorization token is required or not depends on the security level.

These levels determine the nature of the Certificate Authority (CA) checks that are performed when the CA receives a certificate request from a NetBackup host. Select the certificate deployment level according to the security requirements of your NetBackup environment.

See "About NetBackup certificate deployment security levels" on page 244.

In some scenarios, certificate deployment requires the use of authorization tokens that are managed by a NetBackup administrator. The NetBackup administrator creates and shares these tokens with the administrators of individual hosts for certificate deployment on their local hosts. Certificate deployment can happen easily, allowing for scalable deployment across multiple NetBackup hosts without requiring NetBackup administrator intervention.

Table 8-5   Deployment requirements at each certificate deployment level or scenario

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate deployment level setting at **Very High**	Yes. All certificate requests require an authorization token. The master server administrator creates a token to be used on the non-master host: See "Creating authorization tokens" on page 266.	The host administrator of the non-master server host must obtain an authorization token from the master server administrator and use it to deploy the host ID-based certificate. See "Deploying host ID-based certificates" on page 247.
Certificate deployment level setting at **High** (default)	Maybe. Certificates are deployed without tokens on hosts that are known to the master server. The following topic explains what it means to be known to the master server: See "About NetBackup certificate deployment security levels" on page 244. If the host is not known to the master server, the certificate must be deployed using an authorization token. The master server administrator creates a token to be used on the non-master server host. See "Creating authorization tokens" on page 266.	If a host ID-based certificate is deployed, no further action is required. If a token is required, the host administrator of the non-master server host must to obtain one from the master server administrator and use it to deploy the host ID-based certificate. See "Deploying host ID-based certificates" on page 247.

| | Table 8-5 | Deployment requirements at each certificate deployment level or scenario *(continued)* |

Certificate deployment level or scenario	Is an authorization token required?	Deploy host ID-based certificate?
Certificate deployment level setting at **Medium**	No. Certificates may be deployed on all hosts that request one. See "Automatic host ID-based certificate deployment" on page 246. **Note:** A certificate may not be deployed if the master server cannot verify that the requested host name matches the IP from which the certificate request originated.	If a host ID-based certificate is deployed, no further action is required. If the master server cannot verify the host name, a host ID-based certificate must be deployed using a token. See "Deploying host ID-based certificates" on page 247.
Certificate reissue	Yes. A certificate reissue requires a reissue token in most cases.	See "Creating a reissue token" on page 261.
Hosts that cannot communicate with the master server directly (an example of this is NetBackup hosts in a demilitarized zone (DMZ)).	Yes. NetBackup can automatically detect whether a host has connectivity with the master server or not. If there is no connectivity, NetBackup attempts to use the built-in HTTP tunnel on a media server to route the certificate request to the master server. See "About the communication between a NetBackup client located in a demilitarized zone and a master server through an HTTP tunnel" on page 289.	See "Deploying certificates on a client that has no connectivity with the master server" on page 257.
Certificate deployment and generation for NAT clients	Yes. During NetBackup certificate deployment on a NAT client, you must provide an authorization token is must, irrespective of the certificate deployment security level that is set on the master server. This is because, the master server cannot resolve the host name to the IP address from which the request is sent.	For more information on support for NAT clients in NetBackup, refer to the NetBackup Administrator's Guide, Volume I.

Viewing host ID-based certificate details

Details for each host ID-based certificate can be viewed in the **NetBackup Administration Console** or by using the `nbcertcmd` command.

To view certificate details in the NetBackup Administration Console

1 In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management**.

The certificate details are displayed in the right pane.

1 Host Certificate(s) (1 selected)							Search		
Certificate State	∠ Host	Host Type	Issued On	Valid From	∠ Valid Until	Days Remaini...			∠ NetBackup Host ID
⊡ Active	caycevm3...	Server	Sep 12, ...	Sep 12, 201...	Sep 12, 2017 8:5...	363			b9e5a819-547e-4150-91c9-fc48

2 By default, the host IDs are not displayed. (See Table 8-6.)

To display or hide columns, right-click on the pane and select **Columns > Layout**. Select the columns to show or hide in the **Column Layout** dialog box.

Table 8-6   Hidden and displayed certificate details

Column head	Description	Displayed by default
Certificate State	The certificate state (**Active**, **Revoked**, or **Expired**).	Yes
Host	The name of the host to which the certificate is issued.	Yes
Host Type	The type of host (server or client).	Yes
Issued On	The date and time on which the certificate was issued.	Yes
Valid From	The date upon which the certificate becomes valid.	Yes
Valid Until	The date until after which the certificate is invalid.	Yes
Days Remaining Until Expiry	The number of days until the certificate expires.	Yes
Certificate Version	Version of the host ID-based certificate that is deployed on the host.	No
NetBackup Host ID	The unique ID assigned to the host.	No
Serial Number	The serial number of the certificate.	No
Reason For Revocation	The reason for a certification revocation, if the administrator entered a reason at the time of revocation.	No
Last Updated On	The date when the certificate details were last updated.	No

To view certificate details using the nbcertcmd command

◆ To view all of the host IDs that are assigned to a host from different master servers, run the following command on a NetBackup host:

    nbcertcmd -listCertDetails

About NetBackup certificate deployment security levels

Security levels for certificate deployment are specific to NetBackup CA-signed certificates. If the NetBackup web server is not configured to use NetBackup certificates for secure communication, the security levels cannot be accessed.

The NetBackup certificate deployment level determines the checks that are performed before the NetBackup CA issues a certificate to a NetBackup host. It also determines how frequently the NetBackup Certificate Revocation List (CRL) is refreshed on the host.

NetBackup certificates are deployed on hosts during installation (after the host administrator confirms the master server fingerprint) or with the nbcertcmd command. Choose a deployment level that corresponds to the security requirements of your NetBackup environment.

Note: During NetBackup certificate deployment on a NAT client, you must provide an authorization token irrespective of the certificate deployment security level that is set on the master server. This is because, the master server cannot resolve the host name to the IP address from which the request is sent.

For more information on NAT support in NetBackup, refer to the NetBackup Administrator's Guide, Volume I.

See "Using the Certificate Management utility to issue and deploy host ID-based certificates" on page 240.

See "Configuring the certificate deployment security levels" on page 246.

Table 8-7   Description of NetBackup certificate deployment security levels

Security level	Description	CRL refresh
Very High	An authorization token is required for every new NetBackup certificate request. See "Creating authorization tokens" on page 266.	The CRL that is present on the host is refreshed every hour. See "About the host ID-based certificate revocation list" on page 270.

Table 8-7   Description of NetBackup certificate deployment security levels
(continued)

Security level	Description	CRL refresh
High (default)	No authorization token is required if the host is known to the master server. A host is considered to be known to the master server if the host can be found in the following entities: 1 The host is listed for any of the following options in the NetBackup configuration file (Windows registry or the `bp.conf` file on UNIX): ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER For more details on the NetBackup configuration options, refer to the NetBackup Administrator's Guide, Volume I. 2 The host is listed as a client name in the `altnames` file (ALTNAMESDB_PATH). 3 The host appears in the EMM database of the master server. 4 At least one catalog image of the client exists. The image must not be older than 6 months. 5 The client is listed in at least one backup policy. 6 The client is a legacy client. This is a client that was added using the **Client Attributes** host properties. See "Creating authorization tokens" on page 266.	The CRL that is present on the host is refreshed every 4 hours.
Medium	The certificates are issued without an authorization token if the master server can resolve the host name to the IP address from which the request was originated.	The CRL that is present on the host is refreshed every 8 hours.

Configuring the certificate deployment security levels

Use the **NetBackup Administration Console** or the `nbcertcmd` command to configure the certificate deployment security level in the NetBackup domain.

These security levels are specific to NetBackup CA-signed certificates.

To configure the certificate deployment level using the NetBackup Administration Console

1   In the **NetBackup Administration Console**, expand **Security Management** and do one of the following:

   - Go to **Certificate Management**. From the **Actions** menu, select **Configure Security Settings**.

   - Go to **Global Security Settings**.

2   On the **Security level for certificate deployment** screen, slide the indicator to one of three levels: **Very High**, **High** (default), or **Medium**.

3   Click **OK**.

To configure the certificate deployment level using the command line

1   The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to log in:

   ```
   bpnbat -login -logintype WEB
   ```

   See "Web login requirements for nbcertcmd command options" on page 239.

2   Run the following command to view the current security level:

   ```
   nbcertcmd -getSecConfig -certDeployLevel -server
   master_server_name
   ```

3   Run the following command to change the security level:

   ```
   nbcertcmd -setSecConfig -certDeployLevel 0-2 -server
   master_server_name
   ```

   Where `0` is Very High, `1` is High (default), and `2` is Medium.

For information about `nbcertcmd`, see the NetBackup Commands Reference Guide.

Automatic host ID-based certificate deployment

A host ID-based certificate is automatically deployed on the NetBackup master server as part of NetBackup installation.

These certificates are deployed on other NetBackup hosts (after confirming the fingerprint) depending on the certificate deployment level.

The Certificate Authority (CA) on the NetBackup master server can accept or reject the certificate request depending on the certificate deployment level and the ability of the master server to verify the host information.

You can check the list of the deployed certificates on any NetBackup host by using the following command:

```
nbcertcmd -listCertDetails
```

When a certificate request is rejected, the host administrator must request the NetBackup administrator to generate and share an authorization token to deploy the certificate manually.

See "Creating authorization tokens" on page 266.

See "About NetBackup certificate deployment security levels" on page 244.

Deploying host ID-based certificates

Depending on the certificate deployment security level, a non-master host may require an authorization token before it can obtain a host ID-based certificate from the Certificate Authority (master server). When certificates are not deployed automatically, they must be deployed manually by the administrator on a NetBackup host using the nbcertcmd command.

The following topic describes the deployment levels and whether the level requires an authorization token.

See "About NetBackup certificate deployment security levels" on page 244.

Deploying when no token is needed

Use the following procedure when the security level is such that a host administrator can deploy a certificate on a non-master host without requiring an authorization token.

To generate and deploy a host ID-based certificate when no token is needed

1   The host administrator runs the following command on the non-master host to establish that the master server can be trusted:

```
nbcertcmd -getCACertificate
```

See "Setting up trust with the master server (Certificate Authority)" on page 251.

2   Run the following command on the non-master host:

```
nbcertcmd -getCertificate
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

Run the following command to get a certificate from a specific master server:

```
nbcertcmd -getCertificate -server master_server_name
```

3   To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Deploying when a token is needed

Use the following procedure when the security level is such that a host requires an authorization token before it can deploy a host ID-based certificate from the CA.

To generate and deploy a host ID-based certificate when a token is required

1   The host administrator must have obtained the authorization token value from the CA before proceeding. The token may be conveyed to the administrator by email, by file, or verbally, depending on the various security guidelines of the environment.

2   Run the following command on the non-master host to establish that the master server can be trusted:

```
nbcertcmd -getCACertificate
```

See "Setting up trust with the master server (Certificate Authority)" on page 251.

3   Run the following command on the non-master host and enter the token when prompted:

```
nbcertcmd -getCertificate -token
```

Note: To communicate with multiple NetBackup domains, the administrator of the host must request a certificate from each master server using the `-server` option.

If the administrator obtained the token in a file, enter the following:

```
nbcertcmd -getCertificate -file authorization_token_file
```

4   To verify that the certificate is deployed on the host, run the following command:

```
nbcertcmd -listCertDetails
```

Use the `-cluster` option to display cluster certificates.

Deploying host ID-based certificates in an asynchronous manner

Host ID-based certificates are automatically deployed on NetBackup hosts during installation or upgrade. For successful automatic certificate deployment, the host where the certificate needs to be deployed should be connected to the master server.

In certain scenarios, you may want to create, sign, and deploy host ID-based certificates in an asynchronous manner where the host and the master server do not need to be connected at the time of certificate deployment.

To deploy host ID-based certificate in an asynchronous manner

1 This command can be run only by the host administrator.

Create a certificate signing request. Run the following command on the non-master server host where you want to deploy the certificate:

```
nbcertcmd -createCertRequest -requestFile request_file_name
-server master_server_name
```

Optionally, copy the Certificate Signing Request (CSR) file to any NetBackup host.

2 Get a signed certificate from the master server on the host. An authorization token is mandatory. If the host already has a certificate, a reissue token is required.

Run the following command on the host:

```
nbcertcmd -signCertificate -requestFile request_file_name
-certificateFile certificate_file_name -token
```

3 Copy the signed certificate that is generated in step 2 and provide it to the host administrator.

4 This command can be run only by the host administrator.

To deploy the signed certificate on the host, run the following command on the client:

```
nbcertcmd -deployCertificate -certificateFile
certificate_file_name
```

Implication of clock skew on certificate validity

When a master server issues a certificate, it determines for how long the certificate will be valid for the host to use. The master server sets the validity of the certificate based on its own time, recording two timestamps: **Not before** and **Not after**. The certificate is valid only between these two timestamps.

The clock on the master server and the clock on the host that will receive the certificate should be in sync so that the certificate is valid for as long as is expected, given the timestamps.

The hosts can reside in different time zones, as long as the clock on each host is set to the correct time for that host's timezone. As a general practice, NetBackup recommends using a service such as Network Time Protocol (NTP) to automatically keep all clocks on all hosts in the NetBackup domain synchronized.

If the clocks are not in sync, the difference can result in the following consequences:

- If the host clock is ahead of the master server, the validity period of the certificate will be less than expected on that particular host. If the difference is extreme and the clocks vary by more than the certificate's validity period, it is possible that if the master server issued a fresh certificate, it could be treated as expired.

- If the host clock is behind the master server, a fresh certificate issued by the master server could be considered as unusable by the host because the host considers the certificate as not yet valid.

To determine whether the master server clock and the host clock are in sync

1 Run the following command on the host to determine whether the host clock is in sync with the master server clock:

   ```
   nbcertcmd -checkClockSkew -server master_server_name
   ```

2 The command returns one of the following results:

   - If both clocks are in sync, the following displays:

     ```
     The current host clock is in sync with the master server.
     ```

   - If the current host is behind the master server, the command reports the difference in seconds:

     ```
     The current host clock is behind the master server by 36
     seconds(s).
     ```

   - If the current host is ahead of the master server, the command reports the difference in seconds:

     ```
     The current host clock is ahead of the master server by 86363
     second(s).
     ```

   - If the command is run on the master server, the command skips the check and displays the following:

     ```
     Specified server is same as the current host. Clock skew check
     is skipped.
     ```

   If the clock skew on the host is causing a problem with the certificate validity, take corrective actions as necessary.

Setting up trust with the master server (Certificate Authority)

Each NetBackup host must first trust the NetBackup master server, which acts as the Certificate Authority (CA). Trust is essential so that the host can request a host ID-based certificate. The CA certificate can be used to authenticate other hosts in the domain, and is stored in the trust store of each host. Setting up trust involves requesting a certificate from the master server.

See "Automatic host ID-based certificate deployment" on page 246.

Adding a CA certificate to a host's trust store

Run the `nbcertcmd -listCACertDetails` command to see the list of CA certificates that are in the host's trust store. The output displays all of the master servers that the host already trusts.

To establish trust with the master server (CA)

1   The host administrator must have the Root Certificate Fingerprint that was communicated to them through an authentic source. The source was most likely the master server administrator, who communicated the fingerprint by email, by file, or on an internal website. The following topic describes that process:

2   From the NetBackup host, run the following command:

```
nbcertcmd -getCACertificate -server master_server_name
```

3   In the confirmation output, enter **y** to proceed.

For example:

```
nbcertcmd -getCACertificate -server master1
Authenticity of root certificate cannot be established.
The SHA1 fingerprint of root certificate is B8:2B:91:E1:4E:78:D2:
25:86:4C:29:C5:92:16:00:8D:E8:2F:33:DD.
```

Note: The fingerprint that is displayed must match the Root Certificate Fingerprint that the host administrator has received from the master server administrator. Enter **y** to give consent to add the CA certificate to the trust store of the host.

```
Are you sure you want to continue using this certificate ? (y/n): y
The validation of root certificate fingerprint is successful.
CA certificate stored successfully.
```

4   Next, the administrator performs the following task:

For information about this command, see the NetBackup Commands Reference Guide.

Adding a CA certificate via message in the NetBackup Administration Console

The **NetBackup Administration Console** and the **Backup, Archive, and Restore** user interfaces communicate with NetBackup hosts (master server, media server, or client) over a secure channel. NetBackup secures this channel using a NetBackup host ID-based or a host name-based security certificate that the NetBackup Certificate Authority (CA) issues.

Figure 8-1 displays in the **NetBackup Administration Console** in the following situation: A user is running the **NetBackup Administration Console** on a NetBackup host. The user tries to connect to another NetBackup host (a target host) using the **NetBackup Administration Console**. However, the CA that issued the security certificate to the target host is not in the trust store of the host where the user launched the console.

Figure 8-1   Message inquiring whether to add a Certificate Authority (CA) to the trust store

To verify the CA fingerprint that the dialog displays, see the following topic:

See "Finding and communicating the fingerprint of the certificate authority" on page 254.

If the user selects **Yes** in this message, the CA is added to the trust store of the host where the console is running. This host will then trust all hosts that have a certificate signed by the CA that is listed in the message.

Finding and communicating the fingerprint of the certificate authority

The master server administrator must find the fingerprint of the CA certificate and communicate it to the administrator of the individual host so that the host can add the CA certificate to its trust store.

To find the fingerprint of the CA certificate

1   The master server administrator can find the fingerprint using the **NetBackup Administration Console** or the command line:

Using the **NetBackup Administration Console**:

- Expand **Security Management > Certificate Management**.

- On the **Actions** menu, select **View Certificate Authority**. The **Certificate Authority Details** dialog appears.

Certificate Authority Details   ✕
Subject Name: O=vx, OU=root@cayce.rm.com. CN=nbatd
Start Date: Sep 16, 2016 11:37:58 AM
Expiry Date: Sep 11, 2036 12:52:58 PM
Fingerprint: C3:5E:2E:21:78:DF:47:0D:FF:6A:45:7A:0E:7F:1B:98:B1:F2:92:CA
[Copy Fingerprint to Clipboard]   [Close]

The **Copy Fingerprint to Clipboard** option is available to help the administrator communicate the fingerprint to the host administrator.

Using the command line:

- Run the following command on the master server to view the Root Certificate Fingerprint:

```
nbcertcmd -listCACertDetails
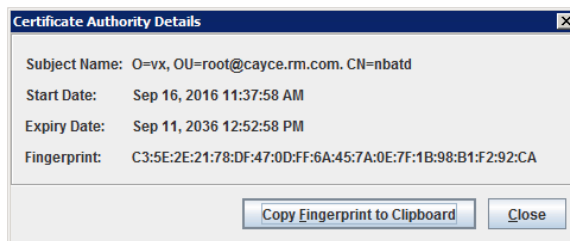

     Subject Name : /CN=nbatd/OU=root@cayce.rm.com/O=vx
       Start Date : Sep 16 10:37:58 2016 GMT
      Expiry Date : Sep 11 11:52:58 2036 GMT
  SHA1 Fingerprint : C3:5E:2E:21:78:DF:47:0D:FF:6A:45:7A:0E:
                     7F:1B:98:B1:F2:92:CA
```

If multiple CA certificates are displayed, use the **Subject Name** to identify the certificate for the desired master.

2   The master server administrator communicates the fingerprint to the host administrator by email, by file, or on an internal web site.

The host administrator uses this fingerprint to verify the fingerprint that displays when the host runs `nbcertcmd -getCACertificate`.

Using the vssat command to view the CA certificate fingerprint

The `vssat` command can also be used to view the CA certificate fingerprint. Use `vssat` with the following options:

`vssat showcred -p nbatd`

However, note the following differences between using `nbcertcmd -listCACertDetails` and `vssat`:

- `vssat` displays the fingerprint as a hash and does not include colon separators.

- If the host trusts multiple Certificate Authorities, the `nbcertcmd` command displays all CA certificates. The **Subject Name** displays the identity of the CA.

Forcing or overwriting certificate deployment

In some situations it may be necessary to use the `-force` option with the `nbcertcmd -getCertificate` command. For example, to force certificate deployment to a host or to overwrite the existing host ID-based certificate information and fetch a new certificate.

Forcing certificate deployment

A host may already have a host ID-based certificate, but needs to overwrite the old certificate with a new one. This is required, for example, when a master server is replaced with a new server. Since the clients have the old certificate to the old server, when the `nbcertcmd -getCertificate` command is run on the clients, it fails with the following error:

`Certificate already exists for the server.`

Use the following procedure to overwrite the existing host ID-based certificate information and fetch a new certificate.

To force certificate deployment on a host

◆   The host administrator runs the following command on the non-master host:

`nbcertcmd -getCertificate -server `*`master_server_name`*` -force`

- Depending on the security setting on the master server, a token may also need to be specified.
  See "Creating authorization tokens" on page 266.

- Use the `-cluster` option to deploy a cluster certificate.

Overwrite the existing host ID-based certificate information and fetch a new certificate

A host may have been issued a certificate, but over time the certificate has become corrupted or the certificate file has been deleted.

The administrator of the non-master host can run the following command to confirm the condition of the certificate:

```
nbcertcmd -listCertDetails
```

- If the certificate is corrupt, the command fails with the following error:
  ```
  Certificate could not be read from the local certificate store.
  ```

- If no certificate details display, the certificate is not available.

Use the following procedure to overwrite the existing host ID-based certificate information and to fetch a new certificate.

To fetch a new host ID-based certificate

◆ The host administrator runs the following command on the non-master host:

```
nbcertcmd -getCertificate -force
```

- Depending on the security setting on the master server, a token may also need to be specified.
  See "Creating authorization tokens" on page 266.

- Use the `-cluster` option to deploy a cluster certificate.

Retaining host ID-based certificates when reinstalling NetBackup on non-master hosts

Administrators may want to uninstall NetBackup from a host, and then perform a clean installation on the same host. See the following procedure for instructions on how to retain the identity of a host through the uninstall/reinstall process.

To retain host ID-based certificates when reinstalling NetBackup

1   Stop all NetBackup services on the host.

2   Back up the following directories:

On Windows:

Install_path\NetBackup\var\VxSS

Install_path\NetBackup\var\webtruststore

On UNIX:

/usr/openv/var/vxss

/usr/openv/var/webtruststore

3   Where NetBackup Cluster Server is used, also back up the following directories:

Shared_disk\var\global\vxss

Shared_disk\var\global\webtruststore

4   Reinstall NetBackup on the host.

5   Restore the data that was backed up in step 2 and step 3.

Deploying certificates on a client that has no connectivity with the master server

NetBackup can detect whether a host has connectivity with the master server or not. If there is no connectivity, NetBackup automatically attempts to use the built-in HTTP tunnel on a media server to route the connection request to the master server.

If NetBackup cannot automatically detect the host connectivity with the master server or find an appropriate media server to route the connection request, you need to manually configure the HTTP tunnel options.

See "About the communication between a NetBackup client located in a demilitarized zone and a master server through an HTTP tunnel" on page 289.

To deploy a certificate on a client that has no connectivity with the master server, refer to the following topic:

See "Deploying host ID-based certificates" on page 247.

Note: As the request is routed via a different host, the master server cannot validate the authenticity of the certificate request, therefore an authorization token is a must.

About host ID-based certificate expiration and renewal

NetBackup host ID-based certificates expire one year after their issue date. They are automatically renewed 180 days before the expiration date. A certificate renewal request is sent periodically until a certificate is successfully renewed. Automatic renewal ensures that the renewal process is transparent to the users.

Note: You can disable automatic renewal of host-ID based certificates using the `DISABLE_CERT_AUTO_RENEW` parameter from the NetBackup configuration file (the Windows registry or the `bp.conf` file on UNIX).

For more information, see the *NetBackup Administrator's Guide, Volume I*.

http://www.veritas.com/docs/DOC5332

The renewal request is always authenticated using the existing certificate. Hence, the renewal process does not require the use of an authorization token, regardless of the certificate deployment security level.

If the existing certificate has not expired, the host administrator can initiate a manual renewal request, as described in the following procedure.

To renew a host ID-based certificate manually

◆ The host administrator runs the following command on the non-master host:

```
nbcertcmd -renewCertificate
```

- Certificates corresponding to NetBackup domains other than the primary domain can be manually renewed by specifying the `-server` option.

- Use the `-cluster` option to renew the cluster certificate of NetBackup clustered server.

In a scenario where the certificate has expired, the administrator of the host must manually reissue the certificate.

See "About reissuing host ID-based certificates" on page 261.

Deleting sensitive certificates and keys from media servers and clients

In the cloning process, use the following command to remove certain sensitive certificates and keys from NetBackup media servers and clients in the following scenarios:

- Run the command on the cloned virtual machine, which is cloned from an active NetBackup host.

- Run the command before creating a gold image of a virtual machine for cloning.

```
nbcertcmd -deleteAllCertificates
```

Note: This command is allowed only on media servers and clients. The command is not allowed on master servers.

This operation deletes or shreds the appropriate sensitive information (certificates and keys) from the following locations:

On Windows:

- `C:\Program Files\Veritas\NetBackup\var\VxSS\certmapinfo.json`

- `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\<certificate>`
  For example:
  `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\`
  `6d92d4dd-ed2d-43de-adb1-bf333aa2cc3c`

- `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\keystore\PrivKeyFile.pem`
  (shredded)

- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\<certificate>`
  For example:
  `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\`
  `certstore\9345b05e-lilycl2nb!1556!nbatd!1556.0`

- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PrivKeyFile.pem`
  (shredded)

- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PubKeyFile.pem`

On UNIX:

- `/usr/openv/var/vxss/certmapinfo.json`

- `/usr/openv/var/vxss/credentials/<certificate>`
  For example:
  `/usr/openv/var/vxss/credentials/`
  `f4f72ef3-2cfc-42a4-ab5a-65fd09e8b63e`

- `/usr/openv/var/vxss/credentials/keystore/PrivKeyFile.pem` (shredded)

- `/var/vxss/at/root/.VRTSat/profile/certstore/<certificate>`

- `/var/vxss/at/root/.VRTSat/profile/certstore/keystore/PubKeyFile.pem`

- `/var/vxss/at/root/.VRTSat/profile/certstore/keystore/PrivKeyFile.pem`
  (shredded)

Cleaning host ID-based certificate information from a host before cloning a virtual machine

Cloning a virtual machine can present the opportunity for identity theft. Multiple hosts should not have the same key pair. This procedure ensures that each copy of the host gets a unique key pair and identity.

Perform the following procedure before cloning a virtual machine (or before creating a gold image of a machine for cloning) if it is a one-time operation.

To clean the host ID-based certificate information from a host before cloning

1   Stop all NetBackup services on the host.

2   Delete all files and directories from the following locations:

On Windows:

`Install_path\NetBackup\var\VxSS\at\*`

`Install_path\NetBackup\var\VxSS\credentials\*`

`Install_path\NetBackup\var\webtruststore\*`

On UNIX:

`/usr/openv/var/vxss/at/*`

`/usr/openv/var/vxss/credentials/*`

`/usr/openv/var/webtruststore/*`

3   Delete the following file:

On Windows: `Install_path\NetBackup\var\VxSS\certmapinfo.json`

On UNIX: `/usr/openv/var/vxss/certmapinfo.json`

4   Where NetBackup Cluster Server is used, perform the following steps in addition:

5   Delete all files and directories from the following locations:

`Shared_disk\var\global\vxss\at\*`

`Shared_disk\var\global\vxss\credentials\*`

`Shared_disk\var\global\webtruststore\*`

6 Delete the following file:

Shared_disk\var\global\vxss\certmapinfo.json

7 Proceed to clone the virtual machine.

About reissuing host ID-based certificates

A certificate must be reissued in any of the following cases:

- The certificate was revoked, and you later determine that you can trust that host again.

- The certificate expired.

- NetBackup was reinstalled on the host where a certificate was already issued.

- The name of the host was changed.

- The key pair for the host was changed.

Reissuing a certificate is one way to prevent malicious users from assuming the identity of an existing NetBackup host that is already registered with the NetBackup master server. In most cases, a reissue token is required for certificate reissue.

- Reissuing a host ID-based certificate for a NetBackup host is different from deploying the certificate for the first time. Use the following procedure to reissue a certificate.
  See "Creating a reissue token" on page 261.

- Once a reissue token is obtained, the certificate reissue process is similar to manual certificate deployment with an authorization token.
  See "Deploying host ID-based certificates" on page 247.

When the master server receives a certificate reissue request, it first revokes all the previously valid certificates for that host and then generates a new certificate when required.

Creating a reissue token

A host ID-based certificate can be reissued if the non-master host is already registered with the master server but its host ID-based certificate is no longer valid. For example, a certificate is not valid when it has expired, is revoked, or is lost.

A reissue token is a type of token that can be used to reissue a certificate. It is a special type of token because it retains the same host ID as the original certificate. Since a reissue token is bound to a specific host, the token cannot be used to request certificates for additional hosts.

To create a reissue a token using the NetBackup Administration Console

1   In the **NetBackup Administration Console**, expand **Security Management**.

2   Select the **Certificate Management** or **Host Management** node.

3   In the right pane, select the host that requires a reissue token.

4   From the **Actions** menu, select **Generate Reissue Token**.

5   In the **Create Reissue Token** dialog, enter a name for the token.

6   Select a date for token validity from the **Valid until** option.

7   In the **Reason** field, enter a reason for the reissue token. The reason appears in the log as an audit event.

8   Click **Create**.

9   The reissue token appears in a dialog. Select **Copy** to save the token value to the clipboard.

10 Convey the token value to the administrator of the non-master host. How the token is conveyed depends on various security factors in the environment. The token may be transmitted by email, by file, or verbally.

   The administrator of the non-master host deploys the token to obtain another host ID-based certificate. See the following topic for instructions:

   See "Deploying host ID-based certificates" on page 247.

To create a reissue a token using the nbcertcmd command

1 The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to login:

```
bpnbat -login -logintype WEB
```

See "Web login requirements for nbcertcmd command options" on page 239.

2 Run one of the following commands on the master server:

Use the host name for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

Note: You must provide the primary name of the host for which you want to reissue the certificate. If you provide any of the host ID-to-host name mappings that are added for the host, the certificate cannot be reissued.

Use the host ID for which the certificate needs to be reissued:

```
nbcertcmd -createToken -name token_name -reissue -hostId host_id
```

Additional parameters can be used to indicate validity duration and the reason for creation.

For information about the nbcertcmd command, see the NetBackup Commands Reference Guide.

Additional steps to request a certificate for a renamed NetBackup host

In addition to reissuing a token, the following steps are required to request a certificate for a renamed NetBackup host.

To request a certificate for a host after a host name change

1 The NetBackup administrator of the master server generates a reissue token for the renamed NetBackup host.

2 Add the new host name as one of the approved host ID-to-host name mappings by using **NetBackup Administration Console**.

See "Adding host ID to host name mappings" on page 214.

Alternatively, you can use the nbhostmgmt -add command-line interface option.

For more information about the nbhostmgmt command, see the NetBackup Commands Reference Guide.

3   The NetBackup administrator must revoke the host ID-based certificate for the renamed host.

See "Revoking a host ID-based certificate" on page 274.

Note: After the certificate is revoked, the host is unable to communicate with the NetBackup Web Management Console service (`nbwmc`). When the host obtains a new certificate using the reissue token, the host can communicate with `nbwmc` again.

---

4   After the certificate is revoked, the administrator of the non-master host must use the reissue token to get a certificate for the renamed host.

See "Deploying host ID-based certificates" on page 247.

Changing the key pair for a host

Consider changing a key pair only if a key is compromised or leaked. Changing a key pair results in both a new host ID-based certificate and a new host name-based certificate.

The following procedure describes changing a key pair for a host, and then getting a new certificate using the new key pair.

Do not perform the procedure for a master server, only a non-master server host.

To change a key pair for a host

1   The NetBackup host administrator backs up the following directories:

On Windows: *Install_path*\NetBackup\var\VxSS\at\systemprofile

On UNIX: /usr/openv/var/vxss/at/root

2   The NetBackup host administrator removes the directory from the host.

3   Restart the NetBackup services on the host.

4   The master server administrator performs the following steps:

- Log in to the NetBackup Web Management Service:
  bpnbat -login -logintype WEB
  See "Web login requirements for nbcertcmd command options" on page 239.

- Revoke the host ID-based certificate:
  nbcertcmd -revokeCertificate -host *host_name*

- Generate a reissue token for the NetBackup host where the key pair is to be changed.
  See "Creating a reissue token" on page 261.

- Deploy a new host name-based certificate:

  ```
  bpnbaz –ProvisionCert host_name
  ```

5 The NetBackup host administrator uses the reissue token to deploy a new host ID-based certificate with an updated key pair.

Use the following command to enter the token directly:

```
nbcertcmd -getCertificate -force -token
```

Use the following command if the token is in a file:

```
nbcertcmd -getCertificate -force -file /directory/token_file
```

6 If the host has more than one master server, repeat the process beginning at step 4 for each master server.

7 Restart the NetBackup services on the NetBackup host where the key was changed.

About Token Management for host ID-based certificates

Master server administrators use the **Token Management** utility to perform the following tasks:

- Create new authorization tokens
  Depending on the security level, an authorization token may be required for a non-master NetBackup host to obtain a host ID-based certificate. The NetBackup administrator of the master server generates the token and shares it with the administrator of the non-master host. That administrator can then deploy the certificate without the presence of the master server administrator.
  See "Creating authorization tokens" on page 266.

- Delete authorization tokens
  See "Deleting authorization tokens" on page 268.

- View authorization token details
  See "Viewing authorization token details" on page 268.

- Clean up invalid or expired authorization tokens
  See "About expired authorization tokens and cleanup" on page 269.

Creating authorization tokens

Depending on the certificate deployment security setting, NetBackup hosts may require an authorization token to obtain a host ID-based certificate from the Certificate Authority (master server).

See "Creating a reissue token" on page 261.

- If the security setting is **Very High**, all certificate requests require a token. Perform the procedure that is described in this topic.

- If the security setting is **High**, certificates are automatically deployed to hosts that are known to the master server. If the host is not known to the master server, the certificate must be deployed using an authorization token. In that case, perform the procedure that is described in this topic.
  To understand what it means to be known to the master server, see the following topic:
  See "About NetBackup certificate deployment security levels" on page 244.

- If the security setting is **Medium**, this procedure may be less likely because certificates are automatically deployed to all hosts that request one. However, the master server must be able to cross verify the IP and host name of the host that is requesting a certificate.

Note: A token is required to request a certificate on behalf of a host that has no connectivity with the master server.

See "Deploying certificates on a client that has no connectivity with the master server" on page 257.

Note: Do not use this procedure to create an authorization token for a NetBackup host whose current certificate is not in a valid state because it is lost, corrupt, or expired. In these cases, a reissue token must be used.

See "About reissuing host ID-based certificates" on page 261.

The NetBackup administrator of the master server can use the **NetBackup Administration Console** or the command line to create the token.

To create a token using the NetBackup Administration Console

1   In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management** > **Token Management**.

2   On the **Actions** menu, select **New Token**.

    The **Create Token** dialog box is displayed.

3   Enter a unique and meaningful name for the token. The field cannot be left
blank.

For example, to create a token to request certificates for multiple hosts that
belong to master_server_1, name the token Token1_MS1. A good practice is
to write a useful description in the **Reason** field for the token.

4   Enter a number for the **Maximum Uses Allowed** option for the number of
times the token can be used. The default is 1, which indicates that one host
can use the token one time.

To use the same token for multiple hosts, enter any value between 1 and
99999. For example, to use the token for 8 hosts, enter 8. The ninth host that
attempts to use the token will not succeed.

5   Use the **Valid for** option to indicate how long the token can be used before it
is invalid and cannot be used. After the **Valid for** date, the master server must
generate another token.

Select a period between 1 and 999 hours or days.

6   Optionally, enter the reason for creating the token. The reason appears in the
audit logs, along with the other entries in the dialog.

7   Select **Create**.

8   The new token appears in a dialog. Select **Copy** to save the token value to
the clipboard.

9   Convey the token value to the administrator of the non-master host. How the
token is conveyed depends on various security factors in the environment. The
token may be transmitted by email, by file, or verbally.

10 The administrator of the non-master host uses the token to obtain a host
ID-based certificate from the Certificate Authority. See the following procedure
for instructions:

See "Deploying host ID-based certificates" on page 247.

To create a token using the nbcertcmd command

◆ Run the following command on the host:

`nbcertcmd -createToken -name *token_name*`

For example:

`nbcertcmd -createToken -name testtoken`

`Token FCBVYUTDUIELUDOE created successfully.`

Additional parameters can be used to indicate maximum uses, validity duration, and the reason for creation.

For information about the `nbcertcmd` command, see the NetBackup Commands Reference Guide.

Deleting authorization tokens

Use the **NetBackup Administration Console** or the command line to delete specific authorization tokens. A token can be deleted even though it has not expired and the **Maximum Uses Allowed** count has not yet been exhausted.

To delete a token using the NetBackup Administration Console

1 In the **NetBackup Administration Console**, expand **Security Management > Certificate Management > Token Management**.

2 In the right pane, select the token to be deleted.

3 Select **Edit > Delete**.

4 Click **Yes** in the confirmation dialog box to delete the token.

To delete a token using the command line

◆ Run the `nbcertcmd -deleteToken` command (with additional parameters).

For information about the `nbcertcmd` command, see the NetBackup Commands Reference Guide.

Viewing authorization token details

Details for each authorization token can be viewed in the **NetBackup Administration Console** or from the command line.

To view token details using the NetBackup Administration Console

1 In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management** > **Token Management**.

2 The token details are displayed in the right pane.

2 Token Records (0 selected)					Search	
Token State	Name	Maximum Uses Allowed	Uses Remaining	Valid From	NetBackup Host ID	Time Remaining Until Expiry
Not Valid	MasterServerInstallationToken_1473830907937	2		1 Sep 14, 2016 10:58:29 AM		
Valid	azaaaa	1		1 Sep 14, 2016 1:30:06 PM		17 hour(s) 46 minute(s)

To view token details using the nbcertcmd command

◆ On the master server, run the `nbcertcmd -listToken` command (with additional parameters) to view the token details.

The token details are displayed.

For information about the `nbcertcmd` command, see the NetBackup Commands Reference Guide.

About expired authorization tokens and cleanup

An authorization token expires in either of the following situations (whichever happens first):

■ When the current date-time combination is later than the token's **Valid for** amount.

■ When the token is used for **Maximum Uses Allowed** requests.

An expired authorization token remains in the token database, but cannot be used to authorize certificate deployment requests.

Expired tokens can be deleted one by one, or they can be cleaned up all at once by using the **Cleanup** operation. The **Cleanup** operation deletes all expired tokens from the token database.

To clean up expired authorization tokens using the NetBackup Administration Console

1 In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management** > **Token Management**.

2 On the **Actions** menu, select **Cleanup**.

3 Click **Yes** in the confirmation dialog box to clean up all expired tokens and delete them from the token database.

To clean up tokens using the command line

◆ Use the `nbcertcmd -cleanupToken` command to delete all the expired tokens.

About the host ID-based certificate revocation list

The NetBackup certificate revocation list (CRL) is a list of host ID-based digital security certificates that have been revoked before their expiration date. The hosts that own revoked certificates should no longer be trusted.

The NetBackup certificate revocation list conforms to the Certificate Revocation List profile that the Internet Engineering Task Force publishes in RFC 5280 at https://www.ietf.org. The NetBackup certificate authority signs the CRL. The NetBackup master server is the certificate authority. The CRL is public and does not require secure transmission. The CRL endpoint is open, free for anyone to access.

Every NetBackup host must have a valid security certificate and a valid CRL so that it can communicate with other NetBackup hosts.

How often NetBackup generates a new CRL

The NetBackup master server generates a new CRL as follows:

- On startup.

- Sixty minutes since the CRL was last generated.

- NetBackup checks every 5 minutes for a newly revoked certificate. It can take NetBackup up to 5 minutes to update the web server after a certificate is revoked.

A CRL expires after 7 days.

How often a NetBackup host gets a CRL

A NetBackup host obtains a CRL when NetBackup is installed on the host. A NetBackup host also obtains a fresh CRL during an upgrade of the NetBackup software.

After installation or upgrade, each host requests a new CRL on a time interval since the host was started. (NetBackup uses a pull method to refresh host CRLs.) The NetBackup master server certificate deployment security level determines the time interval, as shown in the following table.

Table 8-8   CRL refresh interval

Security level	CRL refresh interval
Very high	Hourly
High	4 hours
Medium	8 hours

See "About NetBackup certificate deployment security levels" on page 244.

You can get a new CRL before its scheduled refresh period.

See "Refreshing the CRL on the master server" on page 271.

See "Refreshing the CRL on a NetBackup host" on page 271.

For more information

See "Overview of security certificates in NetBackup" on page 206.

See "About host ID-based certificates" on page 239.

See "About revoking host ID-based certificates" on page 272.

Refreshing the CRL on the master server

Use the following procedure to refresh the CRL on the master server. The procedure gets the current CRL from the NetBackup certificate authority and copies it to the master server. If a host in the environment was recently revoked, you must wait up to 5 minutes before the CRL reflects that the host was revoked.

See "About the host ID-based certificate revocation list" on page 270.

To refresh the CRL on the master server

1 Log in to the master server as an administrator.

For a clustered master server, log in to the active node.

2 For a clustered master server, run the following command:

```
nbcertcmd -getCRL -cluster [-server master_server_name]
```

To get a CRL from a NetBackup domain other than the default, specify the `-server master_server_name` option and argument.

3 Run the following command:

```
nbcertcmd -getCRL [-server master_server_name]
```

Refreshing the CRL on a NetBackup host

Use the following procedure to refresh the CRL on a NetBackup host. The procedure gets the current CRL from the NetBackup certificate authority and copies it to the local host. If a host in the environment was recently revoked, you must wait up to 5 minutes before the CRL reflects that the host was revoked.

See "About the host ID-based certificate revocation list" on page 270.

To refresh the CRL on a NetBackup host

1 Log on as an administrator on the NetBackup host that requires a fresh CRL.

2 Run the following command:

```
nbcertcmd -getCRL [-server master_server_name]
```

To get a CRL from a NetBackup domain other than the default, specify the `-server master_server_name` option and argument.

About revoking host ID-based certificates

When you revoke a NetBackup digital security certificate, NetBackup revokes any other certificates for that host. NetBackup ceases to trust the host, and it no longer can communicate with other NetBackup hosts.

If you revoke a certificate by using the **NetBackup Administration Console**, you must select one of the following reasons:

Affiliation Changed	The host changes affiliation to a different NetBackup domain.
CA Compromise	The certificate authority is compromised.
Cessation of Operation	The host ceases to be a NetBackup host. For example, you decommission a NetBackup media server or client.
Key Compromise	The certificate key is compromised.
Superseded	A new certificate supersedes the certificate to be revoked.
Unspecified	Other, unspecified reasons. Perhaps you want to suspend privileges temporarily while you investigate a security event.

If you revoke a certificate and later determine that you can trust the host, provision a new certificate on that host. You do so by using a reissue token.

See "About reissuing host ID-based certificates" on page 261.

Note: Do not revoke a certificate of the master server. If you do, NetBackup operations may cease.

After you revoke a host's certificate, you should consider doing the following actions in NetBackup:

- Remove the host from backup policies.

- For a NetBackup media server, deactivate it.

You should also consider any actions that are not related to NetBackup to ensure that someone with malicious intent cannot use the certificate and key.

See "About the host ID-based certificate revocation list" on page 270.

Removing trust between a host and a master server

A NetBackup host can trust multiple Certificate Authorities (master servers) at any time. For various reasons, it may be necessary for a NetBackup host to remove trust from a master server that previously had been trusted.

For example, if a NetBackup client is moved from one master server to another, it is advisable to remove trust from the first master server. Security best practices suggest trusting the fewest entities required to function correctly. Also, if a NetBackup host no longer needs to communicate with hosts from a specific NetBackup domain, remove the CA certificate for that master from the trust store of the host.

Note: Removing a CA certificate does not remove the host ID-based or host name-based certificates that the host may have obtained from that CA. The `nbcertcmd -listCertDetails` continues to show the host ID-based certificate.

When the CA certificate is removed from a host, the host ID-based certificate issued by that CA will not automatically renew because the host no longer trusts the CA. The host ID-based certificate eventually expires.

Removing trust between a host and a master server

1 The administrator of the non-master host runs the following command on the host to determine the CA certificate fingerprint of the master server:

```
nbcertcmd -listCACertDetails
```

In this example output, the host has certificates from two master servers:

```
nbcertcmd -listCACertDetails
      Subject Name : /CN=nbatd/OU=root@master1.abc.com/O=vx
        Start Date : Aug 23 14:16:44 2016 GMT
       Expiry Date : Aug 18 15:31:44 2036 GMT
  SHA1 Fingerprint : 7B:0C:00:32:96:20:36:52:92:E8:62:F3:56:
74:8B:E3:2E:4F:22:4C


      Subject Name : /CN=nbatd/OU=root@master2.xyz.com/O=vx
        Start Date : Aug 25 12:09:55 2016 GMT
       Expiry Date : Aug 20 13:24:55 2036 GMT
  SHA1 Fingerprint : 7A:C7:6E:68:71:6B:82:FD:7E:80:FC:47:F6:
8D:B2:E1:40:69:9C:8C
```

2 The administrator wants to remove trust to the second master server and runs the following command on the host:

```
nbcertcmd -removeCACertificate -fingerprint 7A:C7:6E:68:71:
6B:82:FD:7E:80:FC:47:F6:8D:B2:E1:40:69:9C:8C
```

Include the entire fingerprint, including the colons.

Warning: This command removes the CA certificate from the trust store. The trust store is referred to by NetBackup services and by the NetBackup Web Management Console service (`nbwebsvc`).

---

3 The **NetBackup Administration Console** on the master server displays the certificate state as **Active**. However, that certificate does not automatically renew and eventually expires. The NetBackup administrator should revoke the certificate of the host if the host is no longer going to be part of the NetBackup domain.

Revoking a host ID-based certificate

NetBackup administrators may consider revoking a host ID-based certificate under various conditions. For example, if the administrator detects that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled

from the host. A revoked certificate cannot be used to communicate with master server web services.

Security best practices suggest that the administrator explicitly revoke the certificates for any host that is no longer active, regardless of whether the certificate is still deployed on the host, or whether it has been successfully removed from the host.

Note: Do not revoke a certificate of the master server. If you do, NetBackup operations may cease.

To revoke a host ID-based certificate using the NetBackup Administration Console

1   In the **NetBackup Administration Console**, expand **Security Management** > **Certificate Management**.

2   Select the certificate to be revoked.

3   On the **Actions** menu, select **Revoke Certificate**.

4   Select a reason from the drop-down menu and click **Continue**.

The certificate is revoked.

5   After you revoke a host's certificate, do the following actions in NetBackup:

  ■   Remove the host from backup policies.

  ■   For a NetBackup media server, deactivate it.

To revoke a host ID-based certificate using the command line

1   The master server administrator must be logged in to the NetBackup Web Management Service to perform this task. Use the following command to log in:

```
bpnbat -login -logintype WEB
```

2   Run one of the following commands to revoke the certificate using the host name or the host ID.

Revoke using the host name:

```
nbcertcmd -revokeCertificate -host host_name
```

Note: You must provide the primary name of the host for which you want to revoke the certificate. If you provide any of the host ID-to-host name mappings that are added for the host, the certificate cannot be revoked.

Revoke using the host ID:

```
nbcertcmd -revokeCertificate -hostID host_id
```

Additional parameters can be used to indicate a revocation reason code and the master server.

3   After you revoke a host's certificate, do the following actions in NetBackup:

- Remove the host from backup policies.

- For a NetBackup media server, deactivate it.

Note: Revoking a certificate does not delete the certificate from the local store of the non-master host.

Determining a NetBackup host's certificate state

If NetBackup CA-signed certificate is used

You can determine the state of a NetBackup certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems. Three methods exist to determine a certificate state, as follows:

Verify a host certificate from the host itself	The method uses the NetBackup `nbcertcmd` command. See "To verify the host's certificate state from the host" on page 277.
Verify a host certificate from a NetBackup server	The method uses the NetBackup `bptestbpcd` command. See "To verify from a NetBackup server if a different host's certificate is revoked" on page 278.

Verify a host certificate from the **NetBackup Administration Console**	See "To verify a host's certificate using the NetBackup Administration Console" on page 278.

To verify the host's certificate state from the host

1 Optionally, on the NetBackup host run the following command as an administrator to get the most recent certificate revocation list:

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -getCRL [-server` *master_server_name*]

Windows: *install_path*`\NetBackup\bin\nbcertcmd -getCRL [-server` *master_server_name*]

To get a CRL from a NetBackup domain other than the default, specify the `-server` *master_server_name* option and argument.

2 On the NetBackup host, run the following command as an administrator:

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]` `[-server` *master_server_name*]

Windows: *install_path*`\NetBackup\bin\nbcertcmd -hostSelfCheck` `[-cluster] [-server` *master_server_name*]

Use one or both of the following options if necessary:

`-cluster`	Use this option on the active node of a NetBackup master server cluster to verify the certificate of the virtual host.
`-server`	Use this option with the *master_server_name* argument to verify a certificate from a master server other than the default.

3 Examine the command output. The output indicates that either the certificate is or is not revoked.

To verify from a NetBackup server if a different host's certificate is revoked

1 As an administrator on the NetBackup master server or a NetBackup media server, run the following command:

UNIX: `/usr/openv/netbackup/bin/admincmd/bptestbpcd –host` *hostname* `-verbose`

Windows: *install_path*`\NetBackup\bin\bptestbpcd -host` *hostname* `-verbose`

For `-host` *hostname*, specify the host for which you want to verify the certificate.

2 Examine the command output. If the certificate on the specified host is revoked, the command output includes the string `The Peer Certificate is revoked`. If the command output does not include that string, the certificate is valid.

To verify a host's certificate using the NetBackup Administration Console

1 In **NetBackup Administration Console**, expand **Security Management** > **Certificate Management**.

2 For the host of interest, examine the **Certificate State** column for state of the certificate.

If external CA-signed certificate is used

You can determine the state of an external CA-signed host certificate: Active or Revoked. Doing so may help troubleshoot connection and communication problems.

Two methods exist to determine a certificate state, as follows:

Verify a host certificate from the host itself
See "To verify a host certificate from the host itself" on page 278.

Verify a host certificate from a NetBackup server
See "To verify from a NetBackup server if a different host's certificate is revoked" on page 279.

To verify a host certificate from the host itself

1 Refresh the CRLs in the NetBackup CRL cache.

2 On the NetBackup host, run the following command as an administrator:

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]`

Windows: `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster]`

Use the `-cluster` option on the active node of a clustered master server to verify the certificate of the virtual name.

3 Examine the command output. The output indicates whether the certificate is revoked or not.

To verify from a NetBackup server if a different host's certificate is revoked

1 As an administrator on the NetBackup master server or a NetBackup media server, run the following command:

UNIX: `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

Windows: `install_path\NetBackup\bin\bptestbpcd -host hostname -verbose`

For `-host hostname`, specify the host for which you want to verify the certificate.

2 Examine the command output. If the certificate on the specified host is revoked, the command output includes the string 'The Peer Certificate is revoked'. If the command output does not include that string, the certificate is valid.

Getting a list of NetBackup hosts that have revoked certificates

Use the following procedure to obtain a list of NetBackup hosts that have a revoked certificate.

See "About the host ID-based certificate revocation list" on page 270.

To get a list of NetBackup hosts with revoked certificates

1   In a command window, log on to the **NetBackup Web Management Service**
    on the master server, as follows (the logon account must have NetBackup
    administrator privileges):

    UNIX: `/usr/openv/netbackup/bin/bpnbat -login -loginType WEB`

    Windows: `install_path\NetBackup\bin\bpnbat -login -loginType WEB`

2   Run the following command to extract from the CRL a list of certificates that
    are not expired and then filter the results for the word "`Revoked`":

    UNIX: `/usr/openv/netbackup/bin/nbcertcmd -listAllDomainCertificates`
    `| grep Revoked`

    Windows: `install_path\NetBackup\bin\nbcertcmd`
    `-listAllDomainCertificates | findstr Revoked`

Deleting host ID-based certificates

Use this topic to manually delete host ID-based certificate of a NetBackup host.
You may need to delete certificates in certain scenarios, for example: A NetBackup
host is moved from one NetBackup domain to another NetBackup domain. In this
scenario, the current host ID-based certificate needs to be deleted and the host
must have a certificate issued by the new Certificate Authority (CA) that is the new
master server.

Caution: Manually deleting the host ID-based certificates may adversely impact
NetBackup functionality.

Note: During NetBackup software removal, host ID-based certificates are
automatically deleted.

To delete a host ID-based certificate from a NetBackup host

1   Run the following command on the NetBackup host to view the details of all
associated host ID-based certificates.

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails`

Windows: `install_path\NetBackup\bin\nbcertcmd -listCertDetails`

2   To delete a certificate, run the following command on the host:

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -deleteCertificate -hostid`
`host_ID`

Windows: `install_path\NetBackup\bin\nbcertcmd -deleteCertificate`
`-hostid host_ID`

To delete a host ID-based certificate from an active node in a cluster setup

1   Run the following command on the active node to view the details of all
associated host ID-based certificates.

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails -cluster`

Windows: `install_path\NetBackup\bin\nbcertcmd -listCertDetails`
`-cluster`

2   To delete a certificate, run the following command on the active node of the
cluster:

`nbcertcmd -deleteCertificate -hostid host_ID -cluster`

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -hostid host_ID -cluster]`

Windows: `install_path\NetBackup\bin\nbcertcmd -hostid host_ID`
`-cluster`

Host ID-based certificate deployment in a clustered setup

This section provides information on deployment of host name-based and host
ID-based certificates in a NetBackup clustered setup.

For more information on NetBackup clusters, see the *NetBackup Clustered Master
Server Administrator's Guide*.

http://www.veritas.com/docs/DOC5332

About host ID-based certificate deployment on a NetBackup cluster

In a clustered NetBackup master server setup, the host ID-based certificates are deployed as follows:

- One certificate for each cluster node: A certificate resides on the local disk of each node.
- One certificate for the virtual name: A certificate resides on the shared disk of the cluster.

Consider the following example:

If a cluster setup consists of 4 nodes, 5 host ID-based certificates are deployed. One certificate is deployed on each of the 4 nodes and one on the shared disk, which is used for the virtual name of the master server.

Note: Only master servers can be clustered in NetBackup.

About host name-based certificate deployment on a NetBackup cluster

In a clustered NetBackup master server setup, the host name-based certificates are deployed as follows:

- One certificate for each cluster node: A certificate resides on the local disk of each node.
- One certificate for the virtual name on each node: A certificate resides on the local disk of each node.

See "Deploying host name-based certificates" on page 237.

About deployment of a host ID-based certificate on a clustered NetBackup host

Review the following scenarios for certificate deployment on cluster nodes:

- In case of fresh NetBackup installation, certificate on an active node is deployed automatically. You must manually deploy certificates on all inactive nodes.
- In case of disaster recovery, certificates for active and inactive nodes are not recovered. After you install NetBackup in a disaster recovery mode after a disaster, you must manually deploy certificates on all nodes.
  See "Generating a certificate on a clustered master server after disaster recovery installation" on page 288.

Note: In case of upgrade, active or inactive nodes may already have a certificate. You can verify whether a cluster node has a certificate or not.

See "Viewing certificate details of a clustered NetBackup setup" on page 286.

See "Host ID-based certificate deployment on the active master server node" on page 283.

See "Host ID-based certificate deployment on inactive master server nodes" on page 283.

Host ID-based certificate deployment on the active master server node

During NetBackup installation, host ID-based certificates are deployed on the active master server node and the virtual name. The certificate for the active node is deployed on a local disk. The certificate for the virtual name is deployed on the shared disk.

Host ID-based certificate deployment on inactive master server nodes

Certificates on inactive nodes are not deployed during installation. You must manually deploy certificates on all inactive nodes after the installation.

See "Deploying host ID-based certificates on cluster nodes" on page 283.

Deploying host ID-based certificates on cluster nodes

You must manually deploy certificates on all inactive nodes.

In certain scenarios, you need to manually deploy host ID-based certificates also on active nodes.

To manually deploy a host ID-based certificate on a master server cluster node

◆ Run the following commands on the master server cluster node:

- `nbcertcmd -getCACertificate`

- `nbcertcmd -getCertificate [-file *authorization_token_file*]`

See "About Token Management for host ID-based certificates" on page 265.

Revoking a host ID-based certificate for a clustered NetBackup setup

NetBackup administrators may consider revoking a host ID-based certificate under various conditions. For example, if the administrator detects that client security has been compromised, if a client is decommissioned, or if NetBackup is uninstalled from the host. A host with a revoked certificate cannot communicate with other hosts. Every NetBackup host must have a valid security certificate and a valid Certificate Revocation List (CRL) for successful communication.

See "About the host ID-based certificate revocation list" on page 270.

The NetBackup administrator can revoke certificates for a cluster node or the virtual name from any host in a NetBackup domain.

Ensure that you revoke the appropriate certificate.

After the certificate is revoked, you may need to deploy a new host ID-based certificate. Create a reissue token on the clustered node and deploy a new certificate using the reissue token.

See "Creating a reissue token for a clustered NetBackup setup" on page 285.

See "Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token" on page 285.

To revoke a certificate from a cluster node

1   Log in to the NetBackup Web Management Service:

    bpnbat -login -logintype WEB

    See "Web login requirements for nbcertcmd command options" on page 239.

2   Run the following command to revoke a certificate for a cluster node:

    nbcertcmd -revokeCertificate -host *host_name*

    See "Revoking a host ID-based certificate" on page 274.

To revoke a certificate for the virtual name

1   Log in to the NetBackup Web Management Service:

    bpnbat -login -logintype WEB

2   Run the following command to revoke a host ID-based certificate for the virtual name:

    nbcertcmd -revokeCertificate -host *virtual_name*

    See "Revoking a host ID-based certificate" on page 274.

Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token

After a host ID-based certificate is revoked, you can deploy new certificates on a clustered NetBackup setup using reissue tokens.

See "Creating a reissue token for a clustered NetBackup setup" on page 285.

To deploy a new host ID-based certificate on a cluster node

◆ Run the following command to deploy a new certificate on the cluster node using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file -force
```

To deploy a new host ID-based certificate for the virtual name

◆ Run the following command to deploy a new certificate for the virtual name using the reissue token:

```
nbcertcmd -getCertificate -file reissue_token_file_virtual -force
-cluster
```

Creating a reissue token for a clustered NetBackup setup

You need to reissue a certificate to a host in certain scenarios, for example a certificate is revoked for a host and you need to reissue a new certificate to the host.

See "Deploying a host ID-based certificate on a clustered NetBackup setup using reissue token" on page 285.

You need a reissue token to reissue a new certificate to a host.

See "About Token Management for host ID-based certificates" on page 265.

To create a reissue token for a cluster node

1 Log in to the NetBackup Web Management Service with the following command:

```
bpnbat -login -logintype WEB
```

See "Web login requirements for nbcertcmd command options" on page 239.

2 Run the following command to create a reissue token for the required cluster node:

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

See "Creating a reissue token" on page 261.

To create a reissue token for the virtual name

1 Log in to the NetBackup Web Management Service with the following command:

```
bpnbat -login -logintype WEB
```

See "Web login requirements for nbcertcmd command options" on page 239.

2 Run the following command to create a reissue token for the virtual name.

```
nbcertcmd -createToken -name token_name_virtual -reissue -host
virtual_name
```

See "Creating a reissue token" on page 261.

Renewing a host ID-based certificate on a clustered NetBackup setup

Host ID-based certificates for the cluster nodes and the virtual name are automatically renewed. The certificates are automatically renewed 180 days before the expiration date.

You can also renew the certificates manually, if required.

See "About host ID-based certificate expiration and renewal" on page 258.

To manually renew certificate for a cluster node

◆ Run the following command from a cluster node to renew the certificate for the node:

```
nbcertcmd -renewCertificate
```

To manually renew certificate for the virtual name

◆ Run the following command on the active node to manually renew the certificate for the virtual name:

```
nbcertcmd -renewCertificate -cluster
```

Viewing certificate details of a clustered NetBackup setup

Run the following commands to view the certificate details of a cluster node or the virtual name.

To view certificate details of a cluster node

◆ Run the following command on a cluster node:

```
nbcertcmd -listCertDetails
```

See "Viewing host ID-based certificate details" on page 242.

To view certificate details for the virtual name

◆ Run the following command on the active node to view certificate details for the virtual name:

```
nbcertcmd -listCertDetails -cluster
```

```
C:\Program Files\Veritas\NetBackup\bin>nbcertcmd -listCertDetails -cluster
      Master Server : ha-w12-vc-c2-nb
           Host ID : caaf54b9-f47d-4a68-9462-72a2a5d34e9a
         Issued By : /CN=broker/OU=root@ha-w12-vc-c2-nb/O=vx
     Serial Number : 0x5e1c576b0000000f
       Expiry Date : Sep 13 12:38:30 2017 GMT
   SHA1 Fingerprint : 44:A6:0D:56:30:E2:25:A1:FB:32:47:73:D3:6E:F8:00:C3:1C:DB:25

Operation completed successfully.
```

See "Viewing host ID-based certificate details" on page 242.

Removing CA certificates from a clustered NetBackup setup

Run the following commands to remove the CA (Certificate Authority) certificates from a clustered setup.

Caution: Removing the CA certificate from a master server node can adversely impact the NetBackup functionality.

To remove the CA certificates from a cluster node

1 Run the following command on a cluster node to view the fingerprints of the CA certificates:

```
nbcertcmd -listCACertDetails
```

2 Run the following command to remove the CA certificate by providing the appropriate fingerprint:

```
nbcertcmd -removeCACertificate -fingerprint fingerprint
```

To remove the CA certificates for the virtual name

1 Run the following command on the active node to view the fingerprints of the CA certificates for the virtual name:

```
nbcertcmd -listCACertDetails -cluster
```

2 Run the following command on the active node to remove the CA certificate for the virtual name by providing the appropriate fingerprint:nbcertcmd

```
-removeCACertificate -fingerprint fingerprint_virtual -cluster
```

Generating a certificate on a clustered master server after disaster recovery installation

After you complete the disaster recovery of a clustered master server, you must generate a certificate on the active node as well as all inactive nodes. This procedure is required for successful backups and restores of the cluster.

Generating the local certificate on each cluster node after disaster recovery installation

1   Add all inactive nodes to the cluster.

If all the nodes of the cluster are not currently part of the cluster, start by adding them to the cluster. Please consult with your operating system cluster instructions for assistance with this process.

More information about supported cluster technologies is available. Please see the *Veritas NetBackup Clustered Master Server Administrator's Guide*.

http://www.veritas.com/docs/DOC5332

2   Run the nbcertcmd command to store the Certificate Authority certificate.

UNIX: `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`

Windows: `install_path\Veritas\NetBackup\bin\nbcertcmd -getCACertificate`

3   Use the bpnbat command as shown to authorize the necessary changes. When you are prompted for the authentication broker, enter the virtual server name, not the local node name.

`bpnbat -login -loginType WEB`

4   Use the nbcertcmd command to create a reissue token. The *hostname* is the local node name. When the command runs, it displays the token string value. A unique reissue token is needed for each cluster node.

`nbcertcmd -createtoken -name token_name -reissue -host hostname`

5   Use the reissue token with the nbcertcmd command to store the host certificate. This command prompts you for the token string value. Enter the token string from the nbcertcmd -createToken command.

`nbcertcmd -getCertificate -token`

Additional information is available. Please see the section on deploying certificates on master server nodes in the *Veritas NetBackup Security and Encryption Guide*.

See "Disaster recovery packages" on page 236.

About the communication between a NetBackup client located in a demilitarized zone and a master server through an HTTP tunnel

In a NetBackup deployment setup, the client computers can be in a demilitarized zone (DMZ) where the communication takes place only through specific web ports.

All NetBackup clients must be able to communicate with the web management service on the master server to deploy security certificates and authorize peers for secure connections. For example, the NetBackup client sends requests to the master server for deploying certificates, which is essential for secure NetBackup communication. In a DMZ setup, the client might not be able to send web service requests directly to the master server. In this scenario, a NetBackup client sends a connection request and a web service request to the HTTP tunnel on the media server by the HTTP CONNECT proxy method. The HTTP tunnel accepts the connection request and forwards the web service request to the master server.

The HTTP tunneling feature allows the NetBackup clients in a DMZ to send web service requests to the master server. The NetBackup media server forms an HTTP tunnel that forwards the web service request from the NetBackup client to the master server. The further web service communication uses Secure Socket Layer (SSL).

Note: The port number 1556 on the media server must be accessible by the NetBackup client for sending web service requests.

Figure 8-2   NetBackup client and master server communication in a DMZ setup

In a single domain or multi-domain environment, when the NetBackup client in a DMZ tries to send a web service connection request to the master server, it follows a particular sequence::

Table 8-9   Sequence to send a connection request

Sequence	Description
1. The NetBackup client tries to send the connection request directly to the master server.	In a DMZ, the web service connection request might not succeed.

Table 8-9 Sequence to send a connection request *(continued)*

Sequence	Description
2. If the direct connection fails, then the client checks if a media server is specified to use HTTP tunneling to send the web service connection request to the master server.	You can define a preferred media server that the NetBackup client can use for sending the web service connection. Add the WEB_SERVER_TUNNEL option in the registry on Windows client or in the `bp.conf` file on a UNIX client. For more information, refer to the WEB_SERVER_TUNNEL option for NetBackup clients section in the *NetBackup Administrator's Guide Volume I*. http://www.veritas.com/docs/DOC5332
3. If a media server is not specified, then the client refers to a list of media servers that is available in the NetBackup configuration and uses them for sending web service connection requests.	NetBackup client maintains an internal cache file (`websvctunnels.cache`) that contains a list of media servers that are automatically updated based on previous successful connections. The cache file is available in the same location as the `bp.conf` file for both Windows and UNIX.

Additional information

- The following additional options are available for configuring the HTTP Tunnel feature:

  - WEB_SERVER_TUNNEL_USE - You can use this option on the NetBackup clients to configure the default communication behavior using the HTTP Tunnel.

  - WEB_SERVER_TUNNEL_ENABLE - By default, HTTP Tunnel is enabled on the media server. You can use this option on the media servers to disable the HTTP Tunnel feature.

  For more information, refer to the *NetBackup Administrator's Guide Volume I*.
  http://www.veritas.com/docs/DOC5332

- If your NetBackup client configuration does not contain information about the media servers in the domain, run the nbsetconfig command on the master server. The registry on a Windows client or the bp.conf file on a UNIX client includes the master and the media servers that the client selects to send connection and web service requests.

- If you use the nbcertcmd -getCertificate command on the NetBackup client in a DMZ, and if you see one of the following errors:

- EXIT STATUS 5955: The host name is not known to the master server.

- EXIT STATUS 5954: The host name could not be resolved to the requesting host's IP address.

  Use a token to deploy the security certificate because the master server cannot match the IP address of the HTTP tunnel to the identity of the host that requests the certificate.

- NetBackup audit report lists the media server as the user if an HTTP tunnel is used to send a certificate request to the master server.

Adding a NetBackup host manually

Veritas does not recommend manually adding a host in the host database except for specific scenarios. For example, you may need to manually add a host when you recover a Bare Metal Restore (BMR) client to other NetBackup domain using Auto Image Replication (AIR).

For more information on Bare Metal Restore, refer to the *NetBackup Bare Metal Restore Administrator's Guide*.

https://www.veritas.com/support/en_US/article.DOC5332

Note: Before adding a host, you must ensure that the host entry that you want to add does not already exist in the host database.

You can add a host using the command-line interface only.

To add a host in the host database using the command-line interface

1 Run the following command to authenticate your web services login on the master server:

   `bpnbat -login -loginType WEB`

2 Run the following command to add a host:

   `nbhostmgmt -addhost -host` *host name* `-server` *master server*

External CA support in NetBackup

This chapter includes the following topics:

- About external CA support in NetBackup

- Workflow to use external certificates for NetBackup host communication

- Configuration options for external CA-signed certificates

- About certificate revocation lists for external CA

- About certificate enrollment

- About viewing enrollment status of master servers

- Configuring an external certificate for the NetBackup web server

- Configuring the master server to use an external CA-signed certificate

- Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation

- Enrolling an external certificate for a remote host

- Viewing the certificate authorities that your NetBackup domain supports

- Viewing external CA-signed certificates in the NetBackup web UI

- Renewing a file-based external certificate

- Removing certificate enrollment

- Disabling the NetBackup CA in a NetBackup domain

- Enabling the NetBackup CA in a NetBackup domain

■ Disabling an external CA in a NetBackup domain

■ Changing the subject name of an enrolled external certificate

■ About external certificate configuration for a clustered master server

About external CA support in NetBackup

You can now use X.509 certificates that your trusted certificate authority (CA) has issued.

NetBackup supports file-based certificates and Windows certificate store as sources for external certificates. It supports certificates in PEM, DER, and P7B formats.

About the terminology used for certificates in NetBackup

The following terms that are specific to security certificates are used in NetBackup:

■ A certificate authority (CA) other than the NetBackup CA is referred to as an external CA.

■ Certificates that are issued by a CA other than the NetBackup CA are referred to as external CA-signed certificates or external certificates.

■ Certificates that the NetBackup CA has issued are referred to as NetBackup CA-signed certificates or NetBackup certificates.

■ A NetBackup certificate that is used for secure communications over control channel is also referred to as host ID-based certificate.

Important notes about host certificates

■ A NetBackup certificate or a host ID-based certificate is deployed on the master server during NetBackup installation. You need to manually configure an external certificate on the master server after installation.
See "Configuring the master server to use an external CA-signed certificate" on page 315.

■ You can configure an external certificate on a NetBackup host (media server or client) either during installation or after installation.
See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 316.

Requirements for external certificate configuration

■ On Windows platform, if external certificates are used for host communication, the `NT AUTHORITY\SYSTEM` user must be able to access the certificates that are located at `ECA_CERT_PATH`. The `ECA_CERT_PATH` configuration option is available in the Windows registry.

- On Windows platform, universal naming convention (UNC) paths (or network paths) are not supported for the following external CA parameters: certificate chain, certificate's private key, trust store, passphrase file for certificate's private key, and CRL cache.

- This is applicable for the NetBackup web server certificate.
  If the subject alternative name (SAN) is not empty, the certificate should contain all host names that the master server is known by (the host names that are listed in the `SERVER` configuration option entries of other hosts in the domain) in the SAN field of the certificate.

- Requirements for the subject name of the certificate:

  - Subject name should not be empty.

  - Common name of the subject name should not be empty.

  - Subject name should be unique for each host.

  - Subject name should be less than 255 characters.

- Server and client authentication attributes should be set in the certificate.

- Only ASCII 7 characters are supported for the certificate subject and the subject alternative name (SAN).

Command-line options used for external certificate configuration

Use the following command-line options are specific to external certificate configuration:

nbcertcmd	■ `-cleanupCRLCache`
	■ `-createECACertEntry`
	■ `-deleteECACertEntry`
	■ `-ecaHealthCheck`
	■ `-enrollCertificate`
	■ `-getExternalCertDetails`
	■ `-listEnrollmentStatus`
	■ `-removeEnrollment`
	■ `-updateCRLCache`
configureWebServerCerts	■ `-addExternalCert`
	■ `-removeExternalCert`
	■ `-validateExternalCert`

The following command-line options are used for both external and NetBackup certificate configurations:

| `nbcertcmd` | ■ `-listCertDetails` - This command option is by default applicable for NetBackup CA-signed certificate. When used with `-ECA` option, it is applicable for external CA-signed certificates. |
| | ■ `-listCACertDetails` - This command option is by default applicable for NetBackup CA-signed certificate. When used with `-ECA` option, it is applicable for external CA-signed certificates. |

For more information on the commands, refer to the NetBackup Commands Reference Guide.

Workflow to use external certificates for NetBackup host communication

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 9-1   Workflow to use external certificates for NetBackup host communication

Step	Description
Step 1	Ensure the following: ■ The external certificates for the web server, master server, and all hosts are placed at the appropriate locations. ■ In case of file-based certificates, the private key files for the external certificates are placed at the appropriate locations. See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 302. If the private keys are encrypted, passphrase files should be placed at the appropriate locations. See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 303. ■ The CRLs are placed at the required locations on the hosts as per their CRL configuration options and they are accessible. See "About certificate revocation lists for external CA" on page 309.
Step 2	Install the NetBackup software on the master server (or upgrade the master server).
Step 3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See "Configuring an external certificate for the NetBackup web server" on page 313.

Table 9-1   Workflow to use external certificates for NetBackup host
                       communication *(continued)*

Step	Description
Step 4	Configure an external certificate for the NetBackup master server host. See "Configuring the master server to use an external CA-signed certificate" on page 315.
Step 5	Install the NetBackup software on the media server and clients (or upgrade the media server and clients). If the master server is configured to use external certificates, the Installer prompts you to provide external certificate information for the host.
Step 6	**Note:** This step is required for the hosts (media server and clients) that have the current NetBackup software, but are not configured to use external certificate. NetBackup hosts may not have external certificate configuration because of the following reasons: ■ You did not provide the external certificate information during installation or upgrade of the host. ■ The NetBackup master server was not configured to use external certificates during installation or upgrade of the host. Configure an external certificate for a NetBackup host (media server or client) after installation. See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 316.

Configuration options for external CA-signed certificates

To configure a NetBackup master server, media server, or client to use external CA-signed certificate for host communication, you must define certain configuration options in the NetBackup configuration file (`bp.conf` on UNIX platform or Windows registry).

About the mandatory and optional configuration options

■ For external certificate configuration, for file-based certificates, the following configuration options are mandatory:

   ■ `ECA_CERT_PATH`

   ■ `ECA_TRUST_STORE_PATH`

- ■ `ECA_PRIVATE_KEY_PATH`
  If the private key of the external certificate is encrypted, `ECA_KEY_PASSPHRASEFILE` is also mandatory:

- For Windows certificate store, the following configuration options are mandatory:

  - ■ `ECA_CERT_PATH`

- The following options are optional:

  - ■ `ECA_CRL_CHECK`
    If the option is set to `DISABLE` (or `0`) the `ECA_CRL_PATH` option is ignored and revocation status of a peer host's certificate is not verified.
    If the option is set to a value other than `DISABLE` and `0`, revocation status of a peer host's certificate is verified based on `ECA_CRL_PATH`.

  - ■ `ECA_DR_BKUP_WIN_CERT_STORE`
    For Windows certificate store, specify this option if you want to backup the external certificates during catalog backup.

  - ■ `ECA_CRL_PATH_SYNC_HOURS`
    This option is used when `ECA_CRL_CHECK` is enabled and `ECA_CRL_PATH` is defined.

  - ■ `ECA_CRL_REFRESH_HOURS`
    This option is used when `ECA_CRL_CHECK` is enabled, but `ECA_CRL_PATH` is not defined (when CDP is used as a CRL source).
    See

ECA_CERT_PATH for NetBackup servers and clients

The `ECA_CERT_PATH` option specifies the path to the external CA-signed certificate of the host. This option is mandatory.

It supports certificates in PEM and P7B format that can either be DER or PEM encoded - PEM-formatted certificates in the same file or a P7B file that can either be DER or PEM encoded.

If you have an intermediate certificate (from a certificate chain), sequence of the certificates in the path should be as follows: leaf certificate > intermediate certificate

NetBackup supports the following certificate sources:

- Windows certificate store

  Note: The Windows certificate store is not supported for clustered master servers.

■ File-based certificates

Table 9-2   ECA_CERT_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	For file-based certificates, use the following format:
	`ECA_CERT_PATH = Path to the external certificate of the host`
	For example: `c:\server.pem`
	For Windows certificate store, use the following format:
	`ECA_CERT_PATH = Certificate store name\Issuer name\Subject name`
	You can specify multiple certificate selection queries in a comma-separated format.
	`ECA_CERT_PATH = Store name1\Issuer name1\Subject name1,Store name2\Issuer name2\Subject name2`
	See "Specifying Windows certificate store for ECA_CERT_PATH" on page 299.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

Specifying Windows certificate store for ECA_CERT_PATH

NetBackup selects a certificate from any of the local machine certificate stores on a Windows host.

In case of Windows certificate store, `ECA_CERT_PATH` is a list of comma-separated clauses.

Each clause is of the form *Store name\Issuer\Subject*. Each clause element contains a query. `$hostname` is a keyword that is replaced with the fully qualified domain name of the host. Use double quotes when a `\` is present in the actual path. For example, `MY\Veritas\"NetBackup\$hostname"`.

The 'Store name' should be the exact name of the store where the certificate resides. For example: 'MY'

The 'Issuer' is optional. If this is provided, NetBackup picks the certificates for which the Issuer DN contains the provided substring.

The 'Subject' is mandatory. NetBackup picks the certificate for which the Subject DN contains the provided substring.

You must ensure to:

- Add the root certificate to Trusted Root Certification Authorities or Third-Party Root Certification Authorities in the Windows certificate store.

- If you have any intermediate CAs, add their certificates to the Intermediate Certification Authorities in the Windows certificate store.

Example - Certificate locations with WHERE CLAUSE:

- My\Veritas\$hostname, My\ExampleCompany\$hostname
  Where (certificate store is MY, Issuer DN contains Veritas, Subject DN contains $hostname) OR (certificate store name is MY, Issuer DN contains ExampleCompany, Subject DN contains $hostname)

- MY\Veritas\"NetBackup\$hostname"
  Where certificate store name is MY, Issuer DN contains Veritas, Subject DN contains NetBackup\$hostname

- MY\\$hostname
  Where certificate store name is MY, any Issuer DN, Subject DN contains $hostname

- MY\Veritas\NetBackup $hostname
  Where certificate store name is MY, Issuer DN contains Veritas, Subject DN contains NetBackup $hostname

If you provide a space between words, it is considered as a valid character.

Example - Certificate locations with invalid data:

- MY\\
  The Subject DN should have some value.

- My\$hostname
  The Subject DN should have some value.

- \\$hostname
  The certificate store name should have exact value of the store in which the certificate resides.

- MY\CN=Veritas\CN=$hostname

The Subject DN and issuer DN cannot contain =, and also specific tags like CN=.

ECA_TRUST_STORE_PATH for NetBackup servers and clients

The `ECA_TRUST_STORE_PATH` option specifies the file path to the certificate bundle file that contains all trusted root CA certificates.

This certificate file should have one or more certificates in PEM format.

The trust store supports certificates in the following formats:

- PEM
- P7B that can either be DER or PEM encoded

Note: Do not specify the `ECA_TRUST_STORE_PATH` option if you use the Windows certificate store.

This option is mandatory for file-based certificates.

Table 9-3   ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
	If certificate validation is required for VMware or RHV servers, this option must be set on the NetBackup master server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_TRUST_STORE_PATH =` *Path to the external CA certificate*
	For example: `c:\rootCA.pem`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_PRIVATE_KEY_PATH for NetBackup servers and clients

The ECA_PRIVATE_KEY_PATH option specifies the file path to the private key for the external CA-signed certificate of the host. The private key file should be in PEM format.

This option is mandatory for file-based certificates.

If the private key of the certificate is encrypted, you should specify the ECA_KEY_PASSPHRASEFILE option.

See "ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients" on page 303.

For encrypted private keys, NetBackup supports the following formats:

- DES, 3DES, and AES if the private key is in the PKCS #1 format (if encrypted, can be in PEM format)

- DES, 3DES, AES, RC2, and RC4 if the private key is in the PKCS #8 format (if encrypted, can be in PEM or DER format)

Note: You should not specify the ECA_PRIVATE_KEY_PATH option if Windows certificate store is specified for the ECA_CERT_PATH option.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 298.

Table 9-4   ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	ECA_PRIVATE_KEY_PATH = *Path to the private key of the external certificate*
	For example: c:\key.pem
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_KEY_PASSPHRASEFILE for NetBackup servers and clients

The `ECA_KEY_PASSPHRASEFILE` option specifies the path to the text file where the passphrase for the external certificate's private key is stored.

You should specify the `ECA_KEY_PASSPHRASEFILE` option only if the certificate's private key is encrypted.

See "ECA_PRIVATE_KEY_PATH for NetBackup servers and clients" on page 302.

Note: You should not specify the `ECA_KEY_PASSPHRASEFILE` option if you use Windows certificate store.

See "ECA_CERT_PATH for NetBackup servers and clients" on page 298.

Table 9-5   ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_KEY_PASSPHRASEFILE = `*`Path to the passphrase file`*
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_CHECK for NetBackup servers and clients

The `ECA_CRL_CHECK` option lets you specify the revocation check level for external certificates of the host. It also lets you disable the revocation check for the external certificates. Based on the check, revocation status of the certificate is validated against the Certificate Revocation List (CRL) during host communication.

You can choose to use the CRLs from the directory that is specified for the `ECA_CRL_PATH` configuration option in the configuration file (`bp.conf` on UNIX or Windows registry) or the CRL Distribution Point (CDP).

See "ECA_CRL_PATH for NetBackup servers and clients" on page 304.

Table 9-6 ECA_CRL_CHECK information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_CRL_CHECK = CRL check`
	You can specify one of the following:
	■ DISABLE (or 0) - Revocation check is disabled. Revocation status of the certificate is not validated against the CRL during host communication. ■ LEAF (or 1) - Revocation status of the leaf certificate is validated against the CRL. This is the default value. ■ CHAIN (or 2) - Revocation status of all certificates from the certificate chain are validated against the CRL.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH for NetBackup servers and clients

The `ECA_CRL_PATH` option specifies the path to the directory where the Certificate Revocation Lists (CRL) of the external certificate authority (CA) are located.

These CRLs are copied to NetBackup CRL cache. Revocation status of the external certificate is validated against the CRLs from the CRL cache.

CRLs in the CRL cache are periodically updated with the CRLs in the directory that is specified for `ECA_CRL_PATH` based on the `ECA_CRL_PATH_SYNC_HOURS` option.

See "ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients" on page 305.

If the `ECA_CRL_CHECK` option is not set to `DISABLE` (or 0) and the `ECA_CRL_PATH` option is not specified, NetBackup downloads the CRLs from the URLs that are specified in the CRL distribution point (CDP) and uses them to verify revocation status of the peer host's certificate.

See "ECA_CRL_CHECK for NetBackup servers and clients" on page 303.

Note: For validating the revocation status of a virtualization server certificate, the VIRTUALIZATION_CRL_CHECK option is used.

Table 9-7 ECA_CRL_PATH information

Usage	Description
Where to use	On NetBackup servers or clients.
	If certificate validation is required for VMware or RHV servers, this option must be set on the NetBackup master server and respective access hosts, irrespective of the certificate authority that NetBackup uses for host communication (NetBackup CA or external CA).
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format to specify a path to the CRL directory:
	ECA_CRL_PATH = *Path to the CRL directory*
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients

The ECA_CRL_PATH_SYNC_HOURS option specifies the time interval in hours to update the Certificate revocation lists (CRL) in the NetBackup CRL cache with the CRLs in the directory specified for the ECA_CRL_PATH configuration option.

See "ECA_CRL_PATH for NetBackup servers and clients" on page 304.

The ECA_CRL_PATH_SYNC_HOURS option is not applicable if CDP is used for CRLs.

By default, CRLs in the cache are updated every one hour.

During host communication, revocation status of the external certificate is validated against the CRLs from the CRL cache.

Table 9-8 ECA_CRL_PATH_SYNC_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 9-8 ECA_CRL_PATH_SYNC_HOURS information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_CRL_PATH_SYNC_HOURS = Number of hours`
	Minimum number of hours that you can specify - 1 hour
	Maximum number of hours that you can specify - 720 hour
	The default value is one hour.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_CRL_REFRESH_HOURS for NetBackup servers and clients

The `ECA_CRL_REFRESH_HOURS` option specifies the time interval in hours to download the CRLs from the URLs that are specified in the peer host certificate's CRL distribution points (CDP).

The `ECA_CRL_REFRESH_HOURS` option is applicable when you use CDP for CRLs.

After the specified time interval, CRLs of the certificate authority are downloaded from the URLs that are available in CDP.

By default, the CRLs are downloaded from the CDP after every 24 hours.

Table 9-9 ECA_CRL_REFRESH_HOURS information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 9-9 ECA_CRL_REFRESH_HOURS information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_CRL_REFRESH_HOURS = Number of hours`
	Minimum number of hours that you can specify - 0 hour, which indicates that CRLs from the CDP are not periodically downloaded.
	Maximum number of hours that you can specify - 4380 hours
	The default value for the option is 24 hours.
	Note: CRLs are also downloaded from the CDP during host communication if they are expired or not available in the CRL cache, irrespective of the time interval set for the `ECA_CRL_REFRESH_HOURS` option.
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients

The `ECA_DISABLE_AUTO_ENROLLMENT` option lets you disable the automatic enrollment of an external certificate for a host with the given master server. The certificate is automatically enrolled with a master server when a proxy communication takes place with respect to the host for the first time.

You may want to disable the automatic certificate enrollment process and enroll the certificates as and when required.

By default automatic enrollment is enabled.

Table 9-10 ECA_DISABLE_AUTO_ENROLLMENT information

Usage	Description
Where to use	On NetBackup servers or clients.

Table 9-10   ECA_DISABLE_AUTO_ENROLLMENT information *(continued)*

Usage	Description
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	`ECA_DISABLE_AUTO_ENROLLMENT = 1`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

ECA_DR_BKUP_WIN_CERT_STORE for NetBackup servers and clients

The `ECA_DR_BKUP_WIN_CERT_STORE` option specifies whether you want to take a backup of the Windows certificate store information during catalog backup or not.

By default, Windows certificate store information is backed up during catalog backup.

Note: If the Windows certificate store information is not exportable, it cannot be backed up during catalog backup.

Table 9-11   ECA_DR_BKUP_WIN_CERT_STORE information

Usage	Description
Where to use	On NetBackup servers or clients.
How to use	Use the `nbgetconfig` and the `nbsetconfig` commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	If you do not want the catalog backup operation to take a backup of the Windows certificate store information, use the following format:
	`ECA_DR_BKUP_WIN_CERT_STORE = NO`
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

About certificate revocation lists for external CA

Certificate revocation list (CRL) for an external certificate authority (CA) contains a list of digital certificates that the external CA has revoked before the scheduled expiration date and should no longer be trusted.

NetBackup supports PEM and DER formats for CRLs for external CA.

CRLs for all CRL issuers or external CAs are stored in the NetBackup CRL cache that resides on each host.

During secure communication, each NetBackup host verifies the revocation status of the peer host's external certificate with the CRL that is available in the NetBackup CRL cache, based on the `ECA_CRL_CHECK` configuration option.

See "ECA_CRL_CHECK for NetBackup servers and clients" on page 303.

The NetBackup CRL cache is updated with the required CRLs using one of the following CRL sources:

`ECA_CRL_PATH` configuration option	A NetBackup configuration option (from `bp.conf` file on UNIX or Windows registry) that specifies the directory path where the CRLs exist. See "ECA_CRL_PATH_SYNC_HOURS for NetBackup servers and clients" on page 305. See "How CRLs from ECA_CRL_PATH are used" on page 310.
CRL distribution point (CDP)	If you have not specified `ECA_CRL_PATH`, NetBackup downloads the CRLs from the URLs that are specified in the peer host certificate's CDP and caches them in the NetBackup CRL cache. See "How CRLs from CDP URLs are used" on page 311. NetBackup supports downloading CRLs from HTTP and HTTPS URLs that are specified in CDP.

The NetBackup CRL cache contains only the latest copy of a CRL for each CA (including root and intermediate CAs).

The `bpclntcmd -crl_download` service updates the CRL cache during host communication in the following scenarios irrespective of the time interval set for the `ECA_CRL_PATH_SYNC_HOURS` or `ECA_CRL_REFRESH_HOURS` options:

- When CRLs in the CRL cache are expired

- If CRLs are available in the CRL source (`ECA_CRL_PATH` or CDP), but they are missing from the CRL cache

> **Note:** Once the `bpclntcmd -crl_download` service updates the CRLs in the CRL cache, it does not download the CRLs for the same CA for the next 15 min even though a valid download scenario has occurred. If you want to update the CRL within 15 min, terminate the `bpclntcmd -crl_download` service.

How CRLs from ECA_CRL_PATH are used

Use this section if you want to use `ECA_CRL_PATH` as the CRL source for the NetBackup CRL cache.

To use CRLs from ECA_CRL_PATH

1   Ensure that the CRLs for external CAs are stored in a directory and the directory path is accessible by the host.

   You can specify the CRL details that are required for external CA configuration during NetBackup installation or upgrade on the host.

   Select one of the following certificate revocation list (CRL) options during installation or upgrade:

   - **Use the CRL defined in the certificate** - No additional information is required.

   - **Use the CRL at the following path** - You are prompted to provide a path to the CRL.
     If you choose to use the **Do not use a CRL** option, peer host's certificate is not verified with the CRL during host communication.

   For more information, refer to the NetBackup Installation Guide.

2   Specify the CRL directory path for the `ECA_CRL_PATH` configuration option.

3   Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

   During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from `ECA_CRL_PATH`.

   By default, CRLs from the cache are updated every one hour. To change the time interval, set the `ECA_CRL_PATH_SYNC_HOURS` option to a different value.

   To manually update the CRL cache with the `ECA_CRL_PATH` CRLs, run the `nbcertcmd -updateCRLCache` command.

   To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

How CRLs from CDP URLs are used

Use this section if you want to use CRL Distribution Point (CDP) as the CRL source for the NetBackup CRL cache.

To use CRLs from CDP

1   Ensure that the `ECA_CRL_PATH` configuration option is not specified.

2   Ensure that the host can access the URLs that are specified in the peer host's CDP.

3   Ensure that the `ECA_CRL_CHECK` configuration option is set to a value other than `DISABLE`.

    During host communication, the revocation status of the external certificate is verified with the CRL in the NetBackup CRL cache that contains the CRLs from CDP URLs.

    By default, CRLs are downloaded from the CDP after every 24 hours and updated in the CRL cache. To change the time interval, set the `ECA_CRL_REFRESH_HOURS` configuration option to a different value.

    To manually delete the CRLs from the CRL cache, run the `nbcertcmd -cleanupCRLCache` command.

About certificate enrollment

In case of NetBackup CA, certificates are automatically enrolled with the master server during certificate deployment.

In case of external CA, certificates are automatically enrolled with the master server during host communication if the `ECA_DISABLE_AUTO_ENROLLMENT` option is enabled. You can enroll the certificate manually using the `nbcertcmd -enrollCertificate` command.

The enrolled certificates are used for host communication.

See "Removing certificate enrollment" on page 320.

About automatic enrollment of an external certificate

An external certificate of a host is automatically enrolled with a master server when communication takes place for the first time. You can disable the automatic certificate enrollment process and enroll the certificates manually as and when required using the `nbcertcmd -enrollCertificate` command.

See "ECA_DISABLE_AUTO_ENROLLMENT for NetBackup servers and clients" on page 307.

If automatic enrollment is enabled for communicating hosts and both hosts have external certificates configured, NetBackup tries to enroll the external certificates.

The external certificates are enrolled with the associated master server. During any subsequent communications between the hosts associated with this master server, the enrolled external certificates are used.

External certificates are not automatically enrolled in the following scenarios:

- Communication with NAT clients
  For more information on NAT client support in NetBackup, refer to the NetBackup Administrator's Guide Volume I.

- Communication between media servers as part of media server deduplication (MSDP) image replication

- Communication with the **NetBackup Administration Console**

About viewing enrollment status of master servers

To configure a NetBackup host to use an external certificate, you need to define the required configuration options and then enroll a certificate for the host. The enrolled certificate is used for communication between the host and the master server domain that exists in the SERVER option.

See "Configuring the master server to use an external CA-signed certificate" on page 315.

See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 316.

You can view the enrollment status by running the nbcertcmd -listEnrollmentStatus command. The command lists only those records where the subject name matches that of the certificate that is configured for the ECA_CERT_PATH option.

The following enrollment statuses are displayed:

- Not enrolled - The external certificate is not enrolled with this master server domain. The master server is present in master server list in the SERVER option.

- To be updated - The external certificate is required to be enrolled again with this master server domain.

- Enrolled - The external certificate is enrolled with the master server.

See "Enrolling an external certificate for a remote host" on page 318.

Configuring an external certificate for the NetBackup web server

By default, NetBackup uses the security certificates that the NetBackup CA has issued. If you have a certificate that an external CA has issued, you can configure the NetBackup web server to use it for secure communication.

See "Viewing the certificate authorities that your NetBackup domain supports" on page 319.

To configure an external certificate for the web server

1   Ensure that you have valid certificate, private key of the certificate, and trusted CA bundle.

2   Run the following command:

    ```
    configureWebServerCerts -addExternalCert -nbHost -certPath
    certificate path -privateKeyPath private key path -trustStorePath
    CA bundle path [-passphrasePath passphrase file path]
    ```

    Refer to the NetBackup Commands Reference Guide for more details on the command-line options.

    ■   In a clustered setup, to avoid a failover run the following command on the active node:

        ```
        install_path/netbackup/bin/bpclusterutil -freeze
        ```

3   Restart the NetBackup Web Management Console service to reflect the changes.

    On UNIX, run the following commands:

    ■   `install_path/netbackup/bin/nbwmc -terminate`

    ■   `install_path/netbackup/bin/nbwmc start`

    On Windows, use the **Services** application in the **Windows Control Panel**.

    Location of the commands:

Windows	`install_path\NetBackup\wmc\bin\install\`
UNIX	`install_path/wmc/bin/install`

    ■   In a clustered setup, unfreeze the cluster using the following command on the active node:

> *install_path*/netbackup/bin/bpclusterutil -unfreeze

4 Verify that you can access the NetBackup web user interface using a browser, without a certificate warning message.

Updating or renewing external certificate for the web server

You can update or renew the external certificate that you configured for the web server.

To update or renew the external certificate for the web server

1 Ensure that you have the latest external certificate, the matching private key, and the CA bundle file.

2 Run the following command (in a clustered setup, run the command on the active node):

> configureWebServerCerts -addExternalCert -nbHost -certPath *certificate path* -privateKeyPath *private key path* -trustStorePath *CA bundle path*

Removing the external certificate configured for the web server

You can remove the external certificate that is configured for the web server. NetBackup then uses the NetBackup CA-signed certificate for secure communication.

To remove the external certificate configured for the web server

1 Run the following command (in a clustered master server setup, run this command on the active node):

> configureWebServerCerts -removeExternalCert -nbHost

- In a clustered master server setup, run the following command on the active node to freeze the cluster to avoid a failover:

  > *install_path*/netbackup/bin/bpclusterutil -freeze

2 Restart the NetBackup Web Management Console service.

- In a clustered master server setup, run the following command on the active node to unfreeze the cluster:

  > *install_path*/netbackup/bin/bpclusterutil -unfreeze

Configuring the master server to use an external CA-signed certificate

A NetBackup host ID-based certificate is deployed on the master server during installation or upgrade. You can configure the master server to use an external CA-signed certificate after installation. It includes:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 297.

- Enrolling the external certificate for the master server host
  The enrolled certificate is used for communication between the host and the master server domain that is listed in the SERVER configuration option on the host.

See "Viewing external CA-signed certificates in the NetBackup web UI" on page 319.

See "Configuring an external certificate for a clustered master server" on page 328.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server" on page 313.

- External certificates for the NetBackup web server and the master server must be issued by the same root certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (nbwmc service) fails.

- Ensure that the certificate revocation lists (CRLs) for the external CA are stored at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 309.

To configure the master server to use an external certificate

1 Update the NetBackup configuration file (bp.conf file on UNIX or Windows registry) on the master server with the external certificate-specific parameters.

   See "Configuration options for external CA-signed certificates" on page 297.

External CA support in NetBackup | 316
Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate
after installation

For Windows certificate store | Use the `nbsetconfig` command to configure the following parameters:

- ECA_CERT_PATH
- ECA_CRL_CHECK (optional)
- ECA_CRL_PATH (optional)
- ECA_CRL_PATH_SYNC_HOURS (optional)
- ECA_CRL_REFRESH_HOURS (optional)
- ECA_DR_BKUP_WIN_CERT_STORE (optional)

For file-based certificates | Use the `nbsetconfig` command to configure the following parameters:

- ECA_CERT_PATH
- ECA_PRIVATE_KEY_PATH
- ECA_TRUST_STORE_PATH
- ECA_KEY_PASSPHRASEFILE (optional)
- ECA_CRL_CHECK (optional)
- ECA_CRL_PATH (optional)
- ECA_CRL_PATH_SYNC_HOURS (optional)
- ECA_CRL_REFRESH_HOURS (optional)

2 Run the following command on the master server to enroll an external certificate with the master server domain that is defined in the SERVER option:

```
nbcertcmd -enrollCertificate
```

For more details on the command, refer to the NetBackup Commands Reference Guide.

Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation

A NetBackup host (media server or client) is configured to use an external certificate during installation or upgrade. You may choose to do the configuration after installation.

Use this section to configure a host to use an external certificate.

You can use this section to configure an external certificate for a cluster node.

See "About external certificate configuration for a clustered master server" on page 324.

External CA support in NetBackup | 317
**Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate
after installation**

The configuration steps include:

- Defining the external certificate configuration options
  See "Configuration options for external CA-signed certificates" on page 297.

- Ensuring that automatic enrollment is enabled - ECA_DISABLE_AUTO_ENROLLMENT
  is set to TRUE - or enrolling the external certificate manually for the host
  See "Enrolling an external certificate for a remote host" on page 318.
  The enrolled certificate is used for communication between the host and the
  master server domain that is listed in the SERVER configuration option on the
  host.

The enrolled certificate is used for host communication.

See "Viewing external CA-signed certificates in the NetBackup web UI" on page 319.

Important notes

- Ensure that the NetBackup domain is enabled to use external CA-signed
  certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server"
  on page 313.

- It is recommended that you enroll an external certificate for the master server
  host before you enroll one for other hosts.
  See "Configuring the master server to use an external CA-signed certificate"
  on page 315.

- Ensure that the certificate revocation lists (CRLs) for the external CA are stored
  at the required location.
  If CRL distribution point (CDP) is used, ensure that the URLs that are specified
  in the CDP are accessible.
  See "About certificate revocation lists for external CA" on page 309.

To configure a host (media server or client) to use an external certificate

1   Update the configuration file (bp.conf file or Windows registry) with the required
    external certificate-specific parameters on the host:

    See "Configuration options for external CA-signed certificates" on page 297.

<table>
<tr><td>For Windows certificate store</td><td>Use the <code>nbsetconfig</code> command to configure the following parameters:</td></tr>
</table>

For Windows certificate store

Use the `nbsetconfig` command to configure the following parameters:

- ECA_CERT_PATH
- ECA_CRL_CHECK (optional)
- ECA_CRL_PATH (optional)
- ECA_CRL_PATH_SYNC_HOURS (optional)
- ECA_CRL_REFRESH_HOURS (optional)
- ECA_DR_BKUP_WIN_CERT_STORE (optional)

For file-based certificates

Use the `nbsetconfig` command to configure the following parameters:

- ECA_CERT_PATH
- ECA_PRIVATE_KEY_PATH
- ECA_TRUST_STORE_PATH
- ECA_KEY_PASSPHRASEFILE (optional)
- ECA_CRL_CHECK_LEVEL (optional)
- ECA_CRL_PATH (optional)
- ECA_CRL_PATH_SYNC_HOURS (optional)
- ECA_CRL_REFRESH_HOURS (optional)

2 Ensure that the `ECA_DISABLE_AUTO_ENROLLMENT` option is set to `TRUE` using the `nbgetconfig` command. This ensures that automatic enrollment is enabled.

If the option is disabled and you want to manually enroll the certificate, run the following command on the host to enroll an external certificate with the master server domain that is defined in the `SERVER` configuration option on the host:

```
nbcertcmd -enrollCertificate
```

See "About viewing enrollment status of master servers" on page 312.

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

Enrolling an external certificate for a remote host

Use this section to enroll an external certificate for a NetBackup host remotely. This lets the security administrator to enroll external certificate for multiple remote hosts from the same host.

To enroll an external certificate for a remote host (or to perform an enrollment sync operation on a remote host), ensure that the server from which you want to enroll the certificate is listed in the `SERVER` configuration option on the remote host.

To enroll certificate for a remote host

◆   Run the following command on the local host:

    nbcertcmd -enrollCertificate -remoteHost *remote_host_name* -server
    master_server_name

An external certificate is enrolled for the specified remote host with the master server that you provide with the -server option. This master server must be available in the remote host's SERVER configuration option.

See "Configuration options for external CA-signed certificates" on page 297.

For more details on the commands, refer to the *NetBackup Commands Reference Guide*.

Viewing the certificate authorities that your NetBackup domain supports

The **Master server certificate configuration** option in the **NetBackup Administration Console** and on the **NetBackup Web UI** displays the certificate authorities - NetBackup CA, external CA, or both - that your NetBackup domain supports.

- In the **NetBackup Administration Console**, expand **Security Management > Global Security Settings** and click the **Secure Communication** tab to view the supported certificate authorities.

- On the **NetBackup Web UI**, click the **Global Security Settings** option to view the supported certificate authorities.

Viewing external CA-signed certificates in the NetBackup web UI

You can view a list of external certificates that are issued to hosts in your domain using the **NetBackup web UI > Security > Certificates** screen.

For more information, refer to the *NetBackup Web UI Security Administrator's Guide*.

Renewing a file-based external certificate

Use this section to renew a file-based external certificate without restarting NetBackup services.

While you replace the certificate, private key, and passphrase files one by one with all the services up, communication may fail because of mismatch in the certificate - private key pair. To avoid any communication failure, create copies of the files that NetBackup can use if there is a mismatch in the files.

To renew a file-based external certificate

1   Make a copy of the certificate file and rename it with `.old` extension.

   For example, if the certificate file name is `cert.pem`, rename it as `cert.pem.old`.

2   Make a copy of the private key file and rename it with `.old` extension.

3   Carry out the following step if the certificate's private key is encrypted.

   Make a copy of the passphrase file and rename it with `.old` extension.

4   Replace the original certificate, private key, and passphrase files with the renewed certificate, private key, and passphrase files.

5   Ensure that the host communication is successful with the renewed certificate and then delete the old certificate files.

Removing certificate enrollment

You can remove the external certificate enrollment with a certain master server if you do not want to use the certificate for host communication.

To remove certificate enrollment

◆   Run the following command:

   `nbcertcmd -removeEnrollment -server` *master_server_name*

Disabling the NetBackup CA in a NetBackup domain

Use this section to disable the existing NetBackup CA support from your domain when all the hosts in your domain are configured to use external certificates for host communication.

Note: If you have NAT clients in your environment and the NetBackup Messaging Broker (`nbmqbroker`) service is enabled, you may need to restart the service after you disable the NetBackup CA to use external certificates only.

For more information on NAT support in NetBackup, refer to the NetBackup Administrator's Guide, Volume I.

If you have hosts that cannot be configured to use external certificates (NetBackup 8.1.2 or earlier), you should not disable NetBackup CA configuration to avoid communication failure.

To disable NetBackup CA support in your domain

1   Ensure that all the hosts in your domain are configured to use external certificates.

See "Configuring an external certificate for the NetBackup web server" on page 313.

See "Configuring the master server to use an external CA-signed certificate" on page 315.

See "Configuring a NetBackup host (media server, client, or cluster node) to use an external CA-signed certificate after installation" on page 316.

2   After each host in the domain is configured to use external certificates, remove the NetBackup CA support from each host (media servers and clients) in the domain.

Run the following commands on each host in the given order:

- `nbcertcmd -removeCACertificate -fingerPrint `*`NetBackup CA certificate fingerprint`*

- `nbcertcmd -deleteCertificate -hostid `*`host ID of the host`*

3   Remove the NetBackup CA support from the master server.

Run the following commands on the master server in the given order:

- `nbcertcmd -removeCACertificate -fingerPrint `*`NetBackup CA certificate fingerprint`*

- `nbcertcmd -deleteCertificate -hostid `*`host ID of the master server`*

4   Revoke all host ID-based certificates in the domain. This is an optional step.

See "Revoking a host ID-based certificate" on page 274.

5 Remove the NetBackup CA support from the web server. Ensure that you do not need the NetBackup certificates for host communication.

Run the following command on the web server:

```
configureWebServerCerts -removeNBCert
```

For more information on the commands, refer to the NetBackup Commands Reference Guide.

6 Restart the NetBackup Web Management Console (nbwmc) service.

Enabling the NetBackup CA in a NetBackup domain

Use this section to enable a NetBackup domain to use NetBackup CA-signed certificates (or host ID-based certificates) for host communication.

To enable a NetBackup domain to support NetBackup CA configuration

1 Configure the NetBackup web server to use NetBackup (host ID-based) certificates.

■ Run the following command:
```
configureWebServerCerts -addNBCert
```
See "Configuring an external certificate for the NetBackup web server" on page 313.

■ Restart the NetBackup Web Management Console (nbwmc) service.

2 Deploy a NetBackup host ID-based certificate on the master server:

See "Deploying host ID-based certificates" on page 247.

3 Deploy a NetBackup host ID-based certificate on each host.

See "Deploying host ID-based certificates" on page 247.

Disabling an external CA in a NetBackup domain

Use this section to disable an external CA in a NetBackup domain.

To disable an external CA

1 Ensure that each host in the domain is configured to use NetBackup host ID-based certificates.

2 Remove all the external certificate configuration options from the configuration file (`bp.conf` on UNIX or Windows registry), which exists on the host.

For example, `ECA_CERT_PATH`.

See "Configuration options for external CA-signed certificates for a virtual name" on page 325.

3 Remove the external CA support from the master server.

- Remove all the external certificate configuration options from the configuration file (`bp.conf` on UNIX or Windows registry), which exists on the master server.
  For example, `ECA_CERT_PATH`.
  See "Configuration options for external CA-signed certificates for a virtual name" on page 325.

4 Delete all external certificate entries from the NetBackup database.

Run the following command:

```
nbcertcmd -deleteECACertEntry -subject subject name of the
certificate
```

5 Remove the external CA support from the web server.

```
configureWebServerCerts -removeExternalCert
```

For more information on the commands, refer to the NetBackup Commands Reference Guide.

Changing the subject name of an enrolled external certificate

Use this section if you want to change the subject name of an already enrolled external certificate of a host.

To change the subject name of an enrolled external certificate

1 Change the subject name of the certificate.

2 If the host is part of multiple master server domains, you need to carry out this step for all master servers.

Do one of the following:

- Run the following command to manually enroll the certificate:
  Install_Path/bin/nbcertcmd -enrollCertificate

- Run following command to remove the existing enrollment:
  Install_Path/bin/nbcertcmd -removeEnrollment

About external certificate configuration for a clustered master server

You can now use X.509 certificates that your trusted certificate authority (CA) has issued, for a clustered master server.

You should first enable your NetBackup domain to use external CA-signed certificates by configuring the NetBackup web server.

You can then configure the NetBackup clustered master server to use external CA-signed certificates for secure host communication.

See

Important notes

Review the following notes before you configure NetBackup to use external certificates:

- NetBackup certificate or host ID-based certificate is deployed on the master server during NetBackup installation. You need to manually configure an external certificate on the clustered master server after installation.

- In a clustered master server setup, you require to configure one external certificate for each cluster node, which resides on the local disk of each node. Additionally, you need to configure one certificate for the virtual name, which resides on the shared disk of the cluster.

- The NetBackup configuration options (for example, CLUSTER_ECA_CERT_PATH) that are required for external certificate enrollment for the virtual name are stored in the nbcl.conf file. This file resides on the shared disk and external certificate configuration options for each cluster node are stored in the bp.conf file or Windows registry.

- Windows certificate store is not supported as an external certificate source for virtual name. It can be used as a source for certificates for cluster nodes.

- There is no separate CRL configuration option for the virtual name. Based on the ECA_CRL_CHECK configuration option on the node, certificate revocation lists (CRLs) - ECA_CRL_PATH or CDP - of the cluster nodes are used to verify the revocation status of the peer host's certificate during communication. Therefore,

the CRL configuration options should be set before using an external certificate for the master server virtual name.

See "About certificate revocation lists for external CA" on page 309.

Workflow to use external certificates for a clustered master server

To configure NetBackup to use external CA-signed certificates for secure communication, you should carry out the following steps in the given order:

Table 9-12   Workflow to use external certificates in a cluster setup

Step	Process
1	Ensure the following: ■ The certificate for the virtual name is placed at the appropriate location on the shared disk. ■ The external certificates for cluster nodes are placed at the appropriate locations on the nodes. ■ The CRLs are placed at the required locations on the nodes as per their CRL configuration options and are accessible. See "About certificate revocation lists for external CA" on page 309.
2	Install NetBackup software or upgrade the existing software on each cluster node.
3	Enable the NetBackup domain to use external certificates by configuring the NetBackup web server. See "Configuring an external certificate for the NetBackup web server" on page 313.
4	Configure an external certificate for the virtual name and for each cluster node. See "Configuring an external certificate for a clustered master server" on page 328.

Configuration options for external CA-signed certificates for a virtual name

To configure a clustered NetBackup master server to use external CA-signed certificate for host communication, you must define certain configuration options in the nbcl.conf file.

CLUSTER_ECA_CERT_PATH for clustered master server

The CLUSTER_ECA_CERT_PATH option is specific to clustered master server. It specifies the path to the external CA-signed certificate of the virtual name.

Table 9-13   CLUSTER_ECA_CERT_PATH information

Usage	Description
Where to use	On clustered master server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	CLUSTER_ECA_CERT_PATH = *Path to the certificate of the virtual identity*
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_TRUST_STORE_PATH for clustered master server

The CLUSTER_ECA_TRUST_STORE_PATH option is specific to clustered master server. It specifies the path to the certificate bundle file that contains all trusted root CA certificates in PEM format.

Table 9-14   CLUSTER_ECA_TRUST_STORE_PATH information

Usage	Description
Where to use	On clustered master server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	CLUSTER_ECA_TRUST_STORE_PATH = *Path to the external CA certificate*

Table 9-14   CLUSTER_ECA_TRUST_STORE_PATH information *(continued)*

Usage	Description
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_PRIVATE_KEY_PATH for clustered master server

The CLUSTER_ECA_PRIVATE_KEY_PATH option is specific to clustered master server. It specifies the path to the private key for the external CA-signed certificate of the virtual name.

If the virtual name certificate's private key is encrypted, you should define the CLUSTER_ECA_KEY_PASSPHRASEFILE option.

See "CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered master server" on page 327.

Table 9-15   CLUSTER_ECA_PRIVATE_KEY_PATH information

Usage	Description
Where to use	On clustered master server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	CLUSTER_ECA_PRIVATE_KEY_PATH = *Path to the private key of the external certificate*
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

CLUSTER_ECA_KEY_PASSPHRASEFILE for clustered master server

The CLUSTER_ECA_KEY_PASSPHRASEFILE option is specific to clustered master server. It specifies the path to the text file where the passphrase for the virtual name certificate's private key is stored.

CLUSTER_ECA_KEY_PASSPHRASEFILE is optional. You should define this option if the virtual name certificate's private key is encrypted.

See "CLUSTER_ECA_PRIVATE_KEY_PATH for clustered master server" on page 327.

Table 9-16   CLUSTER_ECA_KEY_PASSPHRASEFILE information

Usage	Description
Where to use	On clustered master server.
How to use	Use the nbgetconfig and the nbsetconfig commands to view, add, or change the option.
	For information about these commands, see the NetBackup Commands Reference Guide.
	Use the following format:
	CLUSTER_ECA_KEY_PASSPHRASE_FILE = *Path to the passphrase file*
Equivalent Administration Console property	No equivalent exists in the **NetBackup Administration Console** host properties.

Configuring an external certificate for a clustered master server

Use this section to configure an external CA-signed certificate for a clustered master server. The enrolled certificate is used for host communication.

Requirements

- Ensure that the NetBackup domain is enabled to use external CA-signed certificates by configuring the NetBackup web server.
  See "Configuring an external certificate for the NetBackup web server" on page 313.

- Ensure that external certificates for the NetBackup web server and the virtual name are issued by the same certificate authority.
  If the two certificate authorities do not match, communication between the **NetBackup Administration Console** and the NetBackup Web Management Console service (nbwmc service) fails.

To enroll an external certificate for a clustered master server

1   Update the NetBackup configuration file that is present on the shared disk (nbcl.conf) with the external certificate configuration options.

Use the `nbsetconfig` command to configure the following options:

- `CLUSTER_ECA_CERT_PATH`
- `CLUSTER_ECA_TRUST_STORE_PATH`
- `CLUSTER_ECA_PRIVATE_KEY_PATH`
- `CLUSTER_ECA_KEY_PASSPHRASEFILE` (optional)

You need to configure the certificate revocation list (CRL) configuration options for each node.

2   Run the following command on the master server:

```
nbcertcmd -enrollCertificate -cluster
```

The enrolled certificate is used for communication between the active node and the master server domain that is listed in the SERVER configuration option on the host.

For more details on the command, refer to the *NetBackup Commands Reference Guide*.

3   Configure an external certificate on each cluster node.

About API keys in NetBackup

This chapter includes the following topics:

- About API keys

- Creating API keys

- Managing an API key

- Using an API key

About API keys

NetBackup supports user authetication through API keys.

A NetBackup API key is a pre-authenticated token that lets a NetBackup user run NetBackup commands (such as `nbcertcmd -createToken` or `nbcertcmd -revokeCertificate`) or access NetBackup RESTful APIs.

Unlike a password, an API key can exist for a long time and you can configure its expiration. Therefore, operations like automation that need authentication can run for a long time using API keys.

See "Creating API keys" on page 330.

See "Using an API key" on page 331.

See "Managing an API key" on page 331.

Creating API keys

A user can have only one API key.

You can create API keys in one of the following ways:

- Using the `netbackup/security/api-keys POST` API
  Any user can create an API key using the `api-keys` API

- Using the NetBackup web UI
  For more details on creating API keys using the web UI or RBAC roles, refer to the *NetBackup Web UI Security Administrator's Guide*.

See "Using an API key" on page 331.

See "Managing an API key" on page 331.

Managing an API key

Each API key is associated with an API key tag. You can update or delete an API key using its API key tag in one of the following ways:

- Using the `netbackup/security/api-keys` API
  You can update or delete an API key using its API key tag.

- Using the NetBackup web UI
  For more details on managing API keys using the web UI, refer to the *NetBackup Web UI Security Administrator's Guide*.

See "Creating API keys" on page 330.

See "Using an API key" on page 331.

Using an API key

Once an API key is created, you can use it while you access RESTful APIs or run commands:

See "Creating API keys" on page 330.

Using an API key while accessing NetBackup RESTful APIs

◆ Pass the API key in the API request header to access other NetBackup APIs.

Using an API key while you run NetBackup commands

1 Do one of the following:

- Run the following command:
  `bpnbat -Login -LoginType APIKEY`
  You can run NetBackup commands that require authentication for the next 24 hours without requiring to run `bpnbat -Login`.

- Set a new environment variable called `NETBACKUP_APIKEY` for the API key.

You can run NetBackup commands that require authentication until the API key is valid and the environment variable is set.

2   Run a command such as `nbcertcmd -createToken`.

For more details on NetBackup commands, refer to the *NetBackup Commands Reference Guide*.

Setting an API key environment variable to run NetBackup commands

To use an API key while running NetBackup commands that need user authentication, you need to create an API key and set an environment variable for the API key. Once the environment variable is set, you can run the commands until the API key is valid and the environment variable is set.

On Windows platform, set the API key environment variable in the user context.

Example of an environment variable for an API key:

`NETBACKUP_APIKEY = ` *MasterServer1*:*APIKEY1*

If you want to set multiple API keys, specify the master server and API key mappings in a comma-separated format.

For example:

`NETBACKUP_APIKEY =`
MasterServer1:*APIKEY1*,*MasterServer2*:*APIKEY2*,*MasterServer3*:*APIKEY3*

You can also specify the mappings in a file and the file should be specified with prefix '@'.

For example:

`NETBACKUP_APIKEY = @`*file_path/file_name*

The contents of the file should be as follows:

MasterServer1:*APIKEY1*

MasterServer2:*APIKEY2*

MasterServer3:*APIKEY3*

Data at rest encryption security

This chapter includes the following topics:

Data at rest encryption terminology

The following table describes the data at rest encryption terminology.

Table 11-1   Data at rest encryption terminology

Term	Description
Advanced Encryption Standard (AES)	Specifies the synchronous encryption algorithm that replaced DES.
Asynchronous encryption	Includes the encryption algorithms that use both a public key and private key.
Data Encryption Standard (DES)	Specifies the accepted synchronous data encryption standard from the 1970s until 1998.

Table 11-1   Data at rest encryption terminology *(continued)*

Term	Description
Initialization vector	Specifies a seed value that is used to prime an encryption algorithm. Priming is done to obscure any patterns that would exist when using the same key to encrypt a number of data files. These files begin with the same pattern.
Public Key Encryption	Uses asynchronous encryption.
Synchronous encryption	Includes the encryption algorithms that use the same key for both encryption and decryption. For the same key size, synchronous algorithms are faster and more secure than their asynchronous counterparts.

Data at rest encryption considerations

The following table describes the data at rest encryption limitations.

Table 11-2   Data at rest encryption limitations

Limitation	Description
Computer performance effect of data encryption	Encryption algorithms are like data compressions algorithms in that they are very CPU intensive. Compressing data without the addition of computer hardware (either dedicated or shared), can affect computer and NetBackup performance.
Data compression must be performed before data encryption	Data compression algorithms look for data patterns to compress the data. Encryption algorithms scramble the data and remove any patterns. Therefore if data compression is desired, it must be done before the data encryption step.
Choice of an encryption algorithm	There are many encryption algorithms and associated key sizes. What should a user choose for data encryption? AES (Advanced Encryption Standard) is the standard for data encryption and supports 128, 192, or 256 -bit encryption keys.
Suggested key size	Generally, the larger key the more secure, and the longer into the future the data will stay secure. AES is one of the best choices because it is deemed secure with all three supported (128, 192, 256 bit) key sizes.

Table 11-2   Data at rest encryption limitations *(continued)*

Limitation	Description
FIPS certification for my encryption solution	While FIPS certification may be required for use by the US government, it should not be the only criteria that is used to evaluate an encryption solution.
	Other considerations should be part of any decision-making process as follows:
	■ FIPS certificates only apply to the named version of a product. And then only when the product is used in conformance with the "FIPS security policy" the document that is submitted when the product was validated. Future product versions and non-standard uses would be subject to questioned validation.
	■ The security of algorithms like AES is not in the obscurity of how they work. Rather the security is in the difficulty to deduce an unknown encryption key. The years of scrutiny and peer review for AES, have lead to mature implementations. In fact, tests exist for AES where specific keys and data sets are input, and verified against the expected output.
	■ Data encryption is much like automobile security. Most problems are related to lost or misplaced keys and not related to malfunctioning locks.
	■ Since misuse is more likely to lead to problems, the usability of an encryption product should be part of the consideration.
	Usability considerations include the following: ■ Encryption integration with the product ■ Encryption integration with business processes. ■ Appropriate encryption key granularity ■ Recoverability
Appropriate encryption key granularity	The appropriate encryption key granularity is best explained with the example of home security. A single house key is convenient. You can enter the garage, front door, or backdoor all using the same key. This security is good until the key is compromised (for example, if the key is stolen). Then you need to change all the locks that used the key. An extreme example is to have a key for every drawer and cupboard in a house. Then, a lost key would require the changing of on a single lock.
	The correct solution is somewhere in between. You must understand your tolerance for a compromised or lost key from your business process perspective. A lost key implies all the data that is encrypted with that key is destroyed. A compromised key implies all the data that is encrypted with that key must be decrypted and reencrypted to become secure.

Encryption security questions to consider

Before considering encryption security, the following questions should be asked.

The answers depend upon your particular encryption needs as follows:

- How do I choose the best encryption?

- Why would I use encryption security?

- What protection do I need from possible inside attacks?

- What protection do I need from possible outside attacks?

- What are the specific areas of NetBackup that encryption security protects?

- Do I need to create drawings of NetBackup architecture showing encryption security at work?

- What are my deployment use cases for encryption security?

Comparison of encryption options

The following NetBackup options exist for data at rest encryption:

- NetBackup client encryption, with standard encryption

- NetBackup client encryption, with legacy encryption

- Third-party encryption appliances and hardware devices

The following table shows the available encryption options along with their potential advantages and disadvantages.

Table 11-3   Encryption options comparison

Encryption option	Potential advantages	Potential disadvantages
Client encryption, standard encryption See "Configuring standard encryption on clients" on page 342.	■ The encryption key is on the client computer and not controlled by the NetBackup administrator ■ Can be deployed without affecting the NetBackup master and media servers ■ Can be deployed on a per client basis	■ The encryption key on the client does not scale well to environments where each client must have a unique encryption key and individual encryption key ■ Encryption and compression taking place on the client can affect client performance
Client encryption, legacy encryption See "Configuring legacy encryption on clients" on page 348.	Same advantages as client encryption with standard encryption.	Same disadvantages as client encryption with standard encryption.

Table 11-3   Encryption options comparison *(continued)*

Encryption option	Potential advantages	Potential disadvantages
Third-party encryption appliances and hardware devices	■ Little or no performance effect due to added hardware. ■ Generally NIST FIPS 140 certified.	■ The NetBackup Compatibility lab tests some of these solutions. This testing is neither an endorsement or rejection or a particular solution. This effort verifies that basic functionality was verified when used with a specific version of NetBackup. ■ No integration with NetBackup configuration, operation, or diagnostics. ■ The Disaster recovery scenario is provided by the appliance or device.

About NetBackup client encryption

The NetBackup client encryption option is best for the following:

■ Clients that can handle the CPU burden for compression / encryption

■ Clients that want to retain control of the data encryption keys

■ Situations where the tightest integration of NetBackup and encryption is desired

■ Situations where encryption is needed in terms of a per client basis

Installation prerequisites for encryption security

Encrypted backups require the NetBackup encryption software, which is included in NetBackup server and client installations. To use encryption, you must have a valid license. Refer to the NetBackup Administrator's Guide, Volume I for details on how to administer NetBackup licenses.

NetBackup Administrator's Guide, Volume I

For a list of the platforms on which you can configure NetBackup Encryption, see the NetBackup Release Notes.

About running an encryption backup

You can run an encryption backup as follows:

■ Choosing encryption for a backup
See "About choosing encryption for a backup" on page 338.

■ Standard encryption backup process

See "Standard encryption backup process" on page 338.

- Legacy encryption backup process
  See "Legacy encryption backup process" on page 339.

About choosing encryption for a backup

When a backup is started, the server determines from a policy attribute whether the backup should be encrypted. The server then connects to bpcd on the client to initiate the backup and passes the **Encryption** policy attribute on the backup request.

The client compares the **Encryption** policy attribute to the CRYPT_OPTION in the configuration on the client as follows:

- If the policy attribute is yes and CRYPT_OPTION is REQUIRED or ALLOWED, the client performs an encrypted backup.

- If the policy attribute is yes and CRYPT_OPTION is DENIED, the client performs no backup.

- If the policy attribute is no and CRYPT_OPTION is ALLOWED or DENIED, the client performs a non-encrypted backup.

- If the policy attribute is no and CRYPT_OPTION is REQUIRED, the client does not perform the backup.

The following table shows the type of backup that is performed for each condition:

Table 11-4   Type of backup performed

CRYPT_OPTION	Encryption policy attribute with CRYPT_OPTION	Encryption policy attribute without CRYPT_OPTION
REQUIRED	Encrypted	None
ALLOWED	Encrypted	Non-encrypted
DENIED	None	Non-encrypted

See "Standard encryption backup process" on page 338.

See "NetBackup standard encryption restore process" on page 340.

See "Legacy encryption backup process" on page 339.

See "NetBackup legacy encryption restore process" on page 341.

Standard encryption backup process

The prerequisites for encrypting a standard backup are as follows:

- **Note:** In NetBackup 7.5 and later versions, the encryption software is automatically installed with the NetBackup UNIX server and client installations.

  A key file must exist. The key file is created when you run the `bpkeyutil` command from the server or from the client.

- The **Encryption** attribute must be selected on the NetBackup policy that includes the client.

If the prerequisites are met, the backup takes place as follows:

- The client takes the latest key from the key file.

  For each file that is backed up, the following occurs:

  - The client creates an encryption `tar` header. The `tar` header contains a checksum of the key and the cipher that NetBackup used for encryption.

  - To write the file data that was encrypted with the key, the client uses the cipher that the CRYPT_CIPHER configuration entry defines. (The default cipher is AES-128-CFB.)

  Note: Only file data is encrypted. File names and attributes are not encrypted.

- The backup image on the server includes a flag that indicates whether the backup was encrypted.

Legacy encryption backup process

The prerequisites for encrypting a legacy backup are as follows:

- The encryption software must include the appropriate DES library, as follows:

  - For 40-bit DES encryption, `libvdes40.`suffix; the suffix is `so`, `sl`, or `dll`, depending on the client platform.

  - For 56-bit DES encryption, `libvdes56.`suffix; the suffix is `so`, `sl`, or `dll`, depending on the client platform.

  Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

- A key file must exist as specified with the CRYPT_KEYFILE configuration option. You create the key file when you specify a NetBackup pass phrase with the server `bpinst` command or the client `bpkeyfile` command.

- You must select the **Encryption** attribute on the NetBackup policy that includes the client.

If the prerequisites are met and the backup is to be encrypted, the following occurs:

- The client takes the latest data from its key file and merges it with the current time (the backup time) to generate a DES key. For 40-bit DES, 16 bits of the key are always set to zero.

  For each backed-up file, the following occurs:

  - The client creates an encryption `tar` header. The `tar` header contains a checksum of the DES that NetBackup used for encryption.

  - The client writes the file data that was encrypted with the DES key. Note that only file data is encrypted. File names and attributes are not encrypted.

- The server reads the file names, attributes, and data from the client and writes them to a backup image on the server. The server DOES NOT perform any encryption or decryption of the data. The backup image on the server includes the backup time and a flag that indicates whether the backup was encrypted.

NetBackup standard encryption restore process

The prerequisites for restoring a standard encrypted backup are as follows:

- The encryption software must be loaded onto the client.

  Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

- A key file must exist. The key file is created when you run the `bpkeyutil` command from the server or from the client.

When the restore occurs, the server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag on the restore request.

When a backup takes place properly, the restore occurs as follows:

- The server sends file names, attributes, and encrypted file data to the client to be restored.

- If the client reads an encryption `tar` header, the client compares the checksum in the header with the checksums of the keys in the key file. If the one of the keys' checksum matches the header's checksum, NetBackup uses that key to decrypt the file data. It uses the cipher that is defined in the header.

■ The file is decrypted and restored if a key and cipher are available. If the key or cipher is not available, the file is not restored and an error message is generated.

NetBackup legacy encryption restore process

The prerequisites for restoring a legacy encrypted backup are as follows:

■ The legacy encryption software must be loaded on the client.

Note: The encryption software is automatically installed with the NetBackup UNIX server and client installations.

■ The encryption software must include the 40-bit DES library. The name of the 40-bit DES library is `libvdes40.`suffix; the suffix is `so`, `sl`, or `dll` depending on the client platform.

■ If the CRYPT_STRENGTH configuration option is set to DES_56, the encryption software must also include the 56-bit DES library. The name of the 56-bit DES library is `libvdes56.`suffix; the suffix is `so`, `sl`, or `dll` depending on the client platform.

■ A key file must exist as specified with the CRYPT_KEYFILE configuration option. You create the key file when you specify a NetBackup pass phrase with the server `bpinst` command or the client `bpkeyfile` command.

The server determines from the backup image whether the backup was encrypted. The server then connects to `bpcd` on the client to initiate the restore. The server sends to the client an encryption flag and backup time from the backup image on the restore request.

If the prerequisites are met, the following occurs:

■ The server sends file names, attributes, and encrypted file data to the client to be restored.

■ The client takes its key file data and merges it with the backup time to generate one or more 40-bit DES keys. If the 56-bit DES library is available, the client also generates one or more 56-bit DES keys.

■ If the client reads an encryption `tar` header, the client compares the checksum in the header with the checksums of its DES keys. If the checksum of a DES key matches the checksum in the header, NetBackup uses that DES key to decrypt the file data.

The file is decrypted and restored if a DES key is available. If the DES key is not available, the file is not restored and an error message is generated.

Configuring standard encryption on clients

This topic describes how to configure standard NetBackup encryption.

The following configuration options are in the `bp.conf` file on UNIX clients, and in the registry on Windows clients.

The configuration options are as follows:

- CRYPT_OPTION
- CRYPT_KIND
- CRYPT_CIPHER

You can also use the **NetBackup Administration Console** to configure the options from the server. They are on the **Encryption** tab in the **Client Properties** dialog box.

See the NetBackup Administrator's Guide, Volume I for details.

Managing standard encryption configuration options

The following table describes the three encryption-related configuration options for the standard encryption that can exist on a NetBackup client.

Ensure that the options are set to the appropriate values for your client.

Table 11-5   Three encryption-related configuration options

Option	Value	Description
`CRYPT_OPTION = option`		Defines the encryption options on NetBackup clients. The possible values for *option* follow:
	`denied|DENIED`	Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error.
	`allowed|ALLOWED`	(the default value) Specifies that the client allows either encrypted or unencrypted backups.
	`required|REQUIRED`	Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.
`CRYPT_KIND = kind`		Defines the encryption kind on NetBackup clients. The *kind* option can be set to any of the following option values.

| | Table 11-5 | Three encryption-related configuration options *(continued)* |

Option	Value	Description
	NONE	Neither standard encryption nor legacy encryption is configured on the client.
	STANDARD	Specifies that you want to use the cipher-based 128-bit encryption or 256-bit encryption. This option is the default value if standard encryption is configured on the client.
	LEGACY	Specifies that you want to use the legacy-based encryption, with 40-bit DES or 56-bit DES.
CRYPT_CIPHER = *cipher*		Defines the cipher type to use. It can be set to any of the following option values.
	AES-128-CFB	128-bit Advanced Encryption Standard. This is the default value.
	BF-CFB	128-bit Blowfish
	DES-EDE-CFB	Two Key Triple DES
	AES-256-CFB	256-bit Advanced Encryption Standard

Managing the NetBackup encryption key file

This topic describes how to manage the NetBackup encryption key file.

Note: The key file must be the same on all nodes in a cluster.

Use the bpkeyutil command to set up the cipher-based encryption key file and pass phrase on the NetBackup Encryption client.

- For a Windows client, the full command path is as follows

  install_path\NetBackup\bin\bpkeyutil

- For a UNIX client, the full command path is as follows

  /usr/openv/netbackup/bin/bpkeyutil

You are prompted to add a pass phrase for that client.

NetBackup uses the pass phrase you specify to create the key file, as follows:

- NetBackup uses a combination of the following two algorithms to create a key from the pass phrase that is up to 256 bits.

    - Secure hashing algorithm, or SHA1

    - Message digest algorithm, or MD5

- NetBackup uses the NetBackup private key and 128-bit AES algorithm to encrypt the key.

- The key is stored in the key file on the client.

- At run time, NetBackup uses the key and a random initialization vector to encrypt the client data. The initialization vector is stored in the header of the backup image.

Previous pass phrases remain available in the key file to allow restores of the backups that were encrypted by using those phrases.

Caution: You must remember the pass phrases, including the old pass phrases. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

The key file must be accessible only to the administrator of the client machine.

For a UNIX client, you must ensure the following:

- The owner is root.

- The mode bits are 600.

- The file is not on a file system that can be NFS mounted.

About configuring standard encryption from the server

You can configure most NetBackup clients for encryption by using the bpkeyutil command from the server.

Prerequisites include the following:

- The NetBackup client software must be running on the platforms that support NetBackup encryption (see the NetBackup Release Notes).

- The NetBackup clients must be running the required NetBackup version.

About creating encryption key files on the clients

Use the following guidelines to create encryption key files on the clients:

- If the server is in a cluster and is also an encryption client, all nodes in the cluster must have the same key file.

- The `bpkeyutil` command sets the cipher-based encryption key file and pass phrase on each NetBackup Encryption client.

  - For a Windows server, the full path to the command is as follows:

    ```
    install_path\NetBackup\bin\bpkeyutil
    ```

  - For a UNIX server, the full path to the command is as follows:

    ```
    /usr/openv/netbackup/bin/bpkeyutil
    ```

Creating the key files

For each encryption client, run the following command:

```
bpkeyutil -clients client_name
```

You are prompted for a new pass phrase to add to that client's key file.

To set up several clients to use the same pass phrase, specify a comma-separated list of client names, as follows:

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

To create the key file, NetBackup uses the pass phrase you specify.

NetBackup uses the pass phrase you specify to create the key file, as follows:

- NetBackup uses a combination of the following two algorithms to create a key from the pass phrase that is up to 256 bits.

  - Secure hashing algorithm, or SHA1

  - Message digest algorithm, or MD5

- NetBackup uses the NetBackup private key and 128-bit AES algorithm to encrypt the key.

- The key is stored in the key file on the client.

- At run time, NetBackup uses the key and a random initialization vector to encrypt the client data. The initialization vector is stored in the header of the backup image.

Previous pass phrases remain available in the file for restores of the backups that were encrypted with those phrases.

Caution: You must ensure that pass phrases, whether they are new or were in use previously, are secure and retrievable. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine. For a UNIX client, you must ensure the following:

- The owner is root.

- The mode bits are 600.

- The file is not on a file system that can be NFS mounted.

Best practices for key file restoration

Even when an encrypted backup does not have a key file available, you may be able to restore the files.

Manual retention to protect key file pass phrases

Manual retention is the most secure method for protecting your key file pass phrases.

When you add a phrase by using the `bpkeyutil` command, complete manual retention as follows:

- Write the phrase on paper.

- Seal the paper in an envelope

- Put the envelope into a safe.

If you subsequently need to restore from encrypted backups and you have lost the key file, do the following:

- Reinstall NetBackup.

- Use `bpkeyutil` to create a new key file by using the pass phrases from the safe.

Automatic backup of the key file

The automatic backup method is less secure, but it ensures that a backup copy of your key file exists.

This method requires that you create a non-encrypted policy to back up the key file. If the key file is lost, you can restore it from the non-encrypted backup.

The problem with this method is that a client's key file can be restored on a different client.

If you want to include the key file in the back up to a client, add the key file's path name to the client's include list.

Redirected restores require special configuration changes to allow a restore.

Restoring an encrypted backup file to another client

Redirected restores are described in the following procedure.

To restore an encrypted backup to another client

1 The server must allow redirected restores, and you (the user) must be authorized to perform such restores.

See the NetBackup Administrator's Guide, Volume I for details on redirected restores.

2 Obtain the pass phrase that was used on the other client when the encrypted backup was made. Without that pass phrase, you cannot restore the files.

Note if the pass phrase is the same on both clients, skip to step 5.

3 To preserve your own (current) key file, move or rename it.

4 Use the bpkeyutil command to create a key file that matches the other client's. When the bpkeyutil process prompts you for the pass phrase, specify the other client's pass phrase.

5 Restore the files to the other client.

After you restore the encrypted files from the client, rename or delete the key file that you created in step 4.

Next, you move or rename the original key file to its original location or name. If you do not re-establish your key file to its original location and name, you may not be able to restore your own encrypted backups.

About configuring standard encryption directly on clients

You can also configure NetBackup encryption directly on clients as explained in the following topics:

- Setting standard encryption attribute in policies
  See "Setting standard encryption attribute in policies" on page 348.

- Changing client encryption settings from the server
  See "Changing the client encryption settings from the NetBackup server" on page 348.

Setting standard encryption attribute in policies

You must set the **Encryption** attribute on your NetBackup policy as follows:

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.

- If the attribute is not set, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the **Attributes** tab of the policy in the **NetBackup Administration Console** to set or clear the **Encryption** attribute for a policy.

Refer to the NetBackup Administrator's Guide, Volume I for more information on how to configure policies.

Changing the client encryption settings from the NetBackup server

You can change the encryption settings for a NetBackup client from the **Client Properties** dialog on the NetBackup server.

To change the client encryption settings from the NetBackup server

1   Open the **NetBackup Administration Console** on the server.

2   Expand **Host Properties > Clients**.

3   In the **Clients** list, double click the name of the client that you want to change. The **Client Properties** window displays.

4   Expand **Properties > Encryption** to display the encryption settings for that client.

    See the following topic for information about the configuration options that correspond to the settings in the **Encryption** pane:

    See "Managing standard encryption configuration options" on page 342.

    For additional explanations of the settings, click the **Help** button in the window, or see the NetBackup Administrator's Guide, Volume I.

Configuring legacy encryption on clients

This topic discusses configuring legacy NetBackup encryption.

The configuration options are in the `bp.conf` file on UNIX clients and in the registry on Windows clients.

The options are as follows:

- CRYPT_OPTION

- CRYPT_STRENGTH
- CRYPT_LIBPATH
- CRYPT_KEYFILE

You can also use the **NetBackup Administration Console** to configure the options from the server. They are on the **Encryption** tab in the **Client Properties** dialog box.

Refer to the NetBackup Administrator's Guide, Volume I for details.

You can set the CRYPT_OPTION and CRYPT_STRENGTH options on the `bpinst` `-LEGACY_CRYPT` command. The equivalent option settings are -crypt_option, -crypt_strength, respectively.

About configuring legacy encryption from the client

The following table contains the legacy encryption-related configuration options that are on a NetBackup client. Ensure that these options are set to the appropriate values for your client. These are set if you run the `bpinst -LEGACY_CRYPT` command from the server to the client name.

Table 11-6   Legacy encryption configuration options

Option	Value	Description
CRYPT_OPTION = *option*		Defines the encryption options on NetBackup clients. The possible values for *option* follow:
	denied|DENIED	Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error.
	allowed|ALLOWED	(The default value) Specifies that the client allows either encrypted or unencrypted backups.
	required|REQUIRED	Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.
CRYPT_KIND = *kind*		Defines the encryption type on NetBackup clients. The possible values for *kind* follow:
	NONE	Neither standard encryption nor legacy encryption is configured on the client.

Table 11-6   Legacy encryption configuration options *(continued)*

Option	Value	Description
	`LEGACY`	Specifies the legacy encryption type, either 40-bit DES or 56-bit DES. This option is the default if the legacy encryption type is configured on the client, and the standard encryption type is not configured.
	`STANDARD`	Specifies the cipher encryption type, which can be either 128-bit encryption or 256-bit encryption.
`CRYPT_STRENGTH =` *strength*		Defines the encryption strength on NetBackup clients. The possible values for *strength* follow:
	`des_40|DES_40`	(The default value) Specifies 40-bit DES encryption.
	`des_56|DES_56`	Specifies the 56-bit DES encryption.
`CRYPT_LIBPATH =` *directory_path*		Defines the directory that contains the encryption libraries on NetBackup clients. The *install_path* is the directory where NetBackup is installed and by default is `C:\VERITAS`.
	`/usr/openv/lib/`	The default value on UNIX systems.
	install_path`\NetBackup\` `bin\`	The default value on Windows systems
`CRYPT_KEYFILE =` *file_path*		Defines the file that contains the encryption keys on NetBackup clients.
	`/usr/openv/var/keyfile`	The default value on UNIX systems.
	install_path`\NetBackup\var\` `keyfile.dat`	The default value on Windows systems.

Managing legacy encryption key files

This topic describes managing legacy encryption key files.

Note: The key file must be the same on all nodes in a cluster.

Each NetBackup client that does encrypted backups and restores needs a key file. The key file contains the data that the client uses to generate DES keys to encrypt backups.

You can use the `bpkeyfile` command on the client to manage the key file. Check the `bpkeyfile` command description in the NetBackup Commands Reference Guide for a detailed description.

The first thing that you need to do is to create a key file if it does not already exist. The key file exists if you set a pass phrase from the `bpinst -LEGACY_CRYPT` command from the server to this client name.

The file name should be the same as the file name that you specified with the CRYPT_KEYFILE configuration option as follows:

- For Windows clients, the default key file name is as follows

    install_path\NetBackup\var\keyfile.dat

- For UNIX clients, the default key file name is as follows

    /usr/openv/var/keyfile

NetBackup uses a key file pass phrase to generate a DES key, and it uses the DES key to encrypt a key file.

Generally, you use the key file pass phrase that is hard-coded into NetBackup applications. However, for added security you may want to use your own key file pass phrase.

See "Additional legacy key file security for UNIX clients" on page 357.

Note: If you do not want to use your own key file pass phrase, do not enter a new key file pass phrase. Instead, use the standard key file pass phrase and enter a new NetBackup pass phrase.

You must decide what NetBackup pass phrase to use. The NetBackup pass phrase is used to generate the data that is placed into the key file. That data is used to generate DES keys to encrypt backups.

To create the default key file on a UNIX client that is encrypted with the standard key file pass phrase, enter a command such as the following:

```
bpkeyfile /usr/openv/var/keyfile
Enter new keyfile pass phrase: (standard keyfile pass phrase)
Re-enter new keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: ************************
Re-enter new NetBackup pass phrase: ************************
```

You may enter new NetBackup pass phrases fairly often. Information about old pass phrases is kept in the key file. This method lets you restore any data that was

encrypted with DES keys generated from old pass phrases. You can use the
-change_netbackup_pass_phrase (or -cnpp) option on the `bpkeyfile` command
to enter a new NetBackup pass phrase.

If you want to enter a new NetBackup pass phrase on a Windows client, enter a
command similar to the following example:

```
bpkeyfile.exe -cnpp install_path\NetBackup\var\keyfile.dat
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

Caution: You must ensure that pass phrases, whether they are new or were in use
previously, are secure and retrievable. If a client's key file is damaged or lost, you
need all of the previous pass phrases to recreate the key file. Without the key file,
you cannot restore the files that were encrypted with the pass phrases.

The key file must only be accessible to the administrator of the client machine.

For a UNIX client, you must ensure the following:

- The owner is root.

- The mode bits are 600.

- The file is not on a file system that can be NFS mounted.

You must consider whether to back up your key file. For encrypted backups, such
a backup has little value, because the key file can only be restored if the key file is
already on the client. Instead, you can set up a NetBackup policy that does
non-encrypted backups of the key files of the clients. This policy is useful you require
an emergency restore of the key file. However, this method also means that a
client's key file can be restored on a different client.

If you want to prevent the key file from being backed up, add the key file's path
name to the client's exclude list.

About configuring legacy encryption from the server

You can configure most NetBackup clients for encryption by using the `bpinst`
command from the server.

Prerequisites for this method include the following:

- The NetBackup client software must be running on a platform that supports
  NetBackup encryption.
  Refer to the *NetBackup Release Notes* for details on supported platforms.

- The NetBackup clients must be running the required NetBackup version.
- If a clustered server is a client for NetBackup encryption, ensure that all nodes in the cluster have the same key file.

The `bpinst` command is loaded into the NetBackup bin directory on the server as follows:

- For a Windows server, the bin directory is as follows

  ```
  install_path\NetBackup\bin
  ```

- For a UNIX server, the bin directory is as follows

  ```
  /usr/openv/netbackup/bin
  ```

See the `bpinst` command description in the NetBackup Commands Reference Guide for details about the options that are available with the `bpinst` command.

For examples about how to use `bpinst`:

See "About pushing the legacy encryption configuration to clients" on page 353.

See "About pushing the legacy encryption pass phrases to clients" on page 354.

Normally, you specify client names in the `bpinst` command. However, if you include the -policy_names option, you specify policy names instead. The option affects all clients in the specified policies.

About pushing the legacy encryption configuration to clients

You can use the -crypt_option and -crypt_strength options on the `bpinst` command to set encryption-related configuration on NetBackup clients as follows:

- The -crypt_option option specifies whether the client should deny encrypted backups (denied), allow encrypted backups (allowed), or require encrypted backups (required).
- The -crypt_strength option specifies the DES key length (40 or 56) that the client should use for encrypted backups.

To install the encryption client software and require encrypted backups with a 56-bit DES key, use the following command from the server:

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56 \
-policy_names policy1 policy2
```

The example uses a UNIX continuation character (\) because it is long. To allow either encrypted or non-encrypted backups with a 40-bit DES key, use the following command:

```
bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 \
client1 client2
```

In clustered environments you can do the following:

- Push the configuration to the client only from the active node.
- Specify the host names of the individual nodes (not the virtual names) in the list of clients.

Note: The master server `USE_VXSS` setting in `bp.conf` should be set to `AUTOMATIC`. Use this setting when pushing from an NBAC enabled master to a host that does not have NetBackup previously installed. Also use this setting when NBAC has not enabled the master server's `USE_VXSS` setting in `bp.conf`.

About pushing the legacy encryption pass phrases to clients

To send a pass phrase to a NetBackup client, you can use the `bpinst` options -passphrase_prompt or -passphrase_stdin. The NetBackup client uses the pass phrase to create or update data in its key file.

The key file contains the data that the client uses to generate DES keys to encrypt backups as follows:

- If you use the -passphrase_prompt option, you are prompted at your terminal for a zero to 62 character pass phrase. The characters are hidden while you type the pass phrase. You are prompted again to retype the pass phrase to make sure that is the one you intended to enter.
- If you use the -passphrase_stdin option, you must enter the zero to 62 character pass phrase twice through standard input. Generally, the -passphrase_prompt option is more secure than the -passphrase_stdin option, but -passphrase_stdin is more convenient if you use `bpinst` in a shell script.

To enter a pass phrase for the client named client1 from a NetBackup server through standard input, you would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
This pass phase is not very secure
This pass phase is not very secure
EOF
```

To enter a pass phrase for the client named client2 from a NetBackup server, you would enter commands like the following:

```
bpinst -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

You may enter new pass phrases fairly often. The NetBackup client keeps information about old pass phrases in its key file. It can restore the data that was encrypted with DES keys generated from old pass phrases.

Caution: You must ensure that pass phrases, whether they are new or were in use previously, are secure and retrievable. If a client's key file is damaged or lost, you need all of the previous pass phrases to recreate the key file. Without the key file, you cannot restore the files that were encrypted with the pass phrases.

You must decide whether to use the same pass phrase for many clients. Using the same pass phrase is convenient because you can use a single bpinst command to specify a pass phrase for each client. You can also do redirected restores between clients when they use the same pass phrase.

Note: If you want to prevent redirected restores, you should specify different pass phrases by entering a separate bpinst command for each client.

For clustered environments you can do the following:

- Push the configuration to the client only from the active node.
- Specify the host names of the individual nodes (not the virtual names) in the list of clients.

Note: The master server USE_VXSS setting in bp.conf should be set to AUTOMATIC. Use this setting when pushing from an NBAC enabled master to a host that does not have NetBackup previously installed. Also use this setting when NBAC has not enabled the master server'sUSE_VXSS setting in bp.conf.

Restoring a legacy encrypted backup created on another client

If a server allows redirected restores, you (the user) must be authorized to perform such restores.

Refer to the NetBackup Administrator's Guide, Volume I for details on redirected restores.

To restore an encrypted backup that was created on another client:

1 Obtain the pass phrase that was used on the other client when the encrypted backup was made. Without that pass phrase, you cannot restore the files.

Note if the pass phrase is the same on both clients, skip to step 4.

2 To preserve your own (current) key file, move or rename it.

3 Use the bpkeyfile command to create a key file that matches the other client's. When the bpkeyutil process prompts you for the pass phrase, specify the other client's pass phrase.

```
bpkeyfile -change_key_file_pass_phrase key_file_path
```

The *key_file_path* is the path for a new key file on your client. This key file matches the other client's.

After you enter the command, bpkeyfile prompts you for the client's pass phrase (obtained in step 1).

For more information on the bpkeyfile command, refer to the NetBackup Commands Reference Guide.

4 Restore the files to the other client.

After you restore the encrypted files from the client, rename or delete the key file that you created in step 3.

Next, you move or rename the original key file to its original location or name. If you do not re-establish your key file to its original location and name, you may not be able to restore your own encrypted backups.

About setting legacy encryption attribute in policies

You must set the **Encryption** attribute in your NetBackup policy according to the following:

- If the attribute is set, the NetBackup server requests that NetBackup clients in that policy perform encrypted backups.

- If the attribute is not set, the NetBackup server does not request that NetBackup clients in that policy perform encrypted backups.

You can use the **Attributes** tab of the policy in the **NetBackup Administration Console** to set or clear the **Encryption** attribute for a policy.

Refer to the NetBackup Administrator's Guide, Volume I for more information on how to configure policies.

You can also use the `bpinst` command to set or clear the **Encryption** attribute for NetBackup policies. This method is convenient if you want to set or clear the attribute for several policies.

For example, to set the **Encryption** attribute for policy1 and policy2 from a NetBackup server, enter a command like the following:

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

The 1 parameter sets the encryption attribute (0 would clear it).

Changing client legacy encryption settings from the server

You can change the encryption settings for a NetBackup client from the **Client Properties** dialog on the NetBackup server.

To change the client encryption settings from the NetBackup server

1 In the **NetBackup Administration Console** on the server, expand **Host Properties > Clients**.

2 In the **Clients** list, double click the name of the client you want to change. The **Client Properties** dialog displays.

3 In the **Properties** pane, click **Encryption** to display the encryption settings for that client.

For additional explanation of the settings, click the Help option on the dialog, or refer to the NetBackup Administrator's Guide, Volume I.

Additional legacy key file security for UNIX clients

This topic applies only to UNIX NetBackup clients. The additional security is not available for Windows clients.

Note: Veritas does not recommend using the additional key file security feature in a cluster.

The key file for an encryption client is encrypted using a DES key that is generated from a key file pass phrase. By default, the key file is encrypted using a DES key that is generated from the standard pass phrase that is hard-coded into NetBackup.

Using the standard key file pass phrase lets you perform automated encrypted backups and restores the same way you perform non-encrypted backups and restores.

This method has potential problems, however, if an unauthorized person gains access to your client's key file. That person may be able to figure out what encryption

keys you use for backups or use the key file to restore your client's encrypted backups. For this reason, you must ensure that only the administrator of the client has access to the key file.

For extra protection, you can use your own key file pass phrase to generate the DES key to encrypt the key file. An unauthorized person may still gain access to this key file, but the restore is more difficult.

If you use your own key file pass phrase, backup, and restore are no longer as automated as before. Following is a description of what happens on a UNIX NetBackup client if you have used your own key file pass phrase.

To start a backup or restore on a client, the NetBackup server connects to the `bpcd` daemon on the client and makes a request.

To perform an encrypted backup or restore, `bpcd` needs to decrypt and read the key file.

If the standard key file pass phrase is used, `bpcd` can decrypt the key file automatically.

If you use your own key file pass phrase, `bpcd` can no longer decrypt the key file automatically, and the default `bpcd` cannot be used. You must initiate `bpcd` with a special parameter. See

---

Note: In a clustered environment, if you change the key file on one node, you must make the same change in the key file on all nodes.

Running the bpcd -keyfile command

This topic describes running the `bpcd` command as a stand-alone program.

To run `bpcd` **as a stand-alone program**

1 Use the -change_key_file_pass_phrase (or -ckfpp) option on the `bpkeyfile` command to change the key file pass phrase, as in the following example:

```
bpkeyfile -ckfpp /usr/openv/var/keyfile
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new keyfile pass phrase: (standard keyfile pass phrase)
******
Re-enter new keyfile pass phrase: (standard keyfile pass
phrase) ******
```

If you type a carriage return at the prompt, NetBackup uses the standard key file pass phrase.

2 Stop the existing `bpcd` by issuing the `bpcd -terminate` command.

3 Initiate the `bpcd` command with the -keyfile option. Enter the new key file pass phrase when prompted.

```
bpcd -keyfile
Please enter keyfile pass phrase: ******
```

`bpcd` now runs in the background, and waits for requests from the NetBackup server.

You can change the key file pass phrase at any time with the `bpkeyfile` command and the -ckfpp option. The new key file pass phrase does not take effect until the next time you start `bpcd`.

You can also change the NetBackup pass phrase that is used to generate the DES keys to encrypt backups. Change this phrase at any time with the `bpkeyfile` command and the -cnpp option. Note, however, that the new NetBackup pass phrase does not take effect until you kill the current `bpcd` process and restart `bpcd`.

Terminating bpcd on UNIX clients

To terminate `bpcd` on UNIX clients, use the `bpcd -terminate` command.

Data at rest key management

This chapter includes the following topics:

- Federal Information Processing Standards (FIPS)

- About FIPS enabled KMS

- About the Key Management Service (KMS)

- Installing KMS

- Configuring KMS

- About using KMS for encryption

- KMS database constituents

- Command line interface (CLI) commands

- Troubleshooting KMS

Federal Information Processing Standards (FIPS)

The Federal Information Processing Standards (FIPS) define U.S. and Canadian Government security and interoperability requirements for computer systems. The FIPS 140-2 standard specifies the security requirements for cryptographic modules. It describes the approved security functions for symmetric and asymmetric key encryption, message authentication, and hashing.

For more information about the FIPS 140-2 standard and its validation program, see the National Institute of Standards and Technology (NIST) and the

Communications Security Establishment Canada (CSEC) Cryptographic Module Validation Program website at http://csrc.nist.gov/groups/STM/cmvp.

The NetBackup Cryptographic Module is now FIPS validated. NetBackup KMS uses the NetBackup Cryptographic Module and can now be operated in FIPS mode.

See "About FIPS enabled KMS" on page 361.

About FIPS enabled KMS

NetBackup KMS can now be operated in the FIPS mode, wherein the encryption keys that you create are always FIPS approved. FIPS configuration is enabled by default.

When you create a new key, a salt is always generated with the new key. Providing the salt value is mandatory when you want to recover a key.

Consider the following example; `hrs09to12hrs` is a key created using an older version of NetBackup:

```
Key Group Name : ENCR_Monday

Supported Cipher : AES_256

Number of Keys : 8

Has Active Key : Yes

Creation Time : Wed Feb 25 22:46:32 2015

Last Modification Time: Wed Feb 25 22:46:32 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active
```

The key `hrs09to12hrs` is moved from key group `ENCR_Monday` to a new key group `ENCR_77`.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -modifykey
-keyname hrs09to12hrs -kgname ENCR_Monday -move_to_kgname ENCR_77
```

```
Key details are updated successfully
```

Now list all the keys of the `ENCR_77` key group. Note that the new key `Fips77` would be FIPS approved, but not `hrs09to12hrs` that was created using an older version of NetBackup.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -listkeys
-kgname NCR_77

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :
4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2
```

The new key `Fips77` is FIPS approved and also has a Salt value.

KMS with FIPS compliance is supported on the following platforms:

- MS Windows Server 2012

- Linux.2.6.16 x86-64 Suse-10

- Linux.2.6.18 x86-64 RHEL-5

About the Key Management Service (KMS)

The NetBackup Key Management Service (KMS) feature is included as part of the NetBackup Enterprise Server and NetBackup Server software. An additional license is not required to use this functionality. KMS runs on NetBackup and is a master server-based symmetric Key Management Service. The KMS manages symmetric cryptography keys for the tape drives that conform to the T10 standard. KMS has been designed to use volume pool-based tape encryption. KMS is used with the tape hardware that has a built-in hardware encryption capability. An example of a tape drive that has built-in encryption is the IBM ULTRIUM TD4 cartridge drive. KMS is also used with disk volumes associated with NetBackup AdvancedDisk storage solutions. KMS runs with Cloud storage providers. KMS runs on Windows and UNIX. KMS generates keys from your passcodes or it auto-generates keys. The KMS operations are done through the KMS command line interface (CLI) or the Cloud Storage Server Configuration Wizard (when KMS is used with Cloud storage providers). The CLI options are available for use with both `nbms` and `nbmkmsutil`.

KMS has a minimal effect on existing NetBackup operation system management and yet provides a foundation for future Key Management Service enhancements.

KMS considerations

The following table describes the considerations that relate to the functionality and use of KMS.

Table 12-1   Considerations that relate to the functionality and use of KMS

Consideration	Description
New NBKMS service	The `nbkms` service is a master-server-based service that provides encryption keys to the media server BPTM processes.
New `nbkmsutil` KMS configuration utility	For security reasons, the KMS configuration utility can only be run from the master server as root or administrator.

Table 12-1 Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
NetBackup wide changes	Changes were necessary throughout NetBackup for the following: ■ To allow for the `ENCR_` prefix on the volume pool names. ■ To communicate with the key Management Service. ■ To provide support for the T10 / SCSI standard tape drives with embedded encryption. ■ NetBackup GUI and CLI changes to report the encryption key tag addition to the NetBackup image information The `bpimmedia` and `bpimagelist` were modified. ■ An emphasis on recoverability and ease of use for this NetBackup release The recommended option is that all encryption keys are generated with pass phrases. You type in a pass phrase and the key management system creates a reproducible encryption key from that pass phrase.
KMS installation and deployment decisions	Following are decisions you must make for KMS deployment: ■ Whether to choose KMS random generated keys or pass phrase generated keys ■ Whether to include NBAC deployment
KMS security	No burden is placed on existing NetBackup services with additional security concerns.
Cipher types	The following cipher types are supported in KMS: ■ AES_128 ■ AES_192 ■ AES_256 (default cipher)
KMS recoverability	You can use KMS in such a way where all of the encryption keys are generated from pass phrases. You can record these pass phrases and then use them at a later time to recreate the entire KMS for NetBackup.

Table 12-1   Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description

KMS files	KMS files associated with it where information on the keys is kept, as follows:
	
	■ Key file or key database
	Contains the data encryption keys. The key file is located at /opt/openv/kms/db/KMS_DATA.dat.
	■ Host master key
	Contains the encryption key that encrypts and protects the KMS_DATA.dat key file using AES 256. The host master key is located at /opt/openv/kms/key/KMS_HMKF.dat
	■ Key protection key
	Encryption key that encrypts and protects individual records in the KMS_DATA.dat key file using AES 256. The key protection key is located at /opt/openv/kms/key/KMS_KPKF.dat. Currently the same key protection key is used to encrypt all of the records.
	  ■ Back up KMS files
	  If you want to back up the KMS files, the best practices should be followed. Put the KMS database file on one tape and the HMK files and KPK files on another tape. To gain access to encrypted tapes, someone would then need to obtain both tapes.
	  Another alternative is to back up the KMS data files outside of the normal NetBackup process. You can copy these files to a separate CD, DVD, or USB drive.
	  You can also rely on pass phrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by pass phrases. If you have recorded all of the encryption key pass phrases you can manually recreate KMS from information you have written down. If you only have a few encryption keys you generate this process could be short.

Table 12-1　Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
Key records	Key records contain many fields but the primary records are the encryption key, the encryption key tag, and the record state. Key records also contain some metadata.
	These key records are defined as follows:
	■ Encryption key This key is given to the tape drive. ■ Encryption key Tag This tag is the identifier for the encryption key. ■ Record state Each of the key records has a state. The states are prelive, active, inactive, deprecated, and terminated. ■ Metadata Metadata includes logical name, creation date, modification date, and description.
Key groups	Key groups are a logical name and grouping of key records. All key records that are created must belong to a group. A key group can only have one active state key record at any time. NetBackup supports 100 key groups. Only 30 encryption keys are allowed per key group.
Tape drives and media capabilities	Drive, tape, and NetBackup capabilities must all match for drive encryption to be successful. A number of drives adhere to the T10 standard. Some well-known tape drives we support (that adhere to the T10 standard) are LT0-4, LT0-5, LT0-6, IBM TS1120/30/40, Oracle T10000B/C, and so on.
	You can still run earlier LTO versions for reading and writing but you cannot encrypt the data. For example, if you use LT02 media, that data can be read in LT04 drives but they cannot be written in either unencrypted or encrypted format.
	You must keep track of these drive issues and media issues as you run setup encryption. Not only do you need the drives that are capable of encryption but the media needs to be grouped and capable of encryption. For later decryption the tape must be placed in a drive that is capable of decryption.
	Refer to Table 12-2 for brief information about interoperability between media and tape drives. Veritas recommends that you refer to vendor-specific user guides for detailed information.
	Refer to the article HOWTO56305 for more details.
KMS with NBAC	Information on using KMS with NBAC is included where applicable in various sections of this document. For further information, refer to the NetBackup NBAC documentation.

Table 12-1   Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
KMS with HA clustering	Information on using KMS with HA clustering is included where applicable in various sections of this document. For further information, refer to the NetBackup HA documentation
KMS logging	The service uses the new unified logging and has been assigned OID 286. The `nbkmsutil` command uses traditional logging and its logs can be found in the file `/usr/openv/netbackup/logs/admin/*.log`.
KMS with Cloud	Information on using KMS with Cloud providers is included where applicable in various sections of this document. For further information, refer to the NetBackup Cloud Administrator's Guide.
KMS with AdvancedDisk	Information on using KMS with AdvancedDisk storage is included where applicable in various sections of this document. For further information, refer to the NetBackup AdvancedDisk Storage Solutions Guide.
NBAC and KMS permissions	Typically when using NBAC and the `Setupmaster` command is run, the NetBackup related group permissions (for example, NBU_Admin and KMS_Admin) are created. The default root and administrator users are also added to those groups. In some cases the root and administrator users are not added to the KMS group when NetBackup is upgraded. The solution is to grant the root and administrator users NBU_Admin and KMS_Admin permissions manually.

Table 12-2   Media support for encryption

Media	LTO4 tape drives	LTO5 tape drives	LTO6 tape drives
LTO-2 media	Read only no encryption support	Not supported	Not supported
LTO-3 media	Read and Write no encryption support	Read only no encryption support	Not supported
LTO-4 media	Read and Write encryption enabled	Read and Write encryption enabled	read-only encryption enabled
LTO-5 media	Not supported	Read and Write encryption enabled	Read and Write encryption enabled
LTO-6 media	Not supported	Not supported	Read and Write encryption enabled

KMS principles of operation

KMS works with encryption capable tape drives. KMS is integrated into NetBackup in such a way so as to eliminate difficulties in using NetBackup from a system management perspective. KMS provides encryption key management for tape drives with built-in encryption capabilities. These tape drives adhere to the SCSI standard. A SCSI command enables encryption on the tape drive. NetBackup accesses this capability through the volume pool name.

About writing an encrypted tape

BPTM receives a request to write to a tape and to use a tape from a volume pool with the ENCR_ name prefix. The ENCR_ prefix is a signal to BPTM that the information to be written to tape is to be encrypted.

BPTM contacts KMS and requests an encryption key from the key group with a name that matches the name of the volume pool.

KMS hands back to BPTM an encryption key and a key identifier (known as the encryption key tag).

BPTM places the drive in encryption mode and registers the key tag and identifier tag with the drive. This process is all done with the SCSI security protocol in or out command that has been added to the SCSI specification.

The backup then proceeds as normal.

When the backup is complete, BPTM unregisters the key and tag with the drive and sets the drive back into regular mode.

BPTM then records the tag in the NetBackup image record catalog.

Figure 12-1 shows how the process flows.

Figure 12-1   Process flow for writing an encrypted tape

About reading an encrypted tape

When a tape is read and an area of the tape in encountered where an image is encrypted, BPTM determines: what tag is used and KMS loads that record and key into BPTM. Then BPTM provides the key to the drive and reading the tape proceeds as normal.

KMS terminology

Table 12-3 defines the terms that are associated with KMS.

Table 12-3 Definitions for common KMS terms

Term	Definition
Command line interface (CLI)	From the CLI, you can operate the KMS feature from the provided command line using the `nbkmsutil` command. You can use the CLI to: create a new key group, create a new key, modify key group attributes, modify key attributes, and get details of key groups. You can also get details of keys, delete a key group, delete a key, recover a key, modify the host master key, and get host master key ID. Further you can modify key protection key, get key protection key ID, get keystore statistics, quiesce the KMS database, unquiesce the KMS database.
Host Master Key (HMK)	The host master key contains the encryption key that encrypts and protects the `KMS_DATA.dat` key file using AES 256. The host master key is located at `/opt/openv/kms/key/KMS_HMKF.dat`.
Key	A key is an encryption key that is used to encrypt and decrypt data.
Key group record (KGR)	A key group record contains the details of a key group.
Key Management Service (KMS)	The key Management Service is a master server-based symmetric key Management Service that manages symmetric cryptography keys. Keys are managed for the tape drives that conform to the T10 standard (LTO4). The KMS is located in `/usr/openv/netbackup/bin/nbkms`.
Key record (KR)	A key record contains the details of an encryption key.
KMS database	The KMS database contains the data encryption keys.
Key Protection Key (KPK)	A key protection key is an encryption key that encrypts and protects individual records in the KMS_DATA.dat key file using AES 256. The key protection key is `kms/key/KMS_KPKF.dat`. Currently the same key protection key is used to encrypt all of the records.
Key file (key database)	A key file or key database contains the data encryption keys. The key file `/opt/openv/kms/db/KMS_DATA.dat`.
Key group	The key group is a logical name and grouping of key records. A key group can only have one active state key record at any time. One hundred key groups are supported.
Key record	Key records include the encryption key, encryption key tag, and the record state. Other useful metadata such as logical name, creation date, modification date, and description are also included.

Table 12-3 Definitions for common KMS terms *(continued)*

Term	Definition
Key record states	Key record states are as follows: ■ Prelive, which means that the key record has been created, but has never been used. ■ Active, which means that the key record can be used for encryption and decryption in both backup and restore. ■ Inactive, which means that the key record cannot be used for encryption, but can be used for decryption only during restore. ■ Deprecated, which means that the key record cannot be used for encryption or decryption. ■ Terminated, which means that the key record is not available for use but it can be deleted. ■ Keystore, which means that the keystore is the file that keeps the data encryption keys. ■ Pass phrase, which means that the pass phrase is a user-specified random string. Seed to create encryption keys. You have a choice of creating the HMK, the KPK, and the encryption key with or without a pass phrase. **Note:** Keep track of all pass phrases by recording them and storing them in a safe place for future use. Using a pass phrase has definite benefits. It results in keys with better security strength. And if keys are lost, you can regenerate them by providing the pass phrase that was used to create the original key.
Quiesce	A quiesce sets the KMS DB to read-only administrator mode. Quiescing is required to make a backup of consistent copy of the KMS DB files.
Tag	A tag is a unique identifier (UUID) used to identify an individual key or key group in a keystore.

Installing KMS

The following procedure describes how to install KMS.

Note: For more information on configuring KMS in a Cloud storage environment refer to the NetBackup Cloud Administrator's Guide.

The KMS service is called `nbkms`.

The service does not run until the data file has been set up, which minimizes the effect on environments not using KMS.

To install KMS

1 Run the `nbkms -createemptydb` command.

2 Enter a pass phrase for the host master key (HMK). You can also press **Enter** to create a randomly generated key.

3 Enter an ID for the HMK. This ID can be anything descriptive that you want to use to identify the HMK.

4 Enter a pass phrase for the key protection key (KPK).

5 Enter an ID for the KPK. The ID can be anything descriptive that you want to use to identify the KPK.

The KMS service starts when after you enter the ID and press Enter.

6 Start the service by running the following command:

```
nbkms
```

7 Use the `grep` command to ensure that the service has started, as follows:

```
ps -ef | grep nbkms
```

8 Create the key group. The key group name must be an identical match to the volume pool name. All key group names must have a prefix `ENCR_`.

Note: When using key management with Cloud storage, the `ENCR_` prefix is not required for the key group name.

To create a (non-Cloud storage) key group use the following command syntax.

```
nbkmsutil -createkg -kgname ENCR_volumepoolname
```

The `ENCR_` prefix is essential. When BPTM receives a volume pool request that includes the `ENCR_` prefix, it provides that volume pool name to KMS. KMS identifies it as an exact match of the volume pool and then picks the active key record for backups out of that group.

To create a Cloud storage key group use the following command syntax.

```
nbkmsutil -createkg -kgname cloud_provider_URL:volume_name
```

9 Create a key record by using the `-createkey` option.

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname -activate -desc "message"
```

The key name and message are optional; they can help you identify this key when you display the key.

The `-activate` option skips the prelive state and creates this key as active.

10 Provide the pass phrase again when the script prompts you.

In the following example the key group is called `ENCR_pool1` and the key name is `Q1_2008_key`. The description explains that this key is for the months January, February, and March.

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key -activate -desc "key for
Jan, Feb, & Mar"
```

11 You can create another key record using the same command; a different key name and description help you distinguish they key records:

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for
Apr, May, & Jun"
```

Note: If you create more than one key record by using the command `nbkmsutil -kgname` *name* `-activate`, only the last key remains active.

---

12 To list all of the keys that belong to a key group name, use the following command:

```
nbkmsutil -listkeys -kgname keyname
```

Note: Veritas recommends that you keep a record of the output of the `nbkmsutil` -listkeys command. The key tag that is listed in the output is necessary if you need to recover keys.

The following command and output use the examples in this procedure.

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name        : ENCR_pool1
Supported Cipher      : AES_256
Number of Keys        : 2
Has Active Key        : Yes
Creation Time         : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description           : -
 Key Tag     : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name             : Q2_2013_key
 Current State         : ACTIVE
 Creation Time         : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Apr, May, & Jun
 FIPS Approved Key     : No

 Key Tag     : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name             : Q1_2013_key
 Current State         : INACTIVE
 Creation Time         : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Jan, Feb, & March
 FIPS Approved Key     : No
Number of Keys: 2
```

Using KMS with NBAC

The following changes have been made to NBAC to support the introduction of KMS:

- Addition of the new authorization object `KMS`

- Addition of the new NetBackup user group `NBU_KMS Admin`

The permissions a user has on the KMS object determines the KMS-related tasks you are allowed to perform.

Table 12-4 shows the default KMS permissions for each of the NetBackup user groups.

Table 12-4   Default KMS permissions for NetBackup user groups

Set	Activity	NBU_ User	NBU_ Operator	NBU_ Admin	NBU_ Security Admin	Vault_ Operator	NBU_ SAN Admin	NBU_ KMS Admin
Browse	Browse	---	---	X	---	---	---	X
Read	Read	---	---	X	---	---	---	X
Configure	New	---	---	---	---	---	---	X
Configure	Delete	---	---	---	---	---	---	X
Configure	Modify	---	---	---	---	---	---	X

Besides the KMS permissions listed above, the NBU_KMS admin group also has the following permissions on other authorization objects:

- BUAndRest has Browse, Read, Backup, Restore, List

- HostProperties has Browse, Read

- License has Browse, Read

About installing KMS with HA clustering

In a typical NetBackup environment, it is possible that not all the optional packages are installed, licensed or configured. In such scenarios, any services that pertain to these optional products may not be active all the time. These services are hence not monitored by default and do not cause a NetBackup to failover if they fail. If at a future time an optional product is installed, licensed and configured, its services

can be manually configured then NetBackup can failover. If the fail. In this section, we document the manual steps that set up KMS to get cluster monitored.

Enabling cluster use with the KMS service

You can make the KMS service cluster-enabled by adding it to the list of services that can be monitored.

To enable cluster use with KMS

1   Open the command prompt on the active node of the cluster.

2   Change the directory, as follows:

On Windows: `<NetBackup_install_path>\NetBackup\bin`

On UNIX: `/usr/openv/netbackup/bin`

3   Run the following command:

On Windows: `bpclusterutil -addSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -addSvc nbkms`

4   Follow the optional product-specific steps to enable the product. For NetBackup Key Management Service run the command to create the database, and start the service.

Enabling the monitoring of the KMS service

You can enable the monitoring of the KMS service and failover NetBackup when the service fails.

To enable monitoring of the KMS service and failover NetBackup if it fails

1   Open a command prompt on the active node of the cluster.

2   Change the directory, as follows:

On Windows: `<NetBackup_install_path>\NetBackup\bin`

On UNIX: `/usr/openv/netbackup/bin`

3   Run the following command.

On Windows: `bpclusterutil -enableSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -enableSvc nbkms`

Disabling the monitoring of the KMS service

You can disable monitoring of the KMS service.

To disable monitoring of the KMS service

1 Open a command prompt on the active node of the cluster.

2 Change the directory, as follows:

On Windows: `<NetBackup_install_path>\NetBackup\bin`

On UNIX: `/usr/openv/netbackup/bin`

3 Run the following command:

On Windows: `bpclusterutil -disableSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -disableSvc nbkms`

Removing the KMS service from monitored list

You can remove the KMS service from the list of services that can be monitored.

To remove the KMS service from the list of monitored services

1 Disable monitoring of the optional product service using the previous procedure

2 Follow the optional product-specific steps to remove the product

3 Open the command prompt on the active node of the cluster

4 Change the directory, as follows:

On Windows: `<NetBackup_install_path>\NetBackup\bin`

On UNIX: `/usr/openv/netbackup/bin`

5 Run the following command:

On Windows: `bpclusterutil -deleteSvc "NetBackup Key Management Service"`

On UNIX: `bpclusterutil -deleteSvc nbkms`

Configuring KMS

The configuration of KMS is done by creating the key database, key groups, and key records. Then NetBackup is configured to work with KMS.

To configure and initialize KMS

1   Create the key database, the host master key (HMK), and the key protection key (KPK).

2   Create a key group that matches the volume pool.

3   Create an active key record.

Creating the key database

Use the following procedure to create an empty key database. A key database is created by invoking the service name with the `-createemptydb` option. This process checks and ensures that an existing key database does not already exist, and then proceeds with the creation. Two protection keys need to be created when the KMS is initialized. They are the Host Master Key (HMK) and the Key Protection Key (KPK).

As with all KMS key creation activities, the user is presented with the following options for creating these keys:

■   Keys are generated by pass phrases

■   Randomly generated pass phrases

You are prompted to provide a logical ID to be associated with each key. At the end of this operation, the key database and protection keys are established.

On a Windows system they can be found in the following files:

```
\Program Files\Veritas\kms\db\KMS_DATA.dat
\Program Files\Veritas\kms\key\KMS_HMKF.dat
\Program Files\Veritas\kms\key\KMS_HKPKF.dat
```

On a UNIX system, they can be found in the following files:

```
/opt/openv/kms/db/KMS_DATA.dat
/opt/openv/kms/key/KMS_HMKF.dat
/opt/openv/kms/key/KMS_HKPKF.dat
```

Note: On Windows the following `nbkms` command is run from the `C:\Program Files\Veritas\NetBackkup\bin` directory.

To create the key database

1 Run the following command:

```
nbkms -createemptydb.
```

2 Enter a pass phrase for the Host Master Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.

3 Enter an HMK ID. This ID is associated with the HMK; you can use it to find this particular key in the future.

4 Enter a pass phrase for the Key Protection Key, or press Enter to use a randomly generated key. Re-enter the pass phrase at the following prompt.

5 Enter a KPK ID. The ID can be anything descriptive that you want to use to identify the KPK.

About key groups and key records

A key group is a logical collection of key records where no more than one record is in the active state.

A key group definition consists of the following:

- Name
  Given to a key group. Should be unique within the keystore. Renaming of the key group is supported if the new name is unique within the keystore.

- Tag
  Unique key group identifier (not mutable).

- Cipher
  Supported cipher. All keys belonging to this key group are created with this cipher in mind (not mutable).

- Description
  Any description (mutable).

- Creation Time
  Time of creation of this key group (not mutable).

- Last Modification Time
  Time of last modification to any of the mutable attributes (not mutable).

About creating key groups

The first step for setting up encryption is to create a key group.

In the following example, the key group ENCR_mygroup is created:

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

Note: For this version of KMS, it is important that the group name you create (i.e., `mygroup`), is prefixed with `ENCR_`.

About creating key records

The next step is to create an active key record. The key record can either be created in the prelive state and then transferred to the active state. Or the key record can be created directly in the active state.

A key record consists of the following critical pieces of information:

- Name
  Name that is given to a Key, should be unique within a KG. The renaming of a Key is supported if the new name is unique within the KG.

- Key Tag
  Unique Key identifier (not mutable).

- Key Group Tag
  Unique KG identifier, to which this Key belongs (not mutable).

- State
  Key's current state (mutable).

- Encryption key
  Key, used to encrypt or decrypt the backup or restore data (not mutable).

- Description
  Any description (mutable).

- Creation Time
  Time of Key creation (not mutable).

- Last Modification Time
  Time of last modification to any of the mutable attributes (not mutable).

The following key record states are available:

- Prelive, which indicates that the record has been created, but has not been used

- Active, which indicates that the record and key are used for encryption and decryption

- Inactive, which indicates that the record and key cannot be used for encryption. But they can be used for decryption

- Deprecated, which indicates that the record cannot be used for encryption or decryption

■ Terminated, which indicates that the record can be deleted

Overview of key record states

The key record states include the prelive, active, inactive, deprecated, and terminated. Key record states adhere to a key record life cycle. Once a key has entered the active state (that is set up for encryption), the key must progress in proper order through the lifestyle. The proper order includes passing from one state to its adjacent state. A key cannot bypass any of the states.

Between the active state and terminated state, the record can move one state at a time in either direction. Outside of this state range, the transitions are one directional. Deleted key records cannot be recovered (unless they were created using a pass phrase), and active keys cannot be moved back to prelive state.

Note: Keys can be created in either the prelive state or the active state. Active key records are available for both backup and restore operations. An inactive key is only available for restore operations. Deprecated keys are not available for use. If your key record is in the deprecated state and you attempt to do a backup or restore with that key record, it can fail. A key record that is in the terminated state can be removed from the system.

The following figure shows the process flow for creating keys in a prelive state or an active state.

Figure 12-2   States possible for key creation

Key record state considerations

The following considerations can be followed for key record states.

- Key record state transitions are well-defined and you must go through the whole path of states to delete a key record.

- Setting a key record to active bumps active key record to the inactive state for that group. There can only be one active record in a group.

- The deprecated state is useful for saving a key and restricting its use. If as an administrator you think that a key has been compromised you can manually put a hold on anyone using that key without that key being deleted from the system. You can set the key record to the deprecated state and someone attempting to do a backup or restore with this deprecated key would get an error.

- The key record deletion involves two steps helping to reduce the possibility of accidentally deleting a key. You must first set deprecated keys to terminated and then you can delete the key record. Only terminated key records can be deleted (other than the keys which are in the prelive state).

- You can use the prelive state to create a key record before use.

Prelive key record state

A key record that is created in the prelive state can be made active or deleted.

The prelive state can be used in the following way:

■ The KMS administrator wants to test the creation of a key record without affecting the system. If the record is created correctly it can then be activated. If not created correctly the record can be deleted.

■ The KMS administrator wants to create a key record, but then only activate it at some time in the future. The reasons for this issue may include delay setting the record active until the KMS keystore has been backed up (or the pass phrase has been recorded). Or delay setting the record active until some future time. Key records in the prelive state can be made active or deleted from the system.

Active key record state

Active key records can be used to encrypt and decrypt data. If necessary, the active key record could be made inactive. The active state is one of the three most important data management states. The inactive state and deprecated state are the other two important data management states.

Key records can be created directly in the active state bypassing the prelive state. Key records in the active state can either stay active or be made inactive. Active records cannot go back to the prelive state.

Inactive key record state

Inactive key records can be used to decrypt data. If necessary, the inactive key record could be made active again or moved to the deprecated state. The inactive state is one of the three most important data management states. The active state and deprecated state are the other two important data management states.

Key records in the inactive state can either stay inactive, be made active, or be made deprecated.

Deprecated key record state

Deprecated key records cannot be used to encrypt or decrypt data. If necessary, key records in the deprecated state could be made inactive or terminated. The deprecated state is one of the three most important data management states. The active state and inactive state are the other two important data management states.

The deprecated state can be used in the following ways:

■ The use of a key needs to be tracked or regulated. Any attempt to use a deprecated key can fail, until its state is changed to the appropriate state.

- A key should not be needed any longer, but to be safe is not set to the terminated state.

  Key records in the deprecated state can either stay deprecated, be made inactive, or terminated.

Terminated key record state

The terminated state adds a second step or safety step for deleting a deprecated state key record. A terminated key record can be moved to the deprecated state and ultimately made active again as needed. A terminated key record can also be deleted from the KMS.

Caution: Before deleting a key, make sure that no valid image exists which was encrypted with this key

---

Key records in the terminated state can either stay terminated, be made deprecated, or physically deleted.

About backing up the KMS database files

Backing up the KMS database involves backing up the KMS files.

The KMS utility has an option for quiescing the database files or temporarily preventing anyone from modifying the data files. It is important to run the quiesce option if you plan to copy the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files to another location for backing up purposes.

During quiesce, NetBackup removes write access from these files; only read access is allowed.

When you run `nbkmsutil -quiescedb`, it returns with a quiesce successful statement and an indication of the number of outstanding calls. The outstanding calls number is more of a count. A count is placed on the file for the number of outstanding requests on this file.

After quiesce, you can then back up the files by copying them to another directory location.

After you have copied the files, you can unquiesce the KMS database files by using `nbkmsutil -unquiescedb`.

After the outstanding quiesce calls count goes to zero, the KMS can run the commands that can modify the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files. Write access is once again returned to these files.

About recovering KMS by restoring all data files

If you have made backup copies of the `KMS_DATA.dat`, `KMS_HMKF.dat`, and `KMS_KPKF.dat` files, it is just a matter of restoring these three files. Then startup the `nbkms` service and the KMS system will be up and running again.

Recovering KMS by restoring only the KMS data file

You can restore the backed-up copy of the KMS data file `kms/db/KMS_DATA.dat` by regenerating the `KMS_HMKF.dat` and `KMS_KPKF.dat` files with pass phrases. So, if you have written down pass phrases for the host master key and key protection key, you can run a command to regenerate those files. The system prompts you for the pass phrase and if the pass phrase you now enter matches the pass phrase originally entered, you will be able to reset the files.

To recover KMS by restoring only the KMS data file

1 Run the `nbkms -resetkpk` command.

2 Run the `nbkms -resethmk` command.

3 Startup the `nbkms` service.

Recovering KMS by regenerating the data encryption key

You can regenerate the complete KMS database by regenerating the data encryption keys. The goal is to create a brand new empty KMS database and then repopulate it with all your individual key records.

To recover KMS by regenerating the data encryption key

1 Create an empty KMS database by running the following command

```
nbkms -createemptydb
```

You do not have to use the same host master key and key protection key. You can choose new keys.

2 Run the `nbkmsutil -recoverkey` command and specify the key group, key name, and tag.

```
nbkmsutil -recoverkey -kgname ENCR_pool1 -keyname Q1_2008_key
  -tag
d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
```

If you did not keep an electronic copy of the output of the `nbkmsutil -listkey` command when you created the key, you must enter all 64 characters manually.

3   Enter the pass phrase at the prompt. It must be an exact match with the original pass phrase you previously provided.

Note: If the tag you enter already exists in the KMS database, you cannot recreate the key.

---

4   If the recovered key is the key that you want to use for backups, run the following command to make the key active:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
 -state active
```

The `-recoverkey` option places the key record in the inactive state, and it is brought into the KMS database in the inactive state.

5   If this is a key record that is to be deprecated, run the following command:

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
-state deprecated
```

Problems backing up the KMS data files

There can be problems backing up the KMS data files with the normal NetBackup tapes or with the catalog backup.

Caution: The KMS data files are not included in the NetBackup catalog backups.

If the KPK, HMK, and key files were included in a catalog backup, and the catalog backup tape is lost, the keystore is compromised because the tape contains everything needed to gain access to the keys.

Significant problems can exist if both the catalog backup and data tapes are lost together on the same transport truck, for example. If both tapes are lost together then that situation is not be any better than not ever encrypting the tape in the first place.

Encrypting the catalog is not a good solution either. If the KPK, HMK, and key file were included in a catalog backup, and the catalog backup itself is encrypted, you have done the equivalent of locking the keys in the car. To protect from this problem is why KMS has been established as a separate service for NetBackup and why the KMS files are in a separate directory from the NetBackup directories. However, there are solutions for backing up the KMS data files.

Solutions for backing up the KMS data files

The best solution for backing up KMS data files is to do so outside of the normal NetBackup process, or rely on pass phrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by pass phrases. So if you have recorded all of the pass phrases, then you can recreate the KMS manually from the information you have written down. One way to back up KMS is to place the KMS information on a separate CD, DVD, or USB drive.

Creating a key record

The following procedure shows how to create a key record using a pass phrase and bypassing the prelive state and creating an active key.

Note: If an attempt is made to add a key to a group that already has an active key, the existing key is automatically moved to the inactive state.

To create a key record and create an active key

1 To create a key record enter the following command:

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

2 Enter a pass phrase.

Listing keys from a key group

Use the following procedure to list all or selected keys that you created in a particular key group.

To list the keys in a key group

◆ To list the keys in a key group enter the following command:

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

The nbkmsutil outputs the list in the verbose format by default. Following is a non-verbose listing output.

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000

134220503860000000 -
KR my_latest_key Active 134220507320000000 134220507320000000
key for Jan, Feb, March data
Number of keys: 1
```

The following options helps to list all keys from a specific key group or a specific key from a particular key group:

```
# nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname
<key_name> | -activekey ]
```

```
[ -noverbose | -export ]
```

The `-all` option lists down all the keys from all the key groups. The keys are listed in a verbose format.

The `-kgname` option lists the keys from the specified key group.

The `-keyname` option lists a specific key from the specified key group. It must however be used with the option -kgname.

The `-activekey` option lists an active key from the specified key group name. It must however be used with the `-kgname` option.

Note: The `-activekey` and `-keyname` options are mutually exclusive.

The `-noverbose` option lists the details of the keys and key groups in a formatted form (non-readable). The default is a verbose list.

The `-export` option generates an output that the key_file requires. (The `key_file` is used in`nbkmsutil -export -path <key_container_path > -key_file` file. You can use the output for another key_file.

Run the following command to list all the keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list specific keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

Run the following command to list all keys from all groups:

```
nbkmsutil -listkeys -all
```

Run the following command to list all keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Run the following command to list the active keys from a specific key group:

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

Configuring NetBackup to work with KMS

Configuring NetBackup to work with KMS involves the following topics:

- NetBackup getting key records from KMS
  See "NetBackup and key records from KMS" on page 389.
- Setting up NetBackup to use encryption
  See "Example of setting up NetBackup to use tape encryption" on page 389.

NetBackup and key records from KMS

The first step in configuring NetBackup to work with KMS is to set up a NetBackup-supported, encryption-capable tape drive and the required tape media.

The second step is to configure NetBackup as you would normally, except that the encryption-capable media must be placed in a volume pool with the identical name as the key group you created when you configured KMS.

Note: The Key Management feature requires the key group name and NetBackup volume pool name match identically and both be prefixed with `ENCR_`. This method of configuration-enabled encryption support to be made available without requiring major changes to the NetBackup system management infrastructure.

Example of setting up NetBackup to use tape encryption

The following example sets up two NetBackup volume pools created for encryption (with the `ENCR_` prefix).

The following figure shows the **NetBackup Administration Console** with two volume pools with the correct naming convention to use KMS.

Figure 12-3   NetBackup Administration Console with two volume pools set up
to use KMS

Figure 12-4 shows a NetBackup Policy that is configured to use the volume pool
ENCR_testpool, which is the same name as the key group that you configured
earlier.

Figure 12-4   NetBackup Change Policy dialog box with KMS volume pool

When a NetBackup image has been encrypted, the key tag is recorded and associated with the image. You can see this information through the **NetBackup Administration Console** reports, or in the output of the `bpimmedia` and `bpimagelist` commands.

About using KMS for encryption

You can use KMS to run an encrypted tape backup, verify an encrypted tape backup, and manage keys. The following topics provide examples for each of these scenarios:

- Example of running an encrypted tape backup
  See "Example of running an encrypted tape backup" on page 392.

- Example of verifying an encryption backup
  See "Example of verifying an encryption backup" on page 393.

- About importing KMS encrypted images
  See "About importing KMS encrypted images" on page 392.

About importing KMS encrypted images

Importing KMS encrypted images is a two-phase operation. In phase one, the media header and each fragment backup header is read. This data is never encrypted. However, the backup headers indicate if the fragments file data is encrypted with KMS or not. In summary, phase one does not require a key.

Phase two rebuilds the catalog `.f` file, which requires it to read the encrypted data. The `key-tag` (`KAD` in `SCSI` terms) is stored on the tape by the hardware. The `NBU`/`BPTM` reads the `key-tag` from the drive, and sends it to KMS for a key lookup. If KMS has a key, then the phase two processes continues to read the encrypted data. If KMS has no key, the data is not readable until the KMS has the key recreated. This is when the pass phrase is important.

If you do not destroy keys, then KMS contains all the keys ever used and you can import any encrypted tape. Move the keystore to your DR site and you do not need to recreate it.

Example of running an encrypted tape backup

To run an encrypted tape backup, you must have a policy that is configured to draw from a volume pool with the same name as your key group.

Figure 12-5 shows a NetBackup Policy that you have configured to use the volume pool `ENCR_pool1`.

Figure 12-5 NetBackup Change Policy dialog box with KMS volume pool
ENCR_pool1

Example of verifying an encryption backup

When NetBackup runs a tape-encrypted backup, and you view the Images on
Media, you see the encryption key tag that is registered with the record. This key
tag is your indication that what was written to tape was encrypted. The encryption
key tag uniquely identifies which key was used to encrypt the data. You can run a
report and read down the policy column to determine whether everything on a
particular tape was encrypted.

KMS database constituents

The KMS database consists of three files:

- The keystore file (`KMS_DATA.dat`) contains all the key group and key records along with some metadata.

- The KPK file (`KMS_KPKF.dat`) contains the KPK that is used to encrypt the ciphertext portions of the key records that are stored in the keystore file.

- The HMK file (`KMS_HMKF.dat`) contains the HMK that is used to encrypt the entire contents of the keystore file. The keystore file header is an exception. It contains some metadata like the KPK ID and HMK ID that is not encrypted).

Creating an empty KMS database

An empty KMS database can be created by executing the command `nbkms -createemptydb`.

This command prompts you for the following information:

- HMK pass phrase (leave empty for a random HMK)

- HMK ID

- KPK pass phrase (leave empty for a random KPK)

- KPK ID

The KMS database backup and disaster recovery procedures vary for random and pass phrase-generated KPK and HMK as described below.

To recover when the HMK and KPK were generated randomly

1   Restore the keystore file from a backup.

2   Execute the command `nbkms -info` to find out the KPK ID and HMK ID of the KPK and HMK needed to decrypt this keystore file. The output should also inform you that the HMK and KPK for this keystore file were generated randomly.

3   Restore the HMK file corresponding to the HMK ID from a secure backup.

4   Restore the KPK file corresponding to the KPK ID from a secure backup.

Importance of the KPK ID and HMK ID

To decipher the contents of a keystore file, it is essential to identify the right KPK and HMK that will do the job. The KPK ID and HMK ID enable you to make this identification. Since these IDs are stored unencrypted in the keystore file header, they can be determined even if you only have access to the keystore file. It is

important to choose unique IDs and remember the association of IDs to pass phrases and files to be able to perform a disaster recovery.

About periodically updating the HMK and KPK

The HMK and KPK can be updated periodically using the `modifyhmk` and `modifykpk` options of the KMS CLI. These operations prompt you for a new pass phrase and ID and then update the KPK/HMK. You can choose either a random or a pass phrase-based KPK/HKM at each such invocation.

Note: It is a best practice to use the `-usepphrase` option when modifying the HMK and KPK so that you are required to use a known pass phrase for future recovery. With the -nopphrase option, KMS generates a random pass phrase that is unknown and eliminates the possibility of future recovery if needed.

Backing up the KMS keystore and administrator keys

The important KMS data files can be backed up by making copies of the key database KMS_DATA.dat, the Host Master Key KMS_HMKF.dat, and the Key Protection Key KMS_HKPKF.dat.

On Windows these files are as follows:

```
\Program Files\Veritas\kms\db\KMS_DATA.dat
\Program Files\Veritas\kms\key\KMS_HMKF.dat
\Program Files\Veritas\kms\key\KMS_KPKF.dat
```

On UNIX these files are at this location:

```
/opt/openv/kms/db/KMS_DATA.dat
/opt/openv/kms/key/KMS_HMKF.dat
/opt/openv/kms/key/KMS_KPKF.dat
```

Command line interface (CLI) commands

The following topics describe the command line interface (CLI), as follows:

- CLI usage help
  See "CLI usage help" on page 396.

- Create a new key group
  See "Create a new key group" on page 397.

- Create a new key
  See "Create a new key" on page 397.

- Modify key group attributes
  See "Modify key group attributes" on page 398.

- Modify key attributes
  See "Modify key attributes" on page 398.

- Get details of key groups
  See "Get details of key groups" on page 399.

- Get details of keys
  See "Get details of keys" on page 400.

- Delete a key group
  See "Delete a key group" on page 400.

- Delete a key
  See "Delete a key" on page 401.

- Recover a key
  See "Recover a key" on page 401.

- Modify host master key (HMK)
  See "Modify host master key (HMK)" on page 405.

- Get host master key (HMK) ID
  See "Get host master key (HMK) ID" on page 406.

- Modify key protection key (KPK)
  See "Modify key protection key (KPK)" on page 406.

- Get key protection key (KPK) ID
  See "Get key protection key (KPK) ID" on page 406.

- Get keystore statistics
  See "Get keystore statistics" on page 406.

- Quiesce KMS database
  See "Quiesce KMS database" on page 407.

- Unquiesce KMS database
  See "Unquiesce KMS database" on page 407.

CLI usage help

To get CLI usage help, use the NetBackup Key Management Service (KMS) utility
command (the nbkmsutil command) with the included arguments.

Use nbkmsutil -help -*option* for help on an individual option.

```
# nbkmsutil -help
nbkmsutil [ -createkg ] [ -createkey ]
[ -modifykg ] [ -modifykey ]
[ -listkgs ] [ -listkeys ]
[ -deletekg ] [ -deletekey ]
[ -modifyhmk ] [ -modifykpk ]
[ -gethmkid ] [ -getkpkid ]
[ -quiescedb ] [ -unquiescedb ]
[ -recoverkey]
[ -ksstats ]
[ -help ]
```

Create a new key group

To create a new key group, use the NetBackup Key Management Service (KMS) utility command (the nbkmsutil command) with the included arguments.

```
# nbkmsutil -help -createkg
nbkmsutil -createkg -kgname <key_group_name>
[ -cipher <type> ]
[ -desc <description> ]
```

Note: The default Cipher is AES_256.

-kgname   Specifies the name of the new key group (it has to be unique within the keystore).

-cipher   Specifies the type of cipher that is supported by this key group.

Create a new key

To create a new key, use the NetBackup Key Management Service (KMS) utility command (the nbkmsutil command) with the included arguments.

```
# nbkmsutil -help -createkey
nbkmsutil -createkey [ -nopphrase ]
-keyname <key_name>
-kgname <key_group_name>
[ -activate ]
[ -desc <description> ]
```

Note: The default key state is prelive.

`-nopphrase`	Creates the key without using a pass phrase. If this option is not specified, the user is prompted for a pass phrase.
`-keyname`	Specifies the name of the new key (it should be unique within the key group to which it belongs).
`-kgname`	Specifies the name of an existing key group to which the new key should be added.
`-activate`	Sets the key state to active (default key state is prelive).

Note: From this release, a salt is generated when you create a new key using a pass phrase. In the event where you try to recover a key, the system prompts you for a salt along with the pass phrase and key tag.

Modify key group attributes

To modify the key group attributes, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -modifykg
nbkmsutil -modifykg -kgname key_group_name
[ -name <new_name_for_the_key_group> ]
[ -desc <new_description> ]
```

`-kgname`	Specifies the name of the key group to be modified.
`-name`	Specifies the new name of the key group (should be unique within the keystore).

Modify key attributes

To modify the key attributes use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgname <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -move_to_kgname <key_group_name> ]
```

Note: The `-state` and `-activate` options are mutually exclusive.

`-keyname`	Specifies the name of the key to be modified.
`-kgname`	Specifies the name of the key group to which this key belongs.
`-name`	Specifies the new name of the key (it should be unique within the key group).
`-state`	Specifies the new state of the key (see valid key state transition order).
`-activate`	Sets the key state to active.
`-desc`	Adds the new description to the key.
`move_to_kgname`	Specifies the name of the key group that the key has to be moved to.

Get details of key groups

To get details of key groups, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -listkgs
nbkmsutil -listkgs [ -kgname <key_group_name> |
-cipher <type> |
-emptykgs |
-noactive ]
[ -noverbose ]
```

Note: By default all of the key groups are be listed. If no option is specified, the details of all of the key groups are returned.

`-kgname`	Specifies the name of a key group.
`-cipher`	Gets the details of all the key groups which support specific cipher type.
`-emptykgs`	Gets the details of all the key groups with zero keys in it.
`-noactive`	Gets the details of all the key groups in which there is no active key.
`-noverbose`	Prints the details in formatted form (non-readable) format. The default is verbose. The output is displayed in a human readable form.

The `-export` option generates an output that the key_file requires. The key_file is used in the `nbkmsutil -export -path <key_container_path > -key_file` file. The output can be used for another key_file.

`#` `nbkmsutil -listkeys -all | -kgname <key_group_name>`

`[ -keyname <key_name> | -activekey ]`

`[ -noverbose | -export ]`

Get details of keys

To get details of the keys, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

`#`**`nbkmsutil -help -listkeys`**
`nbkmsutil -listkeys -kgname <key_group_name>`
`[ -keyname <key_name> | -activekey ]`
`[ -noverbose ]`

`-kgname`	Specifies the key group name. The details of all of the keys belonging to a key group are returned.
`-keyname`	Gets the details of the specific key which belongs to a specific key group.
`-activekey`	Gets the details of a specific key group's active key.
`-noverbose`	Prints the details in formatted form (non-readable) format. The default is verbose. The output is displayed in a human readable form.

Delete a key group

To delete a key group, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

Note: Only empty key groups can be deleted.

`# `**`nbkmsutil -help -deletekg`**
`nbkmsutil -deletekg -kgname <key_group_name>`

`-kgname`	Specifies the name of the key group to be deleted. Only empty key groups can be deleted.

Only empty key groups can be deleted with `-deletekg` option. You can however, also force delete a key group even if it is not empty. Run the following command to force delete a key group:

```
# nbkmsutil -deletekg -kgname <key_group_name> -force
```

Delete a key

To delete a key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -deletekey
nbkmsutil -deletekey -keyname <key_name>
-kgname <key_group_name>
```

Note: Keys in either prelive state or terminated state can be deleted.

`-keyname`	Specifies the name of the key to be deleted (to delete, key state has to be in one of prelive, or terminated).
`-kgname`	Specifies the name of the key group to which this key belongs.

Recover a key

To recover a key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

```
# nbkmsutil -help -recoverkey
nbkmsutil -recoverkey -keyname <key_name>
-kgname <key_group_name>
-tag <key_tag>
[ -desc <description> ]
```

Note: The key state would be set to inactive.

The restore could fail if a key that is used in encrypting the backup data is lost (and no copy of it is available). These keys can be recovered (re-created) with the knowledge of the original key's attributes (tag and pass phrase).

`-keyname`	Specifies the name of the key to be recovered (re-created).
`-kgname`	Specifies the name of the key group to which this key should belong.

-tag   Specifies the tag that identifies the original key (we need to use the same tag).

Note: The user is prompted to enter the correct pass phrase to get the right key (the system does not verify the validity of entered pass phrases).

Note: From this release, whenever you recover a key, the system prompts you for a salt. A salt is generated for pass phrase derived keys in this version of KMS. To recover the keys that were generated with an older version of KMS, leave the salt field blank.

About exporting and importing keys from the KMS database

The export and import of keys allows the user to quickly sync multiple NetBackup domains to use the same set of keys or quickly move a set of keys from one domain to another domain. This feature is especially helpful for a disaster recovery-induced restore on a different NetBackup domain.

Exporting keys

The -export command helps to export keys and keys groups across domains. The following list contains important information about exporting keys and key groups:

- Keys are always exported along with their key group.

- Keys and key groups are exported in an encrypted key container (file) on the host where the Key Management Service (KMS) utility (nbkmsutil) is executed. The key container is pass phrase protected.

Note: The same pass phrase must be provided when you want to import the keys and key groups.

- Multiple ways of specifying the export contents are to select specific key groups or to selectively export keys.

Use the -export command as specified:

```
nbkmsutil -export -path <secure_key_container>

[ -key_groups <key_group_name_1 ...> | -key_file <key_file_name> ]
```

By default, the entire keystore is exported.

The `-path` command refers to a fully qualified path where the secure key container is stored.

The `-key_groups` command helps to list the key groups names that separated by spaces.

The `-key_file` command is the file path that lists the keys to be exported in a specific format.

The `<key_group_name>/<key_name>` command helps the user to export keys selectively. You can use a '*' to export all the keys from a particular group as shown:

```
<key_group_name>/*
```

You can use the `nbkmsutil -listkeys -export` command to generate an output in a format that this option requires. Refer `nbkmsutil -listkeys -export` for more details.

For more details about listing keys:

See

Note: The `-key_groups` and `-key_file` commands are mutually exclusive.

Run the following command to export the entire keystore:

```
nbkmsutil -export -path <secure_key_container>
```

Run the following command to export selected key groups:

```
nbkmsutil -export -path

<secure_key_container> -key_groups

<key_group_name_1 key_group_name_2 ...>
```

Run the following command to export selectively export keys:

```
nbkmsutil -export -path

<secure_key_container> -key_file

<key_file_name>
```

Troubleshooting common errors during an export

A set of errors that occur when you export the keys and key groups. This section helps you to troubleshoot them.

- The export can fail when the key container that you specify already exists on the host.
  Specify a different key container file and rerun the export operation.

- Export also fails when you mention incorrect keys or key group names.
  You must correct the keys or key group names and export them again.

Importing keys

The `-import` command helps to import keys and keys groups across domains. The following list contains important information about importing keys and key groups:

- When importing keys and key groups, you must have the key container file that is created during the export operation. You also need the same pass phrase that is used during the export.

- Importing keys is an atomic operation. It reverts backs all updates on encounter of any error during operation.

- Partial import is not supported.

- A preview of the import output is available. Run the `-preview` command to preview the results of the import.

- The import operation can have two modes, one that includes the `-preserve_kgname` command and another that excludes the `-preserve_kgname` command.
  By default, the key groups are imported with following name format:
  `< Original_Kgname_<timestamp> >`
  You can opt to preserve the key group name by explicitly specifying the `<-preserve_kgname>` option.

- Duplicate keys such as the keys with the same key tag or the same key are not imported.

- The import does not support key group merging.

You can however merge the keys, import the key group without using the `<-preserve_kgname>` command. Run the `nbkmsutil -modifykey -keyname <key_name> -kgname <key_group_name>` command to move key from current group to the required group.

For more information about moving keys:

See "Modify key attributes" on page 398.

If the same key(s) or key(s) that have the same key tags exist in a key group, they are ignored during import. Run the following commands to import the keys and key groups:

```
# nbkmsutil -import -path <secure_key_container>

[-preserve_kgname]
```

```
[ -desc <description> ]
```

```
[ -preview ]
```

The `-preserve_kgname` command preserves the key group names during import.

The `-desc <description>` command is a description that is associated with the key groups during import.

The `-preview` command display a preview of the import results.

Run the import operation with the `-preserve_kgname` as follows:

```
nbkmsutil -import -path
```

```
<secure_key_container>
```

```
[-preserve_kgname]
```

When you run the `-import` command with the `-preserve_kgname` command, the import operation tries to import the original key groups names from the key container. If a key group with the same name exists, the import operation fails.

Run the import operation without the `-preserve_kgname` as follows:

```
nbkmsutil -import -path
```

```
<secure_key_container>
```

When you run the `-import` command without the `-preserve_kgname` it imports the key groups, but the key group names are renamed using a suffix, for example a timestamp. Each key group that is renamed always has a unique name.

Troubleshooting common errors during an import

A set of errors that occur when you import the keys and key groups. This section helps you to troubleshoot them.

- During an import, when you import key groups with the `[-preserve_kgname ]` option, and if that group already exists in KMS, the entire operation fails.
  You must either delete or rename the existing key groups or exclude the `[-preserve_kgname ]` option and rerun the import operation.

- NetBackup KMS has a limit of 100 key groups. Each group has a limit of 30 keys. The operation fails if more than 100 key groups are imported.
  You must delete existing unwanted key groups and rerun the import operation.

Modify host master key (HMK)

To modify the host master key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

The HMK is used to encrypt the keystore. To modify the current HMK, the user should provide an optional seed or pass phrase. An ID (HMK ID) should also be provided that can remind them of the specified pass phrase. Both the pass phrase and HMK ID are read interactively.

```
# nbkmsutil -help -modifyhmk
nbkmsutil -modifyhmk [ -nopphrase ]
```

Get host master key (HMK) ID

To get the HMK ID, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments. The HMK ID is then returned.

```
# nbkmsutil -help -gethmkid
nbkmsutil -gethmkid
```

Get key protection key (KPK) ID

To get the KPK ID, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments. The command returns the current KPK ID.

```
# nbkmsutil -help -getkpkid
nbkmsutil -getkpkid
```

Modify key protection key (KPK)

To modify the key protection key, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

The KPK is used to encrypt the KMS keys. Currently, the KPK is per keystore. To modify the current KPK, the user should provide an optional seed or pass phrase. Also, provide an ID (KPK ID) that can remind us of the specified pass phrase. Both the pass phrase and KPK ID are read interactively.

```
# nbkmsutil -help -modifykpk
nbkmsutil -modifykpk [ -nopphrase ]
```

Get keystore statistics

To get the keystore statistics, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command returns the following keystore statistics:

- Total number of key groups

- Total number of keys

- Outstanding quiesce calls

```
# nbkmsutil -help -ksstats
nbkmsutil -ksstats [ -noverbose ]
```

Quiesce KMS database

To quiesce the KMS database, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command sends the quiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned as multiple backup jobs might quiesce the KMS database.

```
# nbkmsutil -help -quiescedb
nbkmsutil -quiescedb
```

Unquiesce KMS database

To unquiesce the KMS database, use the NetBackup Key Management Service (KMS) utility command (the `nbkmsutil` command) with the included arguments.

This command sends an unquiesce request to KMS. If the command succeeds, the current outstanding quiesce count is returned. A count of zero (0) means that the KMS database is completely unquiesced.

```
# nbkmsutil -help -unquiescedb
nbkmsutil -unquiescedb
```

Key creation options

Any use of the NetBackup KMS feature should include creating a backup of the `kms/db` and `kms/key` directories. The protection keys and the key database exist in two separate subdirectories to facilitate splitting these when creating a backup copy.

Note: Due to the small size of these files, that they change infrequently, and that they must not be included on any NetBackup tape that itself is encrypted, the files should be manually copied to backup media.

Note: The recommended approach for creating keys with this version of KMS is to always create keys from pass phrases. This includes both the protection keys (Host Master Key and Key Protection Key), and the data encryption keys associated with the key records). It is recommended that the pass phrases used to create the keys are recorded and stored for recovery purposes.

While allowing the KMS system to randomly generate the encryption keys provides a stronger solution, this usage cannot recover from the loss or corruption of all copies of the keystore and protection keys, and therefore is not encouraged.

Troubleshooting KMS

Use the following procedure to initiate troubleshooting for KMS.

To initiate troubleshooting for KMS

1   Determine what error code and description are encountered.

2   Check to determine if KMS is running and that the following KMS data files exist:

    ```
    kms/db/KMS_DATA.dat
    kms/key/KMS_HMKF.dat
    kms/key/KMS_KPKF.dat
    ```

    If the files do not exist, then KMS has not been configured, or the configuration has been removed. Find out what happened to the files if they do not exist. If KMS has not been configured, the `nbkms` service is not running. If KMS is not running or is not configured, it does not affect NetBackup operation. If you have previously used the `ENCR_` prefix for a volume pool name, this name must be changed as `ENCR_` now has special meaning to NetBackup.

3   Get the KMS configuration information:

    Get a key group listing by running the command `nbkmsutil -listkgs`. Get a listing of all the keys for a key group by running the command `nbkmsutil -listkeys -kgname` *key_group_name*.

4   Get operational log information such as KMS logs by way of VxUL OID 286 and BPTM logs.

5   Evaluate the log information. The KMS errors are handed back to BPTM.

6   Evaluate the KMS errors that are recorded in the KMS log.

Solution for backups not encrypting

If tape backups are not encrypted, consider the following solutions:

- Verify that a backup is not encrypted by checking that the encryption key tag field is not set in the image record.

- Verify that the key group and volume pool names are an exact match.

- Verify that there is a key record in the key group with an active state.

Other non-KMS configuration options to look at include:

- Verify that everything that is related to traditional media management is configured properly.

- Is the NetBackup policy drawing a tape from the correct volume pool.

- Does the encryption-capable tape drive have encryption capable media available. For example is LTO4 media installed in the LTO4 tape drive?

Solution for restores that do not decrypt

If the encrypted tape restores are not decrypting, consider the following solutions:

- Verify that the original backup image was encrypted to begin with by viewing the encryption key tag field in the image record.

- Verify that the key record with the same encryption key tag field is in a record state that supports restores. Those states include active or inactive states.

- If the key record is not in the correct state change the key back to the inactive state.

Other non-KMS configuration solution options to consider:

- Verify that the drive and media support encryption.

- Is the encrypted media being read in an encryption-capable tape drive?

Troubleshooting example - backup with no active key record

The following example shows what happens when you attempt a backup when there is no active key record.

Figure 12-6 shows a listing of key records. Three of them have the key group `ENCR_mygroup` and the same volume pool name. One key group named `Q2_2008_key` was active. At the end of the command sequence, the state of the `Q2_2008_key` key group is set to inactive.

Figure 12-6   Listing of key records

```
fel (root) [385]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name       : ENCR_mygroup
Supported Cipher     : AES_256
Number of Keys       : 3
Has Active Key       : Yes
Creation Time        : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description          : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name             : Q2_2008_key
  Current State        : Active
  Creation Time        : Sat Mar 15 11:02:46 2008
  Last Modification Time: Sat Mar 15 11:02:46 2008
  Description          : key for Apr, May, & Jun
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name             : Q1_2008_key
  Current State        : Inactive
  Creation Time        : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description          : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name             : test
  Current State        : Inactive
  Creation Time        : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description          : -
Number of Keys: 3
fel (root) [383]: nbkmsutil -modifykey -keyname Q2_2008_key -kgname ENCR_mygroup -state
Inactive
Key details are updated successfully
```

Figure 12-7 shows the listing of key records that are produced again, and you can see that the Q2_2008_key state is now listed as inactive.

Figure 12-7   Listing of key records with active key group modified

```
fel (root) [384]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name          : ENCR_mygroup
Supported Cipher        : AES_256
Number of Keys          : 3
Has Active Key          : No
Creation Time           : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description             : -
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name                : Q1_2008_key
  Current State           : Inactive
  Creation Time           : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description             : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name                : test
  Current State           : Inactive
  Creation Time           : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description             : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name                : Q2_2008_key
  Current State           : Inactive
  Creation Time           : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 13:53:33 2008
  Description             : key for Apr, May, & Jun

Number of Keys: 3
```

With no active key, what happens to the backup?

Figure 12-8 shows the BPTM log output. It logs the message within the 1227 error code in the BPTM log.

Figure 12-8   Output from `bptm` command

```
14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JRO111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance
0
14:29:16.384 [19978] <2> KMSCLIB::kmsGetKeyAndKad: Entering function....(KMSClib.cpp:583)
14:29:16.384 [19978] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:29:16.384 [19978] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB_19978_1536015948517350(Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_19978_1536015948517350(Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_19978_1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key
(1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JRO111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2
2 1 4 0 8193 1024 0 8 0
```

The Job Details dialog box shows the detailed status. You can see a message stating what failed and the detailed status. With the information in the previous diagnostics, you can determine the particular problem or to identify what a given problem is related to.

Troubleshooting example - restore with an improper key record state

The following example shows a restore with a key record in an improper state.

Figure 12-9 shows that a record you need is set to deprecated. This following shows the listing. The same command is used to change the state from inactive to deprecated.

Figure 12-9　　　Listing of key records with key group deprecated

```
fel (root) [426]: !385
nbkmsutil -listkeys -kgname ENCR_mygroup

Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : No
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -

  Key Tag   : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name            : Q1_2008_key
  Current State       : Inactive
  Creation Time       : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description         : Key for Jan, Feb, & March

  Key Tag   : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name            : test
  Current State       : Inactive
  Creation Time       : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description         : -

  Key Tag   : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name            : Q2_2008_key
  Current State       : Deprecated
  Creation Time       : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 14:52:59 2008
  Description         : key for Apr, May, & Jun

Number of Keys: 3
```

Figure 12-10 shows the `bptm` log output with the 1242 error returned.

Figure 12-10 `bptm` log output with error 1242

```
14:53:48.782 [21109] <2> io_read_back_header: drive index 0, reading backup header
14:53:48.791 [21109] <2> io_position_for_read: successfully positioned JRO111 to file number 3
14:53:48.796 [21109] <2> io_position_for_read: next block encryption status: LON 0x0000000000000009, algorithm
index 1, encryption status 0x6
14:53:48.796 [21109] <2> io_position_for_read: Kad type 0x0, kad length 32 Kad
[cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
14:53:48.796 [21109] <2> KMSCLIB::kmsGetKeyAndKadByKeyTag: Entering function....(KMSClib.cpp:655)
14:53:48.796 [21109] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:53:48.796 [21109] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:53:48.797 [21109] <2> Orb::init: Created anon service name: NB_21109_1537488329610200(Orb.cpp:600)
14:53:48.798 [21109] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_21109_1537488329610200(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:53:48.818 [21109] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:53:48.818 [21109] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:53:48.842 [21109] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:53:48.844 [21109] <16> get_encryption_key: NBKMS failed with error status: Operation not allowed for key record
in this state (1242)
```

Regenerating keys and certificates

This chapter includes the following topics:

About regenerating keys and certificates

Some of the keys and certificates can be recreated by simply restarting the NetBackup services. If you encounter any error related to keys or certificates, as a

best practice, restart the NetBackup services and verify if the keys or the certificate is recreated. If the key or certificate is not created proceed with the procedures mentioned in the following sections.

Regenerating NetBackup authentication broker keys and certificates

Follow the steps to regenerate NetBackup Authentication Brokers:

- Public and private keys on master server and media server.

- Certificates on the media server and clients.

To regenerate NetBackup authentication broker keys and certificates

1   Restart the NetBackup Authentication service. Ensure that the service is up and running.

2   Run the following command:

    bpnbaz -ConfigureAuth

    Answer **y** when prompted.

    For information on the command, see *NetBackup Commands Reference Guide*.

3   Restart all the NetBackup services. Before you restart the services, ensure that no jobs are running.

    For information on how to restart the services, see the *NetBackup Administrator's Guide, Volume I*.

Regenerating host identity keys and certificates

To regenerate host identity public keys, private keys, and certificates on the master server, media server, and clients:

- Change the key pair for a host.
  Changing a key pair results in both a new host ID-based certificate and a new host name-based certificate.
  See "Changing the key pair for a host" on page 264.

Regenerating web service keys and certificates

Follow the steps to regenerate web service public key and certificate on the master server.

To regenerate web service keys and certificates

1   Generate the security certificate. Run the following command:

  ■   Windows
      ```
      set WEBSVC_PASSWORD=<Password of User>
      nbcertconfig -t -user <User Name>
      ```

  ■   UNIX
      ```
      export WEBSVC_PASSWORD=<Password of User>
      nbcertconfig -t -user <User Name>
      ```

2   Configure NetBackup Authentication service for the web service user and web service. Run the following command:

  ```
  nbcertconfig -u -user <username>
  ```

  ```
  nbcertconfig -m -user <username>
  ```

3   Restart the NetBackup Authentication service.

Regenerating nbcertservice keys and certificates

Follow the steps to regenerate nbcertservice keys and certificates on the master server.

To regenerate nbcertservice keys and certificates

1   Remove the old folder with user name.

2   Generate the security certificate. Run the following command:

  ■   Windows
      ```
      set WEBSVC_PASSWORD=<Password of User>
      nbcertconfig -u -user <User Name>
      ```

  ■   UNIX
      ```
      export WEBSVC_PASSWORD=<Password of User>
      nbcertconfig -u -user <User Name>
      ```

Regenerating tomcat keys and certificates

Follow the steps to regenerate tomcat public key, private key, and certificates on the master server.

Note: The jkskey is a key to decrypt the keystore used by tomcat and is backed up as part of the catalog backup. There is no need to regenerate it.

To regenerate tomcat keys and certificates

1   Generate the security certificate. Run the following command:

■   Windows
    ```
    set WEBSVC_PASSWORD=<Password of User>
    nbcertconfig -t -user <User Name>
    ```

■   UNIX
    ```
    export WEBSVC_PASSWORD=<Password of User>
    nbcertconfig -t -user <User Name>
    ```

2   Regenerate other files in `tomcatcreds` folder apart from the `keystore` and
    the `credentials` file. Run the following command:

■   Windows
    ```
    c:\ProgramFiles\Veritas\NetBackup\wmc\bin\install>configurecerts.bat
    ```

■   UNIX
    ```
    /usr/openv/wmc/bin/install/configurecerts
    ```

Regenerating JWT keys

To regenerate JWT public and private keys on the master server:

■   Close the NetBackup Administrator Console and restart all the NetBackup
    services.
    For information on how to restart the services, see *Veritas NetBackup
    Administrator's Guide, Volume I*.

Regenerating NetBackup gateway certificates

To regenerate nbgateway certificates on the master server:

■   Restart all the NetBackup service.
    For information on how to restart the services, see *Veritas NetBackup
    Administrator's Guide, Volume I*.

Regenerating web trust store certificates

To regenerate web trust store certificates on the master and media server, run the
following command:

```
nbcertcmd -getCACertificate
```

Answer **y** when prompted.

For information on the command, see *Veritas NetBackup Commands Reference Guide*.

Regenerating VMware vCenter plug-in certificates

Follow the steps to regenerate vCenter plug-in certificates on the master server.

To regenerate VMware vCenter plug-in certificates

1   List the existing certificates and identify the existing entry for invalid certificates. Run the following command:

-   Windows

    ```
    C:\Program
    Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
    -list
    ```

-   UNIX

    ```
    /usr/openv/wmc/bin/install/manageClientCerts -list
    ```

2   Delete the invalid certificate. Run the following command:

-   Windows

    ```
    C:\Program
    Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
    -delete
    ```

-   UNIX

    ```
    /usr/openv/wmc/bin/install/manageClientCerts -delete
    ```

3   Generate a new certificate. Run the following command:

-   Windows

    ```
    C:\Program
    Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
    -create <master_server_name>
    ```

-   UNIX

    ```
    /usr/openv/wmc/bin/install/manageClientCerts -create
    <master_server_name>
    ```

4   Register the newly created certificate with the vCenter plug-in.

    For more information, see *VeritasNetBackup Plugin-in for VMware vCenter Guide*.

Regenerating OpsCenter Administrator Console session certificates

To regenerate session certificates on the master server:

- Close the NetBackup Administrator Console and restart all the NetBackup services.

  For information on how to restart the services, see *Veritas NetBackup Administrator's Guide, Volume I*.

Regenerating OpsCenter keys and certificates

Follow the steps to regenerate OpsCenter keys and certificates:

To regenerate OpsCenter keys and certificates

1   Reconfigure Authentication. Run the following commands on theOpsCenterserver :

    ```
    OpsCenter_Install_path\server\bin\stopAt

    OpsCenter_Install_path\server\bin\configureAt

    OpsCenter_Install_path\server\bin\startAt
    ```

2   Restart the OpsCenter services. Run the following commands on the OpsCenter server:

    ```
    OpsCenter_Install_path\server\bin>opsadmin.bat stop

    OpsCenter_Install_path\server\bin>opsadmin.bat start
    ```

For more information in the OpsCenter commands, see *Veritas NetBackup for OpsCenter Administrator's Guide*

Regenerating NetBackup encryption key file

To regenerate NetBackup encryption key file, run the following command:

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

When you are prompted to enter the passphrase, enter the passphrase you had saved originally.

For more information about key files, see See "About creating encryption key files on the clients" on page 344.

To perform this task using the bpkeyutil, see the NetBackup Commands Reference Guide.

NetBackup web services account

This chapter includes the following topics:

- About the NetBackup web services account
- Changing the web service user account

About the NetBackup web services account

Beginning with NetBackup 8.0, the NetBackup master server includes a configured web server to support critical backup operations. This web server operates under user account elements with limited privileges. These user account elements must be available on each master server (or each node of a clustered master server).

NetBackup requires account information for web services as part of the NetBackup master server installation.

More information is available on configuring this account prior to installation and on how to change the account after installation.

See the *NetBackup Installation Guide* for information on how to create the web server user and group.

See "Changing the web service user account" on page 421.

Note: For security purposes, do not allow the web server users or groups to have administrator or superuser privileges.

Changing the web service user account

To support changing web service user accounts, use the utility script `wmcUtils`. This utility script does not validate if a web service user and group exist. Before you use this utility, you must ensure that the web service user and the group exist and the user is part of the group. Consider the following when changing the web service user account:

- If your environment uses Windows domain users, use the `DOMAIN\USER` format.

- If you use a clustered environment on a Windows platform, the NetBackup web services user account must be a `DOMAIN` user. (Example: AD user)

- If you use non-clustered environments, the NetBackup web service user can be a local or a domain user.

- If you use a clustered environment on Linux or UNIX platforms, the NetBackup web service user can be a local user. Additionally, the group can be a local group. The NetBackup web service user must have the same name and UID on all nodes of the cluster. Also, the group must have the same name and GID on all nodes of the cluster. It is recommended to use domain users (Example: NIS) for clustered environments.

Note: Do not use the logged on user to run the `wmcUtils` utility script. If you are logged into an environment as *my_domain\my_user*, you cannot use this account to run the `NetBackup Web Management Console` service. NetBackup does not support this scenario.

To change the web service user account on Windows

1   Open command prompt.

2   Change the directory to: *install_path*`\wmc\bin\install`

3   Run `wmcUtils.bat -changeUser` to change the web service user.

Example: (`nbwebsvc1` is the web service user and `nbwebgrp1` is the user group that `nbwebsvc1` is a member of)

`wmcUtils.bat -changeUser nbwebsvc1 nbwebgrp1`

For more information about the `wmcUtils.bat` utility script, use the `wmcUtils.bat -help` option.

4   (Conditional) If using a clustered environment, run `wmcUtils.bat -changeUser` on the active and the inactive nodes.

5 Enter the web service user password (example: `nbwebsvc1`) when prompted by the script.

The `NetBackup Web Management Console` service is restarted when the correct password is entered. If you enter an incorrect password, a **Logon failure** error is displayed before the `NetBackup Web Management Console` service starts.

6 To verify that the web service user is changed, ensure that *install_path*`\bin\nbcertcmd.exe -ping` works.

Note: The output of `wmcUtils.bat` utility script is captured in the `nbwmc_support.log`. The log is located here:
install_path`\wmc\webserver\logs\nbwmc_support.log`

To change the web service user account on Linux or UNIX

1 Open a shell.

2 Change the directory to: `/usr/openv/wmc/bin/install`

3 Run `wmcUtils -changeUser` to change the web service user.

Example: (`nbwebsvc1` is the web service user and `nbwebgrp1` is the user group that `nbwebsvc1` is a member of)

`usr/openv/wmc/bin/install/wmcUtils -changeUser nbwebsvc1 nbwebgrp1`

For more information about the `wmcUtils` utility script, use the `wmcUtils -help` option.

4 (Conditional) If using a clustered environment, run `wmcUtils.bat -changeUser` on the active and the inactive nodes.

5 Enter the web service user password (example: `nbwebsvc1`) when prompted by the script.

The `NetBackup Web Management Console` service is restarted when the correct password is entered. If you enter an incorrect password, a **Logon failure** error is displayed before the `NetBackup Web Management Console` service starts.

6 To verify that the web service user is changed, ensure that `/usr/openv/netbackup/bin/nbcertcmd -ping` works.

Note: The output of `wmcUtils` utility script is captured in the `nbwmc_support.log`. The log is located here: `/usr/openv/wmc/webserver/logs/nbwmc_support.log`