Symantec NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 7.7

Symantec

Symantec NetBackup™ Security and Encryption Guide

Documentation version: 7.7

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

http://support.symantec.com

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

Contacting Technical Support

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

http://support.symantec.com/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

http://support.symantec.com/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Increasing NetBackup security

This chapter includes the following topics:

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 15.

See "NetBackup Access Control (NBAC)" on page 19.

See "Operating system security" on page 27.

See "Standard NetBackup security" on page 28.

See "Media Server Encryption Option (MSEO) security" on page 29.

See "Client side encryption security" on page 30.

See "NBAC on master, media server, and GUI security" on page 32.

See "NBAC complete security" on page 34.

See "All NetBackup security" on page 35.

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 datacenter 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 datacenter level.

Figure 1-1 World-level security scope

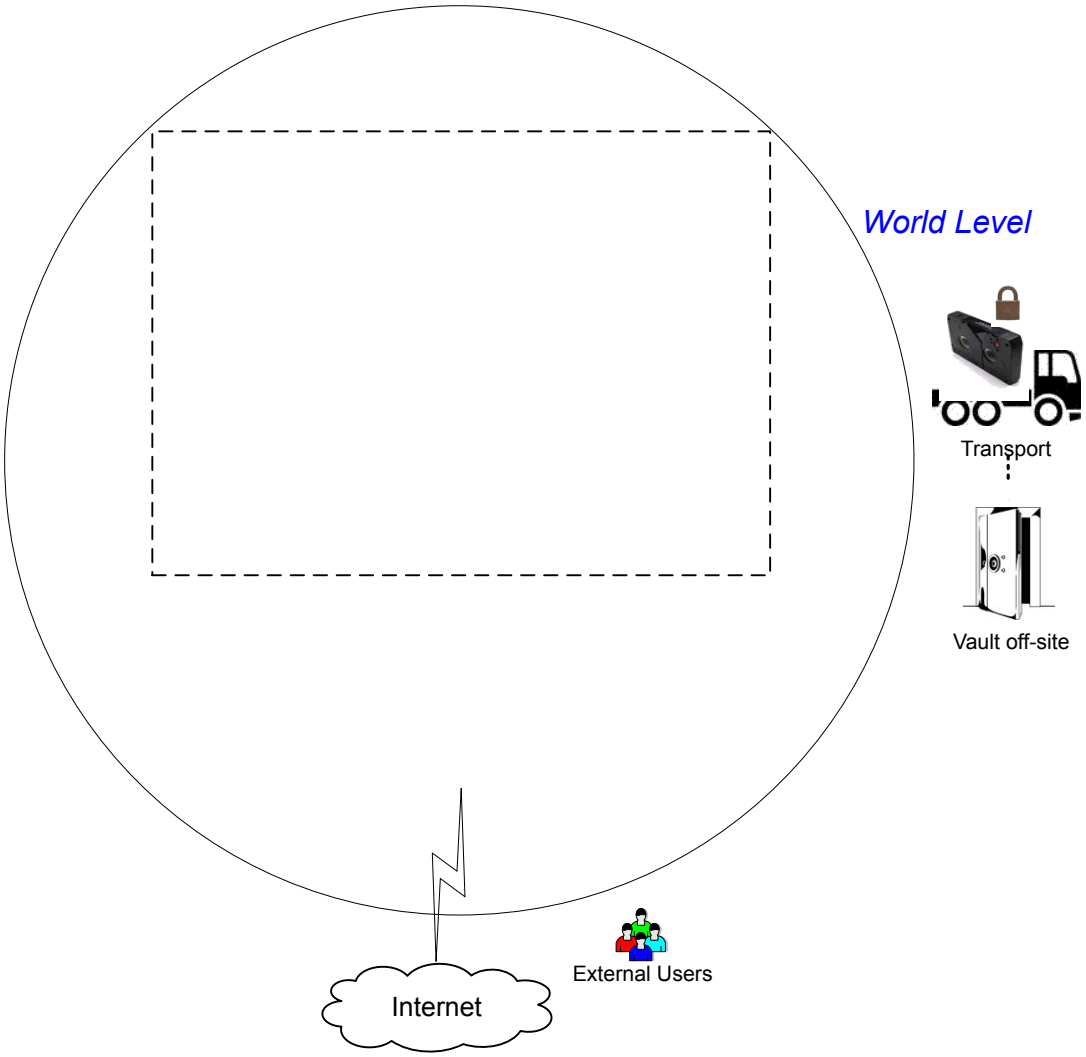


Table 1-2 Types of world-level security

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 datacenters 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 datacenter.

Enterprise-level security

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

Figure 1-2 Enterprise-level security scope

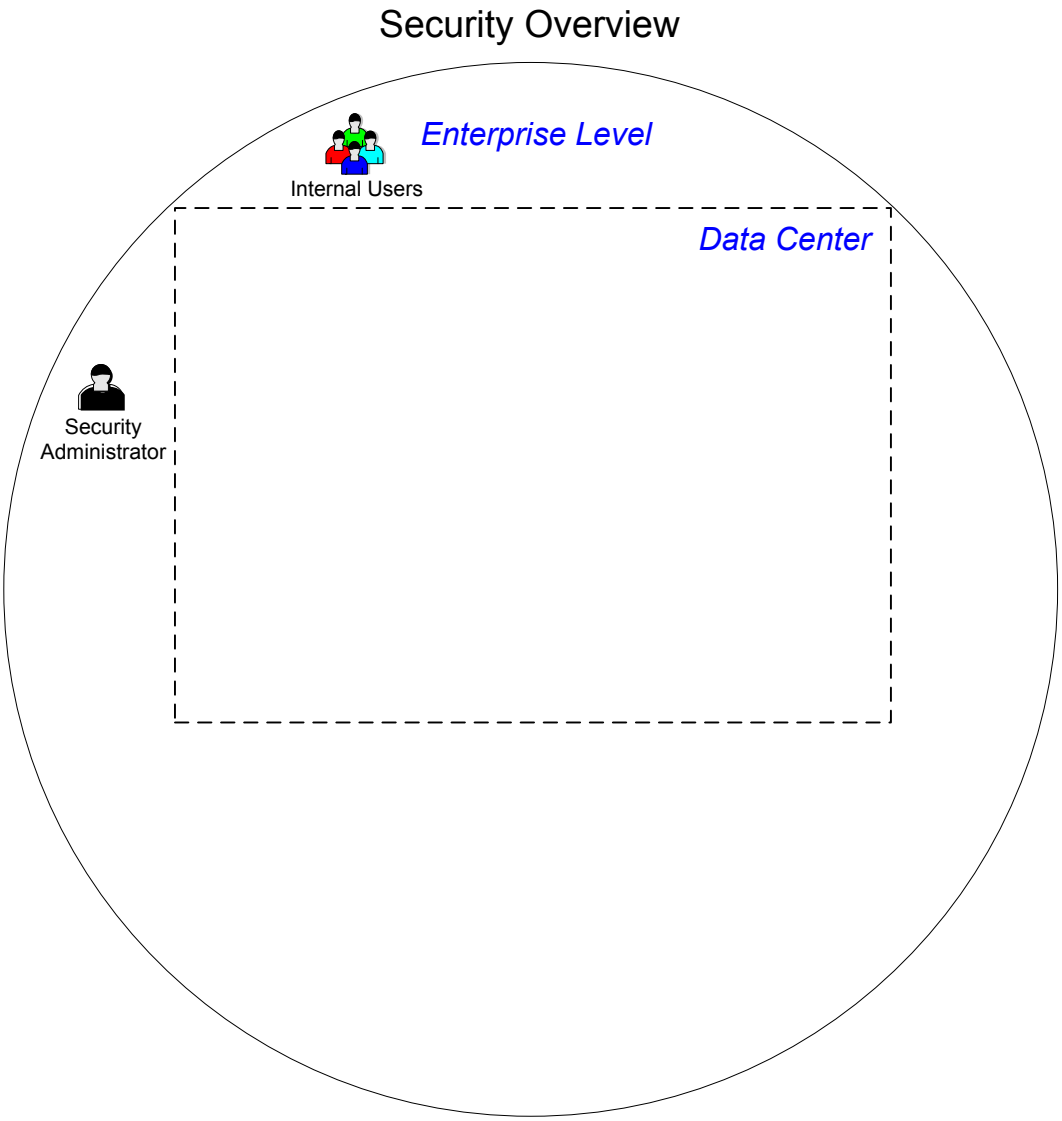


Table 1-3 Types of enterprise-level security

Type	Description
Internal users	Specifies users who have permissions to access and use NetBackup functionality from within the datacenter. 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 datacenter.

Datacenter-level security overview

Datacenter-level security comprises the core of NetBackup security functionality. It can consist of a workgroup, a single datacenter, 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 15.

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 15.

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 with the release of NetBackup 7.1 Security Services are embedded.

  Note: For back media servers and clients with a NetBackup version lower than 7.0, additional components are required from your NetBackup product Authentication and Authorization install kit on the ICS install disk(s).Note that NetBackup 7.0 already includes the client for AT and AZ.

- The NetBackup Product Authentication and Authorization consist of the root broker, authentication broker, authorization engine, and GUI.
- 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 7.6 master server is the root broker in a datacenter installation. There is no provision to use another root broker. The recommendation is to allow trust between root brokers. **Note:** In NetBackup installations prior to 7.0 only one root broker was required in a datacenter installation. Sometimes the root broker was combined with the authentication broker. The root broker authenticates the authentication broker. The root broker does not authenticate clients.
Authentication broker	Authenticates the master server, media server, GUI, 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 datacenter installation. The authentication broker can be combined with the root broker.

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

Component	Description
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 datacenter installation. The authorization engine also communicates over the WAN to authorize other media servers in a multi-datacenter environment.
GUI	Specifies a Remote Administration Console that receives credentials from the authentication brokers. The GUI then may use the credentials to gain access to functionality on the clients, media, and master servers.
MSEO	Specifies the MSEO (media server Encryption Option) that is a software appliance that encrypts data written to tape by the media server (data at rest encryption). The MSEO is an alternative to the client side encryption that can reduce the CPU processing load on the client.
Master server	Communicates with the root broker and authentication broker, GUI, authorization engine, media server, and clients.
NetBackup administrator	Specifies a user who has been granted administrator permissions to access and manage the NetBackup functionality from within the datacenter.
Media server	Communicates with the master server, root broker and authentication broker, authorization engine, MSEO, 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 ■ MSEO (media server Encryption Option) ■ Encryption of data at rest Unencrypted and encrypted data tapes are produced in the datacenter. The unencrypted tape data is written for clients 1 through 5 and stored on-site at the datacenter. The encrypted tapes are written for client 6 and are transported off-site to a vault for disaster recovery protection.

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

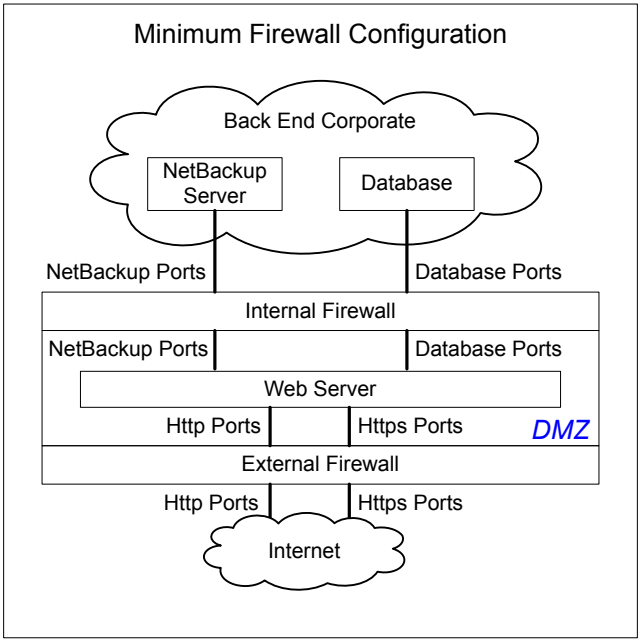
Component	Description
Encryption	Specifies that NetBackup encryption can increase security by providing the following: ■ Greater data confidentiality ■ The loss of physical tape is not as critical if all the data is effectively encrypted ■ The best risk mitigation strategy Ffor more information about encryption: See "Encryption security questions to consider" on page 258.
Data over the wire security	Includes 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 94. 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 108. ■ PBX and VNETD dedicated ports provide increased NetBackup security ■ Central set of ports to monitor and open through firewalls

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: ■ Symantec 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 and pick. It might make sense to review the possibility of blocking NFS, telnet, FTP, email, etc., 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 external firewall with DMZ.

Figure 1-3 Example firewalls and DMZ

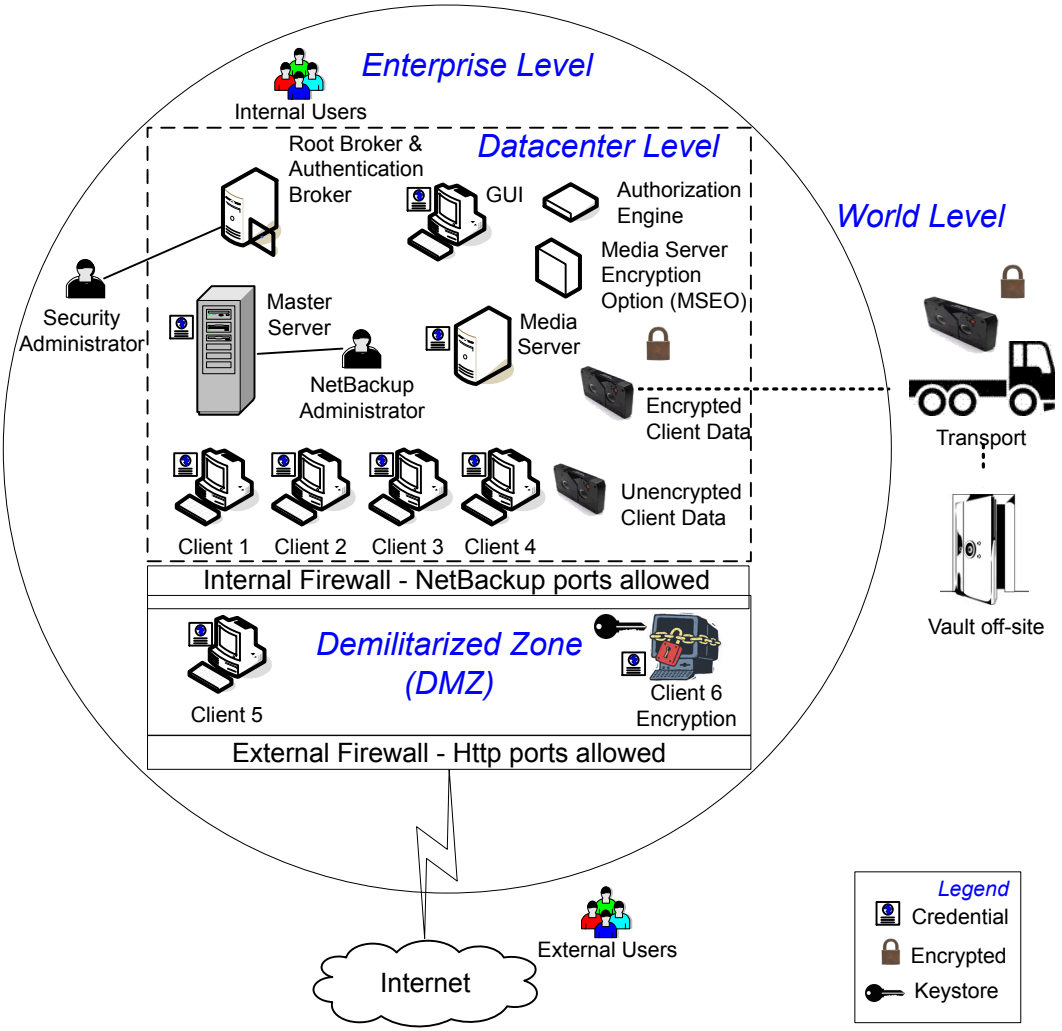


Combined world, enterprise, and datacenter levels

The combined world, enterprise, and datacenter 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 datacenter level occur. At the deepest level, the datacenter level, the core NetBackup security functionality occurs through a workgroup, single datacenter, or multi-datacenter.

The following figure shows the combined world, enterprise, and datacenter 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 datacenter Multi-datacenter
See "Standard NetBackup security" on page 28.	■ Manage as root or administrator ■ Data is not encrypted	Low	Workgroup with NetBackup Single datacenter with standard NetBackup Multi-datacenter with standard NetBackup
See "Media Server Encryption Option (MSEO) security" on page 29.	■ Media server encryption ■ Client to media server traffic is not encrypted ■ May affect CPU performance on the media server ■ Location of keys	Low	Single datacenter with media server Encryption Option (MSEO) Multi-datacenter with media server Encryption Option (MSEO)
See "Client side encryption security" on page 30.	■ 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 datacenter with client side encryption Multi-datacenter with client side encryption
See "NBAC on master, media server, and GUI security" on page 32.	■ NBAC gives authorization tp access master and media servers ■ Authenticates the system and users to access master and media servers	Medium	Single datacenter with NBAC on master and media servers Multi-datacenter with NBAC on master and media servers
See "NBAC complete security" on page 34.	■ NBAC gives authorization throughout the system ■ NBAC gives authentication throughout the entire system (servers, clients, and users)	High	Single datacenter with NBAC complete Multi-datacenter with NBAC complete

Table 1-6 Security implementation types *(continued)*

Security implementation type	Characteristics	Complexity	Security deployment models
See "All NetBackup security" on page 35.	■ Incorporates all NetBackup security types ■ The example diagrams and documentation employ all security mechanisms together	Very High	Single datacenter with all security implemented Multi-datacenter with all NetBackup security

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 upgrades applied to the OS to keep it running at the highest level of system integrity. Upgrades and patches should be kept at the level specified by the vendor.
- Following safe firewall procedures
- Employing least privilege administration
- Limiting root users
- Applying 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 heterogenic environment

NetBackup security vulnerabilities

Symantec 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

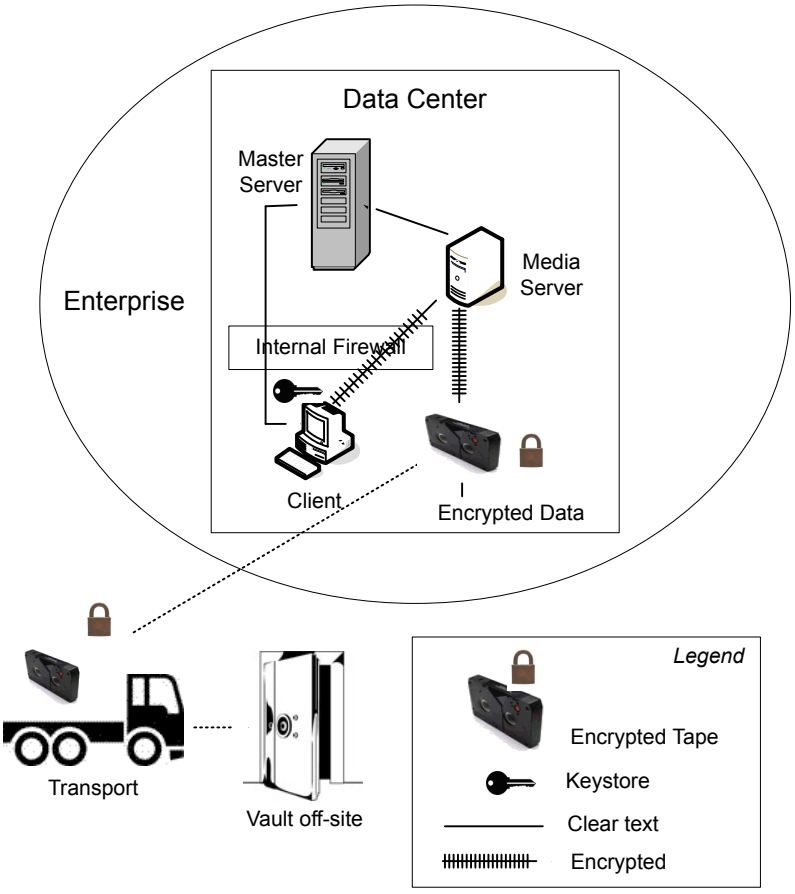
- The importance of accumulative NetBackup updates
- Use the Symantec Web site for information on possible security vulnerability issues:
  www.symantec.com/avcenter/security/SymantecAdvisories.html, or
  www.symantec.com/security
- Use email contacts for possible security vulnerability issues:
  secure@symantec.com

Standard NetBackup security

The standard NetBackup security only includes security offered by the operating system and the hardware components of the datacenter. 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 datacenter. Unencrypted data is usually stored on site, presenting a relatively high risk for no disaster recovery plan. Data 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

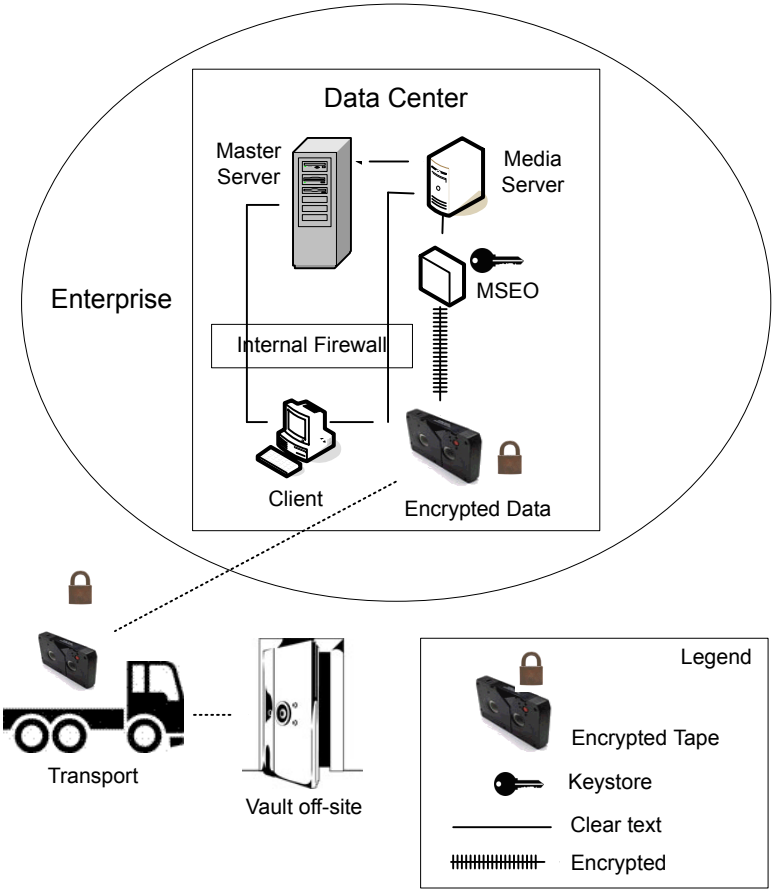


Media Server Encryption Option (MSEO) security

The media server encryption option (MSEO) security type provides a client level data encryption solution. Encrypted tape data is transported and stored in a vault off site lowering data loss risk in a total disaster recovery scenario. The master server, media server, MSEO, and client are all run within a local enterprise datacenter. The MSEO can relieve CPU intensive operations on the individual clients. This is comparing MSEO to client side encryption by moving encryption operations to the media server. However, MSEO can affect CPU performance on the media server. The MSEO to tape traffic is encrypted. Client to media server traffic is not encrypted. Keep the keys on the MSEO device so that encrypted data can be future accessed.

The following figure shows an example of the media server encryption option (MSEO) configuration.

Figure 1-6 Media server encryption option (MSEO)



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. It is not possible to select the encryption check box in the policy attributes interface for these policy types.

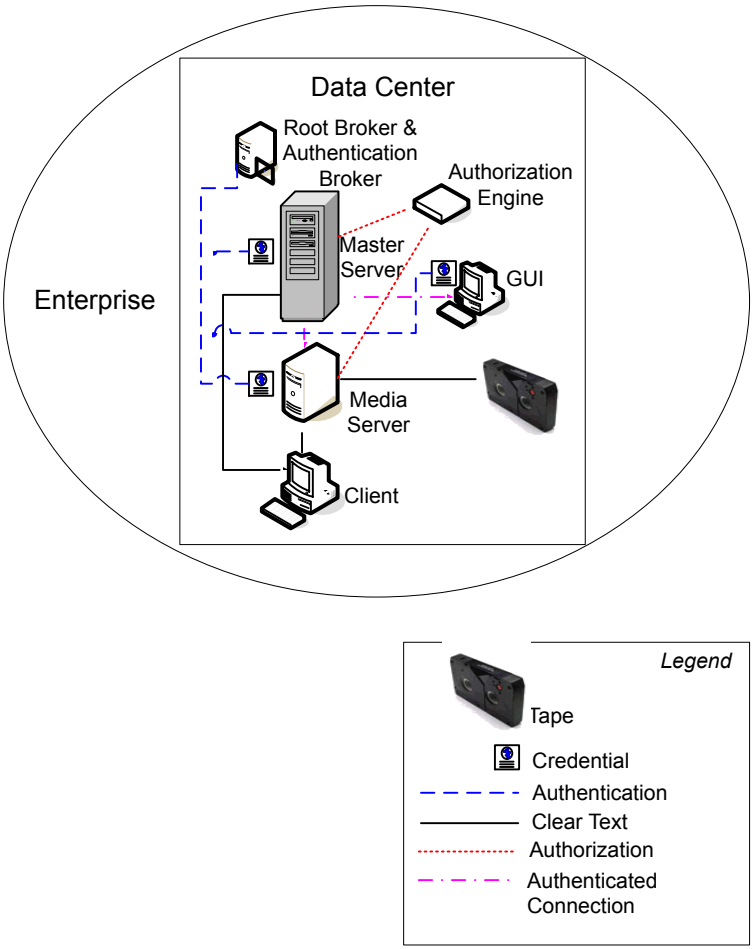
- FlashBackup
- FlashBackup-Windows
- NDMP
- NetWare
- OS/2
- Vault

The media server Encryption Option is applied at the point where data is written to tape and can be used with all of the policy types listed. The exceptions are NDMP policies which write data directly from NDMP servers in NDMP format. Media server Encryption Option is supported for Remote NDMP where the backup is written to tape using a regular media server.

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 1-7 Client side encryption



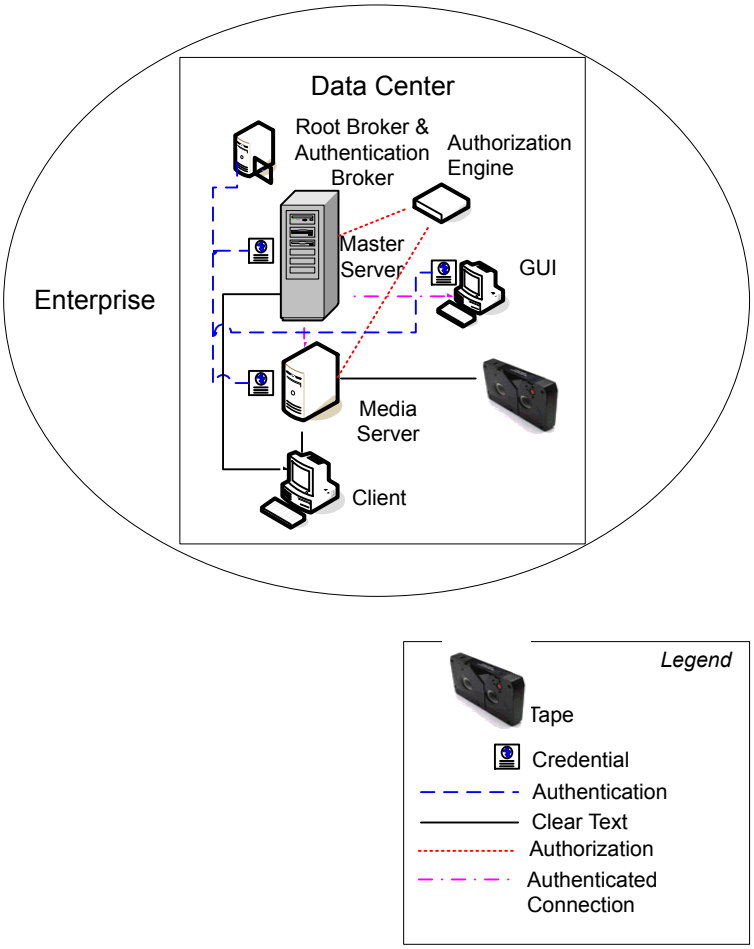
NBAC on master, media server, and GUI security

The NBAC on master server, media server, and GUI security method uses the authentication broker. The broker provides credentials to the master server, the media server, and the GUI. This datacenter 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 GUIs. Non-root

users can logon 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 1-8 NBAC on master and media server

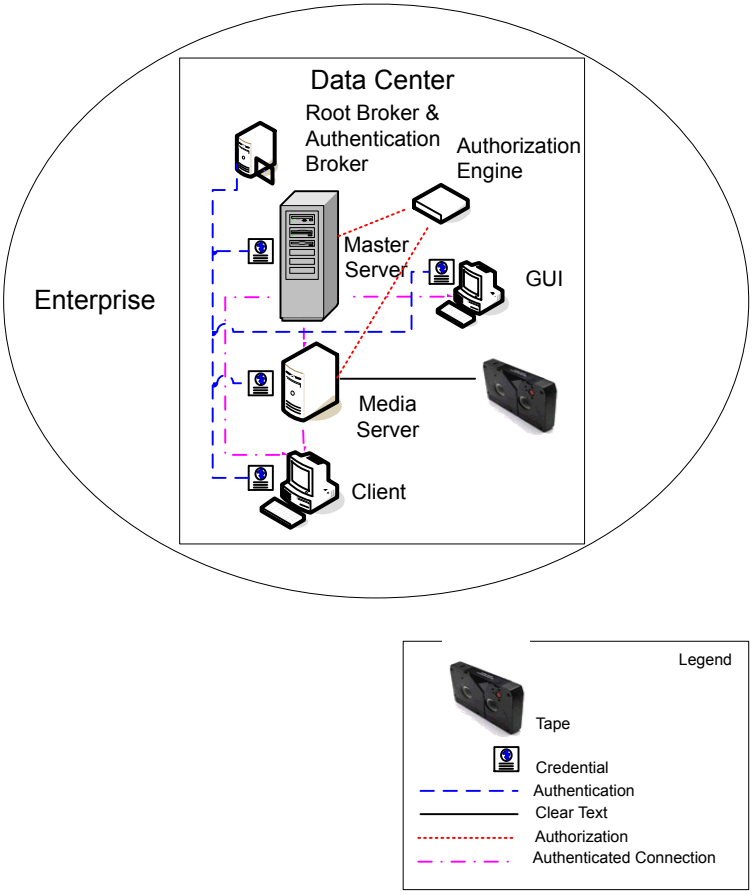


NBAC complete security

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 GUI 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 passwd, local Windows domain) on those hosts supporting an authentication broker.

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

Figure 1-9 NBAC complete

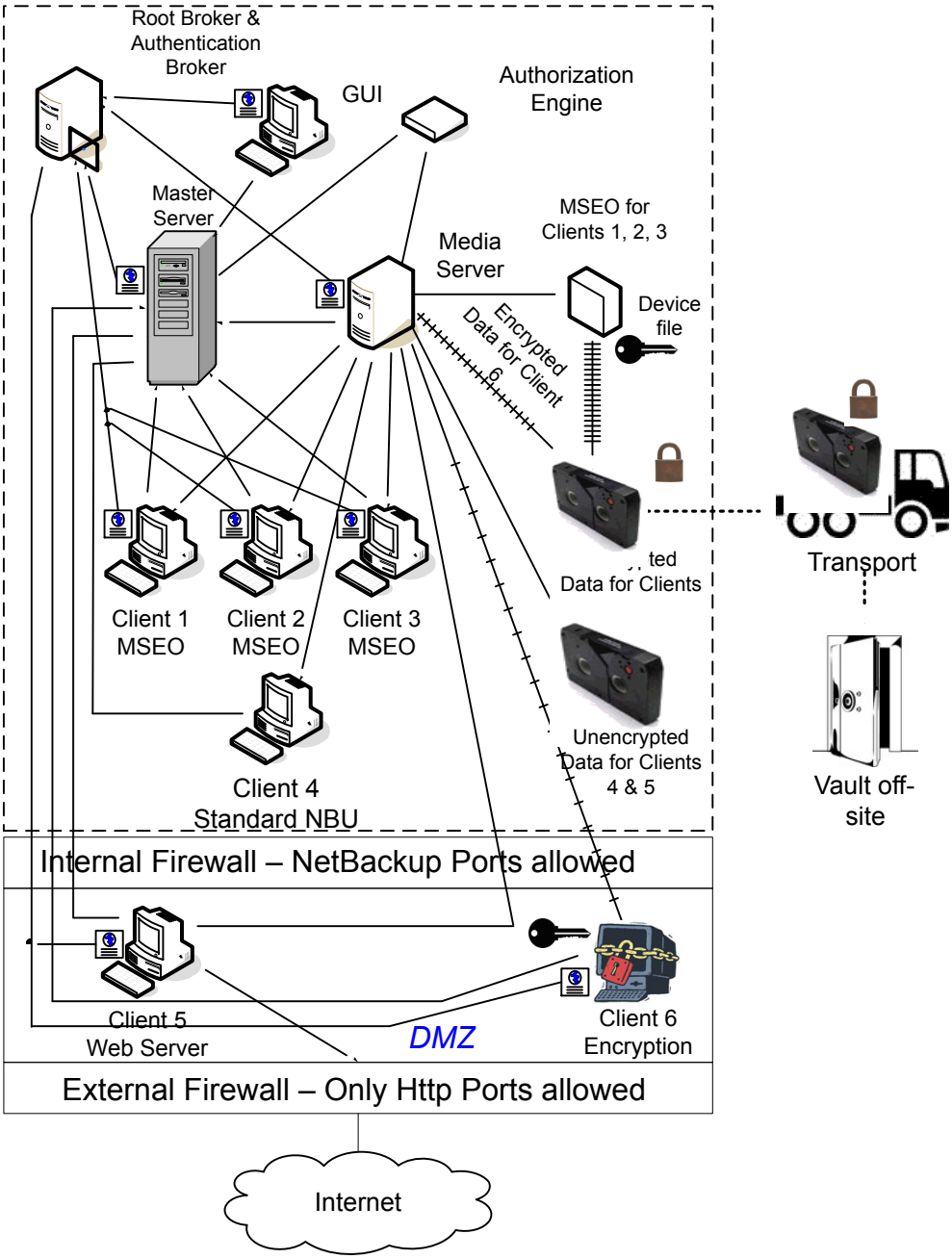


All NetBackup security

All NetBackup security combines all securities together. It represents a very sophisticated environment in which there are different requirements for a variety of clients. The client requirements can necessitate using encryption off host (such as under powered host, or a database backup). Client requirements can also necessitate using encryption on host due to the sensitive nature of the data on the host. Adding NBAC to the security mix allows segregation of administrators, operators, and users within NetBackup.

The following figure shows an example with all of the NetBackup security implemented.

Figure 1-10 All NetBackup security



Chapter 2

Security deployment models

This chapter includes the following topics:

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 39.

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 42.
- See “Single datacenter with Media Server Encryption Option (MSEO)” on page 45.
- See “Single datacenter with client side encryption” on page 48.
- See “Single datacenter with NBAC on master and media servers” on page 50.
- See “Single datacenter with NBAC complete” on page 54.
- See “Single datacenter with all security implemented” on page 57.

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 61.
- See “Multi-datacenter with Media Server Encryption Option (MSEO)” on page 65.
- See “Multi-datacenter with client side encryption” on page 70.
- See “Multi-datacenter with NBAC on master and media servers” on page 75.
- See “Multi-datacenter with NBAC complete” on page 81.
- See “Multi-datacenter with all NetBackup security” on page 87.

Workgroup with NetBackup

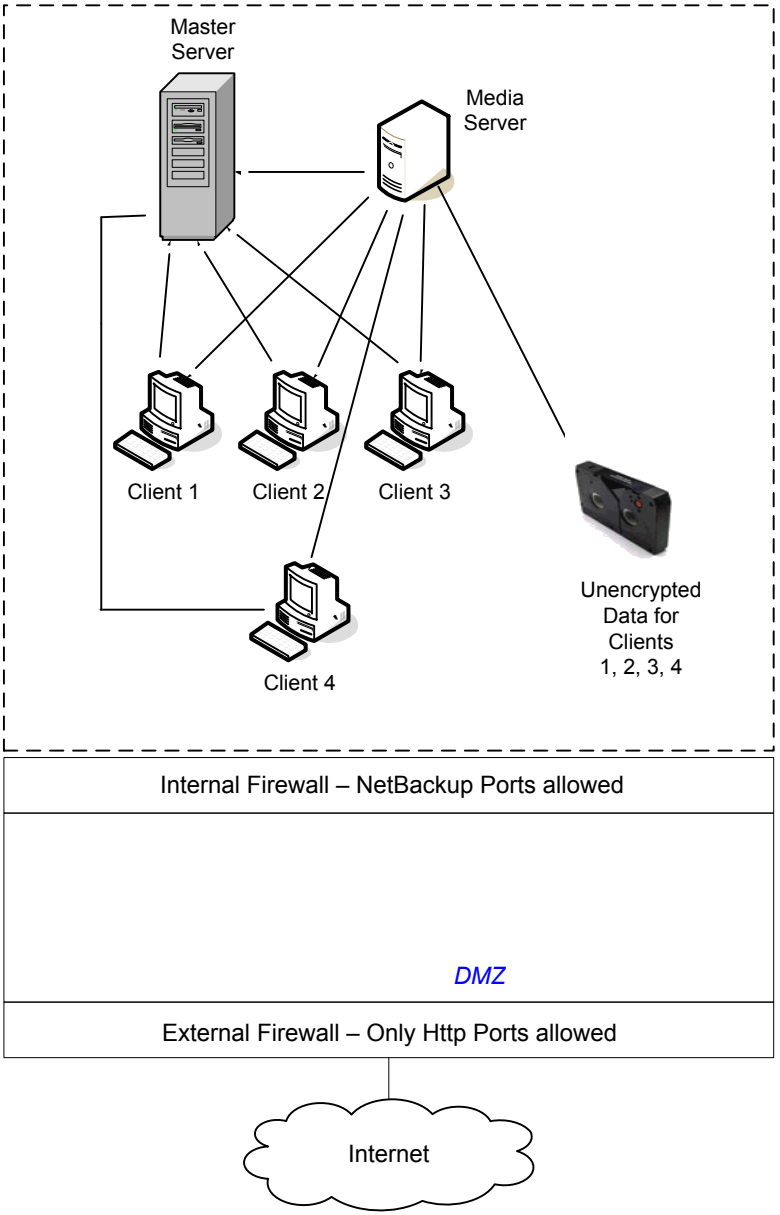
A workgroup with NetBackup is classified as a small group of systems (less than 50). The workgroup is used with NetBackup internally. Typically, this configuration does not have a unified naming service such as NIS or Active Directory. It may not have an authoritative host naming service such as DNS 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

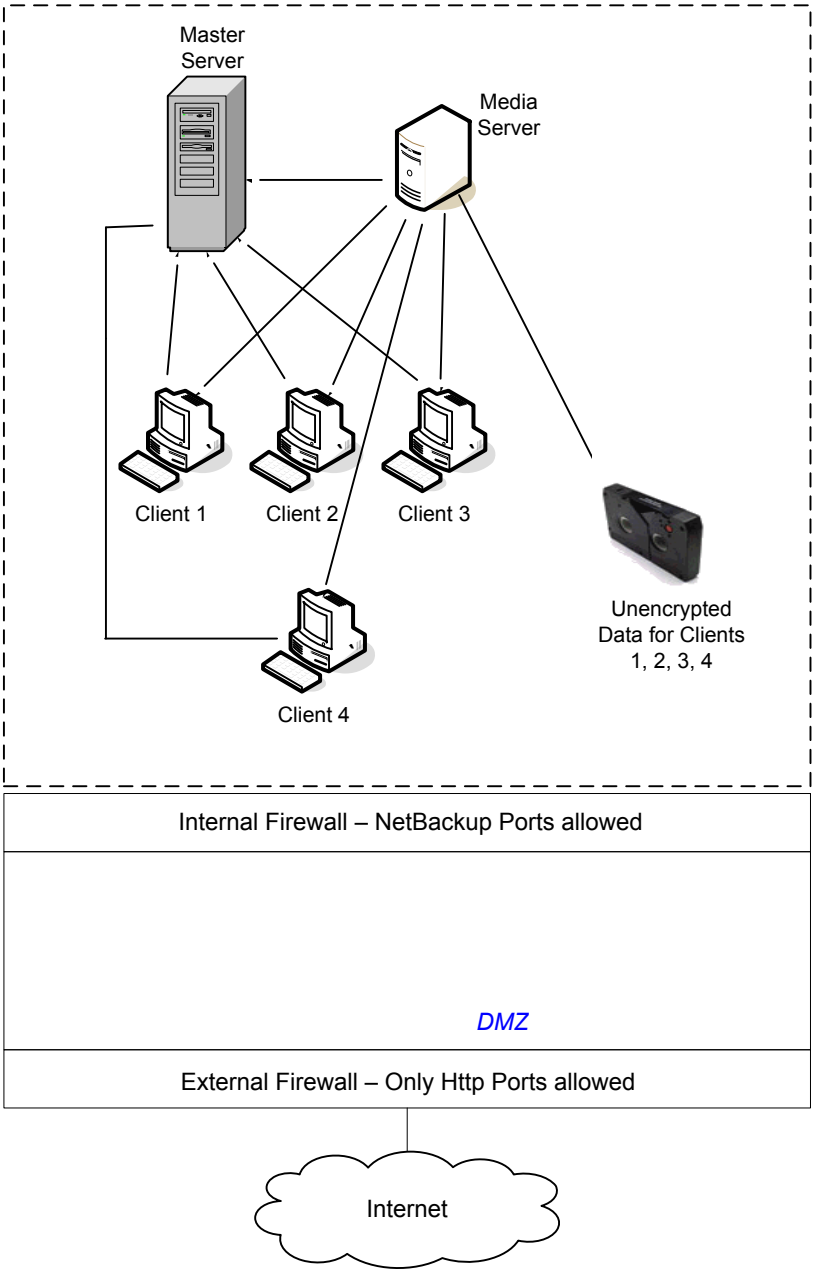
A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or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



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 Media Server Encryption Option (MSEO)

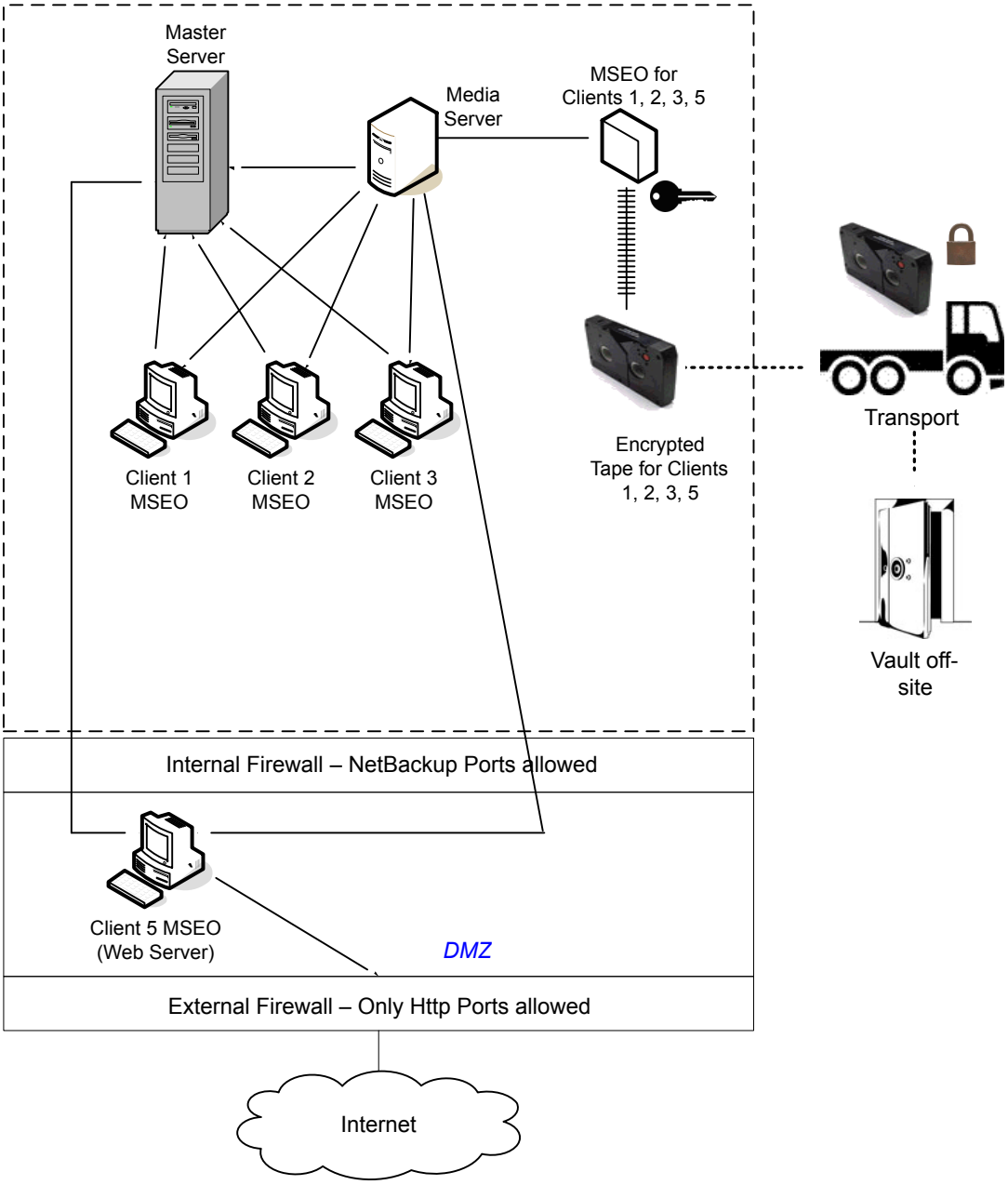
This single datacenter with the Media Server Encryption Option (MSEO) example typically includes more than 50 hosts. All externally facing hosts make use of the Media Server Encryption Option (MSEO). In this example, clients use the MSEO option for all hosts.

The single datacenter with Media Server Encryption Option (MSEO) includes the following highlights:

- The MSEO is a newer option in NetBackup
- Protects data that is sent off-site
- Data is still sent from the client in the clear, implying that passive data interception off the wire is an acceptable risk
- Key management and encryption are managed in a central location equating to a single point of failure. Using the high availability cluster can help.
- Media server must be robust to handle multiple clients at once
- Useful where you need to send encrypted tapes off-site but want to off load encryption from the client, which is CPU intensive
- Must have keys to get data back. Lost keys mean lost data. (See information on key share backup in the Encryption Chapter).

Figure 2-3 shows an example single datacenter with MSEO.

Figure 2-3 Single datacenter with MSEO



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

Table 2-3 NetBackup parts used for a single datacenter with MSEO

Part	Description
Master server	Communicates with the media server, MSEO clients 1, 2 and 3 and the MSEO Web server client 5 in the DMZ.
Media server	Communicates with the master server, MSEO clients 1, 2 and 3 and the MSEO Web server client 5 in the DMZ. The media server communicates with the MSEO device that enables the writing of encrypted data to tape for clients 1, 2, 3, and 5.
MSEO	Specifies that the MSEO hardware appliance off-loads encryption from individual clients and generates encrypted data for clients 1, 2, 3, and 5. That encrypted data is then written to tape. The individual client CPU performance is improved (relative to client side encryption) by using the MSEO appliance.
Tape	Contains MSEO encrypted backup data that is written for clients 1, 2, 3, and 5. The encrypted tape is transported off-site to a vault for disaster recovery protection. **Note:** To decrypt the data, the key(s) used to encrypt the data must be made available.
Transport	Specifies that the transport truck moves encrypted tapes off-site to a secure vault facility. If a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach. Data breach has been reduced through the use of data encryption.
Vault off-site	Provides a safe storage facility at a different location than the datacenter that promotes disaster recovery protection.
Clients	Specifies that clients 1, 2, and 3 are the MSEO type and client 5 is a Web server type (also using the MSEO option). Both types can be managed by the master server and have their encrypted data backed up to tape. Backup is done through the media server attached MSEO hardware appliance. 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	Specifies that it is used by NetBackup to access client 5, Web server, 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 open in the external firewall cannot pass through the internal firewall.
Demilitarized Zone (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.

Table 2-3 NetBackup parts used for a single datacenter with MSEO *(continued)*

Part	Description
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.
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 client side encryption

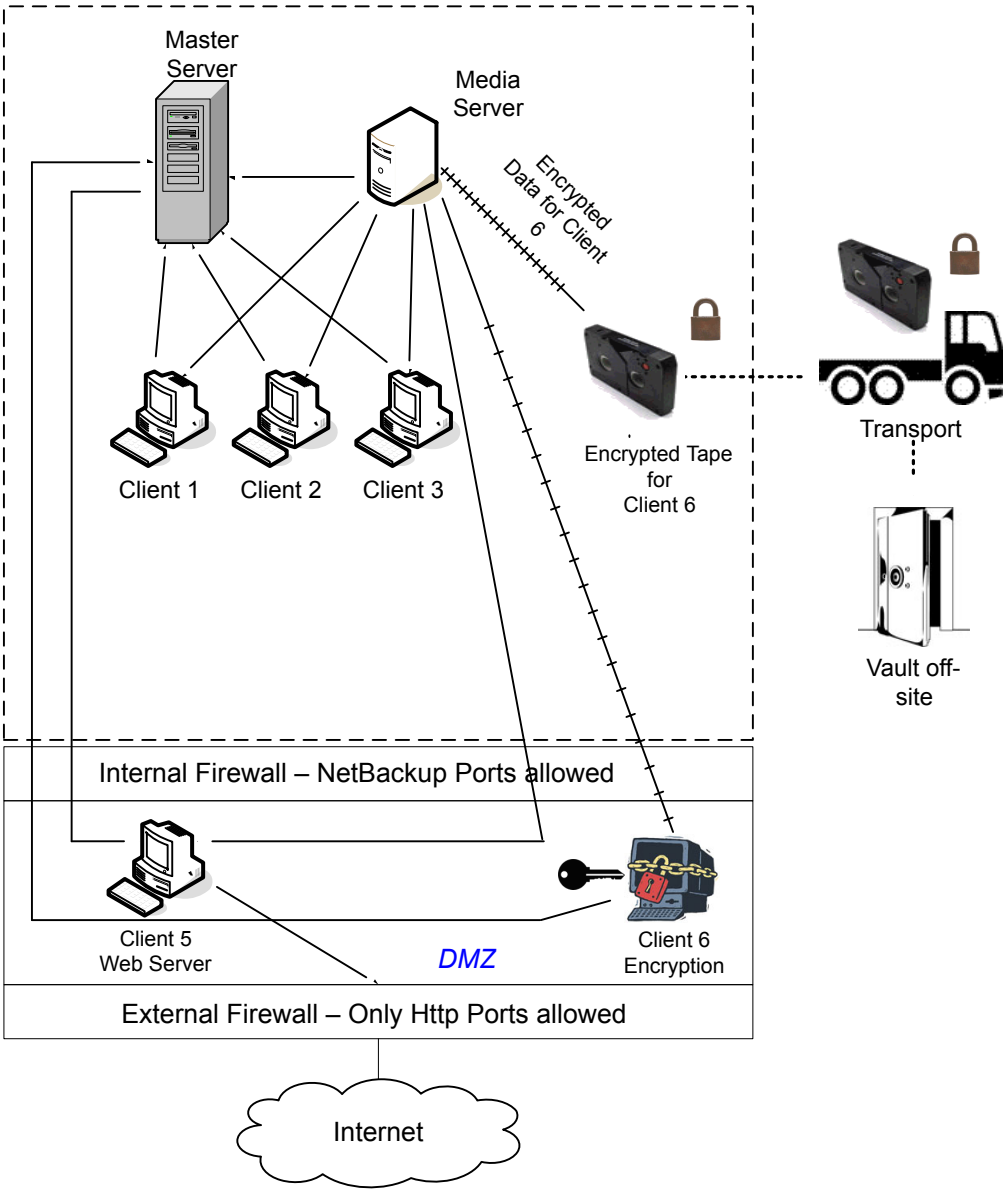
This single datacenter with client side encryption example uses the client side encryption to ensure data confidentiality across the wire as well as on tape. The client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are 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 2-4 shows an example single datacenter with client side encryption.

Figure 2-4 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 2-4 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.

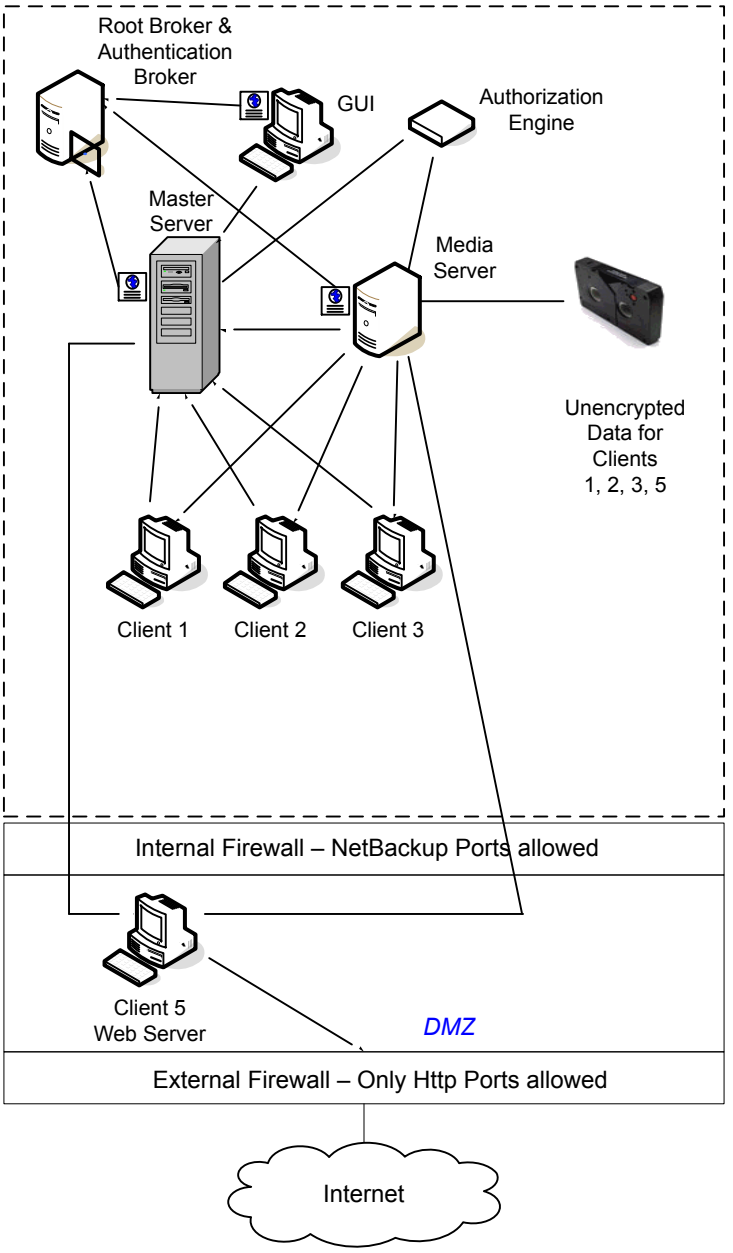
The single datacenter with NBAC on master and media servers includes the following highlights:

- 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 be NetBackup version 5.x and higher

Figure 2-5 shows an example single datacenter with NBAC on master and media servers.

Figure 2-5 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 2-5 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 2-5 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

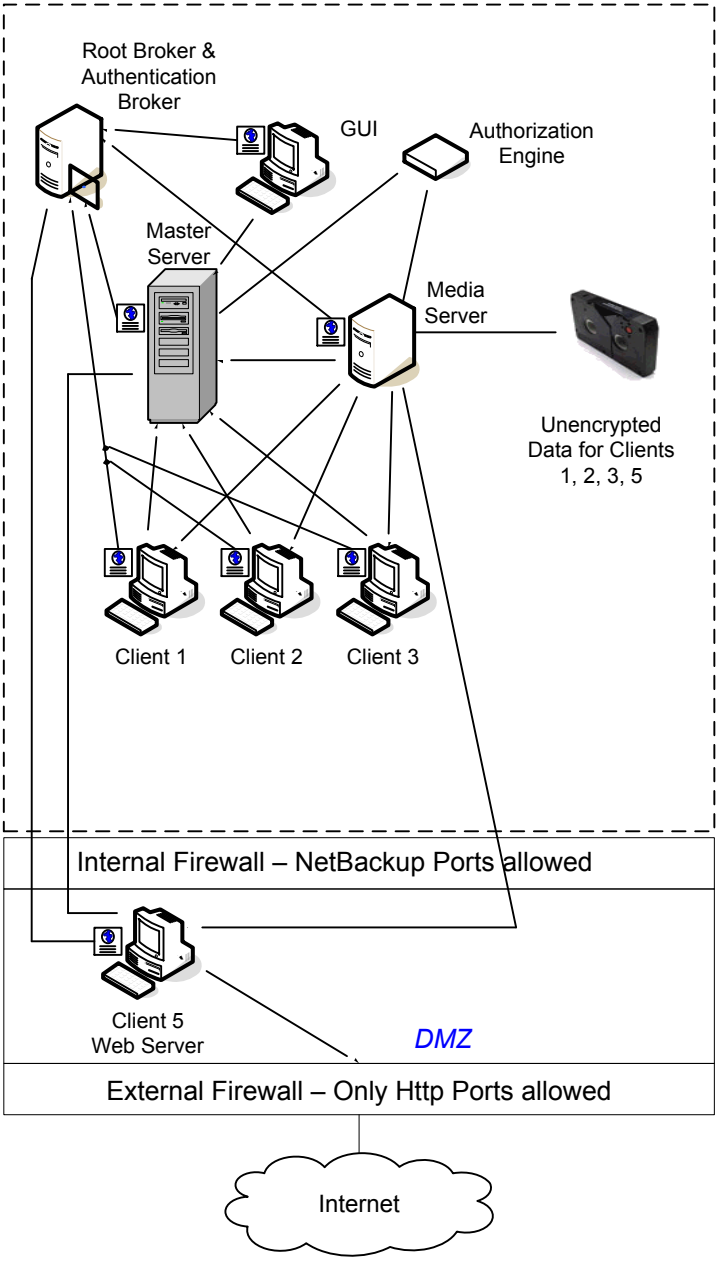
The single datacenter with NBAC complete environment is very similar to the single datacenter with NBAC master and media server. The main differences are that all of the hosts that participate in the NetBackup environment are reliably identified using credentials. And non-root administrators can manage 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
- Requires all hosts to be at NetBackup version 5.0 and greater

Figure 2-6 shows an example single datacenter with NBAC complete.

Figure 2-6 Single datacenter with NBAC complete



The following table describes the NetBackup parts that are used with a single datacenter with NBAC complete.

Table 2-6 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 2-6, 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 2-6 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.

Single datacenter with all security implemented

The example of a single datacenter with all security implemented combines all of the previous examples. It represents a very sophisticated environment in which there exists differing requirements for a variety of clients. Client requirements can necessitate using encryption off host (such as an underpowered host, or a database backup). Client requirements can also necessitate using encryption on host due to the sensitive nature of the data on the host. Adding NBAC to the security mix allows segregation of administrators, operators, and users within NetBackup.

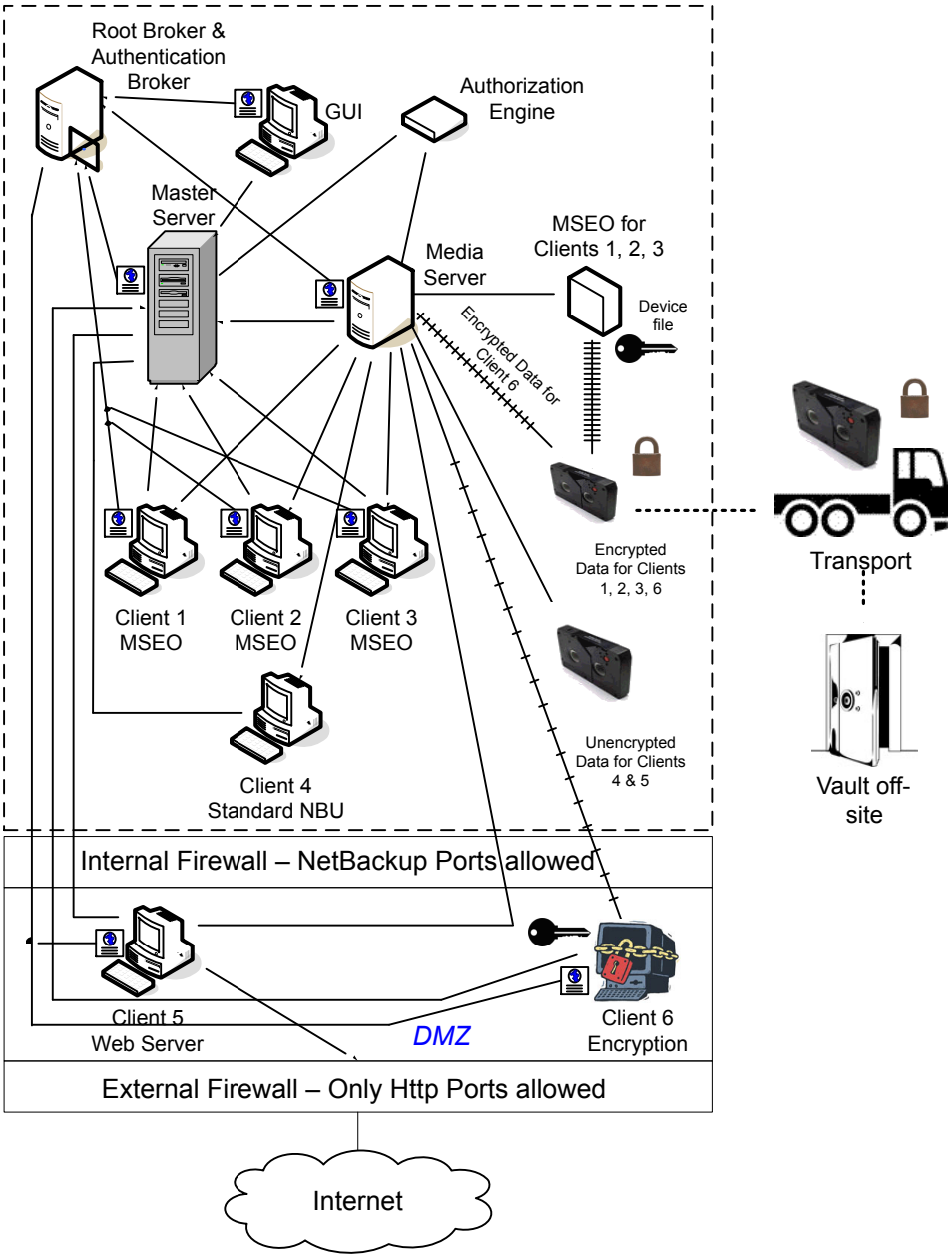
The single datacenter with all security implemented includes the following highlights:

- See the previous single datacenter sections for individual option highlights
- Provides the most flexible and complex environment

- Careful design following a similar model can let you use the strengths of each option

Figure 2-7 shows an example single datacenter with all security implemented.

Figure 2-7 Single datacenter with all security implemented



The following table describes the NetBackup parts that are used with a single datacenter with all of security implemented.

Table 2-7 NetBackup parts for a single datacenter with all security implemented

Part	Description
Master server	Communicates with the media server, root broker, authentication broker, 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 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 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 clients. In the figure, the root broker and authentication broker are shown 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 example only.
Tapes	Specifies that the first tape contains encrypted MSEO backup data written for clients 1, 2, 3, and client encrypted data for client 6. The second tape contains unencrypted backup data that is written for clients 4 and 5.
Transport	Specifies that the transport truck moves encrypted tapes off-site to a secure vault facility. If a tape is lost during transport, the datacenter manager has mitigated the risk. The risk of data exposure has been mitigated through the use of encryption.

Table 2-7 NetBackup parts for a single datacenter with all security implemented *(continued)*

Part	Description
Vault off-site	Specifies that the vault off-site is a safe storage facility at a different location than the datacenter that promotes disaster recovery protection.
Clients	Specifies that clients 1, 2, 3, and 4 are standard NetBackup types. Client 5 is a Web server type. Client 6 uses client side encryption. Upon receiving credentials form the authentication broker, clients 1, 2, 3, 5, and 6 are authenticated to the NetBackup Product Authentication Service domain. Both standard server and Web server types can be managed by the master server and have their unencrypted data backed up to tape through the media server. Client 6 has its encrypted data that is backed up to tape through the media server. Clients 1, 2, and 3 exist in the datacenter. Clients 5 and 6 exists in the DMZ. They communicate to NetBackup using NetBackup only ports through the internal firewall. Client 5 and 6 communicate to the Internet using HTTP only ports through the external firewall.
Internal firewall	Specifies that the internal firewall lets NetBackup 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 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	Specifies that 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 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 that are 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.

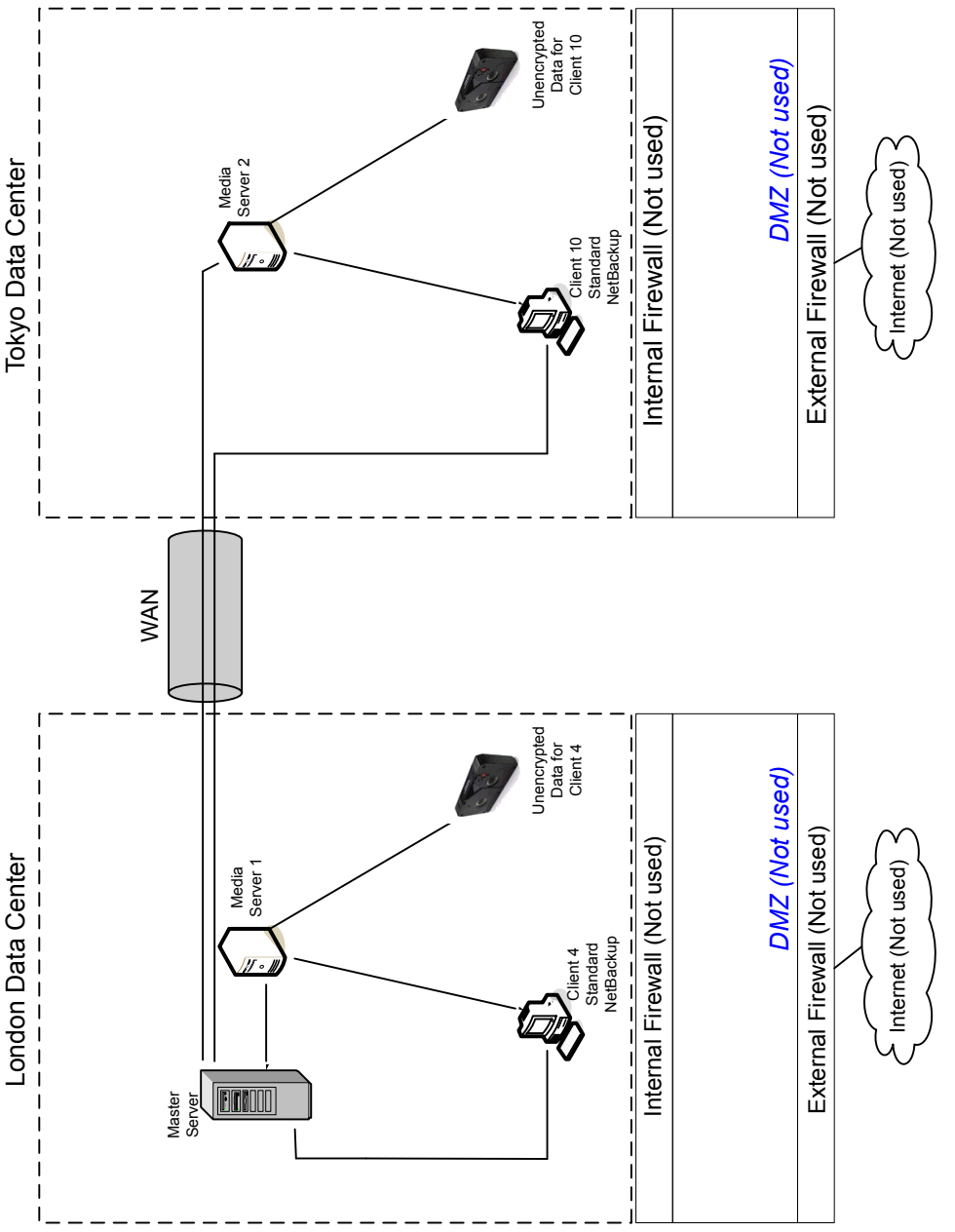
A multi-datacenter includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

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
- Typical configuration that is used for NetBackup 4.5 to 5.x customers with multiple datacenters
- Assumes no fear of passive data interception on the wire as the backup runs

Figure 2-8 shows an example multi-datacenter with standard NetBackup.

Figure 2-8 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 2-8 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 2-8 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 Media Server Encryption Option (MSEO)

A multi-datacenter with Media Server Encryption Option (MSEO) is defined as a medium to large group of hosts (greater than 50) that span two or more geographic regions. The hosts are 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.

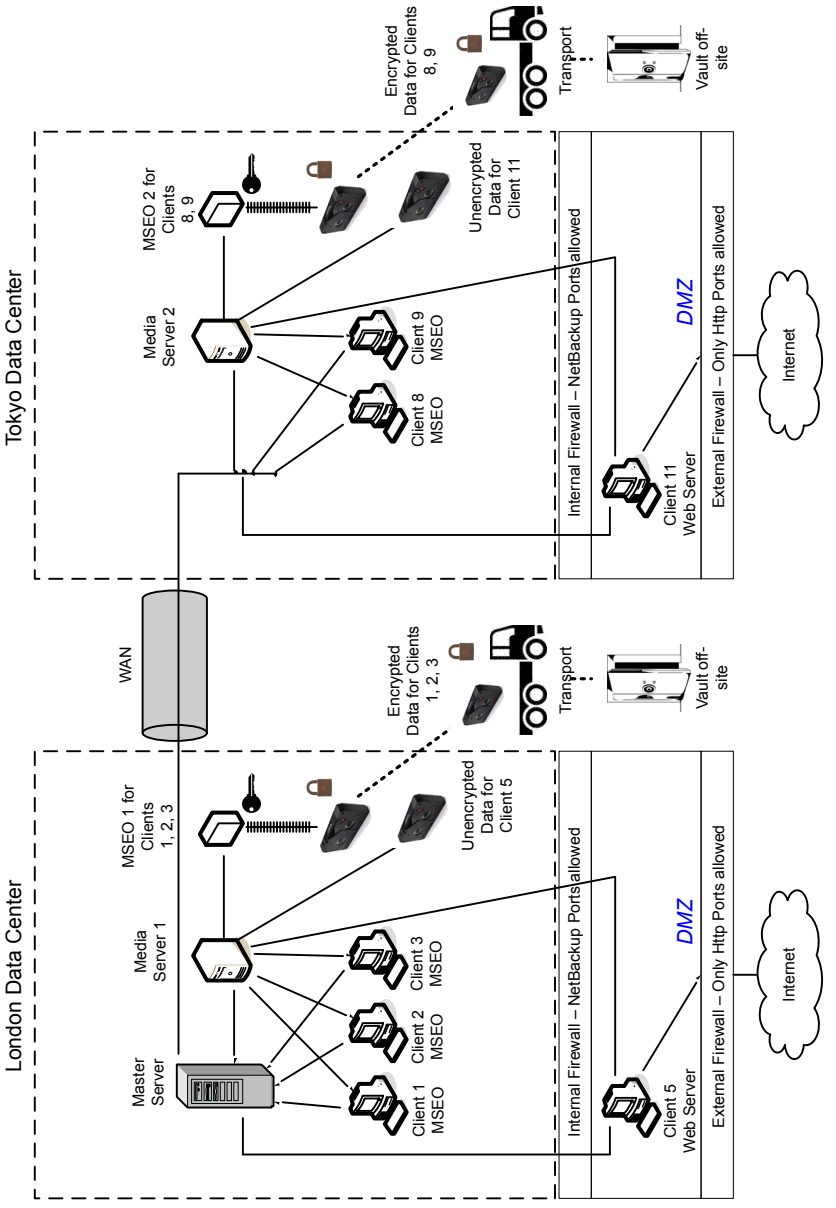
This multi-datacenter example can typically include more than 50 hosts. All externally facing hosts use the Media Server Encryption Option (MSEO). In this example, clients use both encrypted backups for some clients and the MSEO option for other hosts. Data that is too sensitive to be archived off-site is "left at rest" in an unencrypted format.

The multi-datacenter with Media Server Encryption Option (MSEO) includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN
- Newer option in NetBackup
- Useful for protecting off-site data
- Data is still sent from the client in the clear, implying that passive wire interception is an acceptable risk
- Key management and encryption are managed in a central location equating to a single point of failure. Using the high availability cluster can help.
- Media server needs to be robust to handle multiple clients at once
- Useful where you need to send encrypted tapes off-site but want to off load encryption from the client, which is CPU intensive
- Must have keys to get data back. Lost keys means lost data. (See information on key share backup in the Encryption Chapter.)

Figure 2-9 shows an example multi-datacenter with Media Server Encryption Option (MSEO).

Figure 2-9 Multi-datacenter with Media Server Encryption Option (MSEO)



The following table describes the NetBackup parts that are used for a multi-datacenter with MSEO implemented.

Table 2-9 NetBackup parts for a multi-datacenter with MSEO implemented

Part	Description
London datacenter	Contains the master server, media server 1, MSEO 1, clients 1, 2, 3, and client 5 Web server in the DMZ. The London datacenter also contains the encrypted data tape for clients 1, 2, 3, and unencrypted data tape for client 5. The London datacenter connects to the Tokyo datacenter through a dedicated WAN connection.
Tokyo datacenter	Contains the media server 2, MSEO 2, clients 8, 9 and client 11 Web server in the DMZ. The Tokyo datacenter also contains the encrypted data tape for clients 8, 9, and unencrypted data tape for client 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 to the Tokyo datacenter. The WAN provides connectivity between the master server in London to media server 2 with clients 8, 9, 11 in Tokyo.
Master server	Specifies that the master server that is located in the London datacenter, communicates with media server 1 and clients 1, 2, 3, and 5. The master server also uses the WAN to communicate with media server 2, and clients 8, 9, and 11 in Tokyo.
Media servers	Specifies that this 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, MSEO 1, and clients 1, 2, 3, and 5. Media server 1 writes unencrypted data to tape for client 5. Media server 1 also uses MSEO 1 to write encrypted data to tape for clients 1, 2, and 3. The encrypted tape 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 8, 9, and 11 in Tokyo. Media server 2 writes unencrypted data to tape for client 11. Media server 2 also uses MSEO 2 to write encrypted data to tape for clients 8 and 9. The encrypted tape is transported off-site to a vault in Tokyo.
MSEOs	Specifies that the two MSEO hardware appliances off-load encryption from individual clients. The individual client CPU performance is improved (relative to client side encryption) by using the MSEO appliance. The MSEO 1 is in the London datacenter and MSEO 2 is in the Tokyo datacenter. The MSEO 1 generates an encrypted data tape for clients 1, 2, and 3 that can be stored off-site in London. The MSEO 2 generates an encrypted data tape for clients 8 and 9 that can be stored off-site in Tokyo.

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

Part	Description
Tapes	Specifies that both the unencrypted and encrypted data tapes are produced in the London datacenter and in the Tokyo datacenter. The encrypted tape contains MSEO encrypted backup data. In London, the unencrypted tape is written for client 5 and stored on-site at the London datacenter. The encrypted tape is written for clients 1, 2, and 3. The encrypted tape for clients 1, 2, and 3 is transported off-site to a vault in London for disaster recovery protection. In Tokyo, the unencrypted tape is written for client 11 and stored on-site at the Tokyo datacenter. The encrypted tape is written for clients 8 and 9. The encrypted tape for clients 8 and 9 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 there are 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 1, 2, and 3 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 8 and 9 off-site to a secure Tokyo vault facility. **Note:** If a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach. This breach has been reduced through the use of data encryption.
Vaults off-site	Specifies that there are two vaults that are located 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:** Good disaster recovery protection promotes having the encrypted tapes stored at locations separate from the datacenters.
Clients	Specifies that clients are located in both the London and Tokyo datacenters. In London, clients 1, 2, and 3 are of the MSEO type and client 5 is a Web server type (not using MSEO) that is located in the DMZ. Both server types can be managed by the master server. And they can have their encrypted data backed up to tape through media server 1 attached MSEO hardware appliance. 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. Tokyo clients 8 and 9 are of the MSEO type. Client 11 is a Web server type (not using MSEO) located in the DMZ. Both server types can be managed by the master server located in London. And they can have their encrypted data backed up to tape through media server 2 attached MSEO hardware appliance. Client 11 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 2-9 NetBackup parts for a multi-datacenter with MSEO implemented *(continued)*

Part	Description
Internal firewalls	Specifies that the multi-datacenter can use two internal firewalls. One internal firewall is located in London and the other is located in Tokyo. In London, the internal firewall can use NetBackup to access client 5, Web server, located in the DMZ. The Tokyo internal firewall can use NetBackup to access client 11, Web server, in the DMZ. Only selected NetBackup ports and possibly other application ports are enabled for data communication into and out of the DMZ. Other HTTP ports can be open in the external firewall but cannot pass through the internal firewall.
Demilitarized Zones (DMZs)	Specifies that the multi-datacenter can use 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 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.
External firewalls	Specifies that the multi-datacenter with MSEO 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 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. 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 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 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.

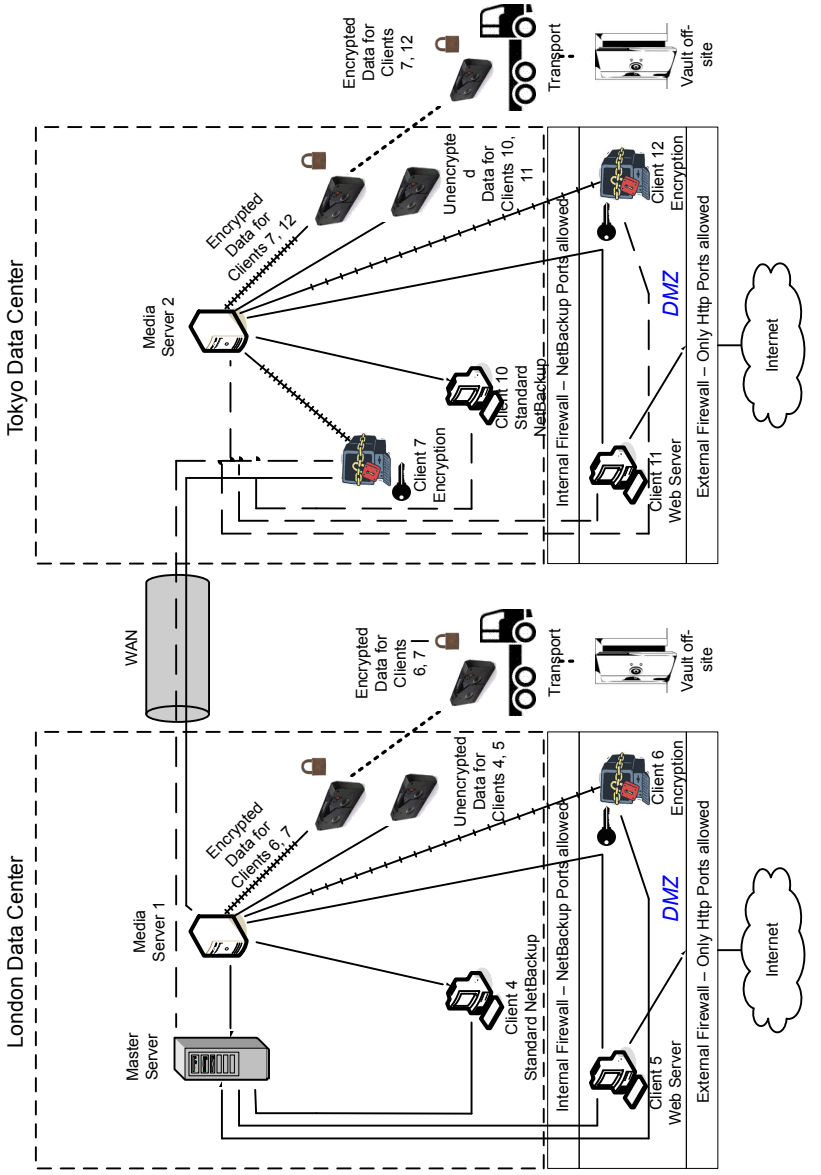
The example multi-datacenter can use client side encryption to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. Risk of data exposure as the tapes are moved off site. This datacenter model assures 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 2-10 shows an example multi-datacenter with client side encryption.

Figure 2-10 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 2-10 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 2-10 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 2-10 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 2-10 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

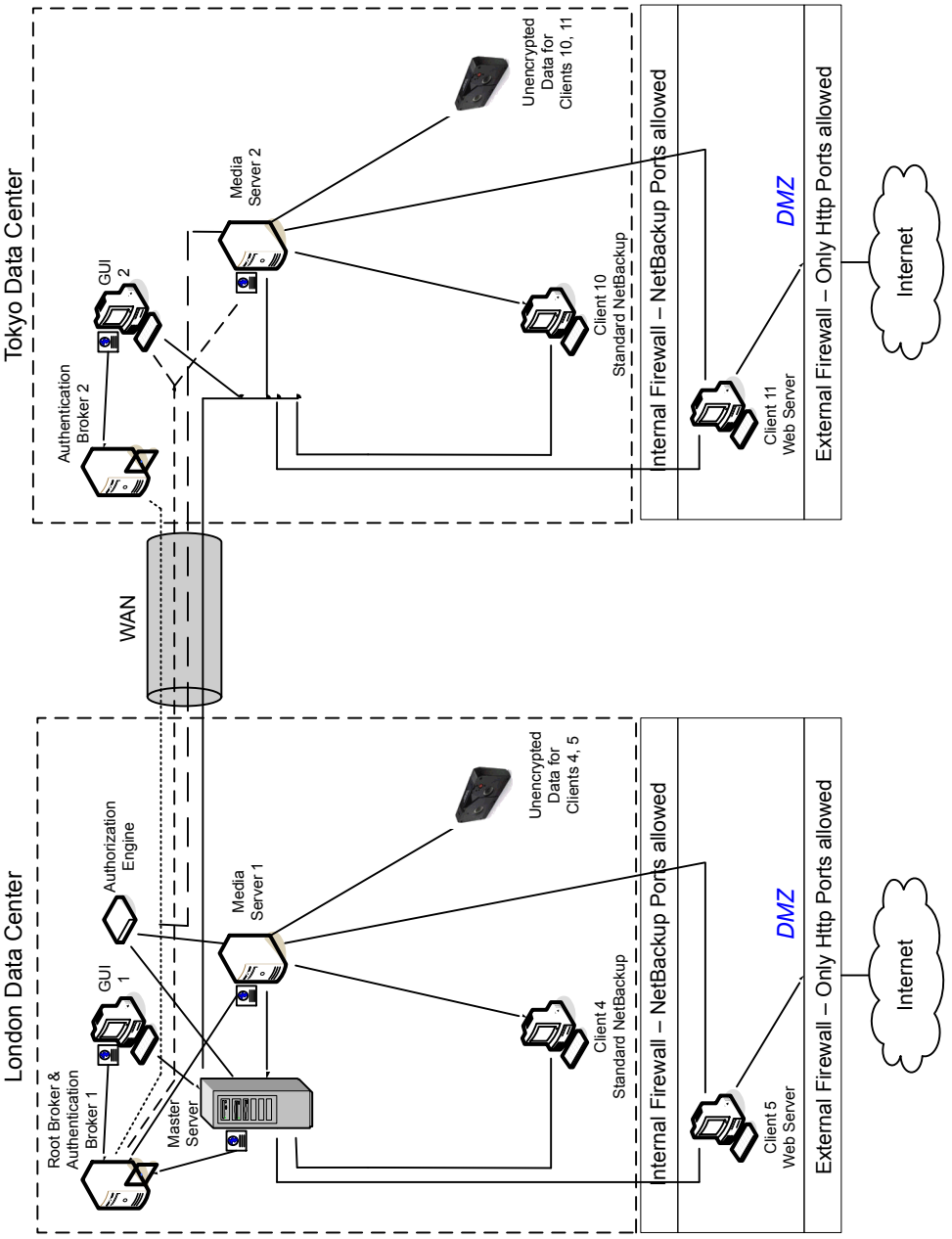
NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

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 5.x and higher

Figure 2-11 shows an example multi-datacenter with NBAC on the master servers and media servers.

Figure 2-11 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 2-11 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 2-11 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 2-11 NetBackup parts used for a multi-datacenter with NBAC on the master and media servers *(continued)*

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 2-11 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.

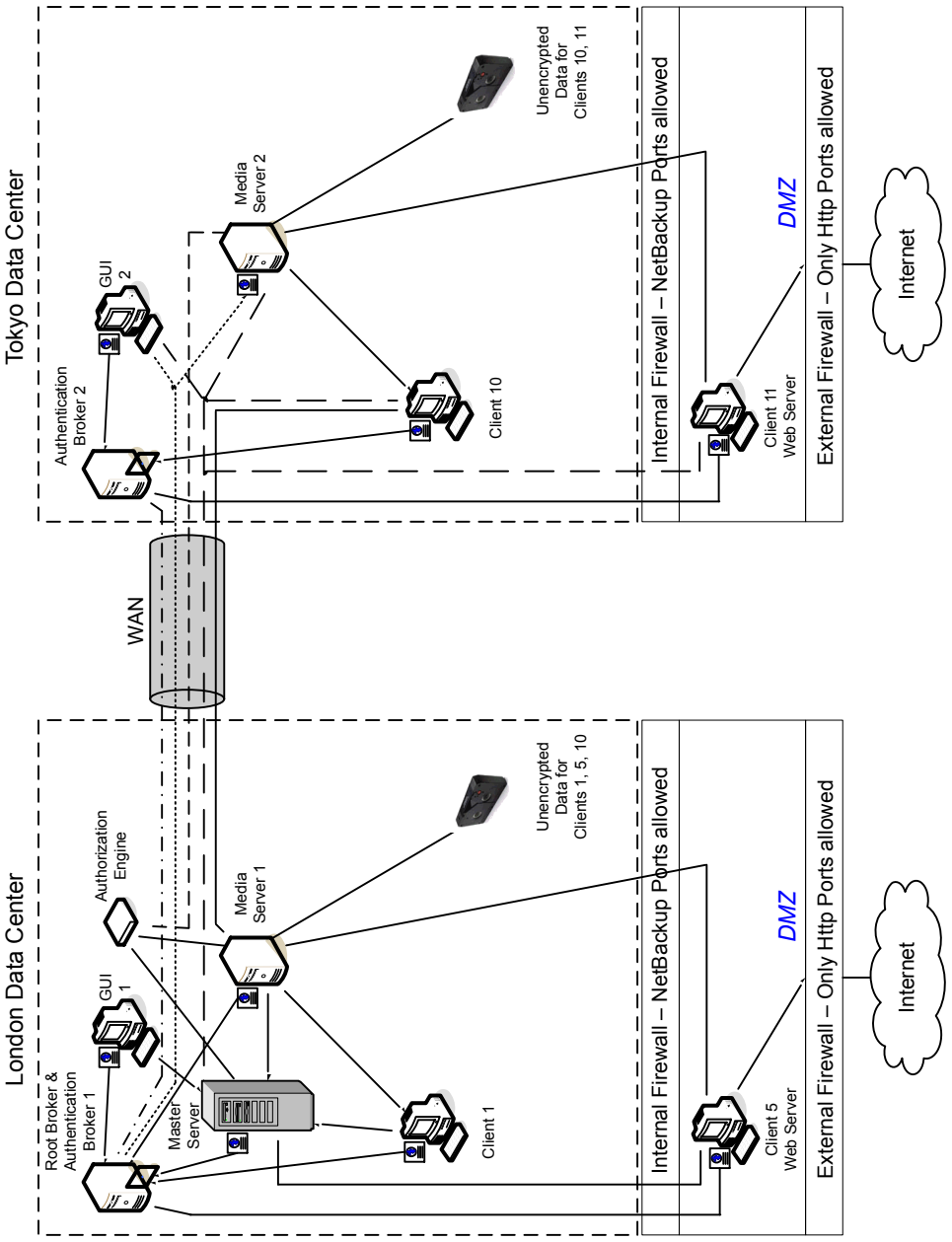
The multi-datacenter with NBAC complete includes the following highlights:

- 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 5.0 and greater

Figure 2-12 shows an example multi-datacenter with NBAC complete.

Figure 2-12 Multi-datacenter with NBAC complete



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

Table 2-12 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 2-12 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 2-12 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 2-12 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.

Multi-datacenter with all NetBackup security

A multi-datacenter that has all of the NetBackup security 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.

This example combines all the previous examples together. It represents a very sophisticated environment in which there can be different requirements for a variety of clients. Client requirements can necessitate using encryption off host (such as an underpowered host, or a database backup). Client requirements can also necessitate using encryption on host due to the sensitive nature of the data on the host. Adding NBAC to the security mix allows the segregation of administrators, operators, and users within NetBackup.

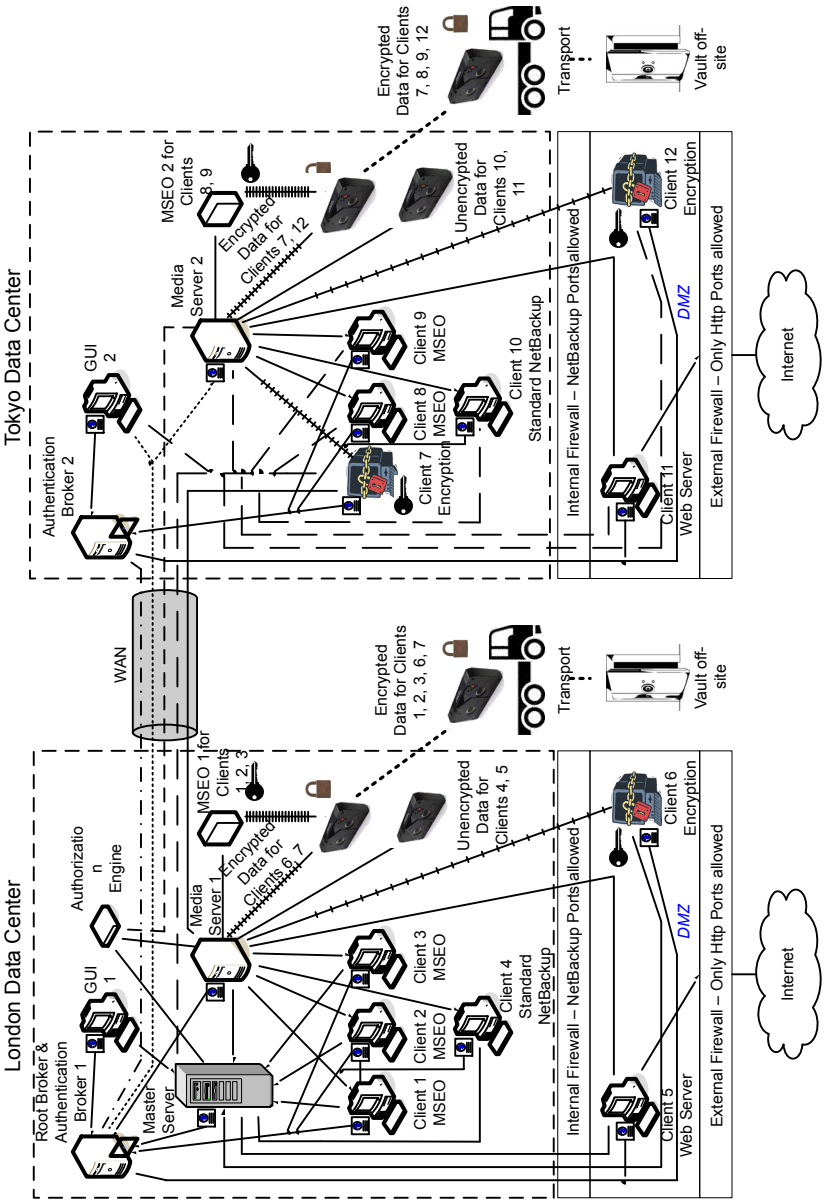
The multi-datacenter with all NetBackup security includes the following highlights:

- NetBackup spans two or more geographic regions through a WAN
- Please see the previous multi-datacenter sections for individual option highlights

- Most flexible and complex environment
- Careful design following a similar model can let you use the strengths of each option

Figure 2-13 shows an example multi-datacenter with all NetBackup security.

Figure 2-13 Multi-datacenter with all NetBackup security



The following table describes the NetBackup parts that are used for a multi-datacenter with all of the NetBackup security implemented.

Table 2-13 NetBackup parts used for a multi-datacenter with all NetBackup security implemented

Part	Description
London datacenter	Contains the root broker, authentication broker 1, GUI 1. It also contains the authorization engine, master server, media server 1, MSEO 1, clients 1 through 6, transport and vault off-site. The London datacenter also contains the encrypted data tape for clients 1, 2, 3, 6, and 7 and the 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 authentication broker 2, GUI 2, media server 2, MSEO 2, clients 7 through 12, transport and vault off-site. The Tokyo datacenter also contains the encrypted data tape for clients 7, 8, 9, and 12 and 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 7 through 12. Finally the WAN connects media server 1 to client 7.
Master server	Specifies that the master server, located in the London datacenter, communicates with the root broker and authentication broker 1, GUI 1, authorization engine, media server 1, and clients 1 through 6. The master server also communicates with GUI 2 and media server 2, and clients 7 through 12 in Tokyo.
Media servers	Specifies that there can be two media servers in this multi-datacenter example. 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. It also communicates with the authorization engine, MSEO 1, and clients 1 through 6, and 7. Media server 1 writes unencrypted data to tape for clients 4 and 5 and encrypted data to tape for clients 1 through 6. 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 MSEO 2, GUI 2, and clients 7 through 12 in Tokyo. Media server 2 writes unencrypted data to tape for clients 10 and 11 and encrypted data to tape for clients 7, 8, 9, and 12.

Table 2-13 NetBackup parts used for a multi-datacenter with all NetBackup security implemented *(continued)*

Part	Description
GUIs	Specifies that there can be two GUIs in this multi-datacenter example. 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 one root broker is 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 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 datacenter installation. Sometimes the authentication broker can be combined with the root broker. In this datacenter installation, there are two authentication brokers used. The authentication broker authenticates the master server, media server, GUI, and clients by establishing credentials with each. The authentication broker also authenticates a user with a command prompt. In London, authentication broker 1 authenticates a credential with the master server, media server 1, GUI 1, and clients 1 through 6. 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 only one authorization engine is required in a multi-datacenter installation. The authorization engine communicates with the master server and media servers 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.

Table 2-13 NetBackup parts used for a multi-datacenter with all NetBackup security implemented *(continued)*

Part	Description
Tapes	Specifies that unencrypted and encrypted 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. The encrypted tape is written for clients 1, 2, 3, 6, and 7, and is transported off-site to a vault in London for disaster recovery. 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, 8, 9, and 12 and is transported off-site to a vault in Tokyo for disaster recovery protection. Even though client 7 is located in Tokyo and is backed up in Tokyo, client 7 is also backed up in London greater security and backup redundancy. **Note:** To decrypt the data, the key(s) used to encrypt the data must be made available.
Transports	Specifies that there can be two transports. One transport is in London and the other is in Tokyo. The transport truck in London moves the encrypted tape for clients 1, 2, 3, 6, and 7 off-site to a secure London vault facility. The transport truck in Tokyo moves the encrypted tape for clients 7, 8, 9, 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 a tape is lost during transport, the datacenter manager has potentially reduced the risk of a data breach by using client side data encryption.
Vaults off-site	Specifies that there can be two vaults off-site. One vault is in London and the other is in Tokyo. Both vaults provide safe encrypted tape storage facilities off-site at different locations than the datacenters. **Note:** Storing the encrypted tapes at a separate location from the datacenter promotes good disaster recovery protection.
Clients	Specifies that clients are located in both the London and Tokyo datacenters. In London, clients 1 through 3 are MSEO encrypted types. Client 4 is a standard NetBackup type. 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 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, clients 7 through 9 are MSEO encrypted types. Client 10 is a standard NetBackup type. Client 11 is a Web server type located in the DMZ. Client 12 is a client side encrypted type 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 2. Note that client 7 can be managed by both media server 1 and 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

Table 2-13 NetBackup parts used for a multi-datacenter with all NetBackup security implemented *(continued)*

Part	Description
Internal firewalls	Specifies that there an 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 and encrypted client 6 in the DMZ. In Tokyo, the internal firewall NetBackup access Web server client 11 and encrypted client 12 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 and encrypted client 6. These clients exist 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 and encrypted client 12. These clients exist 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.
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 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.

Chapter 3

Port security

This chapter includes the following topics:

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: Symantec 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 Symantec 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 96.
- See "About configuring ports" on page 107.
- See "Port requirements for NDMP backups" on page 118.
- See "Known firewall problems encountered when using NetBackup with third-party robotic products" on page 118.

About NetBackup daemons, ports, and communication

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

- See "Standard NetBackup ports" on page 96.
- See "NetBackup master server outgoing ports" on page 97.
- See "NetBackup media server outgoing ports" on page 98.
- See "NetBackup enterprise media management (EMM) server outgoing ports" on page 99.
- See "Client outgoing ports" on page 100.
- See "Windows administration console and Java server outgoing ports" on page 100.
- See "Java console outgoing ports" on page 101.
- See "Additional port information for products that interoperate with NetBackup" on page 102.

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 Daemons and ports used in a standard NetBackup environment

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

Table 3-2 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	Symantec private branch exchange service, VxPBX.
NetBackup master server, media server, or client	`vrts-at-port` 13783	Master	NetBackup authentication service, VxAT. The `nbatd` process listens on port 13783 for back-level media servers and clients. The NetBackup media servers and clients connect using the PBX port.
NetBackup master server or media server	`vrts-auth-port` 13722	NetBackup master server	NetBackup Authorization Service, VxAZ. The `nbazd` process listens on port 13722 for back level media servers and clients. The NetBackup media servers and clients connect using the PBX port.

In a NetBackup environment, the port number is always derived from the source component's client port window or the client reserved port window. A typical NetBackup environment uses the additional daemons and ports described in the following topics:

NetBackup master server outgoing ports

Table 3-3 shows the ports that the master server uses to send data packets.

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.
`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.
`vrts-at-port` 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.
`vrts-auth-port` 13722	Authorization server	Authorizes a user for system administration. Used only when NBAC is enabled.

NetBackup media server outgoing ports

Table 3-4 shows the ports that the media server uses to send data packets. The table shows the port name, port number, the 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.
`vrts-at-port` 13783	Authentication server	Authenticates users and machines. Used only when NetBackup access control (NBAC) is enabled.
`vrts-auth-port` 13722	Authorization server	Authenticates a user for system administration. Used only when NBAC is enabled.

NetBackup enterprise media management (EMM) server outgoing ports

Table 3-5 shows the ports that the EMM server uses to send data packets.

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.
`veritas_pbx` 1556	Media 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	Administrative console or Java server	Connect-back for information about device, media, and storage databases.
`vrts-at-port` 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.
`vrts-auth-port` 13722	Authorization server	Authorizes a user for system administration.

Client outgoing ports

Table 3-6 shows the ports that clients use to send data packets.

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`.
`vrts-at-port` 13783	Authentication server	Authenticates users or machines.

Windows administration console and Java server outgoing ports

Table 3-7 shows the ports that the Windows administration console and the Java Server use to send data packets.

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

Table 3-7 Windows administration console and 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.
`vrts-at-port` 13783	Authentication server	Establishes user credentials for administration.

Java console outgoing ports

Table 3-8 shows the ports that the Java console uses to send data packets.

Table 3-8 Java 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`. Used only when the Java console's NetBackup software level is less than NetBackup 7.6.
`vnetd` 13724	Java server	Establishes sockets with the legacy Java server, `bpjava`. Used only when the Java console's NetBackup software level is less than NetBackup 7.6.

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

NetBackup Cloud uses 5637 as the default port number for the nbcssc service.

Additional port information for products that interoperate with NetBackup

The following topics describe port information that is important if you use NetBackup with OpsCenter, Backup Exec, and other products that interoperate with NetBackup:

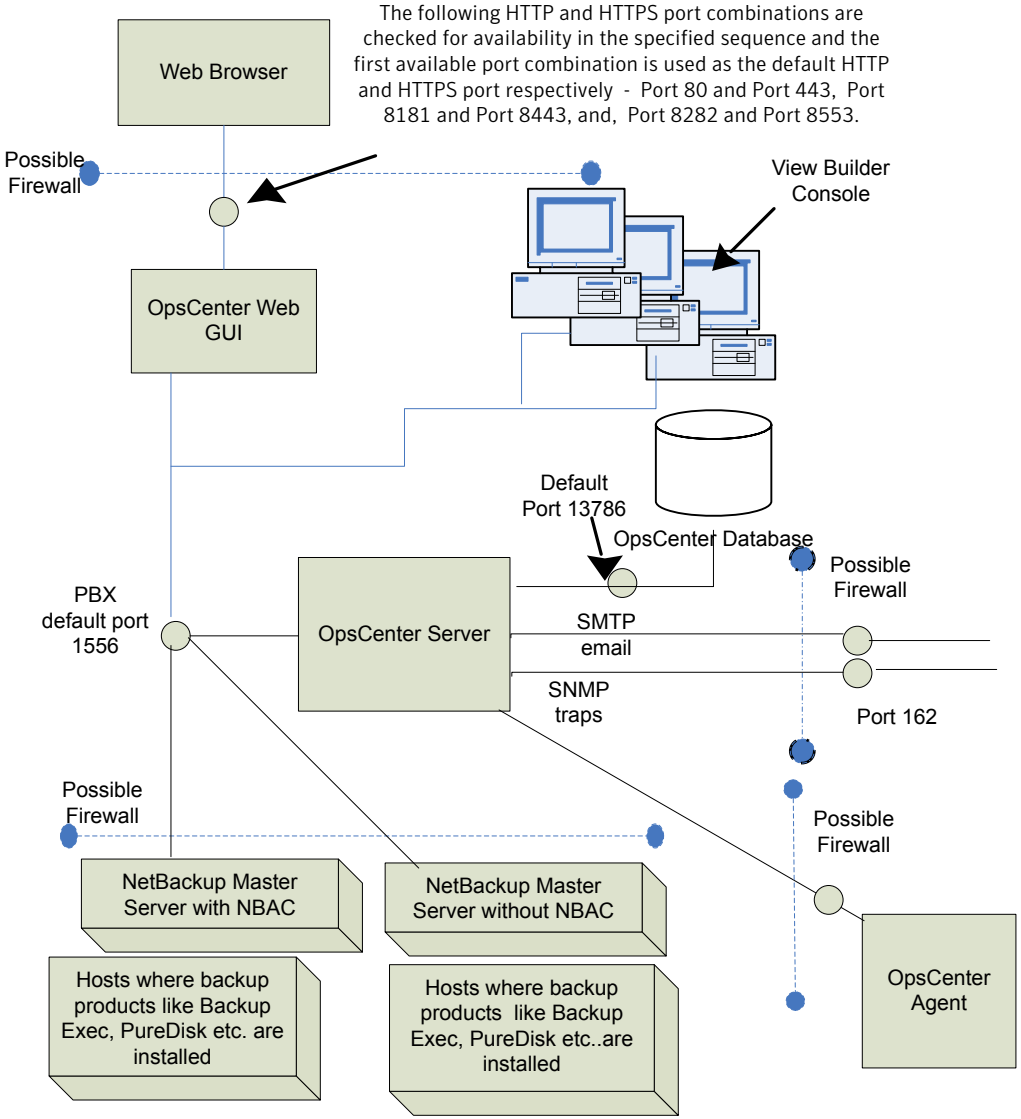
- See "About communication and firewall considerations" on page 103.
- See "Ports required to communicate with backup products" on page 104.
- See "Web browser to NetBackup Web GUI connection" on page 105.
- See "About NetBackup Web GUI to NetBackup server software communication" on page 106.
- See "About NetBackup server to NetBackup master server (NBSL) communication" on page 106.
- See "About SNMP traps" on page 107.

- See “About NetBackup Web GUI/NetBackup server to Sybase database communication” on page 107.
- See “About NetBackup Web GUI to NetBackup server email communication” on page 107.

About communication and firewall considerations

The following image shows the key NetBackup components and the communication ports that are used.

Figure 3-1 Key NetBackup components and how they communicate



Ports required to communicate with backup products

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

Table 3-10 lists the ports that must be opened on NetBackup Agent to collect data from various backup products.

Table 3-10 Ports required to communicate with other backup product

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

Web browser to NetBackup Web GUI connection

Web browsers use Insecure hypertext transfer protocol (HTTP) and Secure hypertext transfer protocol (HTTPS) to communicate with the NetBackup Web GUI. These protocols use TCP/IP.

For HTTP, specific ports are checked for availability in a particular sequence and the first available port is used by default.

Table 3-11 lists how the default HTTP and HTTPS ports are selected.

Table 3-11 Default HTTP and HTTPS ports

Sr. No.	HTTP port number	HTTPS port number	Description
1.	80	443	Port 80 and Port 443 are checked for availability. ■ If port 80 and port 443 are available, port 80 is used as the default HTTP port and port 443 is used as the default HTTPS port. ■ In case, some other application like a Web server uses one or both ports, then the next port combination is checked for availability.

Table 3-11 Default HTTP and HTTPS ports *(continued)*

Sr. No.	HTTP port number	HTTPS port number	Description
2.	8181	8443	Port 8181 and Port 8443 are checked for availability. ■ If port 8181and port 8443 are available, port 8181 is used as the default HTTP port and 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.	8282	8553	Port 8282 and Port 8553 are checked for availability.

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

About NetBackup Web GUI to NetBackup server software communication

The NetBackup Web GUI uses Symantec Private Branch Exchange (PBX) to communicate with the NetBackup server software. The default port is 1556. The PBX port is opened for input and output traffic.

About NetBackup server to NetBackup master server (NBSL) communication

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

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

- Initial data load
- Listening for change notifications or events

Whenever NetBackup server software starts, when data collection for a master server is enabled or when a master server is added to NetBackup, 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 NetBackup server software

listens to the notifications that are sent by NBSL for any change in NetBackup data. Then NetBackup updates the NetBackup database.

Symantec 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 that is used is 1556. Configuring the PBX port is not supported in OpsCenter 7.5.

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 NetBackup Web GUI/NetBackup server to Sybase database communication

The NetBackup Web GUI communicates with the NetBackup 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 NetBackup components on the NetBackup server.

About NetBackup Web GUI to NetBackup server email communication

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 NetBackup 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 108.
- See “Specifying firewall connection options on a NetBackup server or client” on page 109.
- See “Specifying firewall connection options for destination computers from a source computer” on page 112.
- See “Editing port information in configuration files” on page 114.
- See “Updating client connection options” on page 115.

- See "Updating port settings for the Media Manager in the vm.conf file" on page 115.

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 Java or Windows interface

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.

Specifying firewall connection options on a NetBackup server or client

Within a NetBackup environment, you can define the connection options between a computer that initiates a connection (the source computer) and a computer that receives information (the destination computer).

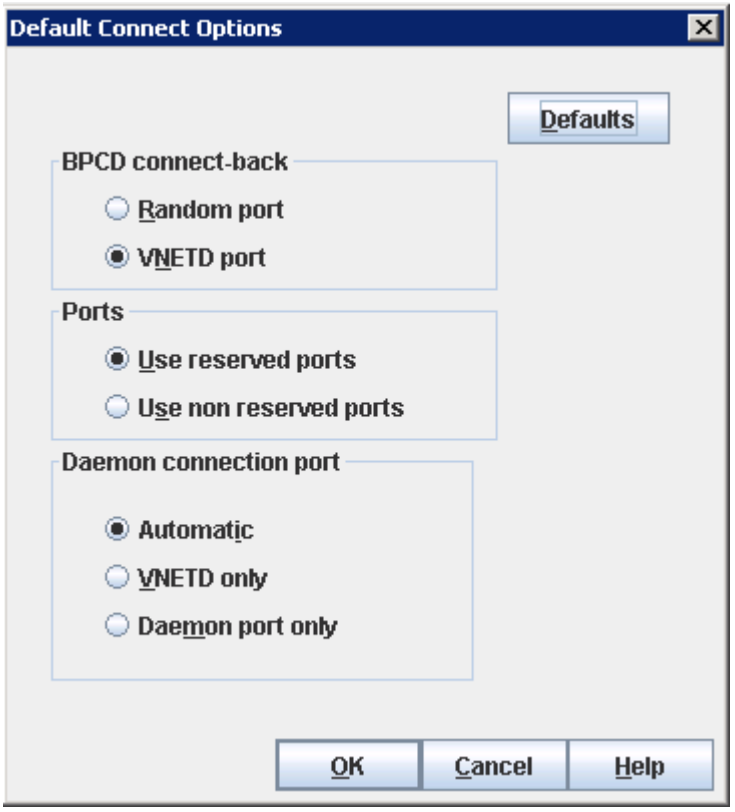
In addition, you can set the default connection options for all of the other destination computers from the source computer. For example, if there is a firewall between the master server and the media servers, you can specify all the connection options from the NetBackup master server.

If the destination computer runs a NetBackup version that is earlier than the NetBackup master server, the ability to specify connection options from the source computer depends on the NetBackup release level on the destination computer. For more information, see the documentation for the NetBackup release level that matches the destination computer.

To specify Firewall connection options from a source computer

1. In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.
2. Double click the host you want to configure.
3. Click **Firewall**.
4. Click **Change** in the **Default Connect Options** pane.

   A display similar to the following appears:



The following information applies to the **Default Connect Options** display:

- If the source computer is a NetBackup client the display includes only the **Daemon connection port** setting.
- If both the source and destination computers are at the NetBackup 6.5 release level or later, the **BPCD connect-back** and the **Ports** settings generally have no effect. By default, NetBackup uses nonreserved ports and does not use call-back.

The remaining steps in this procedure explain how to set the connection options.

5 (Optional) Change the **BPCD connect-back** setting.

Choose one of the following:

- **Random port**. Default for NetBackup 5.1 and earlier.
  Specifies that the host computer use the legacy `bpcd` random port callback method to connect to other computers.
- **VNETD port**. Default for releases later than NetBackup 5.1.

Specifies that the host computer use the vnetd daemon to connect to other computers.

6 (Optional) Change the **Ports** setting.

Choose one of the following:

- **Use reserved ports**. Default.
  When in effect, the source computer connects to bpcd on the destination computers that use a reserved port number.
- **Use nonreserved ports**.
  When in effect, the source computer connects to bpcd on destination computers using a nonreserved port number.
  Make sure to perform step 8 of this procedure, which ensures that other computers in the NetBackup environment also are configured for nonreserved ports.

7 (Optional) Change the **Daemon connection port** setting.

Choose one of the following:

- **Automatic**. Default for NetBackup 5.0 and later.
  Specifies that other computers connect to this host by using the vnetd daemon, if possible. If a connection via vnetd is not possible, use the daemon's legacy port number.
- **VNETD only**.
  Specifies that other computers connect to this host by using only the vnetd daemon. If your site's firewall rules prevent connections to this host through the legacy port number, make sure that this setting is in effect.
- **Daemon port only**. Default for releases earlier than NetBackup 5.0.
  Specifies that other computers use the legacy port number to connect to this host.
  For releases earlier than NetBackup 5.0, connections to bpcd always use the legacy bpcd port number.
  For NetBackup release 5.0 and later, connections to bpcd can be made with the vnetd port number if both the source and the destination computers use NetBackup 5.0 or later.
  When bpcd connections are made using the vnetd port number, the **Ports** and **BPCD connect-back** options are ignored. In this case, NetBackup uses nonreserved source port numbers, the vnetd destination port number, and no callback.

This setting does not affect connections to `veritas_pbx`, `veritas-at-port`, and `veritas-auth-port`. Those connections always use the legacy or IANA defined port numbers.

8 (Conditional) Configure other computers in the NetBackup environment to use nonreserved ports.

Perform this step if you selected **Use nonreserved ports**.

If any hosts in your environment run NetBackup 6.5 or earlier, make sure that the host allows connections on nonreserved ports, which is the default. Click **NetBackup Administration Console > Host Properties > Universal Settings**, and make sure that **Accept connections on nonreserved ports** is checked. For more information about this property, see your NetBackup 6.5 documentation.

Configure the clients to use nonreserved ports. You can accomplish this task from the NetBackup administration console in the **Connect Options** tab of the **Client Attributes** dialog box. For more information about how to use the options on this tab, see the NetBackup Administrator's Guide.

Specifying firewall connection options for destination computers from a source computer

The following procedure describes how to specify Firewall connect options on a source computer that apply to specific destination computers. For example, you can perform this procedure from a master server and specify connect options for clients.

To specify Firewall connection options on a source computer that apply to destination computers

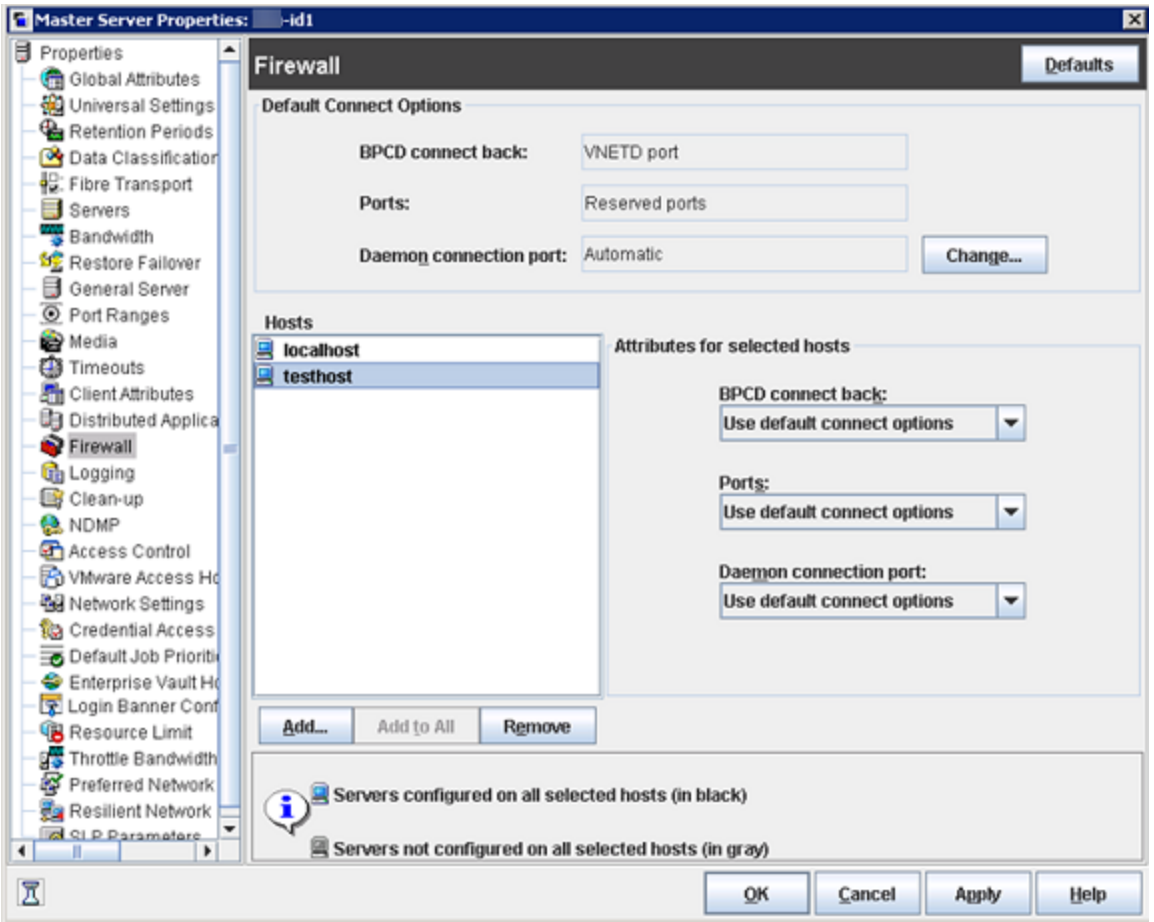
1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.

2 Double click the host you want to configure.

3 Click **Firewall**.

4 Click **Add** in the **Hosts** pane. Add a destination host (usually another NetBackup server) to the hosts list.

The host list is shown in the following figure:



5 (Optional) Select appropriate options under **Attributes for selected hosts**.

For information about the **BPCD connect-back**, **Ports**, and **Daemon connection port** attributes, see the following:

See “Specifying firewall connection options on a NetBackup server or client” on page 109.

If you select **Use default connect options**, NetBackup uses the values that appear under the **Default Connect Options** list.

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.

Symantec 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`

For hosts that run NetBackup 5.1 and earlier releases, examine the `vm.conf` file. You need to specify the Media Manager connection options manually on hosts that run these earlier releases.

Table 3-12 shows the `vm.conf` file settings that affect ports.

Table 3-12 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

Table 3-12 Port usage-related Media Manager configuration settings *(continued)*

Setting	Description
CONNECT_OPTIONS	**Note:** The CONNECT_OPTIONS setting affects only connections to hosts that run NetBackup 7.0 and earlier. When NetBackup connects to hosts that run NetBackup 7.0.1 and later, NetBackup uses the veritas_pbx port. Specifies the destination port number that can be used to connect to the Media Manager services. The format is as follows: CONNECT_OPTIONS = *host* 0 0 0|1|2 This setting accepts four space-separated arguments. The arguments are as follows. For *host*, specify the name of the media server to which other computers need to connect. After the *host* name, type 0 0. The arguments in these positions are not used. After 0 0, type 0, 1, or 2 to specify the connection method to the Media Manager service on the target computer. The connection method specifications are as follows: ■ If 0, the host uses the vnetd port. If that attempt fails, the hosts uses the legacy port number. ■ If 1, the host uses only vnetd to connect to the server. ■ If 2, the host uses the legacy Media Manager port. Default for 5.1 and earlier servers. You can specify multiple CONNECT_OPTIONS settings in the vm.conf file. For NetBackup, if the vm.conf file does not contain any CONNECT_OPTIONS entries, the Media Manager selects the port based on the bp.conf file settings for DEFAULT_CONNECT_OPTIONS and CONNECT_OPTIONS. For example, the following settings specify that the Media Manager connections to server3 use vnetd as the destination port: CONNECT_OPTIONS = server3 0 0 1
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 3-13 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.
Remote NDMP (5.0 / 5.1)	For remote NDMP (5.0 / 5.1), a firewall is not suggested between the DMA and the NDMP hosts because the DMA can be on the same computer as the NDMP tape server. You need an unlimited number of ports available to perform the data movement between the NDMP tape server and the NDMP data server.

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.

Chapter 4

Auditing NetBackup Operations

This chapter includes the following topics:

About NetBackup auditing

An audit trail is a record of user-initiated actions in a NetBackup environment. Essentially, auditing gathers the information to help answer who changed what and when they changed it.

Auditing NetBackup operations can help provide information in the following areas:

General tracking	Customers can gain insight from audit trails while they investigate unexpected changes in a NetBackup environment. For example, it might be found that the addition of a client or a backup path has caused a significant increase in backup times. The audit report can indicate that an adjustment to a schedule or to a storage unit configuration might be necessary to accommodate the policy change.
Regulatory compliance	Auditing creates a record of who changed what and when it was changed. The record complies with guidelines such as those required by the Sarbanes-Oxley Act (SOX).
Corporate change management	For customers who must adhere to internal change management policies, NetBackup auditing offers a method to adhere to such policies.
Troubleshooting	The information from NetBackup auditing helps NetBackup Support to troubleshoot problems for customers.

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

The Audit Manager provides the mechanism to query and report on auditing information. For example, an administrator can search specifically for information based on when an action occurred, the actions performed by a specific user, the actions performed in a specific content area, or changes to the audit configuration.

When auditing is configured (by default auditing is enabled), the following NetBackup user-initiated actions are recorded and available to view by using the `nbauditreport` command or by using Symantec NetBackup OpsCenter:

- The following NetBackup entities are audited:
  - **Policies**
    Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists.
  - **Activity Monitor**
    Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record.
  - **Storage units**
    Adding, deleting, or updating storage units.

Note: Actions that are related to **Storage Lifecycle Policies** are not audited.

- **Storage servers**
  Adding, deleting, or updating storage servers.
- **Disk pools** and **Volume pools**
  Adding, deleting, or updating disk or volume pools.
- **Host properties**
  Updating host properties. (NetBackup Access Control (NBAC) must be enabled for host property auditing to occur.)

- Initiating a restore job.
  A restore job is the only job type for which the initiation is audited. For example, when a backup job begins, no audit record is created.
- Enabling or disabling NetBackup Auditing.
- Starting and stopping the NetBackup Audit Manager (`nbaudit`).

Note: Enabling and disabling auditing settings or starting and stopping `nbaudit` are all audited, even if auditing is disabled.

- Changes to the `bp.conf` file (UNIX) or the registry (Windows).
  For NetBackup to audit changes to the `bp.conf` file or the registry, NetBackup Access Control (NBAC) must be enabled. These changes must be made by using either `bpsetconfig`, `nbsetconfig`, or the **Host Properties** utility in the **NetBackup Administration Console**. Manual changes to the `bp.conf` file or the registry are not audited.
  See "Auditing host property changes" on page 132.
  See the following topic for more information about configuring NetBackup Access Control: See "Configuring NetBackup Access Control (NBAC)" on page 153.

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

Any failed actions.	Failed actions are logged 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 ramifications 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 is displayed in the Activity Monitor.
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.

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 Symantec NetBackup OpsCenter.

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

To view the current audit settings

1. From a command prompt, locate the `nbemmcmd` command on the master server in the following directory:
   - On Windows:
     Install_path\Veritas\NetBackup\bin\admincmd
   - On UNIX:
     /usr/openv/netbackup/bin/admincmd
2. Enter the `nbemmcmd` command using the following syntax:

   ```
   nbemmcmd -listsettings -machinename masterserver
   ```

   Where *masterserver* is the master server in question.

   Note: The options are case-sensitive.

3. The output lists many configuration settings. Among them are the following:
   - `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.

Configuring auditing on a NetBackup master server

Auditing is enabled by default in new installations. However, the default may be enabled or disabled after an upgrade, depending on the setting before the upgrade.

NetBackup auditing can be configured directly on a NetBackup master server or by using Symantec NetBackup OpsCenter.

The master server settings for enabling or disabling audit logging and setting the retention period are configured in the **Manage > Hosts** section of OpsCenter. Within OpsCenter, the expiration setting for Audit logs is configured under **Settings > Purge**.

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

To configure auditing on a master server, use the nbemmcmd command with the -changesetting option.

To configure NetBackup auditing on a master server

1. From a command prompt, locate the nbemmcmd command on the master server in the following directory:
   - On Windows:
     Install_path\Veritas\NetBackup\bin\admincmd
   - On UNIX:
     /usr/openv/netbackup/bin/admincmd
2. Enter the nbemmcmd command using the following syntax:

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename masterserver
   ```

   Where -AUDIT DISABLED turns off auditing on the master server that is indicated.

   Note: The options are case-sensitive.

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

   For example:

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename server1
   ```

3 Configure the audit retention period using the following syntax:

```
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. If no retention period is indicated, the default audit retention period is 90 days.

Note: An audit retention period value of `0` (zero) indicates that the records are never deleted.

OpsCenter downloads the audit records periodically and retains them for a period of time that is configurable in OpsCenter. Retaining the audit records on the master server is only necessary if you want to view audit reports using the command line on the master server.

See the following topic for more information.

See "Retaining and backing up audit trail records" on page 132.

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

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

The two options can be combined in one command line, as in the following example:

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

4 Run `nbauditreport` to display a report of the audited information.

See "Viewing the audit report" on page 133.

User identity in the audit report

The audit report lists the identity of the user who performed a specific action. The identity includes the user name, the domain, and the domain type of the authenticated user.

The user name that is captured in the audit report, depends on the following:

- By default, only a root or an administrator user can perform NetBackup Operations through a CLI as well as through the NetBackup Administration

Console. The root or the administrator are hence audited with root or administrator user name.

- When either Enhanced Auditing or NBAC is enabled, the actual user name of the user who performed NetBackup Operations through the CLI or through the NetBackup Administration Console are recorded in the audit report.
- By default, only the root or administrator user can perform NetBackup Operations through CLIs as well as NetBackup Admin Console and hence audited with root or administrator user name.
- All tasks would be audited as root or administrator when neither Enhanced Auditing nor NBAC is enabled.

See "About using NetBackup Access Control (NBAC)" on page 150.

See "About Enhanced Auditing" on page 126.

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 would find useful.

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

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, and Storage Units.

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

Table 4-1 Commands and categories supported for Enhanced Auditing

Command	Category
bpplcatdrinfo	Policy
bpplclients	Policy
bppldelete	Policy
bpplinclude	Policy
bpplinfo	Policy
bppllist	Policy
bpplsched	Policy
bpplschedrep	Policy
bpplschedwin	Policy
bpplvalid	Policy
bppolicynew	Policy
bpdbjobs	Jobs
bpstuadd	Storage Unit
bpstuddel	Storage Unit
bpsturep	Storage Unit
bpstulist	Storage Unit

Enabling Enhanced Auditing

NetBackup must be configured using the `bpnbaz -SetupExAudit` command to enable Enhanced Auditing. The following steps help you in the configuration:

To configure NetBackup for Enhanced Auditing

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

Note: On a cluster setup, you must run this command on both the active as well as the passive node.

2 Restart the NetBackup services.

See "Configuring Enhanced Auditing" on page 128.

Configuring Enhanced Auditing

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

- Having 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 128.
- 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 129.

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.

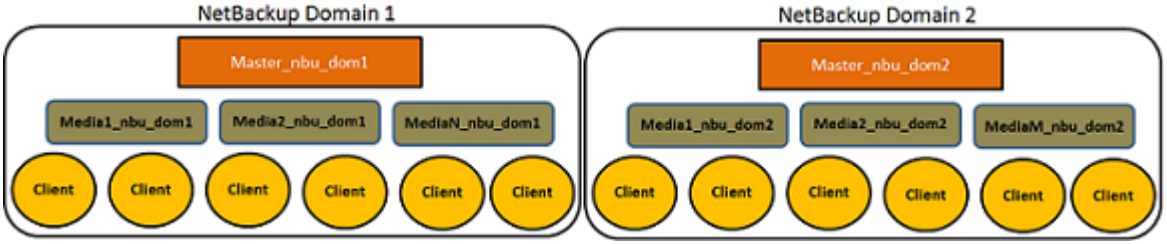
Note: Executing these steps is a one-time activity.

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:



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 129. 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 128.)

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 129. 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

You can disable Enhanced Auditing in NetBackup. When you enable Enhanced Auditing, the USE_AUTHENTICATON option is set to ON, you must set it to OFF to disable Enhanced Auditing. The following steps help you:

To disable Enhanced Auditing

1. Run the `bpsetconfig` command on the master server.
2. Set `bpsetconfig> USE_AUTHENTICATON=OFF`.
3. Restart the NetBackup services.

Auditing host property changes

NetBackup audits host property changes if the administrator uses either the `bpsetconfig` or the `nbsetconfig` commands, or the equivalent property in the **Host Properties** utility.

The following criteria must be met for auditing to take place:

- The environment must be configured for NetBackup Access Control (NBAC).
- The host on which the `bp.conf` file or the registry changes are made must be at NetBackup 7.1 or later.
- The administrator must use either the `bpsetconfig` or the `nbsetconfig` commands, or the equivalent property in the **Host Properties** utility for auditing to occur. Changes that are made directly to the `bp.conf` file or to the registry are not audited. That is, the changes that are made without `bpsetconfig` or `nbsetconfig`.

  For example, taking a client offline is not performed using the `bpsetconfig` or the `nbsetconfig` command, so this operation would not show up in the audit log.

Retaining and backing up audit trail records

By default, audit records are kept for 90 days. To change the default, use the `nbemmcmd -changesetting` command with the `-AUDIT_RETENTION_PERIOD` option.

See “Configuring auditing on a NetBackup master server” on page 124.

Based on the configured retention setting, the NetBackup Audit Service (`nbaudit`) deletes expired audit records once every 24 hours at 12:00 A.M. (local time).

The audit records are kept in audit tables that are part of the NetBackup database. The tables are retained for as long as the `-AUDIT_RETENTION_PERIOD` indicates and are backed up as part of the NetBackup catalog backup.

To make sure 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`.

Symantec NetBackup OpsCenter downloads the audit records periodically from the EMM database. OpsCenter retains the records for a period of time that is configured within OpsCenter. Therefore, retaining the audit records on the NetBackup master server is only necessary if you want to view audit reports using the command line on the master server. Audit records can also be exported from OpsCenter.

Viewing the audit report

To view the audit report, use either the `nbauditreport` command on a NetBackup master server or view the settings using Symantec NetBackup OpsCenter.

Within OpsCenter, the **Monitor > Audit Trails** section provides the details of the Audit logs and lets you export that information to Excel or save as a .pdf file.

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

If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the `nbaudit` log.

The Audit alert notification button in the **NetBackup Administration Console** can notify administrators when an audit failure occurs.

See "Audit alert notification for audit failures" on page 139.

The failure to create an audit record has no effect on the user action that was performed.

If the user action succeeds, an exit code is returned that reflects the successful action. If auditing of the action fails, NetBackup status code 108 is returned (`Action succeeded but auditing failed`).

Note: The **NetBackup Administration Console** (Windows and UNIX (`jnbSA`)) does not return an exit status code 108 when auditing fails.

To view the NetBackup audit report

1 From a command prompt, locate the `nbauditreport` command on the master server in the following directory:

- On Windows:
  Install_path\Veritas\NetBackup\bin\admincmd
- On UNIX:
  /usr/openv/netbackup/bin/admincmd

2 In its simplest form, enter the nbauditreport command using the following syntax:

```
nbauditreport
```

The nbauditreport can also be used with a number of options.

Note: The options are case-sensitive.

-help	Use for assistance with the command at the command prompt.
-sdate <"MM/DD/YY [HH:[MM[:SS]]]">	Use to indicate the start date and time of the report data you want to view.
-edate <"MM/DD/YY [HH:[MM[:SS]]]">	Use to indicate the end date and time of the report data you want to view.
-ctgy POLICY	Use -ctgy POLICY to display information pertaining to policy changes.
-ctgy JOB	Use -ctgy JOB to display information pertaining to jobs.
-ctgy STU	Use -ctgy STU to display information pertaining to storage units.
-ctgy STORAGESRV	Use -ctgy STORAGESRV to display information pertaining to storage servers.
-ctgy POOL	Use -ctgy POOL to display information pertaining to storage pools.
-ctgy AUDITCFG	Use -ctgy AUDITCFG to display information pertaining to audit configuration changes.
-ctgy AUDITSVC	Use -ctgy AUDITSVC to display information pertaining to the starting and stopping of the NetBackup Audit service (nbaudit).

`-ctgy BPCONF`	Use `-ctgy BPCONF` to display information pertaining to changes in the `bp.conf` file.
`-ctgy USER`	Use the -ctgy USER to display information pertaining to addition and deletion of users in the Enhanced Auditing mode.
`-user <username[:domainname]>`	Use to indicate the name of the user for whom you'd like to display audit information.
`-fmt SUMMARY`	If no report output format option (`-fmt`) is specified, the `SUMMARY` option is used by default.
`-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.
`-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.
`[-notruncate]`	Use the `-notruncate` option to display the old and new values of a changed attribute on separate lines in the details section of the report. **Note:** `-notruncate` is valid only with the `-fmt DETAIL` option.
`[-pagewidth <NNN>]`	Use the `-pagewidth` option to set the page width for the details section of the report. **Note:** `-pagewidth` is valid only with the `-fmt DETAIL` option.

`[-order <DTU|DUT|TDU|TUD|UDT|UTD>]`	The `-order` option is valid only with `-fmt PARSABLE`. Use it to indicate the order in which the information appears. Use the following parameters: ■ `D` (Description) ■ `T` (Timestamp) ■ `U` (User)

3 The audit report contains the following details:

`DESCRIPTION`	The details of the action that was performed. The details include the new values that are given to a modified object and the new values of all attributes for a newly created object. The details also include the identification of any deleted objects.
`USER`	The identity of the user who performed the action. The identity includes the user name, the domain, and the domain type of the authenticated user. See "User identity in the audit report" on page 125.
`TIMESTAMP`	The time that the action was performed. The time is given in Coordinated Universal Time (UTC) and indicated in seconds. (For example, `12/06/11 10:32:48`.)
`CATEGORY`	The category of user action that was performed. The `CATEGORY` displays only with the `-fmt DETAIL|PARSABLE` options. Examples include the following: ■ `AUDITSVC START`, `AUDITSVC STOP` ■ `POLICY CREATE`, `POLICY MODIFY`, `POLICY DELETE`
`ACTION`	The action that was performed. The `ACTION` displays only with the `-fmt DETAIL|PARSABLE` options. Examples include the following: ■ `START`, `STOP` ■ `CREATE`, `MODIFY`, `DELETE`

REASON	The reason that the action was performed. A reason displays if a reason was specified in the command that created the change. The bpsetconfig and the nbsetconfig commands accept the -r option. See "Using the command line -reason or -r option" on page 137. The reason displays only with the -fmt DETAIL|PARSABLE options.
DETAILS	An account of all of the changes, listing the old values and the new values. Displays only with the -fmt DETAIL|PARSABLE options.

If an exit status appears in the output, look up the code in the **NetBackup Administration Console** (Troubleshooter), the online Help, or the Status Codes Reference Guide.

Figure 4-1 shows the default contents of an audit report that was run on server1.

Figure 4-1 Summary audit report example

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP               USER           DESCRIPTION
09/23/2010 14:40:54     root@server1   Policy 'test_pol_1' was created
09/23/2010 14:40:54     root@server1   Schedule 'full' was added to Policy
'test_pol_1'
09/22/2010 17:10:23     root@server1   Audit setting(s) of master server 'server1'
were modified

Audit records fetched: 3
```

Using the command line -reason or -r option

Many commands offer the -reason option for administrators to use to indicate why the action was performed. The reason displays in the audit report.

The -reason string must be no more than 512 characters. Command lines that accept the -reason option display an error if the string is over 512 characters.

Keep in mind that the audit reason cannot begin with a dash character (-). The reason also cannot contain a single quotation mark (\').

The following commands accept the -reason option (or -r option in the case of bpsetconfig or nbsetconfig):

- bpdbjobs
- bpplcatdrinfo

- bpplclients
- bppldelete
- bpplinclude
- bpplinfo
- bpplsched
- bpplschedrep
- bppolicynew
- bpsetconfig

Note: The bpsetconfig and nbsetconfig commands accept the -r option instead of the -reason option.

- bpstuadd
- bpstudel
- bpsturep
- nbdecommission
- nbdevconfig
- nbsetconfig
- vmpool

For more information on using the commands, see the NetBackup Commands Reference Guide.

nbaudit log behavior

The nbaudit log is found in the following location:

- On Windows:
  Install_path\Veritas\NetBackup\logs\nbaudit
- On UNIX:
  /usr/openv/logs/nbaudit

If auditing is enabled but a user action fails to create an audit record, the audit failure is captured in the nbaudit log.

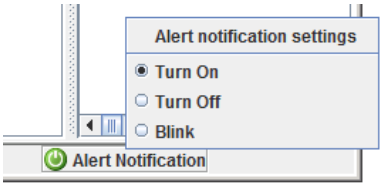
The Audit alert notification button in the **NetBackup Administration Console** can notify administrators when an audit failure occurs.

The `nbaudit` service behaves in the following manner when it creates audit records:

- The audit record limits the details of an entry to a maximum of 4096 characters. (For example, the Policy name.) The remaining characters are truncated while stored in the audit database.
- The audit record limits the restore image IDs to a maximum of 1024 characters. The remaining characters are truncated while stored in the audit database.
- Rollback operations are not audited.
  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.

Audit alert notification for audit failures

The Audit alert notification option is located in the status bar at the bottom of the **NetBackup Administration Console**. If it is configured to do so, the option can indicate when an auditable action has failed to create an audit record. For example, if a policy attribute is changed but the NetBackup Audit Manager (`nbaudit`) is not running.

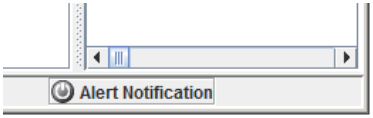


To configure Audit alert notification, right-click the Audit alert option in the status bar:

Table 4-2 Audit alert notification settings

Turn on	When it is set to **Turn on**, a pop-up message displays in the following situation: Auditing is enabled, but an auditable action is performed in the **NetBackup Administration Console** and has failed to create an audit record. A pop-up message appears to alert the administrator about the failure.

Table 4-2 Audit alert notification settings *(continued)*

Blink	When it is set to **Blink**, the option blinks in the event of an auditing failure. Click the option to display the failure message.
Turn off	When it is set to **Turn off**, an auditing failure does not display a notification. The option appears as gray.  **Note: Turn off** does not mean that auditing is disabled. Auditing continues, but audit failure messages in the **NetBackup Administration Console** are disabled.

Chapter 5

Access control security

This chapter includes the following topics:

About access control in NetBackup

NetBackup provides three types of access controls, the Java-based access control, NetBackup Access Control (NBAC) and Enhanced Auditing.

- The Java-based access control is the default. It is a view-based access control and is limited to the NetBackup-Java Administration Console interface. A CLI user must be root or administrator to perform NetBackup operations, whereas NetBackup Administration Console is accessible by any non-root or non-administrator user. The user can only view those nodes as per the permissions that are defined in the auth.conf file.
  For detailed information about the Java-based access control, refer to the 'Using the NetBackup Administration Console' chapter in the NetBackup Administrator's Guide, Volume I.
- NetBackup Access Control (NBAC) is the role-based access control that can be used for master servers, media servers, and clients 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 (to monitor jobs) or administrators (have full permission to access, configure, and operate any

NetBackup authorization object). It can also have Security administrators who can only configure access control.

- Separate the administrators, so that root permission is not required to administer the system. You can have separate administrators for the systems other than administrators for applications.
  See "About using NetBackup Access Control (NBAC)" on page 150.

- Enhanced Auditing 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 none of them. The feature does not offer role-based access control unlike NBAC.
  See "About Enhanced Auditing" on page 126.

Refer to the following table for key differences between the access control methods:

Table 5-1

Key parameters	Java GUI - auth.conf based access control (default mode)	NBAC	Enhanced Auditing
Who can access?	A root or administrator has access through the CLI. Non-root and non-administrator users have access through the Java GUI	Non-root or non-administrators have access through CLI or Java GUI.	Non-root or non-administrators have access through CLI or Java GUI.
What can be accessed?	CLI users have no access control, Java GUI users have access control through the auth.conf file.	Granular access control.	Binary (Coarse) access control.
How is user audited?	User is audited as a root or administrator.	User is audited with the real user name.	User is audited with the real user name.
What can work with others?	This can work with Enhanced Auditing. Access control is according to the entry in the auth.conf file.	NBAC can work independently.	This can work with Java GUI authorization. Access control is according to the entry in the auth.conf file.

User management

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.symantec.com:Debbie`
-DelUser	Helps the user to revoke NetBackup administrator privileges.	`bpnbaz -DelUser unixpwd:v-123790b.punin.sen.symantec.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.symantec.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

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 to perform user authentication.

The log-on process for UNIX and Windows users varies, refer to the following information:

UNIX

- An `bpnbat -login` is not mandatory for a root user.
- A non-root user is however required to perform an `bpnbat -login`.

Windows

- The administrator logs on automatically through the Single Sign On (SSO) option.
- A standard user also logs on through the SSO option. But if the SSO fails, the user must log do a `bpnbat -login`. The user can also run the `bpnbat -GetBrokerCert` command to establish a trust with the server.

Impact of Access Control via Enhanced Auditing on Java interface authorization

Command line and Java interface access works differently when you configure Enhanced Auditing. Entries in the auth.conf file supersede the access control for the NetBackup Administration Console.

See "User management" on page 143.

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

Table 5-3 User access *(continued)*

auth.conf entry	CLI access	Java interface access
Debbie has NetBackup administrator privileges, but has no entry in the auth.conf file.	Complete access	Complete 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

Chapter 6

NetBackup Access Control Security (NBAC)

This chapter includes the following topics:

About using NetBackup Access Control (NBAC)

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 key 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 from 7.0 to 7.0.1. 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 more information about the `bpnbaz -configureauth` command refer to the NetBackup Commands Reference Guide.

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-Java 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 AIX, HP-UX, 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 153.

Configuring NetBackup Access Control (NBAC)

Note: The manual authentication and authorization client installs need to be done for older media servers and client hosts (less than NetBackup version 7.5). NetBackup version 7.5 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 155.

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 157.

3 Configure clients for NBAC.

See “Installing and configuring access control on clients” on page 159.

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 160. 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 150. 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 183. 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 157.

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 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.
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.

   See "NBAC configure commands summary" on page 160.

   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 159.

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
```

Establishing a trust relationship between the broker and the Windows remote console

The following procedure establishes a trust relationship between the master server (broker) and the administration client.

Establishing a trust relationship between the broker and the Windows remote console

1 Run the following command from the master server:

```
    Install_path\Veritas\NetBackup\bin\
admincmd>bpgetconfig USE_VXSS AUTHENTICATION_DOMAIN
>VXSS_SETTINGS.txt
```

Sample output of `VXSS_SETTINGS.txt`:

```
USE_VXSS = AUTOMATIC
AUTHENTICATION_DOMAIN = <domain_name> "" WINDOWS <broker_host> 0
```

2 Copy `VXSS_SETTINGS.txt` to the administration client.

3 Run the following command from the administration client:

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>bpsetconfig
"<absolute_path>\VXSS_SETTINGS.txt"
```

When you run this command, it matches the settings on the administration client with those on the broker. It sets the administration client to log on automatically to the broker.

4 Launch the **NetBackup Administration Console** from the administration client, a request to establish a trust with the broker should occur. Once the trust is agreed to, the **NetBackup Administration Console** should be available.

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.

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 Symantec product uses them.

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.

Upgrading NetBackup when an older version of NetBackup is using a root broker installed on a remote machine

You can use the following steps for upgrading NetBackup when an older version of NetBackup is using a root broker installed on a remote computer.

Upgrading NetBackup when an older version of NetBackup is using a root broker installed on a remote machine

1. Before upgrading to NetBackup, stop the NetBackup services and disable NBAC by setting `USE_VXSS=PROHIBITED`. To set the new value for `USE_VXSS`, run the following command. Then start the NetBackup upgrade.

   On UNIX platforms, use

   ```
   /usr/openv/netbackup/bin/admincmd/bpsetconfig
   bpsetconfig> USE_VXSS=PROHIBITED
   bpsetconfig>Crtl + D (to save and quit).
   ```

   On Windows, use

   ```
   C:\Program Files\Veritas\NetBackup\bin\admincmd\bpsetconfig
   bpsetconfig> USE_VXSS=PROHIBITED
   bpsetconfig> Crtl + Z + Enter (to save and quit).
   ```

2. Once the NetBackup upgrade is completed then migrates the remote root broker (RB) and local shared authentication broker (AB) into NetBackup by using the `atutil` tool which is shipped with NetBackup.

3. Copy the `atutil` utility from the NetBackup computer to the root broker computer.

   On UNIX Platforms, copy the `/usr/openv/netbackup/sec/at/bin/atutil` file from NetBackup computer to the root broker computer.

   On Windows, copy the `C:\Program Files\Veritas\NetBackup\sec\at\bin\atutil.exe` file from NetBackup computer to the root broker computer.

4. Change directory to where the `atutil` command was copied. Then export the root broker by running the `atutil export -r -f <RB output xml file> -p <password>` command.

5. Copy the exported file to NetBackup computer.

6 Import the root broker into the NetBackup computer by executing the following command.

On UNIX platforms, execute `/usr/openv/netbackup/sec/at/bin/atutil import -z /usr/openv/var/global/vxss/eab/data/ -f <RB output xml file> -p <password>`

On Windows, execute `C:\Program Files\Veritas\NetBackup\sec\at\bin\atutil import -z C:\Program Files\Veritas\NetBackup\var\global\vxss\eab\data -f <RB output xml file> -p <password>`

On cluster computers, the *-z* option should point to the shared drive.

7 Configure the NetBackup authentication service in `R+AB` mode by running the following command.

On UNIX platforms, run `/usr/openv/netbackup/sec/at/bin/vssregctl -s -f /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf -b "Security\Authentication\Authentication Broker" -k Mode -t int -v 3`

On Windows, run `C:\Program Files\Veritas\NetBackup\sec\at\bin\vssregctl -s -f C:\Program Files\VERITAS\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf -b "Security\Authentication\Authentication Broker" -k Mode -t int -v 3`

On cluster computers set the *–f* option to point to the shared drive.

8 Set the value of `USE_VXSS to AUTOMATIC` to start the authentication service. To set a new value for `USE_VXSS` run following command.

On UNIX platforms,

```
/usr/openv/netbackup/bin/admincmd/bpsetconfig
bpsetconfig> USE_VXSS=AUTOMATIC
bpsetconfig> Crtl + D (to save and quit).
```

On Windows,

```
C:\Program Files\Veritas\NetBackup\bin\admincmd\bpsetconfig
bpsetconfig> USE_VXSS=AUTOMATIC
bpsetconfig> Crtl + Z + Enter (to save and quit).
```

9 Start the NetBackup authentication service by running the following command.

On UNIX platforms, run `/usr/openv/netbackup/bin/nbatd`.

On Windows, run `net start nbatd`.

10 Reset the value of USE_VXSS to PROHIBITED.

On UNIX platforms manually edit the `/usr/openv/netbackup/bp.conf` file and set `USE_VXSS to PROHIBITED`.

On Windows, open the registry entry for `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\Config` and set the value of `USE_VXSS to PROHIBITED`.

11 Export the shared AB domain and import it into NetBackup by running the following command.

On UNIX platforms, execute the following commands in sequence.

```
/usr/openv/netbackup/sec/at/bin/atutil export -t ab -f
 <AB output xml file> -p <password>
/usr/openv/netbackup/sec/at/bin/atutil import -z
/usr/openv/var/global/vxss/eab/data/ -f <AB output xml file> -p
 <password>.
```

On Windows, execute the following commands in sequence.

```
C:\Program Files\Veritas\NetBackup\sec\at\bin\atutil export -t
 ab -d broker -f <AB output xml file> -p <password>
C:\Program Files\Veritas\NetBackup\sec\at\bin\atutil import -z
 C:\Program Files\Veritas\NetBackup\var\global\vxss\eab\data -f
<AB output xml file> -p <password>
```

On cluster computers the *–z* option should point to the shared drive.

12 Start the NetBackup authorization service by executing the following commands.

On UNIX platforms, run `/usr/openv/netbackup/bin/nbazd -f`.

On Windows, run `net start nbazd`.

13 Log on to the shared AZ service.

On UNIX platforms, run `/opt/VRTSaz/bin/vssaz login --domain localhost`.

On Windows x86 platforms, run `C:\Program Files\VERITAS\Security\Authorization\bin\ vssaz login --domain localhost`.

On Windows X64 platforms, run `C:\Program Files (x86)\VERITAS\Security\Authorization\bin\ vssaz login --domain localhost`.

14 Find the NetBackup APS name from the shared AZ using the following command.

On UNIX platforms, run `/opt/VRTSaz/bin/vssaz listaps`.

On Windows x86 platforms, run `C:\Program Files\VERITAS\Security\Authorization\bin\ vssaz listaps`.

On Windows X64 platforms, run `C:\Program Files (x86)\VERITAS\Security\Authorization\bin\ vssaz listaps`.

15 Export the NetBackup resource collection from the shared AZ by running the following command.

On UNIX platforms, run `/opt/VRTSaz/bin/vssaz rcexport --toplevelrcname <NBU APS name>`.

On Windows x86 platforms, run `C:\Program Files\VERITAS\Security\Authorization\bin\vssaz rcexport --toplevelrcname <NBU APS name>`.

On Windows x64 platforms, run `C:\Program Files (x86)\VERITAS\Security\Authorization\bin\vssaz rcexport --toplevelrcname <NBU APS name>`.

16 Log out from the shared AZ using the following command.

On UNIX platforms, run `/opt/VRTSaz/bin/vssaz logout`.

On Windows x86 platforms, run `C:\Program Files\VERITAS\Security\Authorization\bin\ vssaz logout`.

On Windows x64 platforms, run `C:\Program Files (x86)\VERITAS\Security\Authorization\bin\ vssaz logout`.

17 Log on to NetBackup AZ using the following command.

On UNIX platforms, run `/usr/openv/netbackup/sec/az/bin/vssaz login --domain localhost`.

On Windows, run `C:\Program Files\Veritas\NetBackup\sec\az\bin\ vssaz login --domain localhost`.

18 Import the NetBackup resource collection from shared AZ into NetBackup using the following command.

On UNIX platforms, run `/usr/openv/netbackup/sec/az/bin/vssaz rcimport --location /var/VRTSaz/objdb/export/<OID>/rc_<OID>.xml`.

On Windows x86 platforms, run `C:\Program Files\Veritas\NetBackup\sec\az\bin\ vssaz rcimport --location C:\Program Files\VERITAS\Security\Authorization\data\objdb\export\<OID>\rc_<OID>.xml`.

On Windows x64 platforms, run `C:\Program Files\Veritas\NetBackup\sec\az\bin\ vssaz rcimport --location C:\Program Files (x86)\VERITAS\Security\Authorization\data\objdb\export\<OID>\rc_<OID>.xml`.

19 Restart the NetBackup service in `USE_VXSS = PROHIBITED` mode.

20 Run the `setupmaster` command.

21 Restart the NetBackup service.

Configuring NetBackup Access Control (NBAC) for NetBackup pre-7.0 media server and client computers

Note: This procedure is applicable only for NetBackup pre-7.0 media server and client computers. NetBackup release 7.0 and forward uses embedded clients.

You can use the following procedure to configure the NetBackup Access Control (NBAC) for NetBackup pre-7.0 media and client computers.

Configuring the NetBackup Access Control (NBAC) for NetBackup pre-7.0 media server and client computers

1. Install the Authentication and Authorization client packages on the target computer.

   If the target computer is a NetBackup client, then install the authentication client only. If the target computer is a NetBackup media server, install both the authentication clients and authorization clients.

   You can choose to install both the client binaries and server binaries on the target computer, but there is no need to configure the servers. You need to install the authentication packages and authorization packages that are available on the Infrastructure Common Services (ICS) DVDs shipped with the older NetBackup media. The authentication binaries and authorization binaries available with NetBackup 7.6 may not be compatible with the older NetBackup media servers or clients.

   On UNIX platforms, use the `installics` utility to install the authentication packages and authorization packages.

   On Windows, use `VxSSVRTSatSetup.exe` and `VRTSazSetup.exe`.

   Refer to the older NetBackup documentation for more details on how to install authentication and authorization clients.

2. Run `bpnbaz -setupmedia` from the master server and provide passwords for pre-7.0 media servers.

3. Set up the proper access control host properties for the target media server or the client host.

   For the media servers: See "Accessing the master server and media server host properties" on page 174.

   For the clients: See "Accessing the client host properties" on page 179.

4. Restart the NetBackup process on the target media server or the client computer.

Manually configuring the Access Control host properties

Note: Run the `bpnbaz -setupClient`, `bpnbaz -setupMedia`, and `bpnbaz -setupMaster` commands to do this configuration automatically. You only need to do this configuration if you want to change defaults or add additional brokers. Also do this for the back revision media server and client hosts.

Use the following topics to manually configure the **Access Control** host properties.

Note: You must set the master server **NetBackup Authentication and Authorization** property to **Automatic** until the clients are configured for access control. Then, change the **NetBackup Authentication and Authorization** property on the master server to **Required**.

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 CLI that adds OpsCenter server name to the NBU master. That takes care of the trust establishment part from the NBU side.

The Symantec 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 might consist of a Symantec 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 Symantec OpsCenter server (OPS) setup trust with each of the master servers (A, B, and C). This trust ensures that the Symantec 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 Symantec 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 Symantec 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 Symantec OpsCenter server (OPS).
- The master server B sets up trust with Symantec OpsCenter server (OPS).
- The master server C sets up trust with Symantec OpsCenter server (OPS).
- The Symantec OpsCenter server OPS sets up trust with master server A.
- The Symantec OpsCenter server OPS sets up trust with master server B.
- The Symantec OpsCenter server OPS sets up trust with master server C.

Note: NetBackup 7.6 and OpsCenter 7.6 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 7.6 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 173.

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.

Accessing the master server and media server host properties

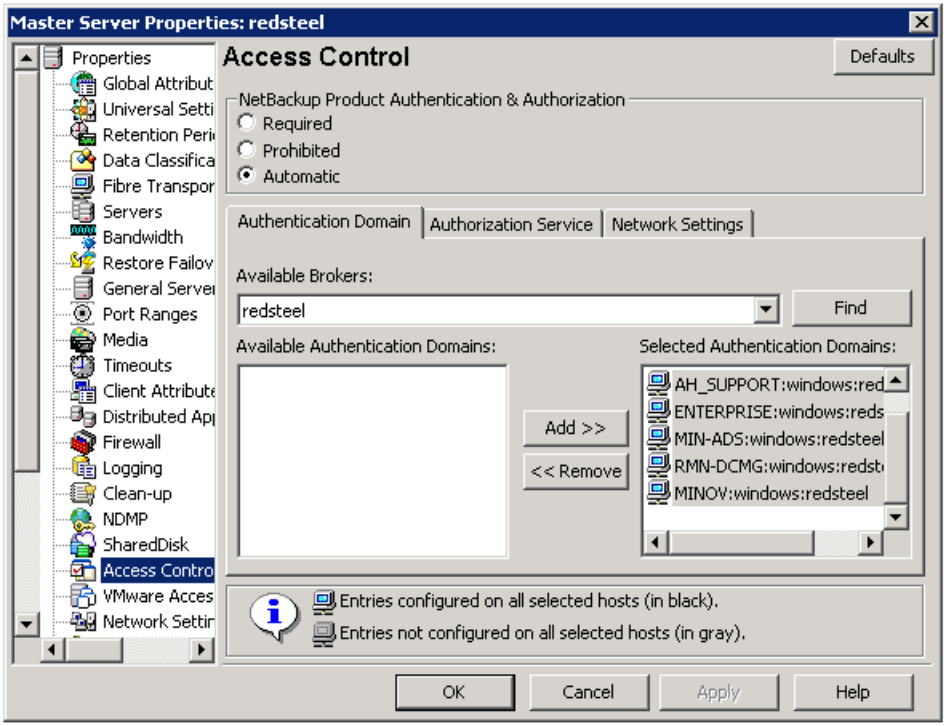
To access the master server and media server host properties in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > master server or media server > *Select server* > Access Control**.

Access control host properties

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.

Figure 6-1 shows the **Access Control** host properties dialog box.

Figure 6-1 Access control host properties dialog box



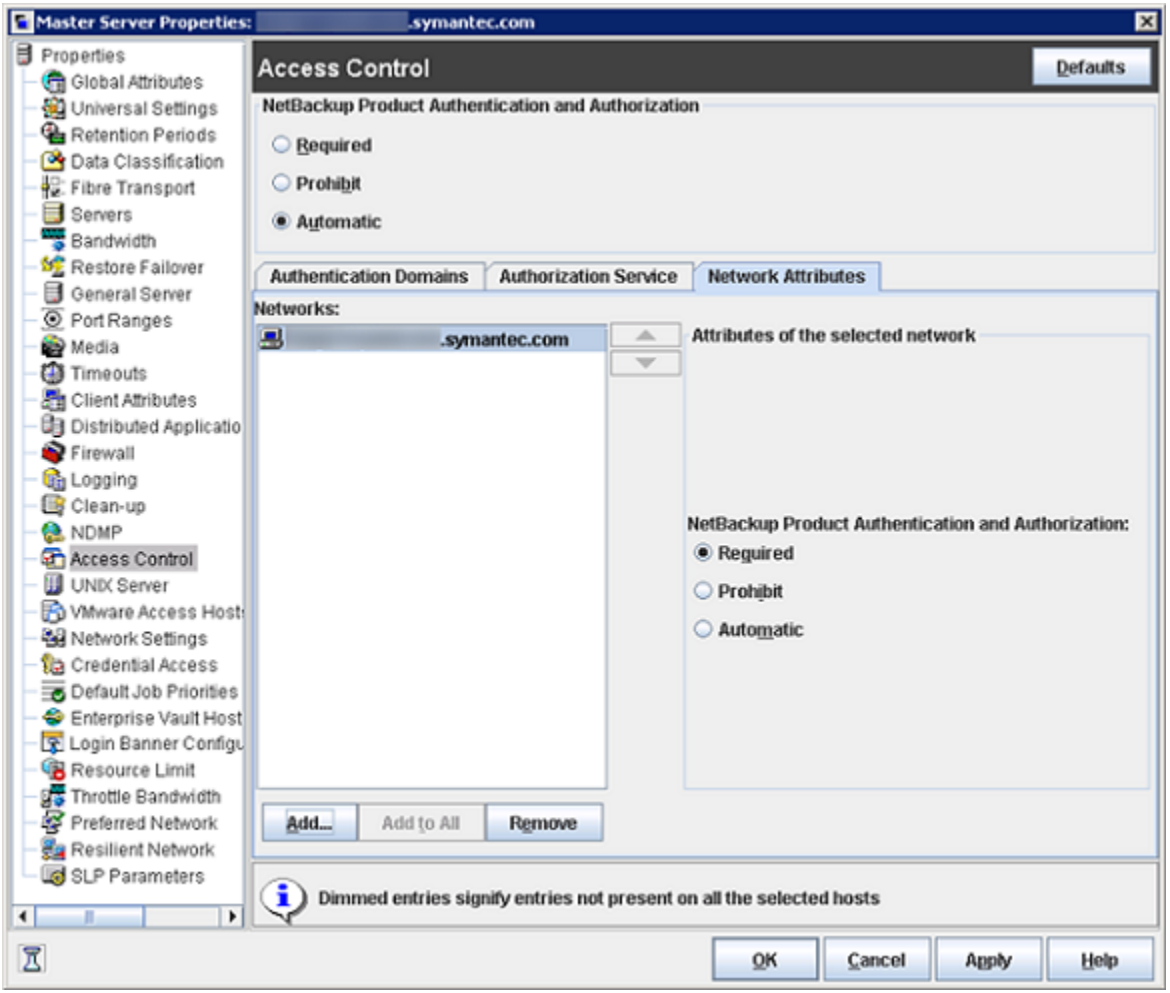
When **Automatic** is selected, you can specify computers or the domains required to use **NetBackup Product Authentication and Authorization**. Otherwise, you can specify the computers that are prohibited from using the **NetBackup Product Authentication and Authorization**.

Network Settings tab

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

Figure 6-2 shows the **Network Settings** tab.

Figure 6-2 Network Settings tab



Each new NetBackup client or media server (version 5.0 or higher) 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.

Authentication Domain tab

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

- Which authentication servers support which authentication mechanisms

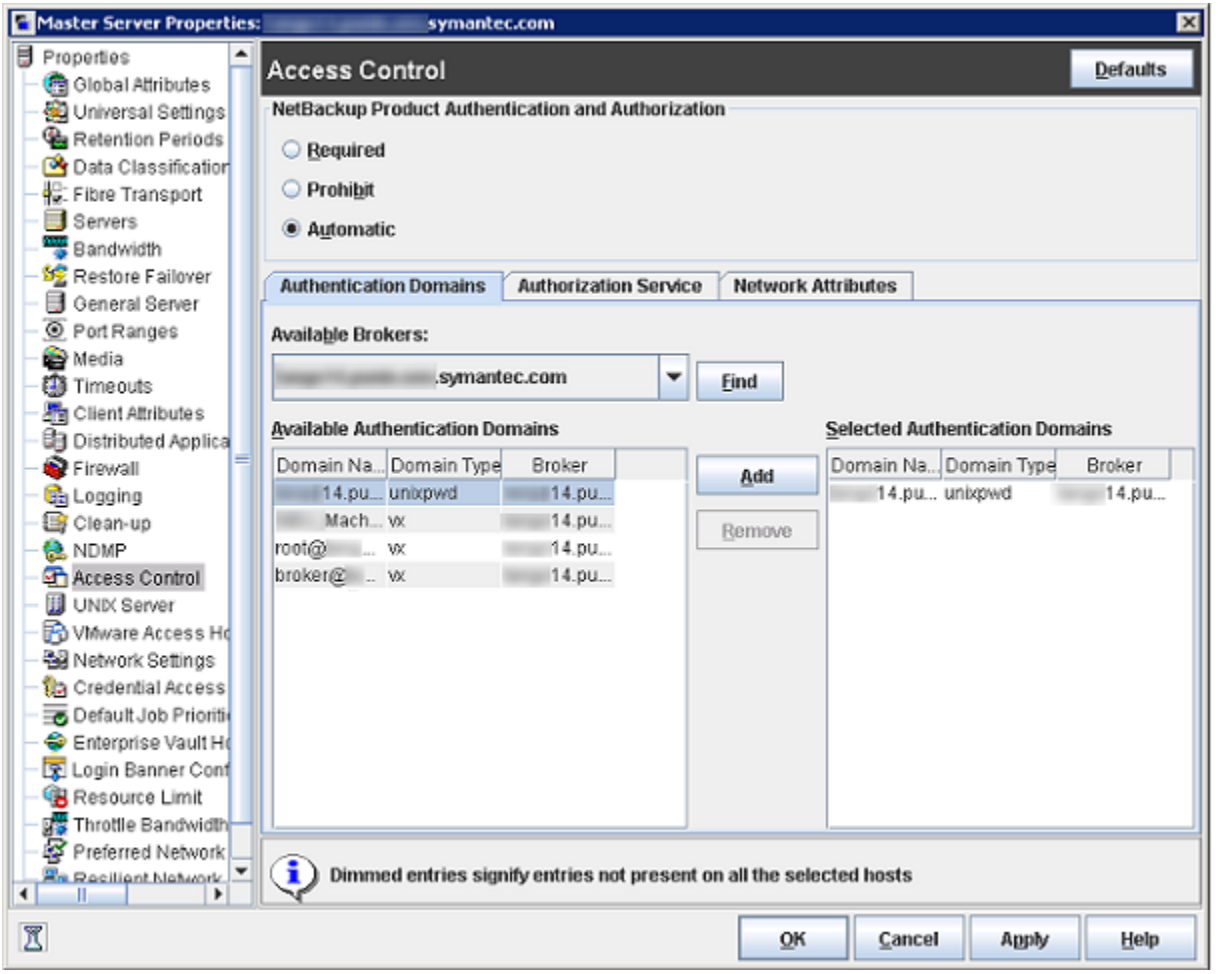
- What each domain supports.

Add the domain that you want users to authenticate against.

The following examples contain six authentication domains.

Figure 6-3 shows the **Authentication Domain** tab.

Figure 6-3 Authentication Domain tab



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).

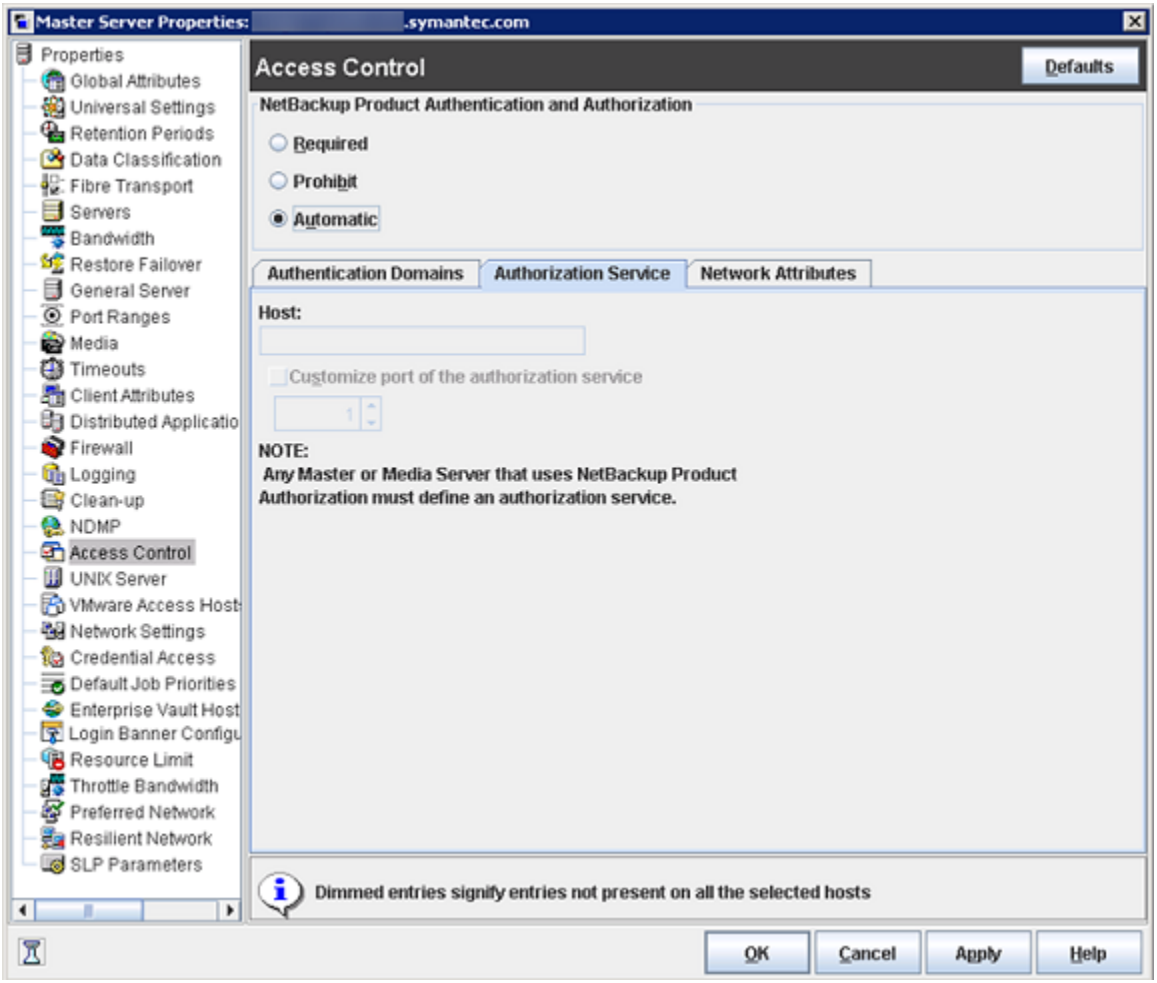
Authorization Service tab

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.

Figure 6-4 shows the authorization service tab.

Figure 6-4 Authorization Service tab



Accessing the client host properties

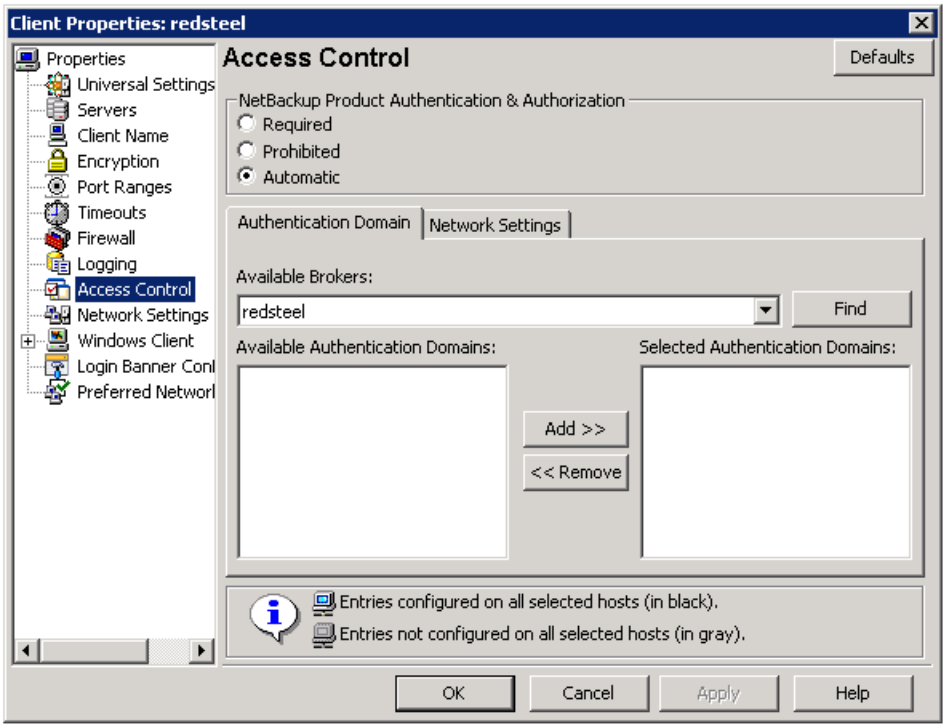
To access the client host properties in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Clients > *Select client(s)* > Access Control**.

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**.)

The following figure shows the **Access Control** host properties for the client.

Figure 6-5 Access control host properties for the client



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

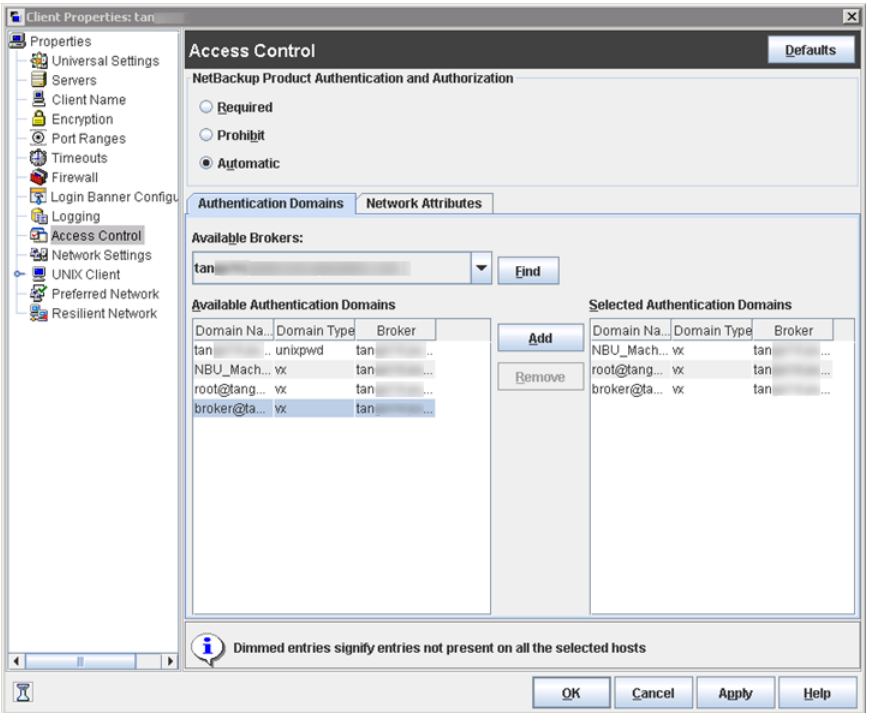
Authentication Domain tab for the client

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.

Figure 6-6 shows the **Authentication Domain** tab and the selected authentication domains.

Figure 6-6 Authentication Domain tab for client

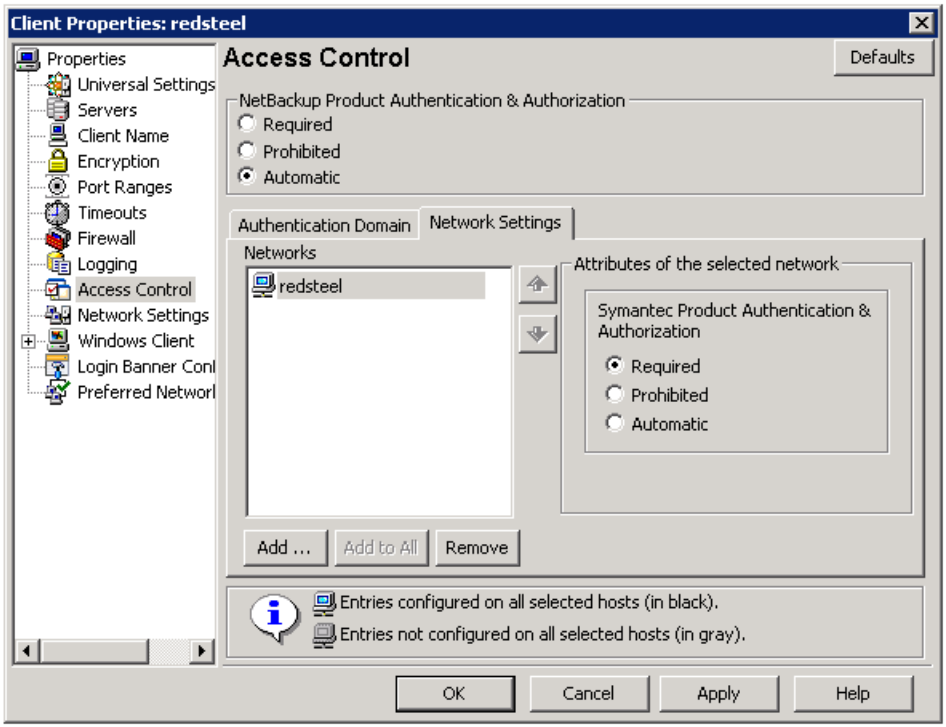


Network Settings tab for the client

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

Figure 6-7shows the **Network Settings** tab for the client.

Figure 6-7 Network Settings tab for the client



Access management troubleshooting guidelines

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 183.

These verification points include:

- Windows verification points
  See "Windows verification points" on page 211.
- UNIX verification points
  See "About the UNIX verification procedures" on page 191.
- 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 199.

- 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 204.

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 6-4 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: Symantec 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`

Table 6-4 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips

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.
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`. See the NetBackup Troubleshooting Guide for instructions on proper logging.

Table 6-4 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips

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 7.5 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`.
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.

Table 6-4 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips

NetBackup Authentication and Authorization ports	The NetBackup Authentication and Authorization daemon services use ports 13783 and 13722 for back-level media server and clients. For 7.5 and later versions it uses 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 6-4 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 6-4 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 221. `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 221.
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 6-4 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 that `nbazd` fails with an error on Solaris x64	A known issue exists in which `nbazd` fails with the following error on Solaris x64. `ld.so.1: nbazd: fatal: relocation error: R_AMD64_PC32: file /usr/lib/64/libCrun.so.1: symbol __1cH__CimplMex_terminate6F_v_: value 0x28001a4b2ba does not fit` To resolve the issue install patch `119964-*`.
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.

Table 6-4 Configuration and troubleshooting topics and tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips
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`.

Troubleshooting NBAC issues

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

Table 6-5 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.

Table 6-5 NBAC issues *(continued)*

Issue and Cause	Solution
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 226.
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*.

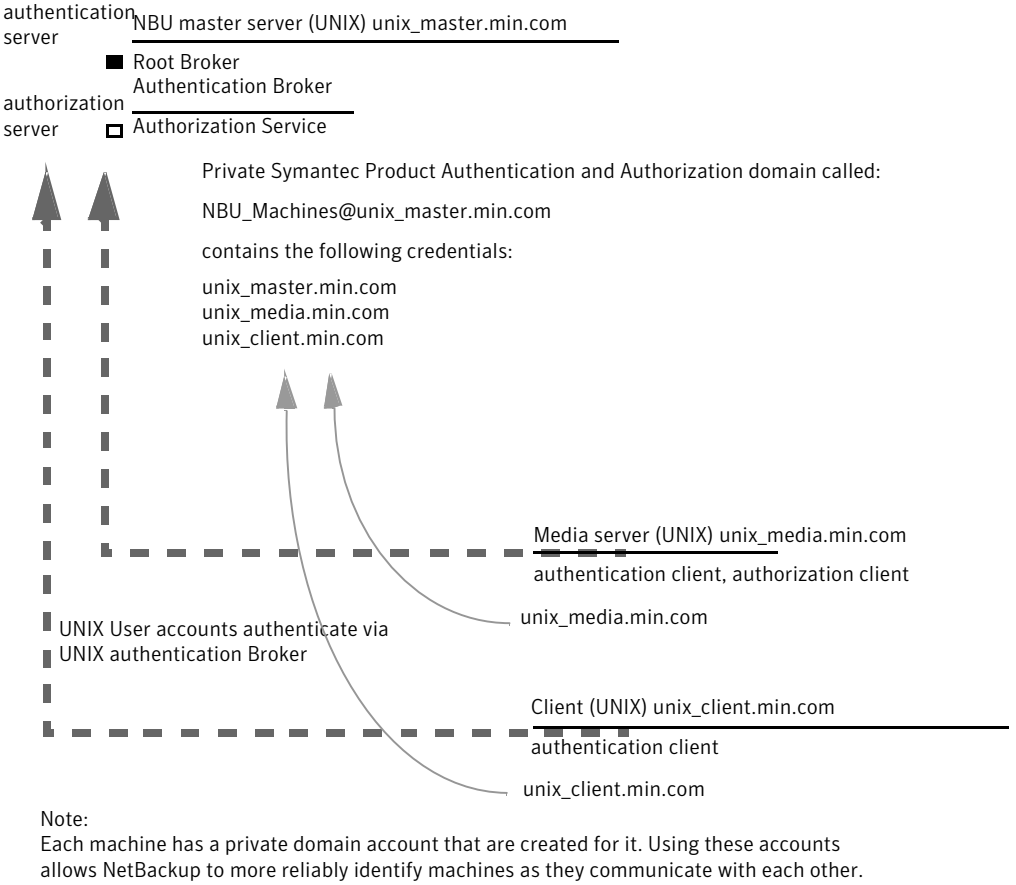
About the UNIX verification procedures

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 192.
- UNIX media server verification
  See "UNIX media server verification" on page 195.
- UNIX client verification
  See "UNIX client verification" on page 197.

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

Figure 6-8 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 6-6 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:
	
	`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.`
	
	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 6-6 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 6-6 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 6-7 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:
	
	`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.`
	
	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:
	
	`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.`
	
	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.

Table 6-7 Verification process for the UNIX media server *(continued)*

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 6-8 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`

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.`

Table 6-8 Verification procedures for the UNIX client *(continued)*

Procedures	Description

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`

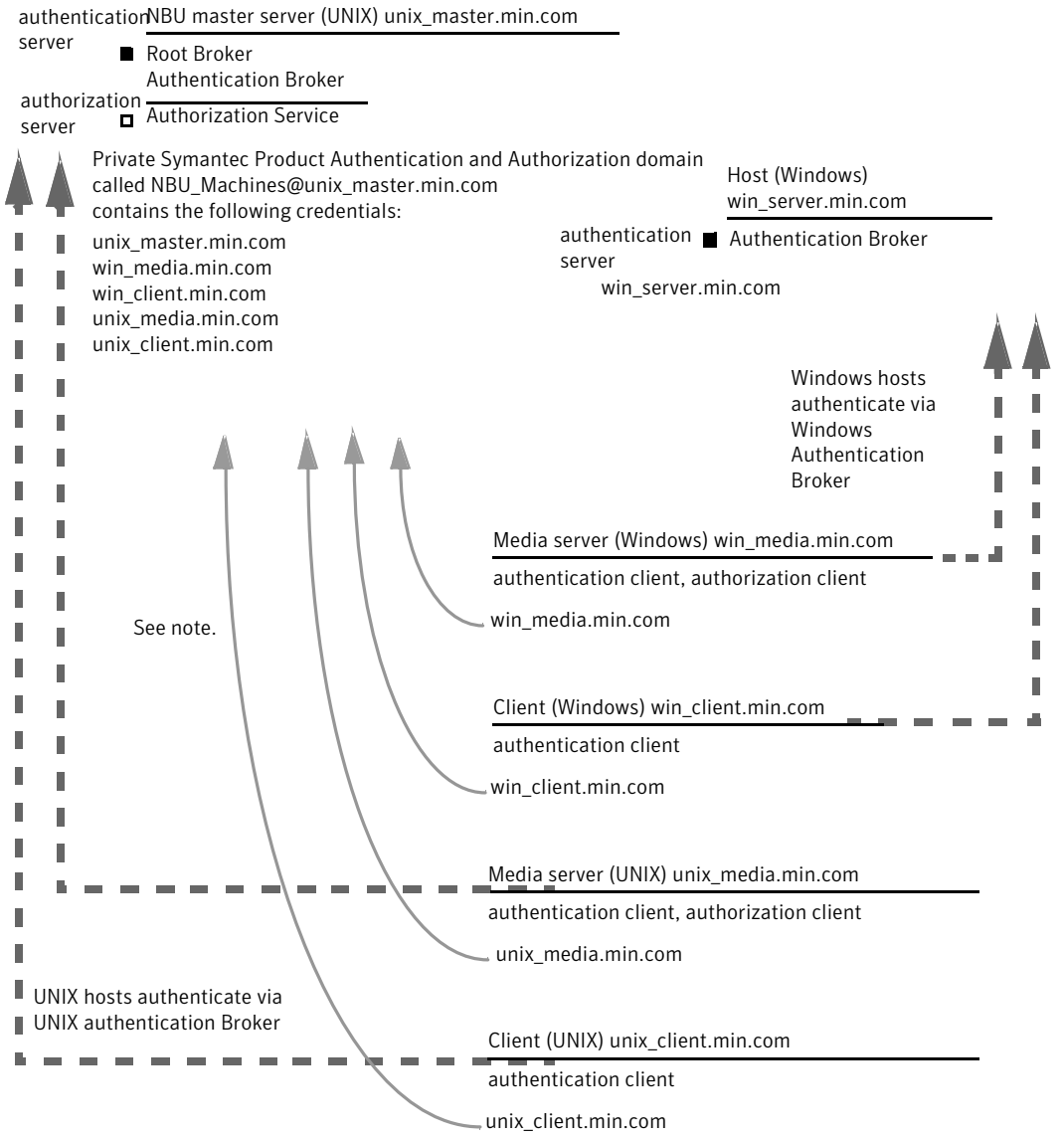
Verification points in a mixed environment with a UNIX master server

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 6-9 is an example of a mixed configuration that contains a UNIX master server.

Figure 6-9 Example mixed configuration containing a UNIX master server



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 192.

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 6-9 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 195.

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:
	`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.`

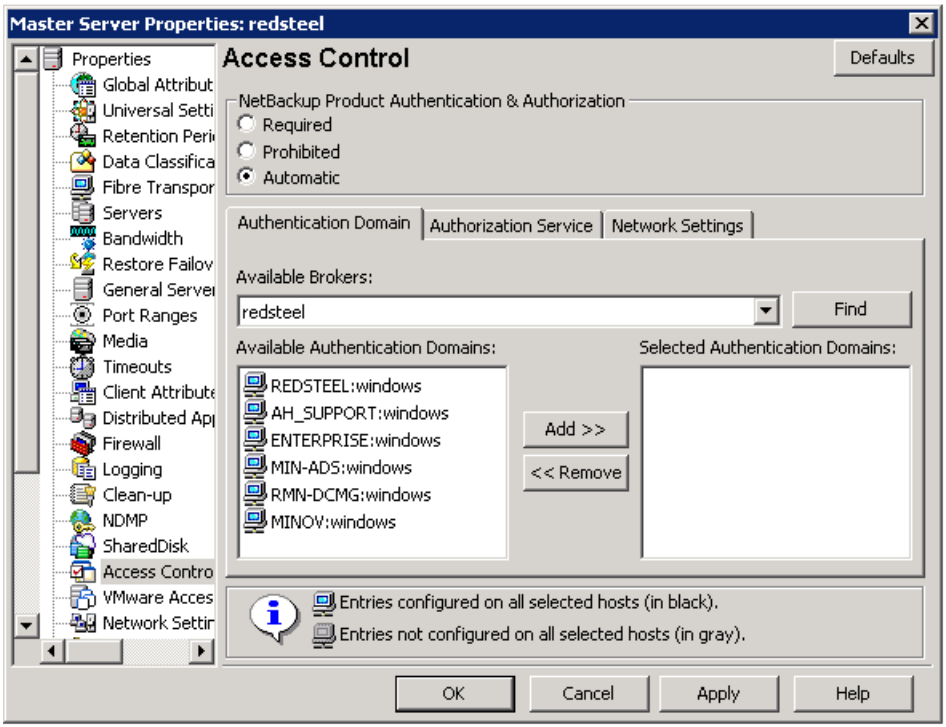
Table 6-9 Verification procedures for a mixed UNIX master server *(continued)*

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`
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 6-10 for a display on how to match the platform to the most useful authentication domains.

Figure 6-10 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 197.

The following table describes the procedures to verify Windows clients.

Table 6-10 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

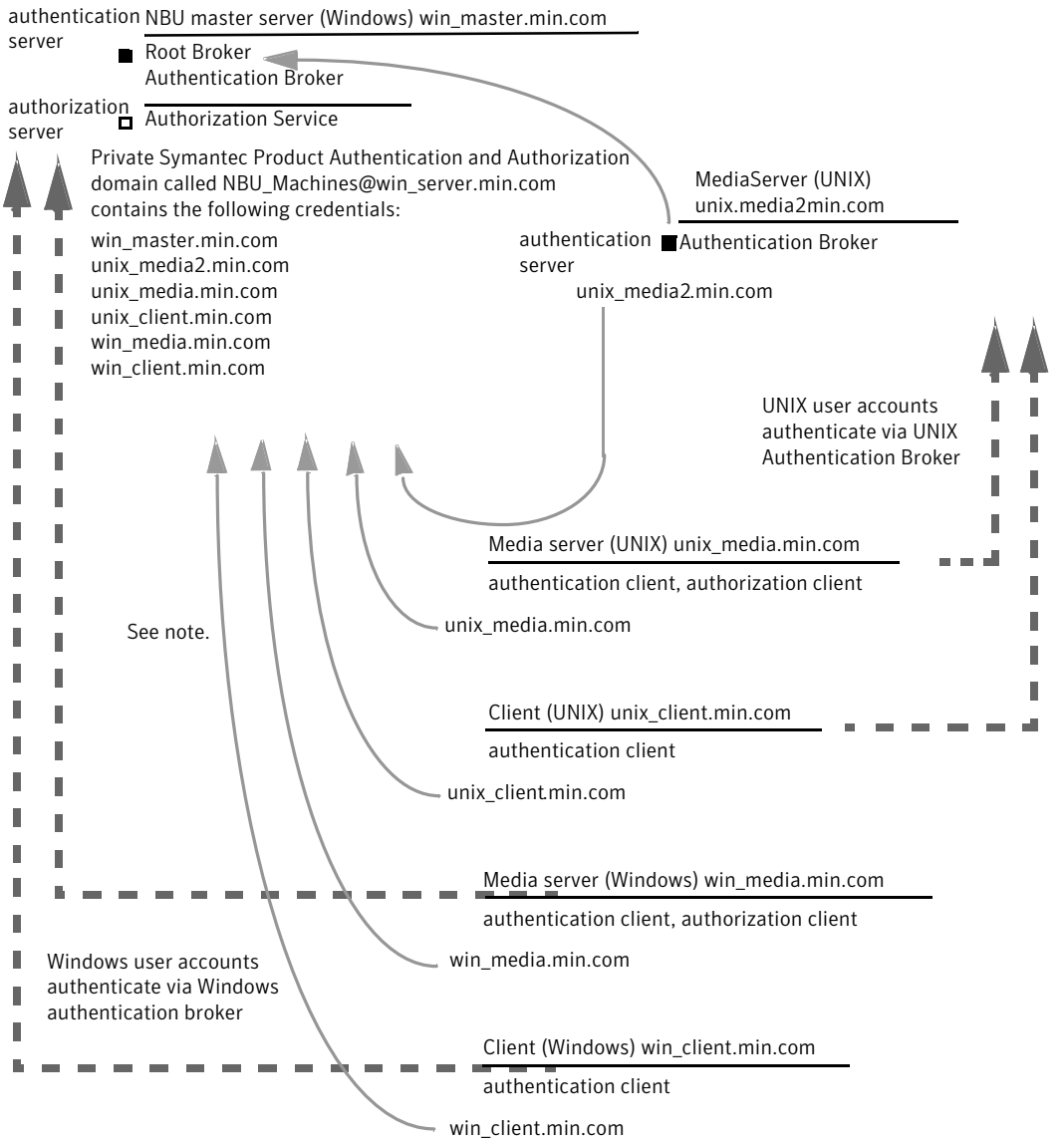
The following procedures can help you verify that the master server, media server, and client are configured correctly. They should be configured for a heterogeneous NetBackup Access Control environment. The master server is a Windows computer.

- Master server verification points for mixed Windows master
  See "Master server verification points for a mixed Windows master server" on page 207.
- Media server verification points for mixed Windows master
  See "Media server verification points for a mixed Windows master server" on page 207.
- Client verification points for mixed Windows master

See "Client verification points for a mixed Windows master server" on page 209.

Figure 6-11 is an example configuration that contains a Windows master server.

Figure 6-11 Example mixed configuration containing a Windows master server



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 212.

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 6-11 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 216.

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 6-11 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:
	
	`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.`
	
	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 6-11 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 6-12 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: See "Client verification points for Windows" on page 218.

Table 6-12 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:
	`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.`

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_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.`

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.

Windows verification points

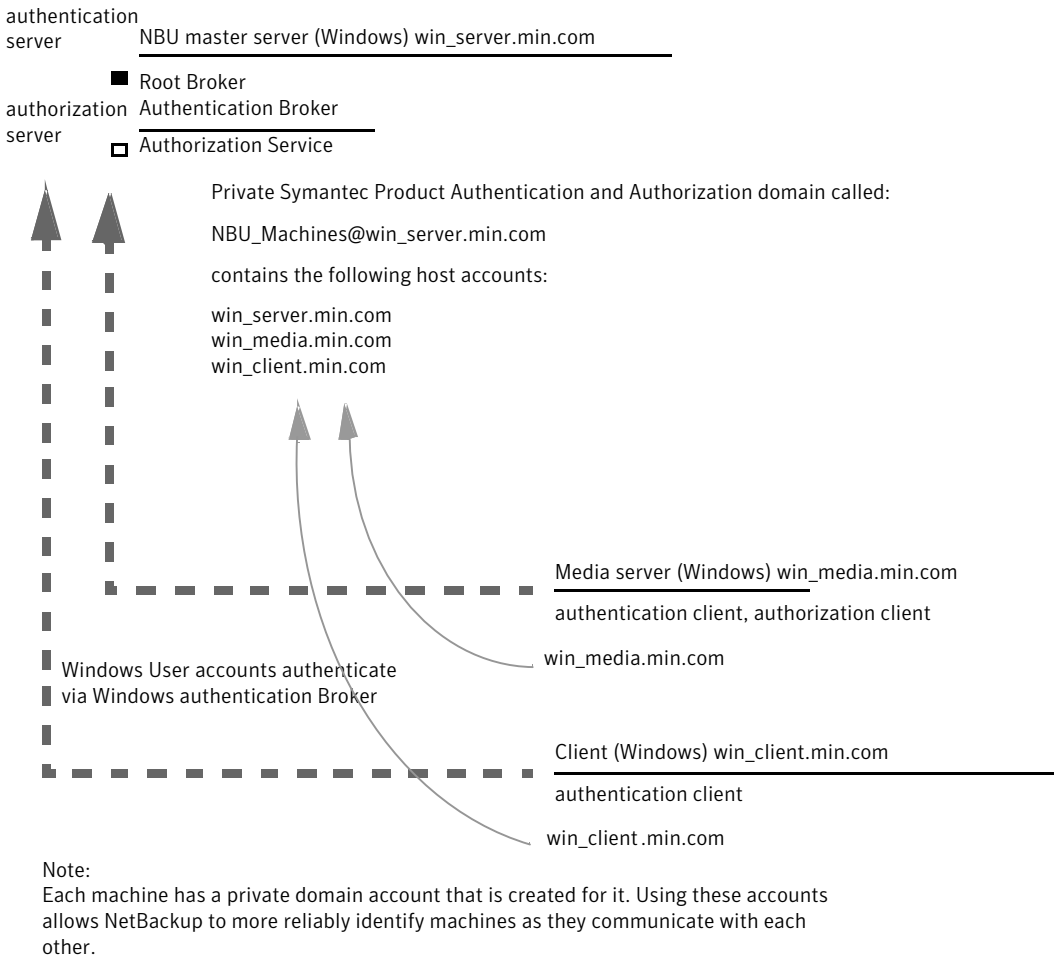
The following configuration procedures can help you verify that the master server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See “Master server verification points for Windows” on page 212.
- See “Media server verification points for Windows” on page 216.
- See “Client verification points for Windows” on page 218.

Figure 6-12 shows an example configuration containing Windows systems only.

Figure 6-12 Example configuration containing Windows systems only



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 6-13 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 6-13 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.
	`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.`
	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 6-13 Master server verification procedures for Windows *(continued)*

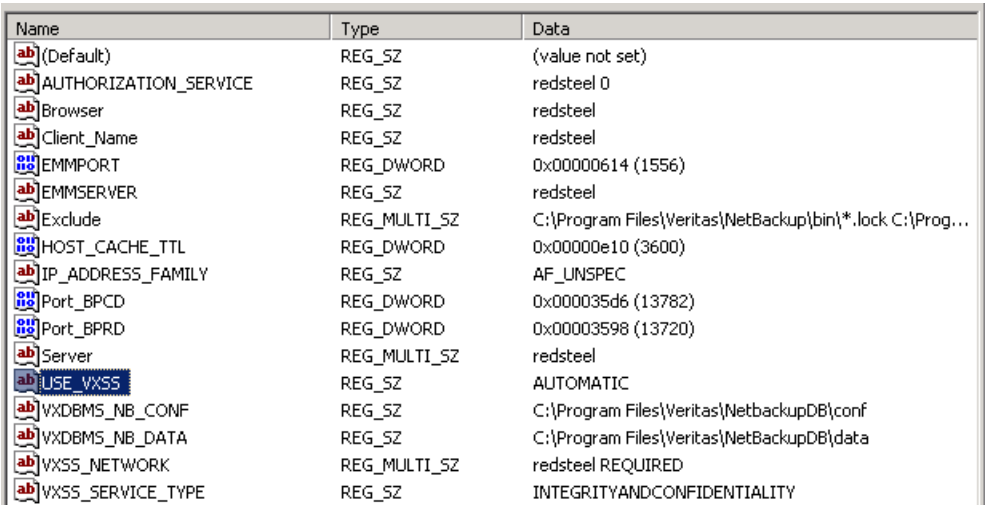
Procedure	Description

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 6-13 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 6-13 Host properties settings



Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHORIZATION_SERVICE	REG_SZ	redsteel 0
Browser	REG_SZ	redsteel
Client_Name	REG_SZ	redsteel
EMMPORT	REG_DWORD	0x00000614 (1556)
EMMSERVER	REG_SZ	redsteel
Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin*.lock C:\Prog...
HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
IP_ADDRESS_FAMILY	REG_SZ	AF_UNSPEC
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	redsteel
USE_VXSS	REG_SZ	AUTOMATIC
VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetbackupDB\conf
VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetBackupDB\data
VXSS_NETWORK	REG_MULTI_SZ	redsteel REQUIRED
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 6-14 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:
	
	`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.`
	
	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 6-14 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:
	
	`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.`
	
	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 6-15 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:
	
	`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.`
	
	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.
	
	`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.`
	
	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 6-15 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.

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 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 221.

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 Symantec 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 Symantec 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.symantec.com

Name: Dan

Password:*****

You do not currently trust the server:
amp.sec.punin.sen.symantec.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.symantec.com

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

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

Authentication method: Symantec 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.

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 224.
- The creation of user groups.
  See "User groups" on page 225.

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 238.

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.

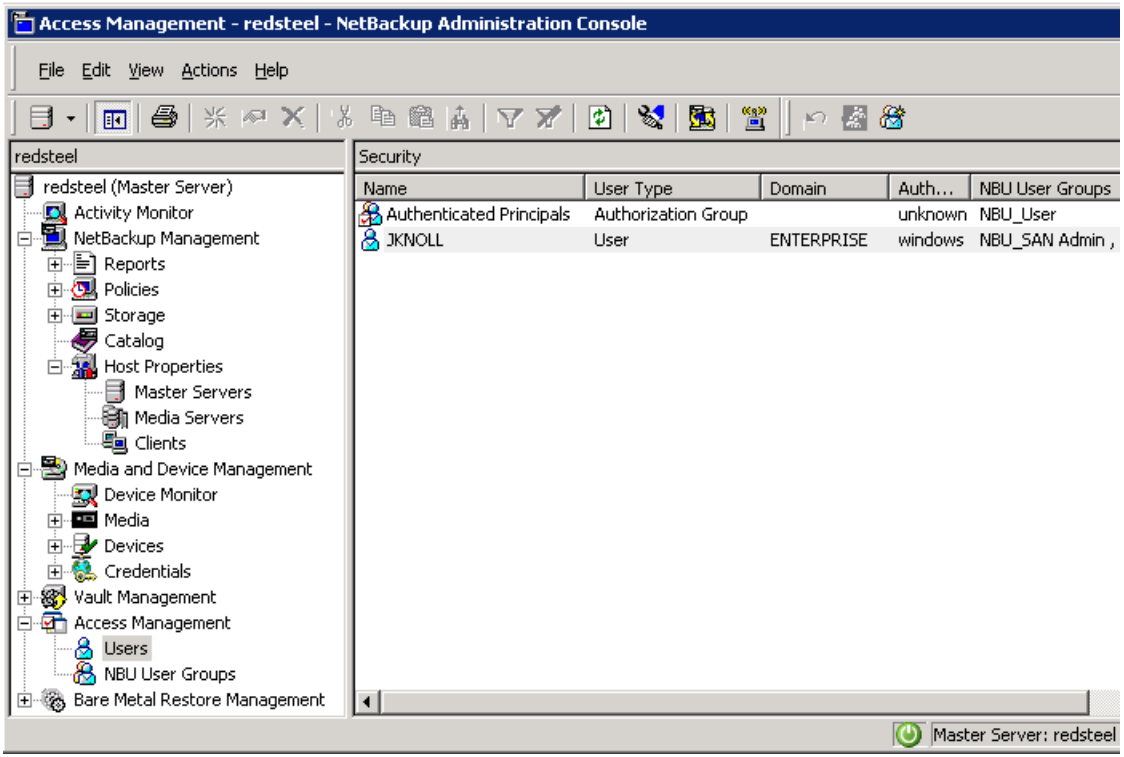
Individual users

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.

Figure 6-14 shows individual authenticated users.

Figure 6-14 Individual users



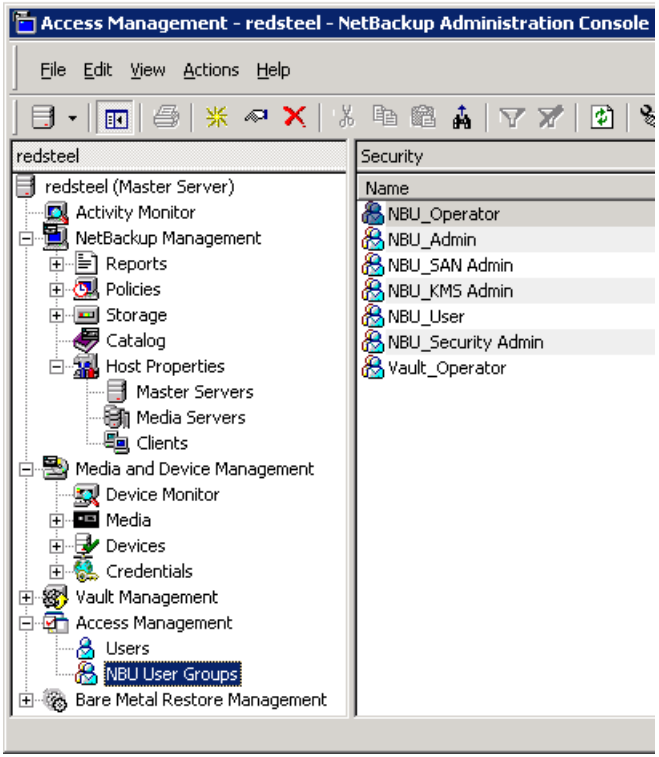
All authenticated users are implicit members of the NBU_Users user group. All other groups must have members defined explicitly. The NetBackup Security Administrator can delete a manually added member to other groups. However, the Security Administrator may not delete the predefined implicit members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

Figure 6-15 show a list of user groups.

Figure 6-15 User groups



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. Symantec 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.

   See "Users tab" on page 230.
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. See "Permissions tab" on page 235.

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

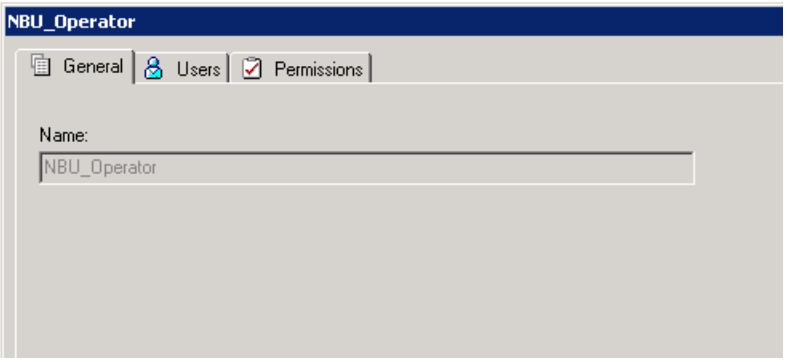
Once a NetBackup user group has been created, the user group cannot be renamed. The alternative to directly renaming a user group is to follow these steps: copy the user group, give the copy a new name, ensure the same membership as the original, then delete the original NetBackup user group.

General tab

The **General** tab contains the name of the user group. If you create a new user group, the **Name** text box can be edited.

The following figure shows the **General** tab.

Figure 6-16 General tab

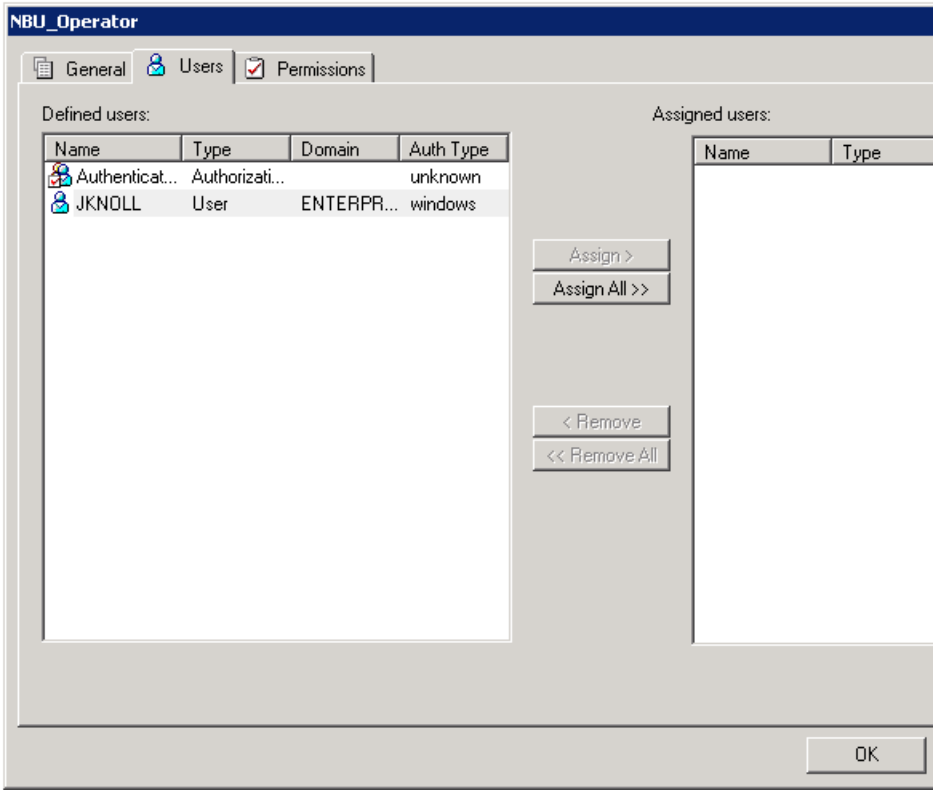


Users tab

The **Users** tab contains the controls that assign and remove users from user groups.

The following figure shows the **Users** tab.

Figure 6-17 Users tab



Defined Users pane on the Users tab

The **Defined Users** pane displays a list of all of the users that are defined within other groups.

- **Assign** option.
  Select a user in the **Defined Users** pane and click **Assign** to assign that user to a user group.
- **Assign All** option.
  Click **Assign All** to add all of the defined users to the user group.

Assigned Users pane on the Users tab

The **Assigned Users** pane displays the defined users who have been added to the user group.

- **Remove** option.
  Select a user in the **Assigned Users** pane and click **Remove** to remove that user from the user group.
- **Remove All** option.
  Click **Remove All** to remove all assigned users from the **Assigned Users** list.

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 234.

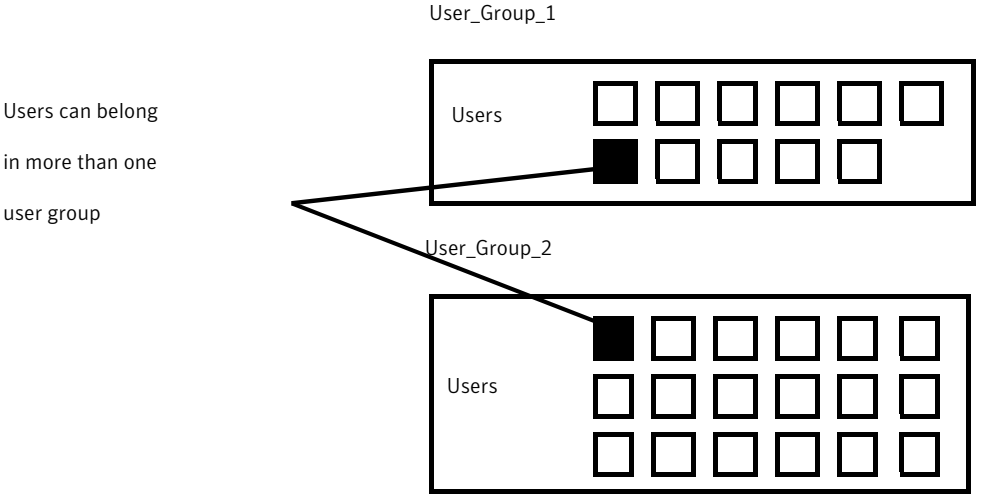
About defining a user group and users

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 6-18 shows defining a user group.

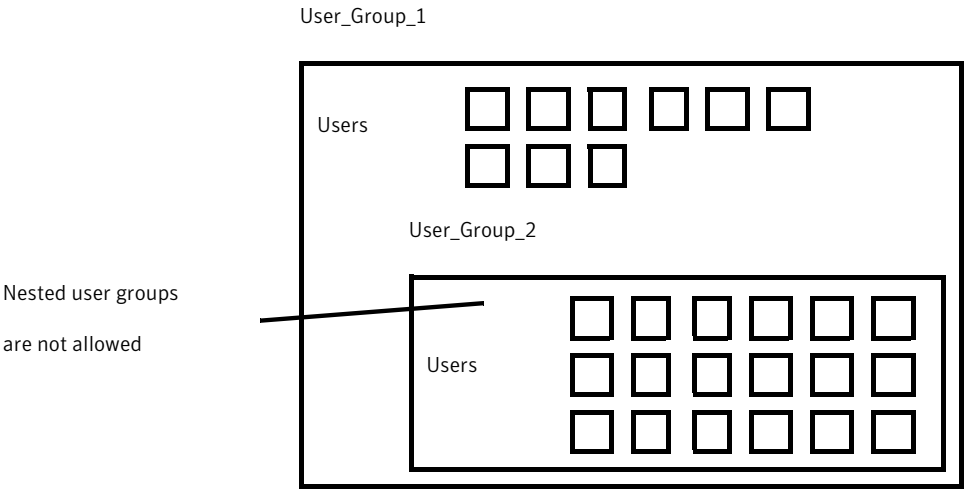
Figure 6-18 Defining a user group



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 6-19 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.

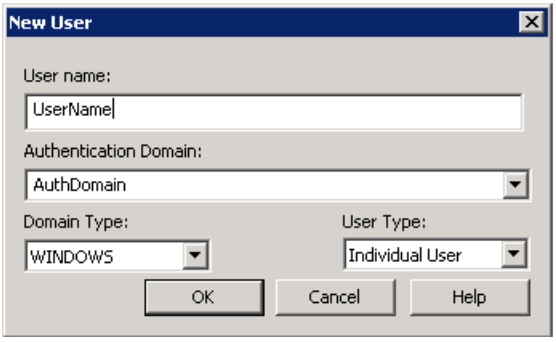
Assigning a user to a user group

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**.

   A display similar to the following appears:



4. Enter the user name and the authentication domain. Select the domain type of the user: NIS, NIS+, PASSWD, Windows, or Vx. See the *Symantec Product Authentication and Authorization Administrator's Guide* for more information on domain types.
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.

Permissions tab

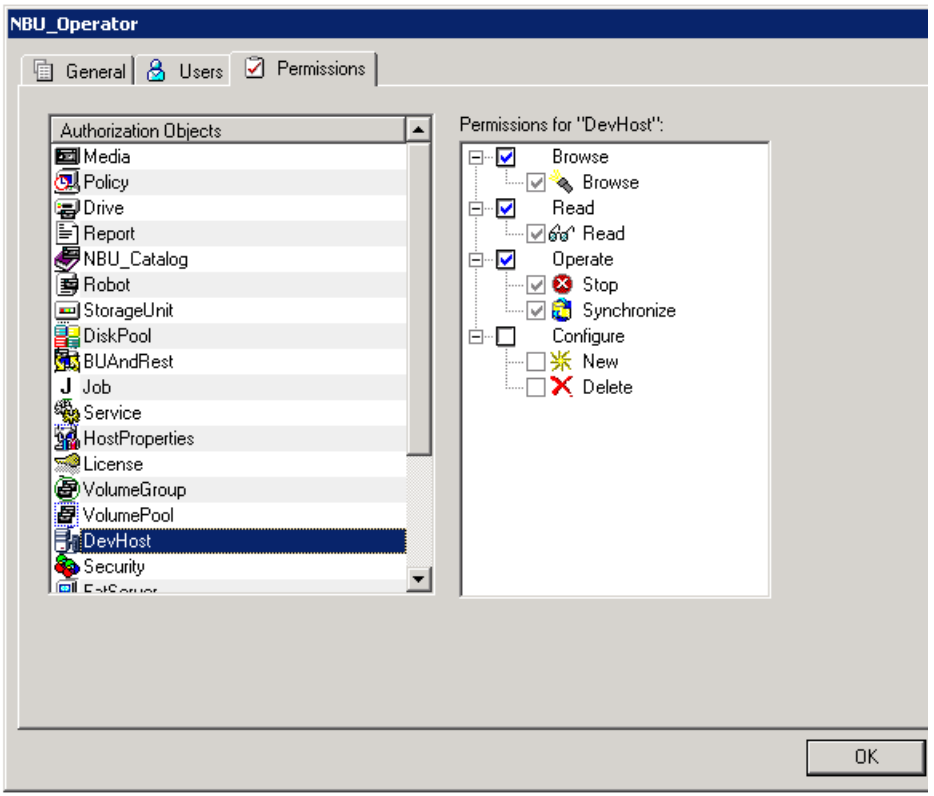
The **Permissions** tab contains a list of the NetBackup authorization objects and configurable permissions that are associated with each object.

About authorization objects and permissions

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

The following figure shows the authorization objects.

Figure 6-20 Authorization objects



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.

Granting permissions

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

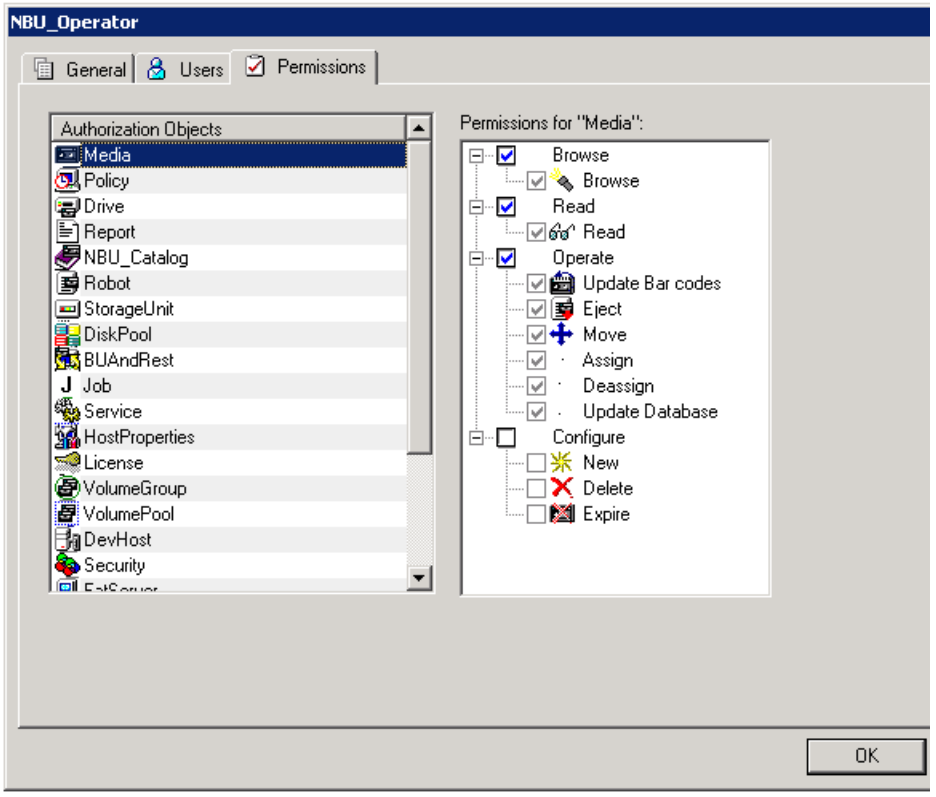
To grant a permission to the members of a user group

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.

The following figure shows an example of a permissions list.

Figure 6-21 Permissions list



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: http://entsupport.symantec.com/docs/336967.

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.

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.

- See "Key management system (kms) group authorization object permissions" on page 252.

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	---	---	---	---	---

Table 6-18 Policy authorization object permissions *(continued)*

Set	Activity	NBU_ Operator	NBU_ Admin	NBU_SAN Admin	NBU_User	NBU_ Security Admin	Vault_ Operator	NBU_KMS Admin
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	---	---	---	---	---

Table 6-21 NBU_Catalog 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	---	---	---	---	---
	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	---	---	---	---	---	---	---
	List	---	---	X	X	---	---	X

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 Services/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	---

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
Read	Read	X	X	---	---	---	X	---
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	---	---	---	--

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
Operate	Discover	---	X	X	---	---	---	---
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	---

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
Read	Read	X	X	---	---	---	X	---
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

Chapter 7

Data at rest encryption security

This chapter includes the following topics:

- Media server encryption option administration

Data at rest encryption terminology

The following table describes the data at rest encryption terminology.

Table 7-1 Data at rest encryption terminology

Term	Description
Asynchronous encryption	Includes the encryption algorithms that use both a public key and private key.
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.
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.
Advanced Encryption Standard (AES)	Specifies the synchronous encryption algorithm that replaced DES.
Data Encryption Standard (DES)	Specifies the accepted synchronous data encryption standard from the 1970s until 1998.
Public Key Encryption	Uses asynchronous encryption.

Data at rest encryption limitations

The following table describes the data at rest encryption limitations.

Table 7-2 Data at rest encryption limitations

Limitation	Description
Computer performance affect 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.

Table 7-2 Data at rest encryption limitations *(continued)*

Limitation	Description
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.
AES became the standard	AES replaced the previous standard, DES which was secure through about 1998. Then, computer processing speed enhancements and parallel processing techniques finally showed DES to be vulnerable to attack in 10s of hours. At that point, the US Government solicited a replacement for DES. An algorithm called Rijndael (pronounced Rhine dahl), became the front runner. After about 5 years of peer review, and review by the US Government, a specific configuration of Rijndael became AES. In June 2003, the US Government announced that AES can be used for classified information. "The design and strength of all key lengths of the AES algorithm are 128, 192 and 256. These are sufficient to protect classified information up to the SECRET level. TOP SECRET information requires the use of either the 192 or 256 key lengths. The implementation of AES in products is intended to protect national security systems. Information is reviewed and certified by NSA before their acquisition and use." For more information, refer to this website : http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf.
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.
NIST FIPS 140	NIST (National Institute of Science and Technology) FIPS (Federal Information Processing Standard) 140 is a government program. This program certifies data encryption solutions for the federal government. The program requires that encryption solution providers document their product from both a use perspective and security interface perspective. Then, submit the product to an accredited 3rd party reviewer for validation. Upon successful review, the product is issued a validation certificate.

Table 7-2 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, and is a likely added level of comfort 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. I can enter my garage, front door, or backdoor all using the same key. This security is great until the key is compromised (i.e. key that is stolen by criminals). Then I need to change all the locks that used this key. The absurd extreme would be someone having 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 probably 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?

NetBackup data at rest encryption options

The following topic contains a comparison of the following three NetBackup data at rest encryption options:

See Table 7-3 on page 259.

- Option 1 - NetBackup client encryption
  See “Option 1 - NetBackup client encryption” on page 259.
- Option 2 - Media server encryption
  See “Option 2 - Media server encryption” on page 283.
- Option 3 - third-party encryption appliances and hardware devices

Encryption options comparison

The following table shows the three encryption options along with their potential advantages and disadvantages.

Table 7-3 Encryption options comparison

Encryption option	Potential advantages	Potential disadvantages
See "Option 1 - NetBackup client encryption" on page 259.	■ 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
See "Option 2 - Media server encryption" on page 283.	■ Will not affect client computer performance ■ Master / Media server centralized keys	■ Master / Media server centralized keys ■ Limited options for detailed Key Granularity ■ Not tightly integrated with NetBackup configuration and operation ■ Encryption and compression taking place on the media server can affect media server performance
Option 3 - third-party encryption appliances and hardware devices	■ Generally little (or no performance) affect 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. ■ Disaster recovery scenario that is provided by the Appliance or Device.

Option 1 - 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

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 260.
- Standard encryption backup process
  See "Standard encryption backup process" on page 261.
- Legacy encryption backup process
  See "Legacy encryption backup process" on page 261.

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 7-4 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 261.

See "NetBackup standard encryption restore process" on page 262.

See “Legacy encryption backup process” on page 261.

See “NetBackup legacy encryption restore process” on page 263.

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: 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 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: 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.

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: In NetBackup 7.5 and later versions, 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.

Installation prerequisites for encryption security

To configure and run encrypted backups, the NetBackup Encryption software must be available on the NetBackup clients. The NetBackup encryption software is included with NetBackup server and client installations.

If clients require encrypted backups, the servers to which they connect must run NetBackup 7.6 server software. For a list of the platforms on which you can configure NetBackup Encryption, see *the NetBackup Release Notes*.

Installing encryption on a UNIX NetBackup server

The NetBackup UNIX server and client installations include encryption software. Use the following procedure to make sure that a license key for NetBackup encryption has been registered on the NetBackup master server.

To confirm that NetBackup encryption is registered on a UNIX NetBackup master server

- Make sure that a license key for NetBackup Encryption has been registered on the NetBackup master server.

  On a UNIX NetBackup master server, log on as root and use the following command to list and add keys:

  ```
  /usr/openv/netbackup/bin/admincmd/get_license_key
  ```

  Note that the existing 40 -bit or 56-bit encryption license keys are valid for upgrades.

Installing encryption on a Windows NetBackup server

The NetBackup Windows server and client installations include encryption software. Use the following procedure to make sure that a license key for NetBackup Encryption has been registered on the NetBackup master server.

To confirm that NetBackup encryption is registered on a Windows NetBackup master server

- On the Windows master server, log on as an Administrator. Use the **Help > License Keys** menu in the **NetBackup Administration Console** to list and add keys.

  Note that existing 40-bit encryption or 56-bit encryption license keys are valid for upgrades.

About installing encryption locally on a NetBackup UNIX client

No local installation is necessary for a NetBackup UNIX client. The encryption software is automatically installed with the NetBackup UNIX client installation. You can then configure the client encryption settings. See "About configuring standard encryption on clients" on page 265.

About installing encryption locally on a NetBackup Windows client

No local installation is necessary for a NetBackup Windows client. The encryption software is automatically installed with the NetBackup Windows client installation. See "About configuring standard encryption on clients" on page 265.

About 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 7-5 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.
	`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.

Table 7-5 Three encryption-related configuration options *(continued)*

Option	Value	Description
`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 NetBackup 7.0 or later

About creating encryption key files on clients notes

Use the following guidelines to create encryption key files on clients notes as follows:

- 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 up 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 prevent the key file from being backed up to a client, add the key file's path name to the client's exclude 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 272.
- Changing client encryption settings from the server
  See "Changing the client encryption settings from the NetBackup server" on page 272.

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 266.

   For additional explanations of the settings, click the **Help** button in the window, or see the NetBackup Administrator's Guide, Volume I.

About configuring legacy encryption

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 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 NetBackup 7.0 or later.
- 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 275.

See "About pushing the legacy encryption pass phrases to clients" on page 276.

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.

Legacy encryption configuration options

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 7-6 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.
	`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.

Table 7-6 Legacy encryption configuration options *(continued)*

Option	Value	Description
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/netbackup/keyfile	The default value on UNIX systems.
	install_path\NetBackup\bin\keyfile.dat	The default value on Windows systems.

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's`USE_VXSS` setting in `bp.conf`.

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\bin\keyfile.dat

- For UNIX clients, the default key file name is as follows

  /usr/openv/netbackup/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 281.

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/netbackup/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\bin\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.

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: Symantec 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 "Running the bpcd -keyfile command" on page 282.

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/netbackup/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.

Option 2 - Media server encryption

NetBackup media server encryption is ideally suited for the following:

- Media servers that can handle the burden for compression / encryption

- NetBackup administrators that want centralized and coarse key management granularity
- Situations where tight NetBackup operational integration is not needed

Media server encryption option administration

This topic describes the media server encryption administration.

Information about administering the media server encryption option is located in other supporting documents. The *NetBackup Media Server Encryption Option Administrator's Guide* and the *NetBackup Media Server Encryption Option Release Notes* are separate documents that can be found on the Symantec Support web site at the following location.

www.symantec.com/business/support/index?page=content&id=DOC4879

Chapter 8

Data at rest key management

This chapter includes the following topics:

- Troubleshooting example - backup with no active key record
- Troubleshooting example - restore with an improper key record state

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 hence NetBackup KMS can now be operated in FIPS mode. See “About FIPS enabled KMS” on page 288.

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.

Note: FIPS encryption is supported for NetBackup 7.7 and later versions.

All keys that are created using the 7.7 or later versions would be FIPS approved. Upon upgrade, the keys that were created using an older version of NetBackup are not FIPS approved. The keys are not converted to FIPS approved keys even when they are moved to a key group that is created using NetBackup 7.7 or later versions.

When you create a new key using 7.7 or later versions, 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
```

Post upgrade to NetBackup 7.7, 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
- HP-UX IA64 11.31
- AIX 5.3 TL12 SP2
- AIX 5.3 TL12 SP2

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 8-1 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.
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.

Table 8-1 Considerations that relate to the functionality and use of KMS *(continued)*

Consideration	Description
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 8-1 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 8-1 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 7.5 supports 100 key groups. NetBackup 7.0 supported 20 key groups. Only 10 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 8-2 for brief information about interoperability between media and tape drives. Symantec 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 8-1 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 from 7.0 to 7.0.1. The solution is to grant the root and administrator users NBU_Admin and KMS_Admin permissions manually.

Table 8-2 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.

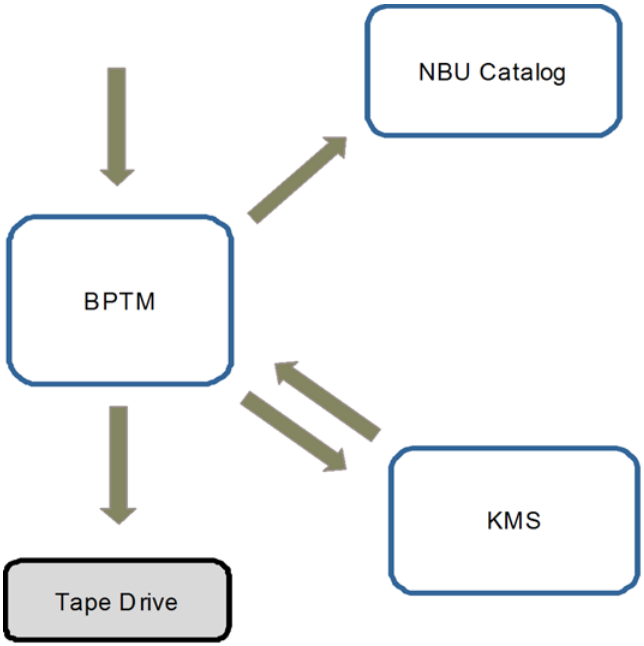
The backup then proceeds as normal.

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 8-1 shows how the process flows.

Figure 8-1 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 8-3 defines the terms that are associated with KMS.

Table 8-3 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 8-3 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 -creatkg -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 -creatkg -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: Symantec 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
```

See “About installing KMS with HA clustering” on page 303.

See "Using KMS with NBAC" on page 303.

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 8-4 shows the default KMS permissions for each of the NetBackup user groups.

Table 8-4 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\NetBackup\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. This ID is associated with the KPK; you can use it to find this particular key in the future.
6. Enter KPK ID: 10.

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

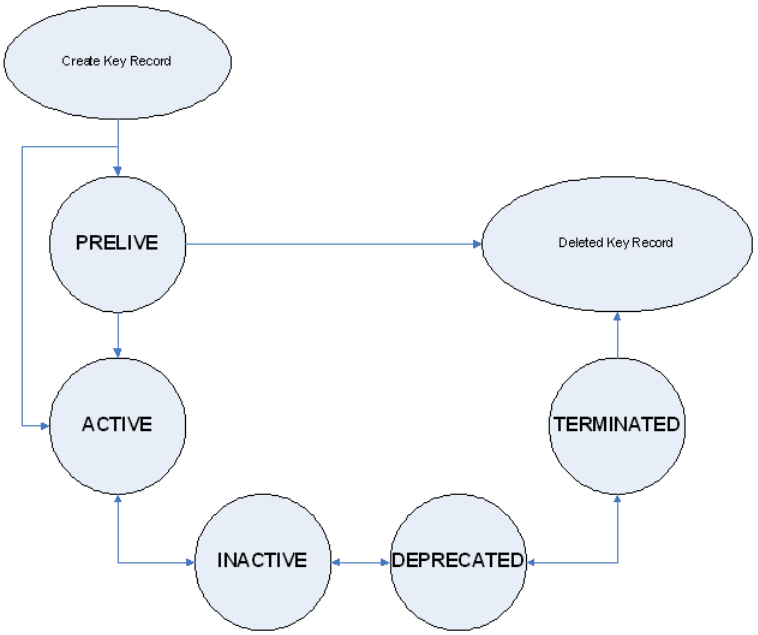
The key record states include the prelive, active, inactive, deprecated, and terminated. Key record states adhere to a key record life cycle. Once a key has entered the active state (that is set up for encryption), the key must progress in proper order through the lifestyle. The proper order includes 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 8-2 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 317.
- Setting up NetBackup to use encryption
  See "Example of setting up NetBackup to use tape encryption" on page 318.

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 8-3 NetBackup Administration Console with two volume pools set up to use KMS

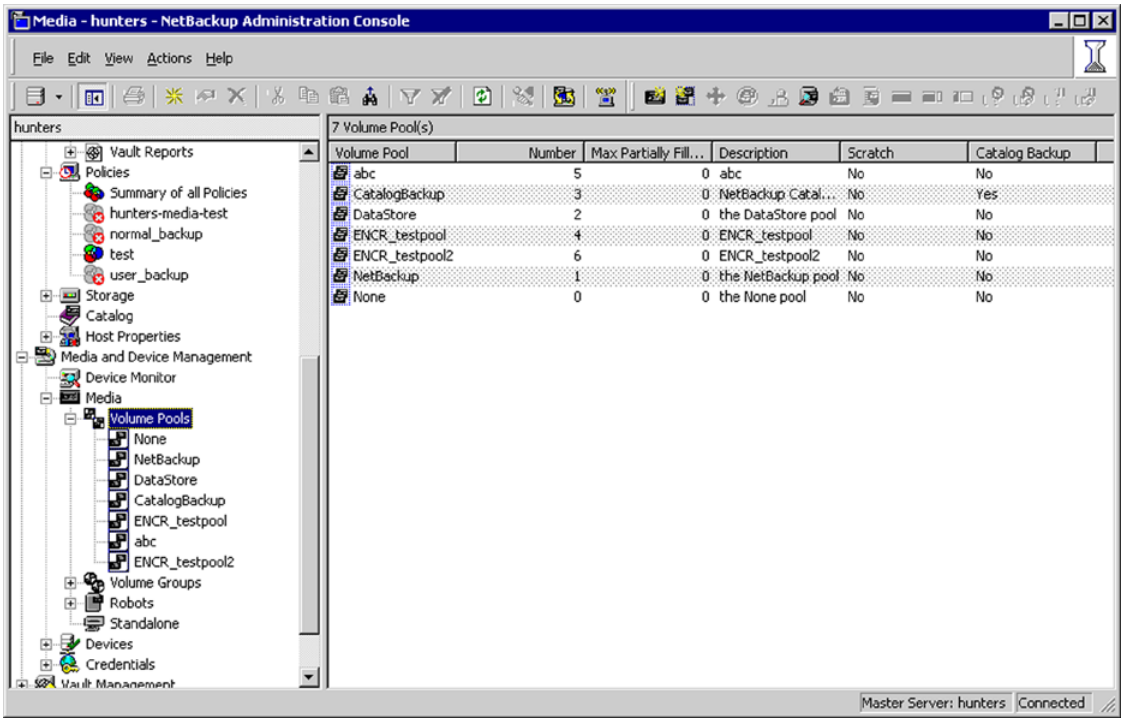
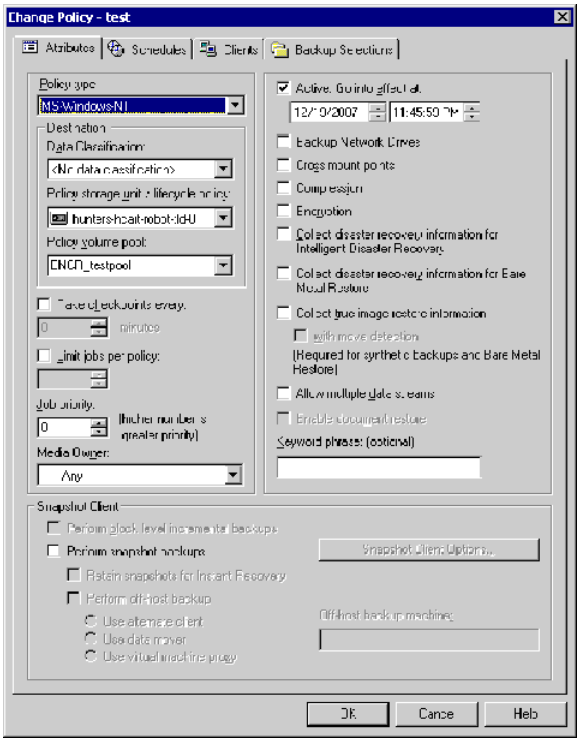


Figure 8-4 shows a NetBackup Policy that is configured to use the volume pool `ENCR_testpool`, which is the same name as the key group that you configured earlier.

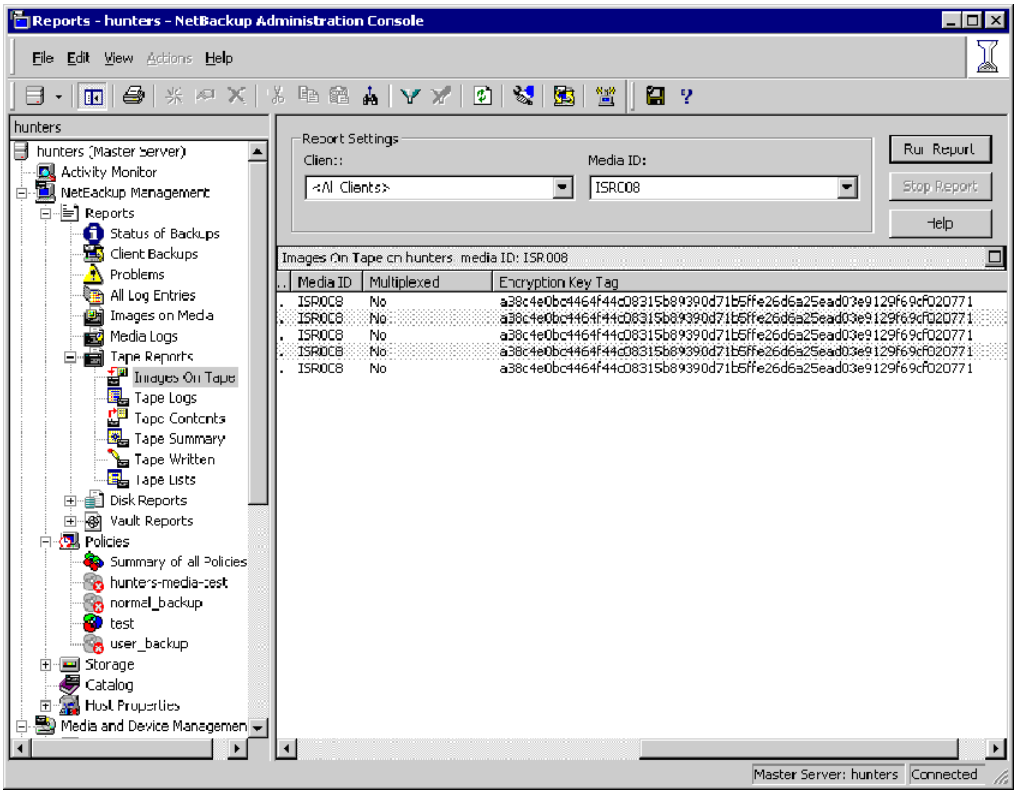
Figure 8-4 NetBackup Change Policy dialog box with KMS volume pool



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.

The following figure shows an **Images on Tape** report that has encryption key tags displayed.

Figure 8-5 Images on Tape with tape encryption keys displayed



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:

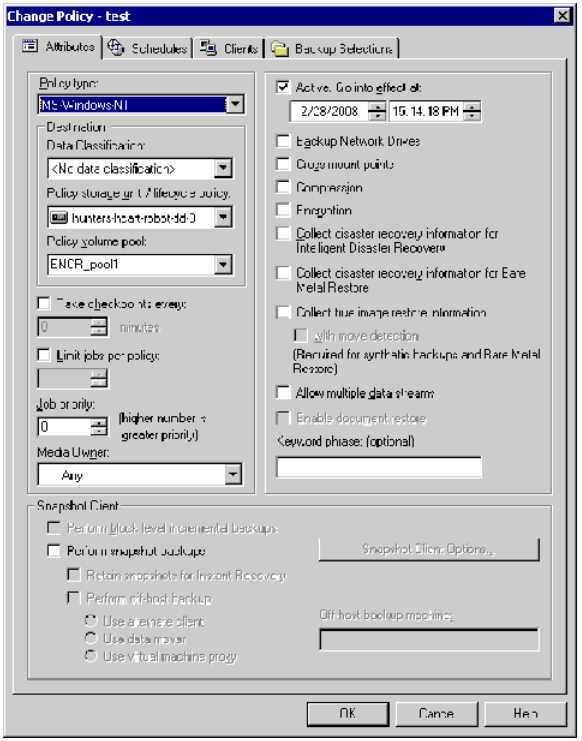
- Example of running an encrypted tape backup
  See "Example of running an encrypted tape backup" on page 321.
- Example of verifying an encryption backup
  See "Example of verifying an encryption backup" on page 321.
- About importing KMS encrypted images
  See "About importing KMS encrypted images" on page 322.

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 8-6 shows a NetBackup Policy that you have configured to use the volume pool `ENCR_pool1`.

Figure 8-6 NetBackup Change Policy dialog box with KMS volume pool ENCR_pool1

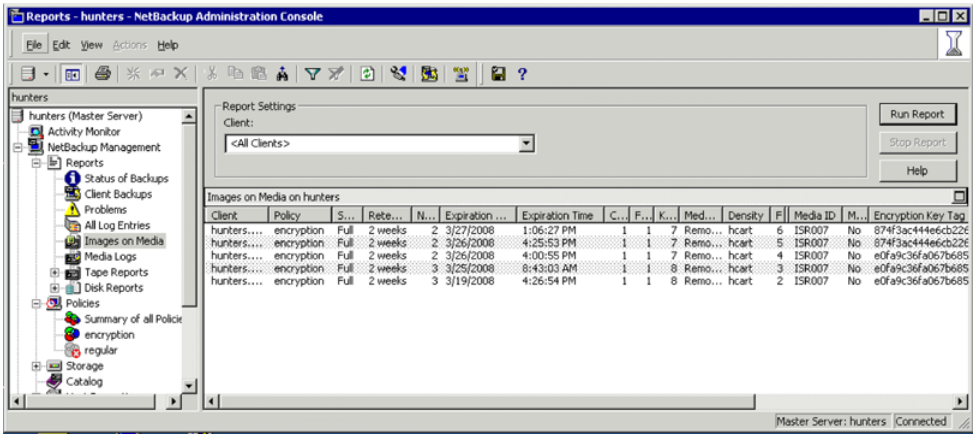


Example of verifying an encryption backup

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.

Figure 8-7 shows an Images on Media report that has encryption key tags displayed.

Figure 8-7 Images on Media with tape encryption keys displayed



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.

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 325.
- Create a new key group
  See “Create a new key group” on page 326.
- Create a new key
  See “Create a new key” on page 326.
- Modify key group attributes

See “Modify key group attributes” on page 327.

- Modify key attributes
  See “Modify key attributes” on page 327.
- Get details of key groups
  See “Get details of key groups” on page 328.
- Get details of keys
  See “Get details of keys” on page 329.
- Delete a key group
  See “Delete a key group” on page 329.
- Delete a key
  See “Delete a key” on page 330.
- Recover a key
  See “Recover a key” on page 330.
- Modify host master key (HMK)
  See “Modify host master key (HMK)” on page 335.
- Get host master key (HMK) ID
  See “Get host master key (HMK) ID” on page 335.
- Modify key protection key (KPK)
  See “Modify key protection key (KPK)” on page 335.
- Get key protection key (KPK) ID
  See “Get key protection key (KPK) ID” on page 335.
- Get keystore statistics
  See “Get keystore statistics” on page 336.
- Quiesce KMS database
  See “Quiesce KMS database” on page 336.
- Unquiesce KMS database
  See “Unquiesce KMS database” on page 336.

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 "Listing keys from a key group" on page 316.

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 327.

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 8-8 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 8-8 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 8-9 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 8-9 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 8-10 shows the BPTM log output. It logs the message within the 1227 error code in the BPTM log.

Figure 8-10 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
```

What does this error look like in the Activity Monitor?

Figure 8-11 shows that a status code 83 - media open error message returned.

Figure 8-11 Activity monitor with status code 83

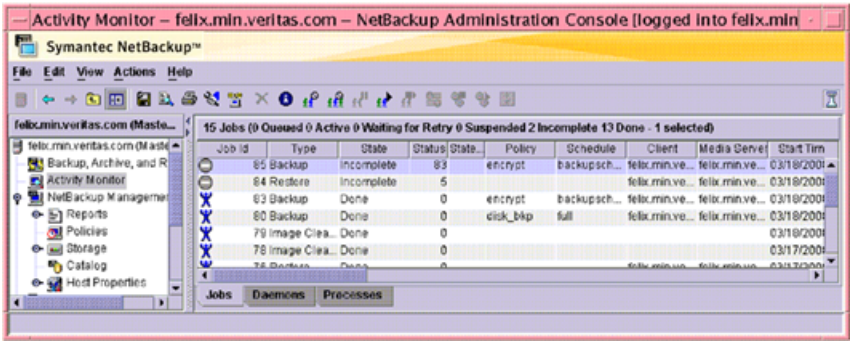


Figure 8-12 shows the detailed status. You can see a message stating that `nbksm` failed with error status key group does not have and active key (1227). With the information in the previous diagnostics, you can determine the particular problem or to identify what a given problem is related to.

Figure 8-12 Job details dialog box

Troubleshooting example - restore with an improper key record state

The following example shows a restore with a key record in an improper state.

Figure 8-13 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 8-13 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
```

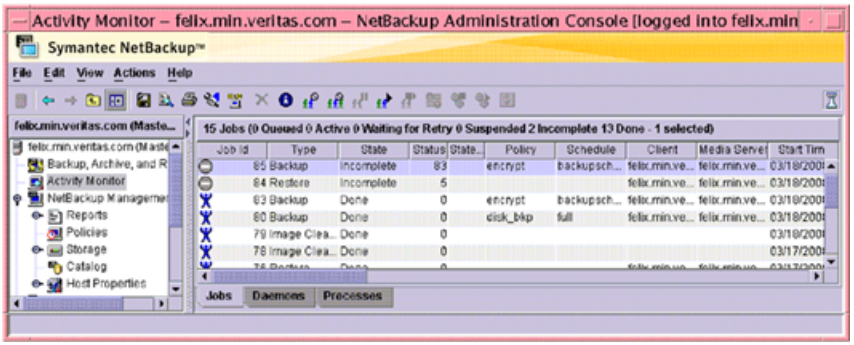
Figure 8-14 shows the `bptm` log output with the 1242 error returned.

Figure 8-14 `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)
```

Figure 8-15 shows a status code 5 - restore failed to recover the requested files.

Figure 8-15 Activity monitor with status code 5



Index

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W