

Symantec NetBackup™ Security and Encryption Guide

UNIX, Windows, and Linux

Release 7.5



Symantec NetBackup™ Security and Encryption Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.5

Legal Notice

Copyright © 2012 Symantec Corporation. All rights reserved.

Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 Web site at the following URL:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

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

Technical Support	4
Chapter 1 Increasing NetBackup security	17
About NetBackup security and encryption	18
NetBackup security implementation levels	18
World level security	19
Enterprise level security	21
Datacenter level security	23
NetBackup security components	23
NetBackup Access Control (NBAC)	25
Combined world, enterprise, and datacenter levels	30
NetBackup security implementation types	31
Operating system security	33
NetBackup security vulnerabilities	34
Standard NetBackup security	34
Media Server Encryption Option (MSEO) security	35
Client side encryption security	36
NBAC on master, media server, and GUI security	38
NBAC complete security	40
All NetBackup security	41
Chapter 2 Security deployment models	43
Workgroups	44
Single datacenters	44
Multi-datacenters	44
Workgroup with NetBackup	45
Single datacenter with standard NetBackup	48
Single datacenter with Media Server Encryption Option (MSEO)	51
Single datacenter with client side encryption	54
Single datacenter with NBAC on master and media servers	56
Single datacenter with NBAC complete	60
Single datacenter with all security implemented	64
Multi-datacenter with standard NetBackup	68
Multi-datacenter with Media Server Encryption Option (MSEO)	72
Multi-datacenter with client side encryption	77

Multi-datacenter with NBAC on master and media servers	82
Multi-datacenter with NBAC complete	88
Multi-datacenter with all NetBackup security	94

Chapter 3

Port security	101
About ports	103
NetBackup ports	103
About overriding or modifying port numbers	104
Default 7.5 NetBackup ports	104
Default port numbers for NetBackup 7.5	105
Master server outgoing ports	106
Media server outgoing ports	107
EMM server outgoing ports	109
Client outgoing ports	110
Windows administration console or Java server outgoing ports	111
Java console outgoing ports	112
About configuring ports	112
About accepting remote connections from non-reserved ports	113
Disabling random port assignments in the NetBackup configuration	113
Random port assignments in the media manager configuration	114
Specifying firewall connect options on a NetBackup server or client	114
Ports options	116
BPCD connect-back options	116
Daemon connection port options	117
Specifying firewall connect options for a source computer to apply to specific destination computers	118
Firewall connection options on Media Manager	119
About communication and firewall considerations	120
Ports required to communicate with backup products	122
Web browser to NetBackup Web GUI connection	123
About NetBackup Web GUI to NetBackup server software communication	124
About NetBackup server to NetBackup master server (NBSL) communication	124
About SNMP traps	124
Configuring the NetBackup master server to communicate with the OpsCenter server	124
About NetBackup Web GUI/NetBackup server to Sybase database communication	125

About NetBackup Web GUI to NetBackup server email communication	125
About specifying NetBackup-Java connection options	125
Specifying client attributes	126
Specifying ports (reserved or non-reserved) that connect a master server or media server to a client	127
Specifying a BPCD connect-back method that connects a master server or media server to a client	130
Specifying a daemon connection port that connects a master server or media server to a client	132
Specifying port ranges	134
BPJAVA_PORT and VNETD_PORT ports	136
Changing the ports for BPCD and BPRD on Windows	137
Disabling the ping on the NetBackup Administration Console on Windows	137
About ICMP pinging NDMP	138
About NDMP in a firewall environment	138
About the ACS storage server interface	139
About known firewall problems when using NetBackup with other products	140
About configuring port usage without a GUI	141
About port usage settings in the NetBackup configuration - bp.conf	141
Port usage-related NetBackup configuration settings	142
About configuring port usage client attribute settings - bpclient command	147
Specifying the bpclient command	148
Port usage-related Media Manager configuration settings - vm.conf	150
 Chapter 4	
Access control security	153
About using NetBackup Access Control (NBAC)	156
NetBackup access management administration	159
About NetBackup Access Control (NBAC) configuration	159
Configuring NetBackup Access Control (NBAC)	160
NBAC configuration overview	160
Configuring NetBackup Access Control (NBAC) on standalone master servers	161
Installing the NetBackup 7.5 master server highly available on a cluster	162
Configuring NetBackup Access Control (NBAC) on a clustered master server	163

Configuring NetBackup Access Control (NBAC) on media servers	164
Installing and configuring NetBackup Access Control (NBAC) on clients	166
Establishing a trust relationship between the broker and the Windows remote console	169
NBAC configure commands summary	169
Upgrading NetBackup Access Control (NBAC)	174
About including authentication and authorization databases in the NetBackup hot catalog backups	174
Upgrading NetBackup 7.5 when an older version of NetBackup is using a root broker installed on a remote machine	174
Configuring NetBackup Access Control (NBAC) for NetBackup pre-7.0 media server and client computers	179
Manually configuring the Access Control host properties	180
Unifying NetBackup Management infrastructures with the setuptrust command	181
Using the setuptrust command	182
Accessing the master server and media server host properties	183
Access control host properties	183
Network Settings tab	184
Authentication Domain tab	185
Authorization Service tab	186
Accessing the client host properties	187
Access control host properties dialog for the client	187
Authentication Domain tab for the client	188
Network Settings tab for the client	189
Access management troubleshooting guidelines	190
Troubleshooting topics for NetBackup Authentication and Authorization	191
About the UNIX verification procedures	199
UNIX master server verification	200
UNIX media server verification	203
UNIX client verification	205
Verification points in a mixed environment with a UNIX master server	207
Master server verification points for a mixed UNIX master server	209
Media server verification points for a mixed UNIX master server	209
Client verification points for a mixed UNIX master server	211
Verification points in a mixed environment with a Windows master server	212

Master server verification points for a mixed Windows master server	215
Media server verification points for a mixed Windows master server	215
Client verification points for a mixed Windows master server	217
Windows verification points	219
Master server verification points for Windows	220
Media server verification points for Windows	224
Client verification points for Windows	226
Using the Access Management utility	228
About determining who can access NetBackup	229
Individual users	229
User groups	230
NetBackup default user groups	231
Configuring user groups	233
Creating a new user group	233
Creating a new user group by copying an existing user group	234
Renaming a user group	234
General tab	235
Users tab	235
Defined Users pane on the Users tab	236
Assigned Users pane on the Users tab	237
Adding a new user to the user group	237
About defining a user group and users	237
Logging on as a new user	239
Assigning a user to a user group	239
Permissions tab	240
About authorization objects and permissions	240
Granting permissions	242
Viewing specific user permissions for NetBackup user groups	243
Authorization objects	244
Media authorization object permissions	245
Policy authorization object permissions	245
Drive authorization object permissions	246
Report authorization object permissions	247
NBU_Catalog authorization object permissions	247
Robot authorization object permissions	248
Storage unit authorization object permissions	248
DiskPool authorization object permissions	249
BUAndRest authorization object permissions	250
Job authorization object permissions	250
Service authorization object permissions	251
HostProperties authorization object permissions	252

License authorization object permissions 252

Volume group authorization object permissions 253

VolumePool authorization object permissions 253

DevHost authorization object permissions 254

Security authorization object permissions 254

Fat server authorization object permissions 255

Fat client authorization object permissions 255

Vault authorization object permissions 256

Server group authorization object permissions 256

Key managment system (kms) group authorization object permissions 257

Chapter 5 Data at rest encryption security 259

Data at rest encryption terminology 261

Data at rest encryption limitations 261

Encryption security questions to consider 264

NetBackup data at rest encryption options 264

Encryption options comparison 264

Option 1 - NetBackup client encryption 265

About running an encryption backup 266

About choosing encryption for a backup 266

Standard encryption backup process 267

Legacy encryption backup process 267

NetBackup standard encryption restore process 268

NetBackup legacy encryption restore process 269

Installation prerequisites for encryption security 270

Installing encryption on a UNIX NetBackup server 270

Installing encryption on a Windows NetBackup server 271

About installing encryption locally on a NetBackup UNIX client 271

About installing encryption locally on a NetBackup Windows client 271

About configuring standard encryption on clients 272

Managing standard encryption configuration options 272

Managing the NetBackup encryption key file 273

About configuring standard encryption from the server 274

About creating encryption key files on clients notes 275

Creating the key files 275

Best practices for key file restoration 276

Manual retention to protect key file pass phrases 276

Automatic backup of the key file 277

Restoring an encrypted backup file to another client 277

About configuring standard encryption directly on clients 278

Setting standard encryption attribute in policies	278
Changing the client encryption settings from the NetBackup server	278
About configuring legacy encryption	279
About configuring legacy encryption from the server	279
Legacy encryption configuration options	280
About pushing the legacy encryption configuration to clients	282
About pushing the legacy encryption pass phrases to clients	282
Managing legacy encryption key files	284
Restoring a legacy encrypted backup created on another client	286
About setting legacy encryption attribute in policies	287
Changing client legacy encryption settings from the server	288
Additional legacy key file security for UNIX clients	288
Running the bpcd -keyfile command	289
Terminating bpcd on UNIX clients	290
Option 2 - Media server encryption	290
Media server encryption option administration	291

Chapter 6

Data at rest key management	293
About the Key Management Service (KMS)	296
KMS considerations	296
KMS principles of operation	300
About writing an encrypted tape	301
About reading an encrypted tape	302
KMS terminology	302
Installing KMS	304
Using KMS with NBAC	307
About installing KMS with HA clustering	307
Enabling cluster use with the KMS service	308
Enabling the monitoring of the KMS service	308
Disabling the monitoring of the KMS service	309
Removing the KMS service from monitored list	309
Configuring KMS	309
Creating the key database	310
About key groups and key records	311
About creating key groups	312
About creating key records	312
Overview of key record states	313
Key record state considerations	314
Prelive key record state	315
Active key record state	315
Inactive key record state	315

Deprecated key record state	315
Terminated key record state	316
About backing up the KMS database files	316
About recovering KMS by restoring all data files	317
Recovering KMS by restoring only the KMS data file	317
Recovering KMS by regenerating the data encryption key	317
Problems backing up the KMS data files	318
Solutions for backing up the KMS data files	319
Creating a key record	319
Listing keys	320
Configuring NetBackup to work with KMS	320
NetBackup and key records from KMS	320
Example of setting up NetBackup to use tape encryption	321
About using KMS for encryption	323
Example of running an encrypted tape backup	324
Example of verifying an encryption backup	324
About importing KMS encrypted images	325
KMS database constituents	325
Creating an empty KMS database	326
Importance of the KPK ID and HMK ID	326
About periodically updating the HMK and KPK	327
Backing up the KMS keystore and administrator keys	327
Command line interface (CLI) commands	327
CLI usage help	328
Create a new key group	329
Create a new key	329
Modify key group attributes	330
Modify key attributes	330
Get details of key groups	331
Get details of keys	331
Delete a key group	332
Delete a key	332
Recover a key	333
Modify host master key (HMK)	333
Get host master key (HMK) ID	334
Get key protection key (KPK) ID	334
Modify key protection key (KPK)	334
Get keystore statistics	334
Quiesce KMS database	335
Unquiesce KMS database	335
Key creation options	335
Troubleshooting KMS	336
Solution for backups not encrypting	337

Solution for restores not decrypting	337
Troubleshooting example - backup with no active key record	337
Troubleshooting example - restore with an improper key record state	341
Index	343

Increasing NetBackup security

This chapter includes the following topics:

- [About NetBackup security and encryption](#)
- [NetBackup security implementation levels](#)
- [World level security](#)
- [Enterprise level security](#)
- [Datacenter level security](#)
- [NetBackup security components](#)
- [NetBackup Access Control \(NBAC\)](#)
- [Combined world, enterprise, and datacenter levels](#)
- [NetBackup security implementation types](#)
- [Operating system security](#)
- [NetBackup security vulnerabilities](#)
- [Standard NetBackup security](#)
- [Media Server Encryption Option \(MSEO\) security](#)
- [Client side encryption security](#)
- [NBAC on master, media server, and GUI security](#)
- [NBAC complete security](#)

■ [All NetBackup security](#)

About NetBackup security and encryption

NetBackup security and encryption provide protection for all parts of NetBackup operations. The parts that are made secure include the NetBackup master server, media server, 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 wire 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 18.

See [“NetBackup security components”](#) on page 23.

See [“NetBackup Access Control \(NBAC\)”](#) on page 25.

See [“Operating system security”](#) on page 33.

See [“Standard NetBackup security”](#) on page 34.

See [“Media Server Encryption Option \(MSEO\) security”](#) on page 35.

See [“Client side encryption security”](#) on page 36.

See [“NBAC on master, media server, and GUI security”](#) on page 38.

See [“NBAC complete security”](#) on page 40.

See [“All NetBackup security”](#) on page 41.

NetBackup security implementation levels

NetBackup security is implemented at the following levels. The following table describes the NetBackup security implementation levels.

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

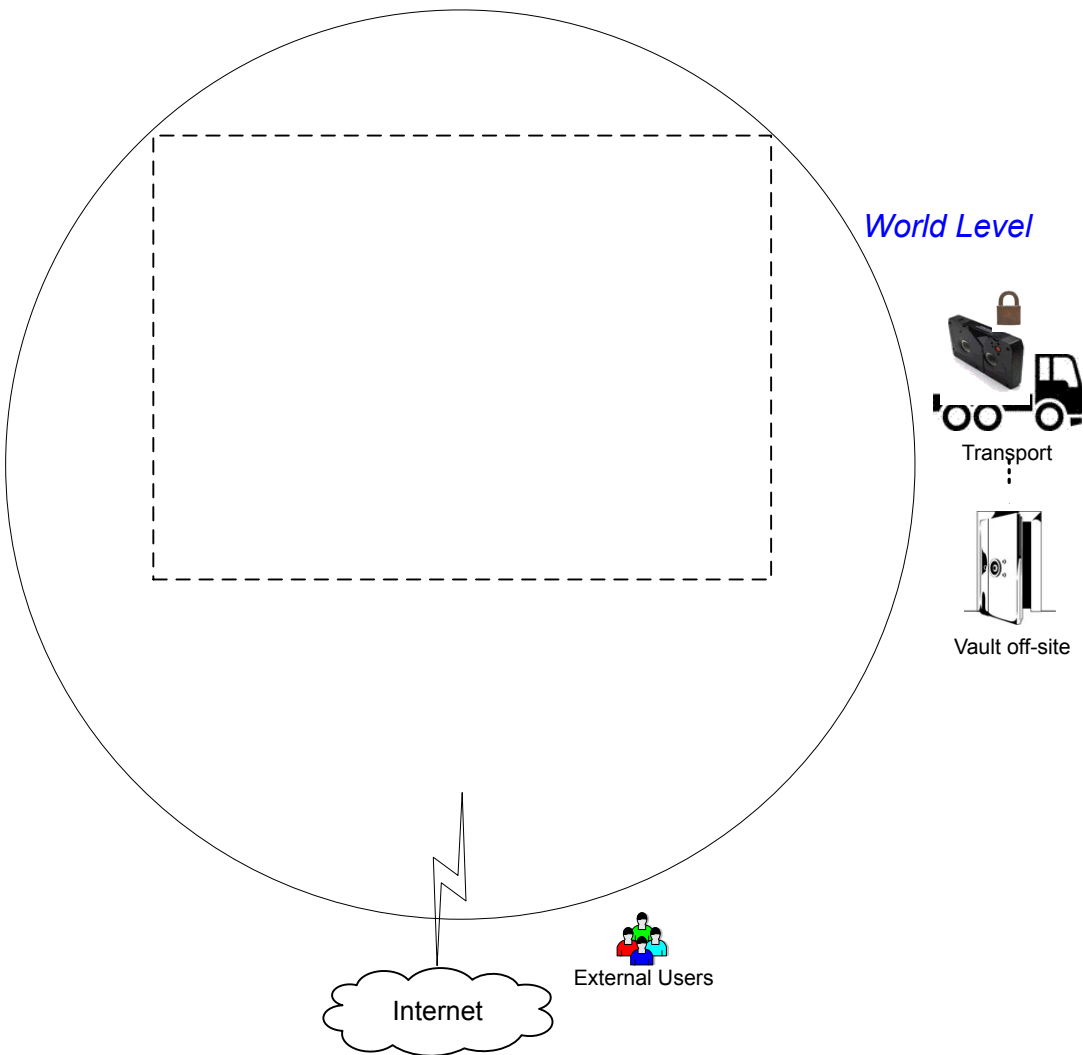
The NetBackup security implementation perspective begins in a very broad sense at the world level. Security become more detailed at the enterprise level. Ultimately, security becomes very specific at the datacenter level.

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 and includes the following world level types.

The following figure shows the world level which is the broadest type of NetBackup security implementation.

Figure 1-1 World level



The following table describes the types of world level security.

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 as the external firewall prevents NetBackup ports from being accessed.

Table 1-2 Types of world level security (*continued*)

Type	Description
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 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 the transport truck moves encrypted client tapes off-site to secure vault facilities.
World level vault off-site	Provides safe encrypted tape storage facilities off-site at a different location than the current datacenter.

Enterprise level security

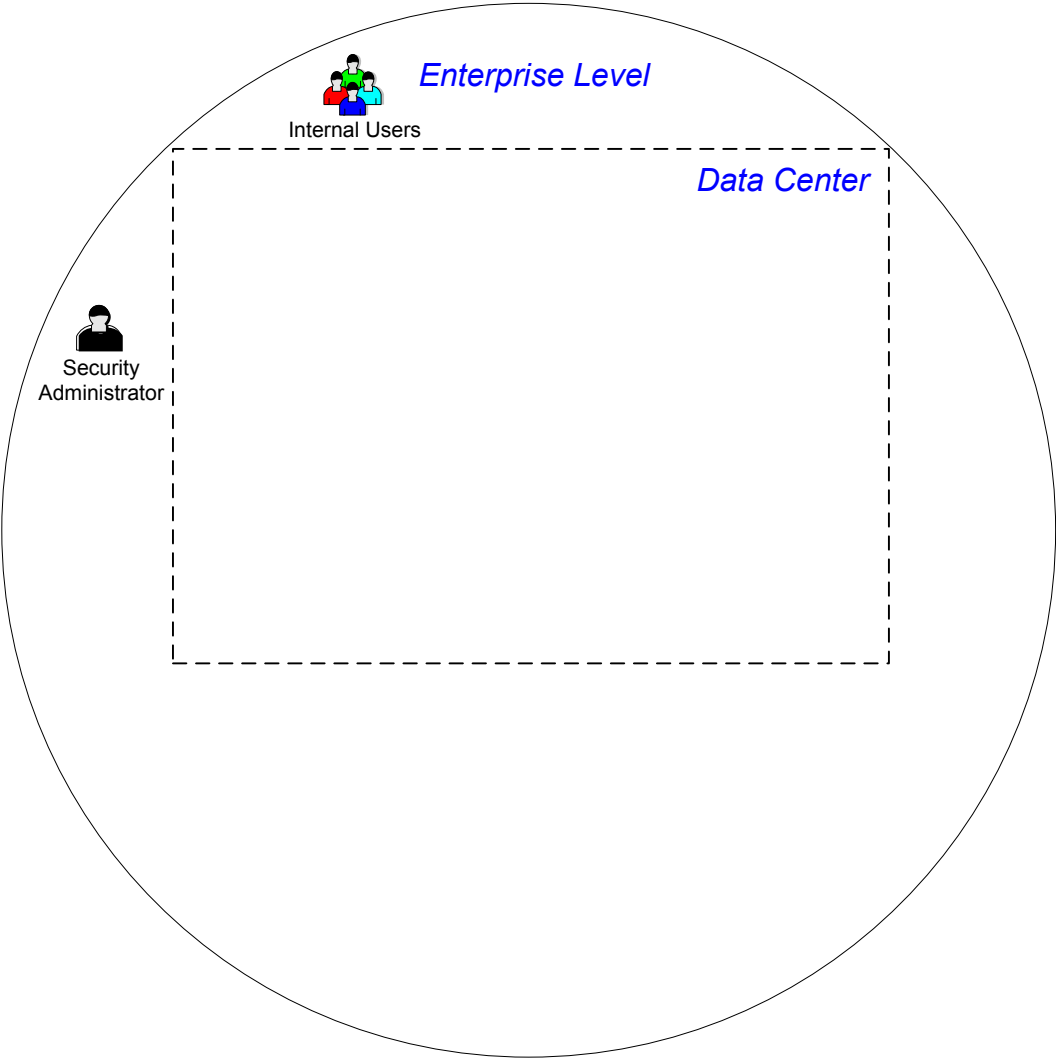
The enterprise level contains more tangible parts of NetBackup security implementation, and includes the following enterprise level items.

The following figure shows the enterprise level which encompasses internal users, security administrators, and the datacenter level.

Figure 1-2

Enterprise level

Security Overview



The following table describes the types of enterprise level security.

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 DBAs, 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

The datacenter level of security can consist of a workgroup, a single datacenter, or a multi-datacenter. The following table describes the types of datacenter level security.

Table 1-4 Types of datacenter level security

Type	Description
Workgroup	Specifies a small group of systems (less than 50) used with NetBackup in a wholly internal fashion.
Single datacenter	Specifies a medium to large group of hosts (greater than 50) and can back up hosts within the 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 Wide Area Networks (WAN). This configuration can also include hosts in the DMZ that are backed up.

NetBackup security components

The specifics of NetBackup security occur at the workgroup, single datacenter, and the multi-datacenter levels.

NetBackup provides basic security protection as follows:

- Relies on the minor security of `bpjava`
- Relies on operating system file system user security
- Changes the default EMM database password
- Uses proper file permissions

- Stops casual access to system data through the NetBackup command line and attempted raw file system access
- Requires the privileged escalator administrator or SUDO (superuser do) to use NetBackup
- NBAC is considered to be more advanced.
- To maintain the highest level of security protection, NetBackup needs to be kept current at the proper security patch level.
- Patches to the most recent patch level of your supported version of NetBackup

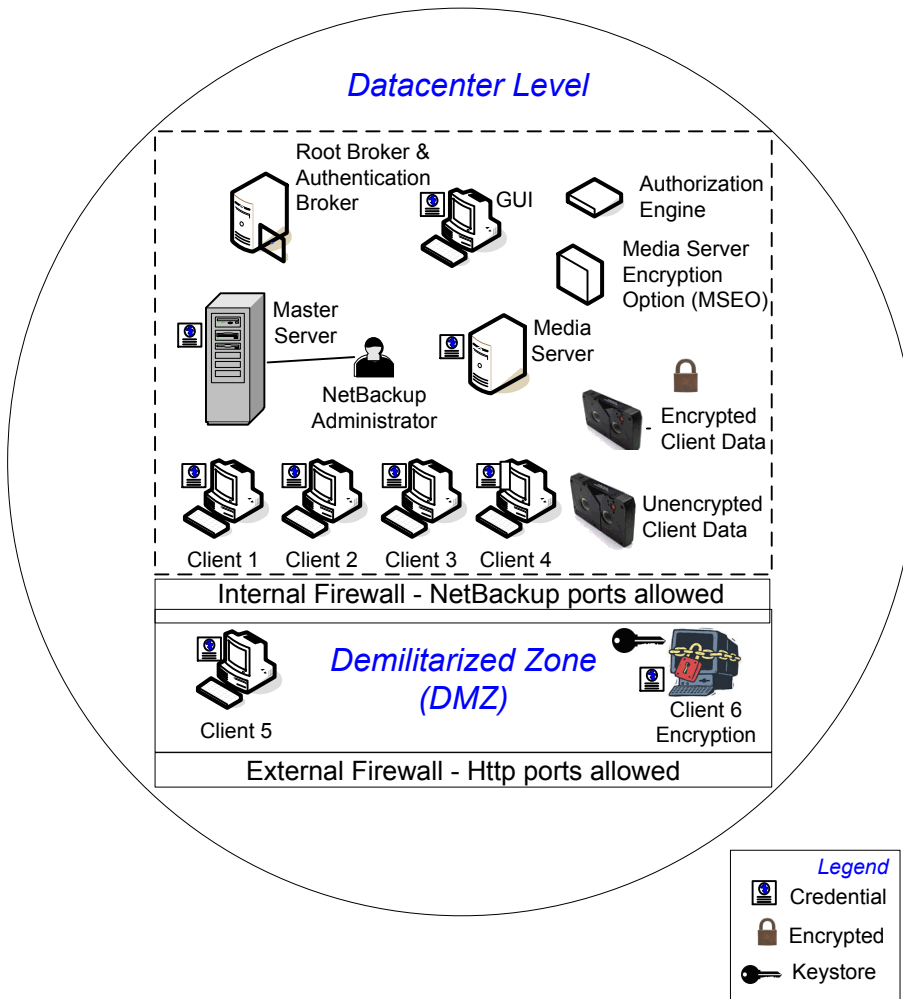
The following table describes the individual NetBackup components that contain security, including master server security, media server security, and client security.

Table 1-5 NetBackup components that contain security

Component	Description
Master server security	The NetBackup master servers can be made more secure by adding product security, including NetBackup authentication and authorization service. You can also add the client encryption option for physical tape safety, and operating system security.
Media server security	The NetBackup media servers can be made more secure by adding operating system security to the hardware computer the clients can use. You can also add product security, including NetBackup authentication and authorization service.
Client security	The NetBackup clients can be made more secure by adding product security, including NetBackup authentication and authorization service, client encryption option, and operating system security.

The following figure shows the datacenter level where the core of NetBackup security functionality occurs. See “[NetBackup Access Control \(NBAC\)](#)” on page 25. for a description of each NetBackup component that is used in security.

Figure 1-3 Datacenter level



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 18.

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.

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

Table 1-6 NetBackup components used in security

Component	Description
Root broker	<p>The NetBackup 7.5 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.</p> <p>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.</p> <p>See Figure 1-3 on page 25, which shows the root broker and authentication broker as being the same component.</p> <p>The root broker authenticates the authentication broker. The root broker does not authenticate clients.</p>
Authentication broker	<p>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.</p>
Authorization engine	<p>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.</p>

Table 1-6 NetBackup components used in security (*continued*)

Component	Description
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	<p>Specifies that the tape security in NetBackup can be increased by adding the following:</p> <ul style="list-style-type: none"> ■ Client side encryption ■ MSEO (media server Encryption Option) ■ Encryption of data at rest <p>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.</p>

Table 1-6 NetBackup components used in security (continued)

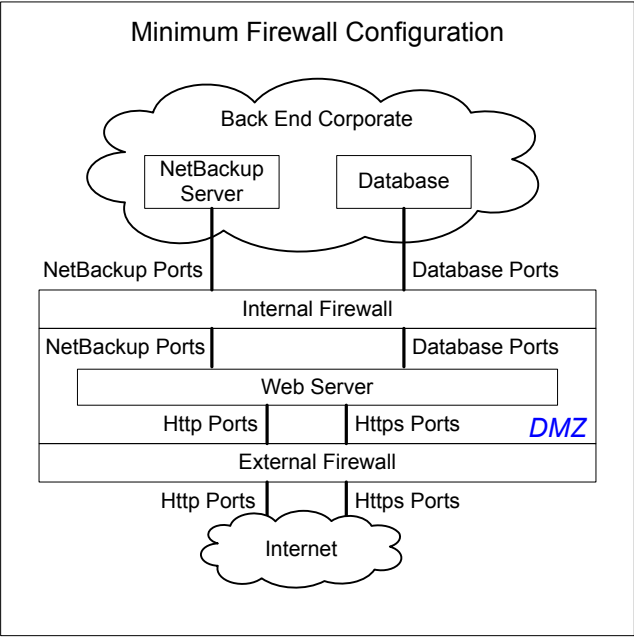
Component	Description
Encryption	<p>Specifies that NetBackup encryption can increase security by providing the following:</p> <ul style="list-style-type: none">■ Greater data confidentiality■ The loss of physical tape is not as critical if all the data is effectively encrypted■ The best risk mitigation strategy <p>See “Encryption security questions to consider” on page 264. for more information on encryption.</p>
Data over the wire security	<p>Includes communication between master servers, media servers, clients, and communication using ports through firewalls and over WANs.</p> <p>See “About ports” on page 103. for more information on ports.</p> <p>The data over the wire part of NetBackup can help increase security in the following ways:</p> <ul style="list-style-type: none">■ 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 (see port topic) in NetBackup and in other products See “Disabling random port assignments in the NetBackup configuration” on page 113.■ PBX and VNETD dedicated ports provide increased NetBackup security■ Central set of ports to monitor and open through firewalls

Table 1-6 NetBackup components used in security (*continued*)

Component	Description
Firewall security	<p>Specifies that the NetBackup firewall support can help increase security.</p> <p>Important points about firewall security include the following:</p> <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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)	<p>Specifies that the demilitarized zone (DMZ) increases security as follows:</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>Figure 1-4 shows an example internal and external firewall with DMZ.</p>

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

Figure 1-4 Example firewalls and DMZ

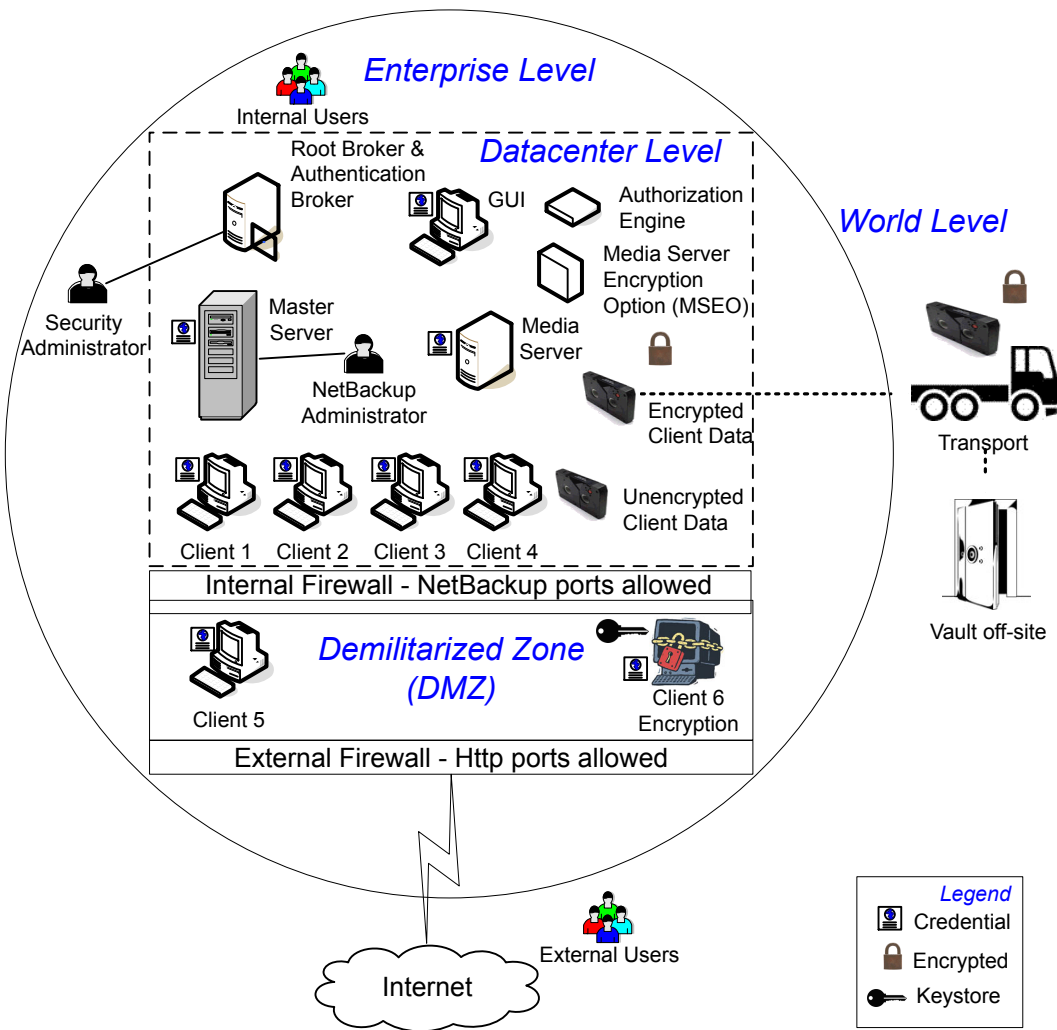


Combined world, enterprise, and datacenter levels

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 1-5 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 1-7 Security implementation types

Security implementation type	Characteristics	Complexity	Security deployment models
See “Operating system security” on page 33.	<ul style="list-style-type: none"> ■ Operating system dependent ■ Varies based on system components 	Variable	Workgroup Single datacenter Multi-datacenter
See “Standard NetBackup security” on page 34.	<ul style="list-style-type: none"> ■ 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 35.	<ul style="list-style-type: none"> ■ 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 36.	<ul style="list-style-type: none"> ■ 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 38.	<ul style="list-style-type: none"> ■ 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

Table 1-7 Security implementation types (*continued*)

Security implementation type	Characteristics	Complexity	Security deployment models
See “ NBAC complete security ” on page 40.	<ul style="list-style-type: none"> ■ 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
See “ All NetBackup security ” on page 41.	<ul style="list-style-type: none"> ■ 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:

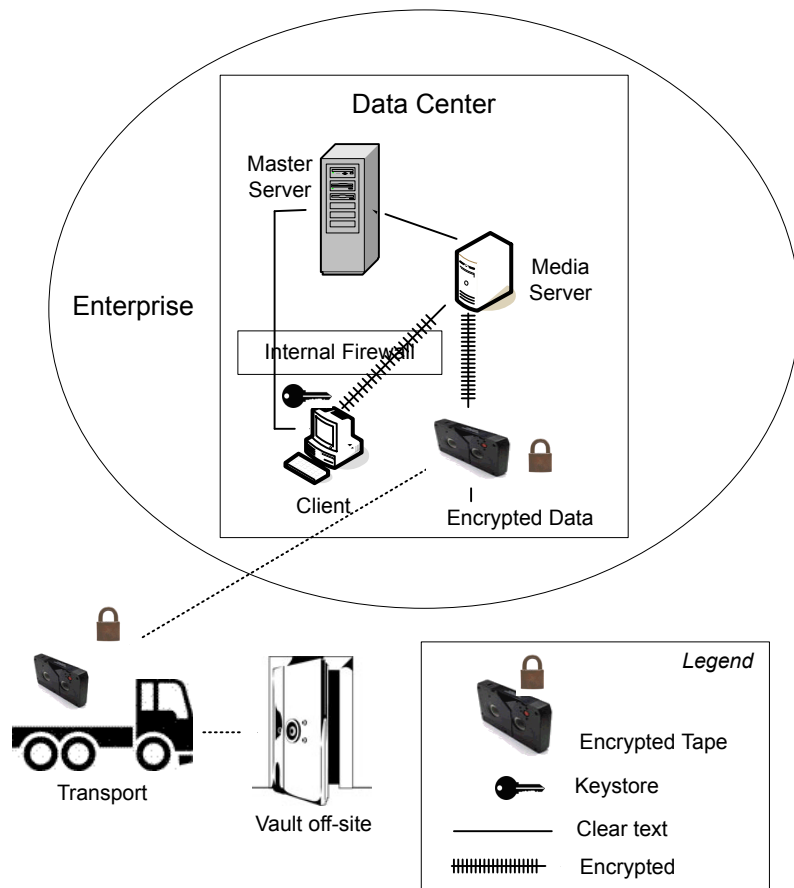
- A full NetBackup update is provided with the next NetBackup maintenance patch
- The importance of accumulative NetBackup updates
- Use the Symantec Web site for information on possible security vulnerability issues:
www.symantec.com/avcenter/security/SymantecAdvisories.html, or
www.symantec.com/security
- 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 hardware components. 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 1-6 Standard NetBackup

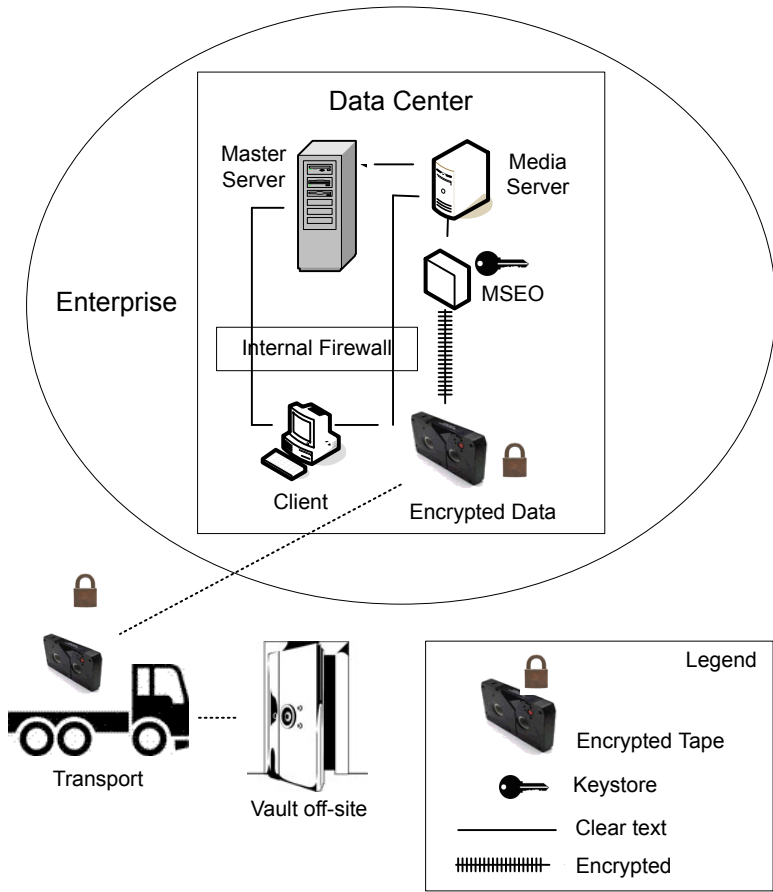


Media Server Encryption Option (MSEO) security

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 1-7 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.

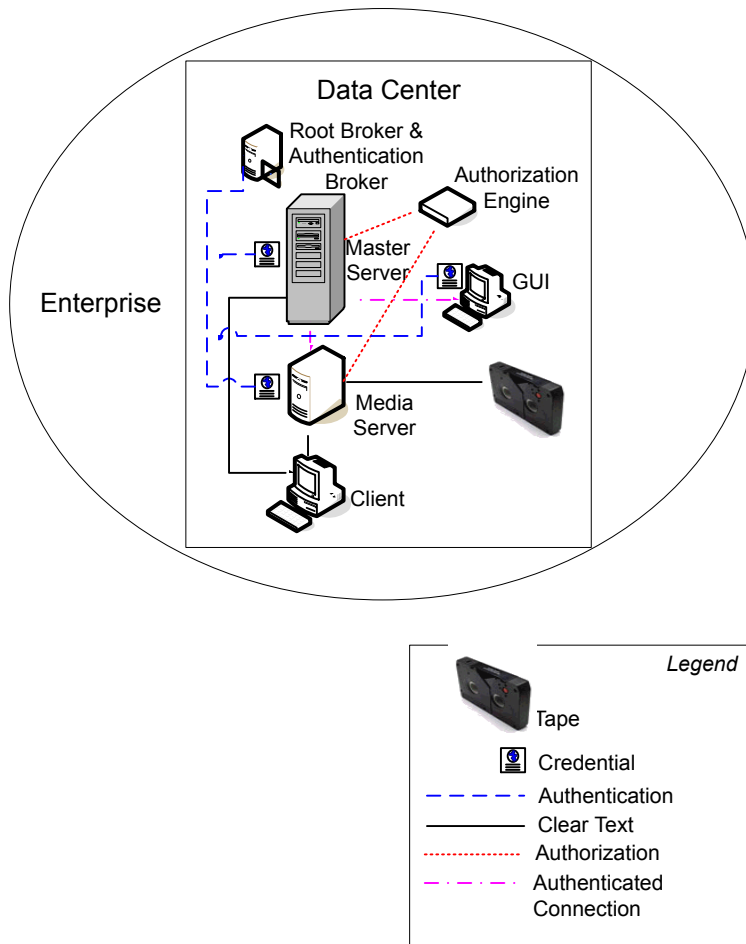
- FlashBackup
- FlashBackup-Windows
- NDMP
- NetWare
- OS/2
- Vault

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 1-8 Client side encryption



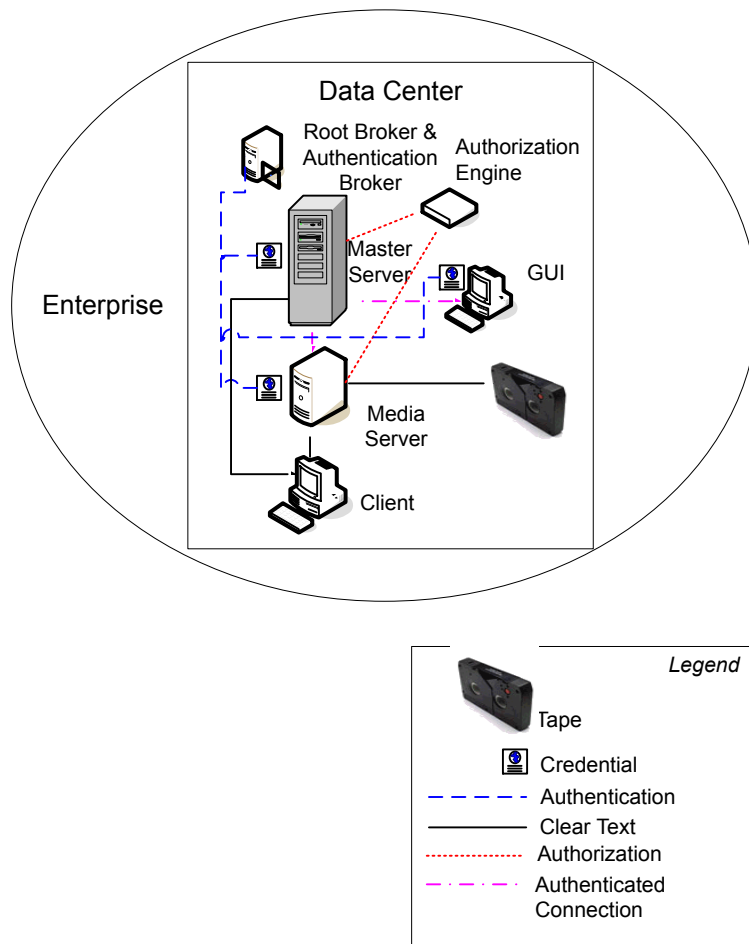
NBAC on master, media server, and GUI security

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 1-9 NBAC on master and media server

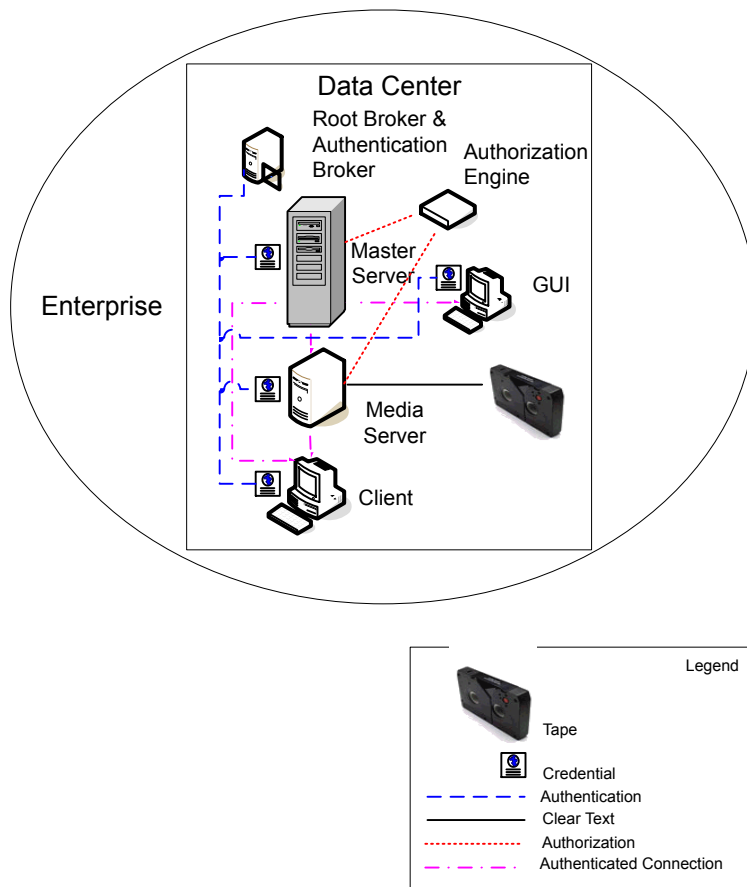


NBAC complete security

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 1-10 NBAC complete

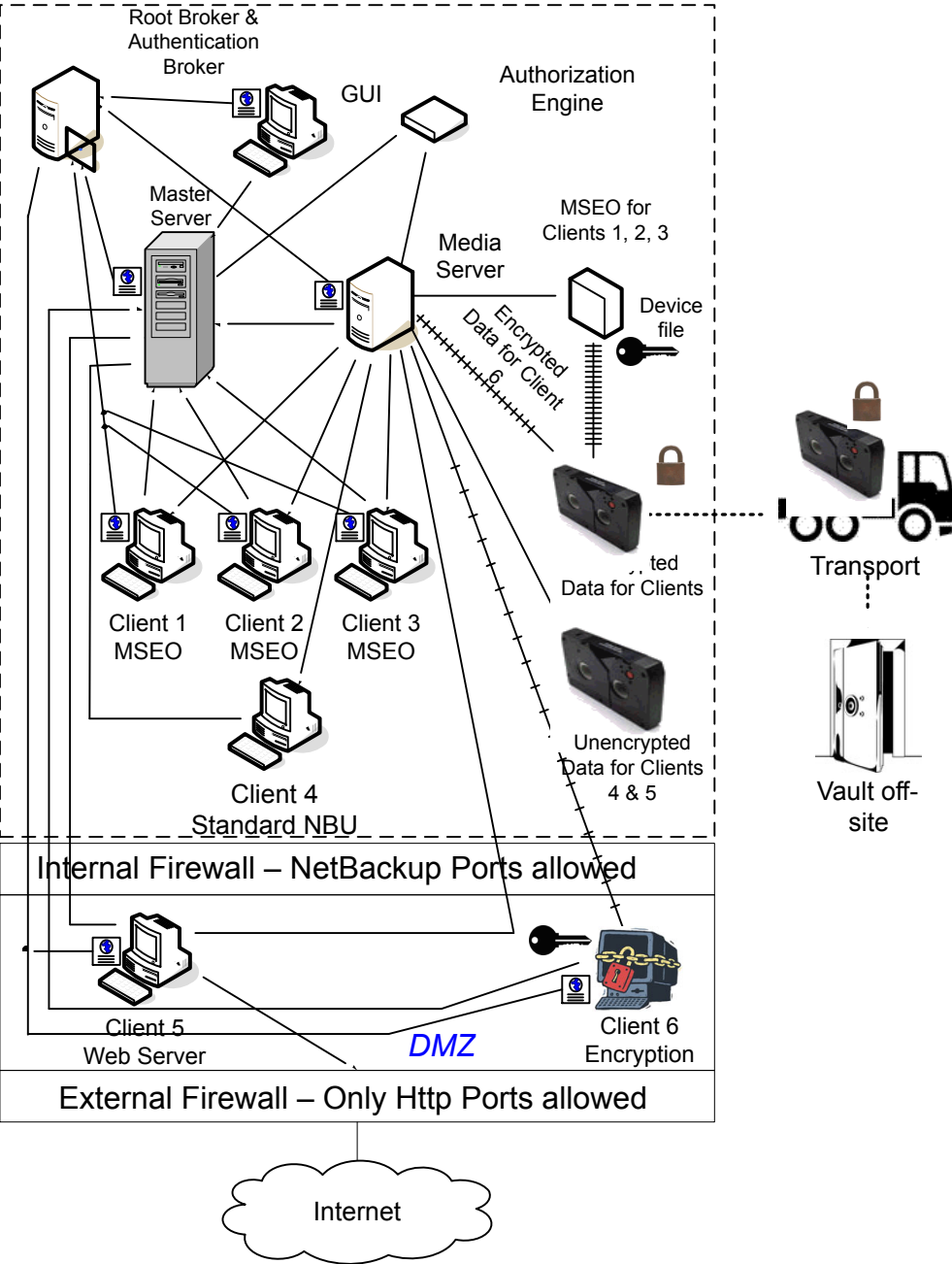


All NetBackup security

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 1-11 All NetBackup security



Security deployment models

This chapter includes the following topics:

- Workgroups
- Single datacenters
- Multi-datacenters
- Workgroup with NetBackup
- Single datacenter with standard NetBackup
- Single datacenter with Media Server Encryption Option (MSEO)
- Single datacenter with client side encryption
- Single datacenter with NBAC on master and media servers
- Single datacenter with NBAC complete
- Single datacenter with all security implemented
- Multi-datacenter with standard NetBackup
- Multi-datacenter with Media Server Encryption Option (MSEO)
- Multi-datacenter with client side encryption
- Multi-datacenter with NBAC on master and media servers
- Multi-datacenter with NBAC complete
- Multi-datacenter with all NetBackup security

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 45.

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 48.
- See [“Single datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 51.
- See [“Single datacenter with client side encryption”](#) on page 54.
- See [“Single datacenter with NBAC on master and media servers”](#) on page 56.
- See [“Single datacenter with NBAC complete”](#) on page 60.
- See [“Single datacenter with all security implemented”](#) on page 64.

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 68.
- See [“Multi-datacenter with Media Server Encryption Option \(MSEO\)”](#) on page 72.
- See [“Multi-datacenter with client side encryption”](#) on page 77.
- See [“Multi-datacenter with NBAC on master and media servers”](#) on page 82.
- See [“Multi-datacenter with NBAC complete”](#) on page 88.
- See [“Multi-datacenter with all NetBackup security”](#) on page 94.

Workgroup with NetBackup

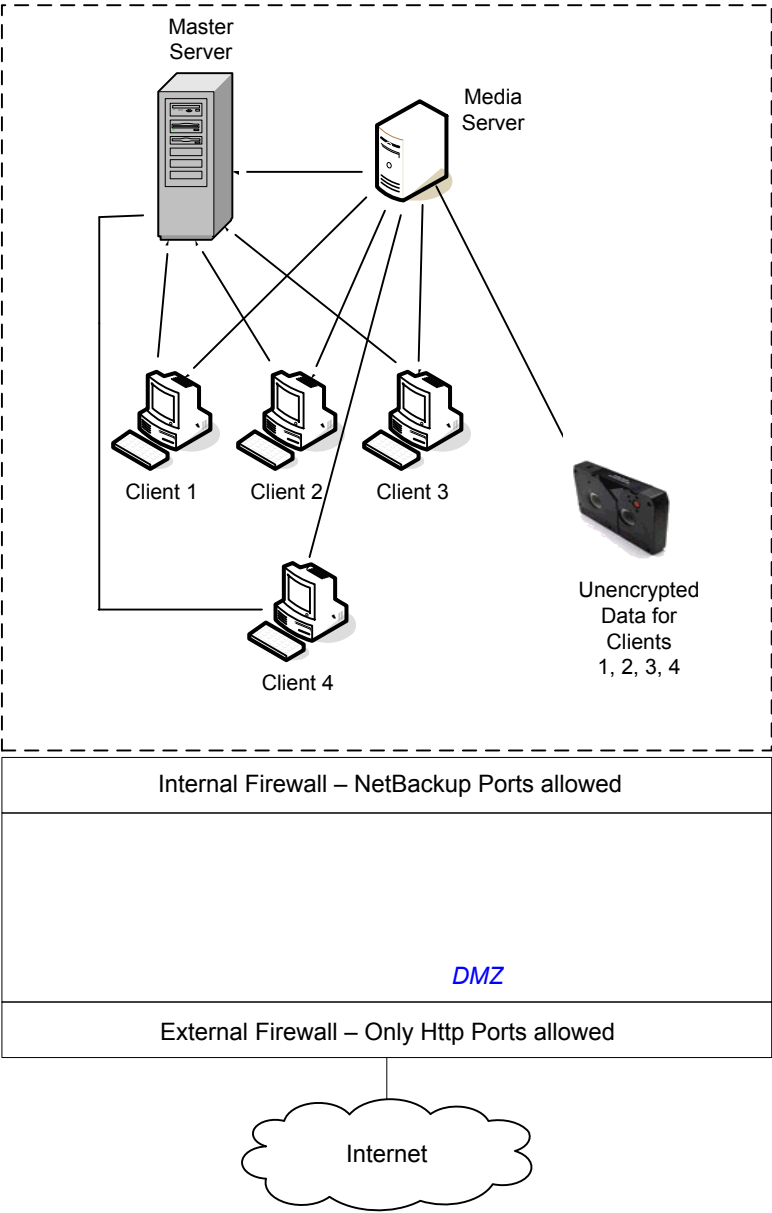
A workgroup with NetBackup is classified as a small group of systems (less than 50). The workgroup is used with NetBackup internally. Typically, this configuration does not have a unified naming service such as NIS or Active Directory. It may not have an authoritative host naming service such as DNS 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	<p>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.</p> <p>Note: In this example, there are no clients beyond the internal firewall. So the NetBackup ports should not be open through the internal firewall.</p>
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	<p>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.</p> <p>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.</p>

Single datacenter with standard NetBackup

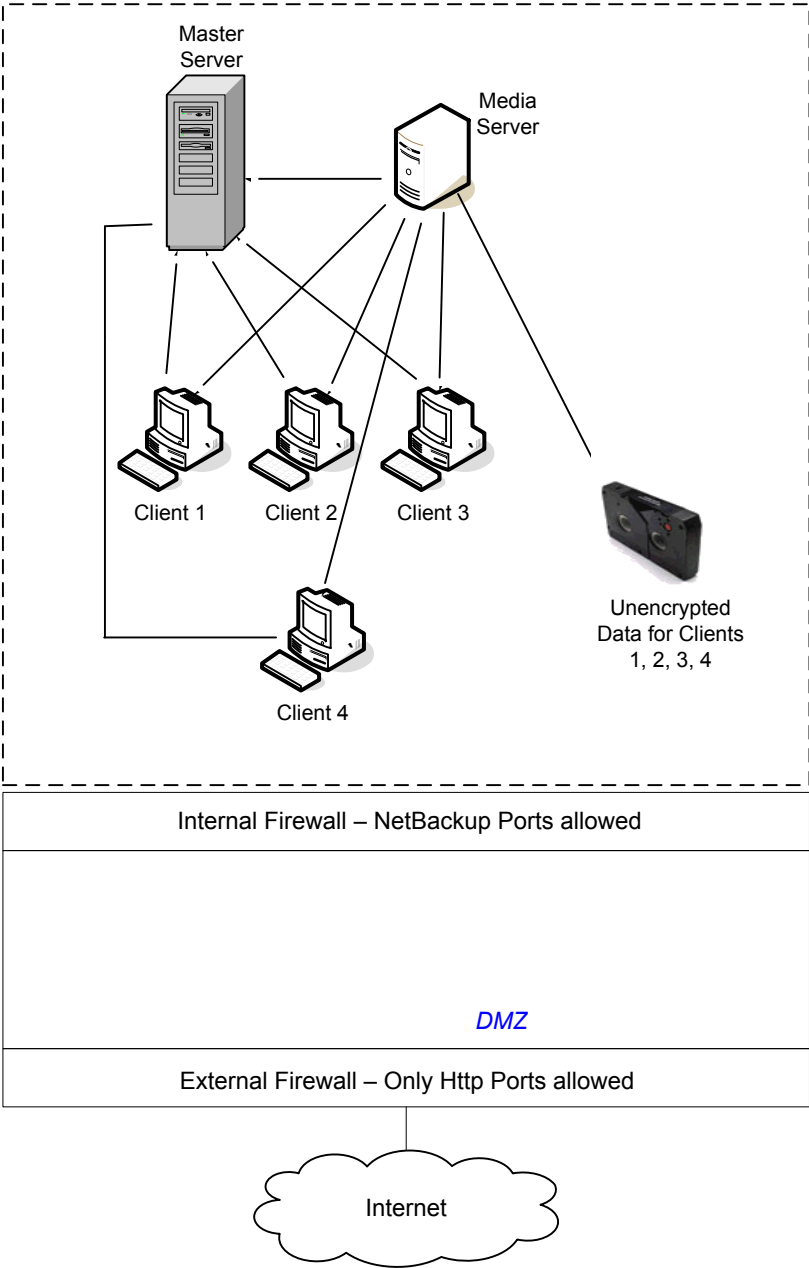
A single datacenter with standard NetBackup is defined as a medium to large group of hosts (greater than 50). It includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or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

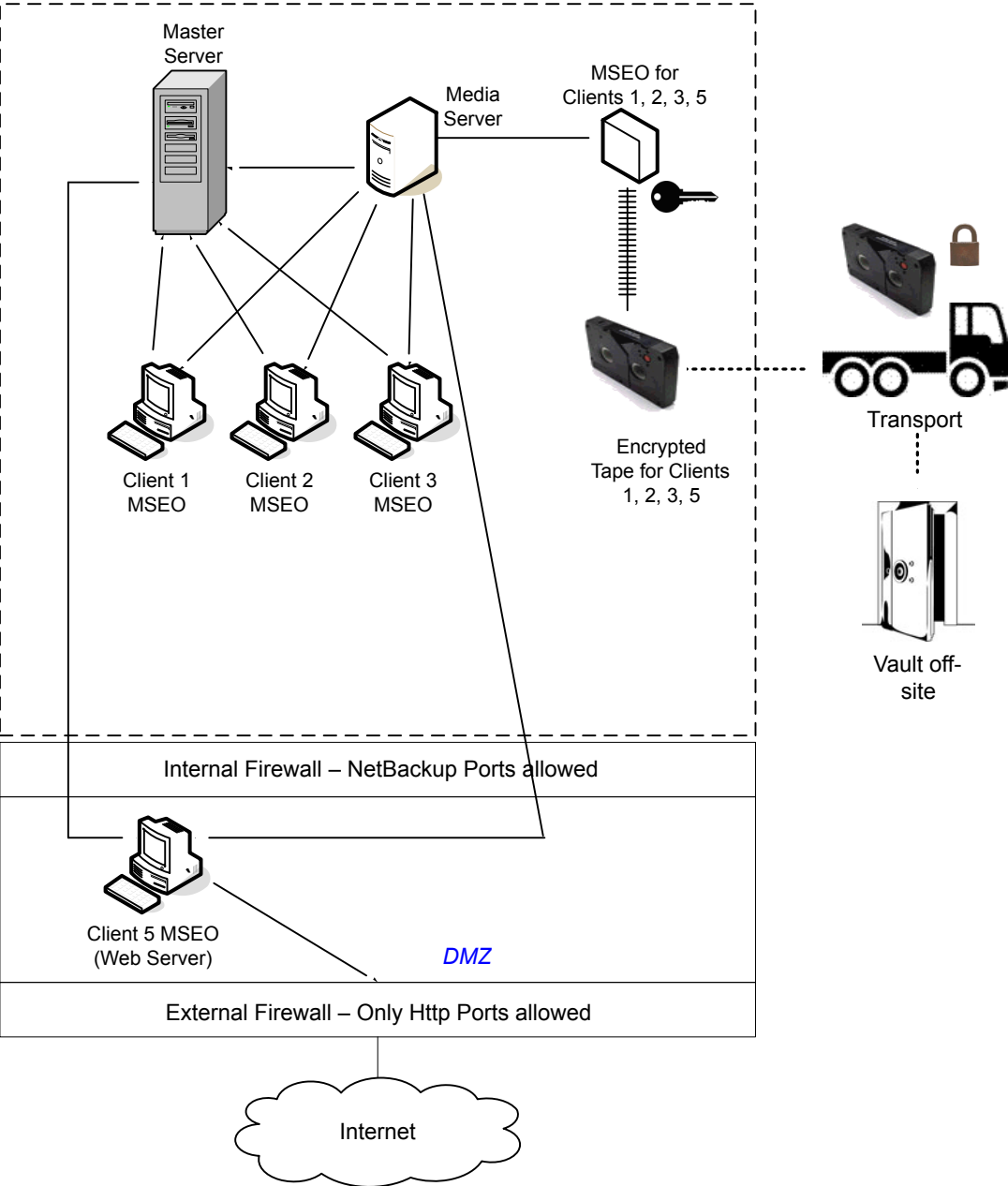
This single datacenter with the Media Server Encryption Option (MSEO) example typically includes more than 50 hosts. All externally facing hosts make use of the Media Server Encryption Option (MSEO). In this example, clients use the MSEO option for all hosts.

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

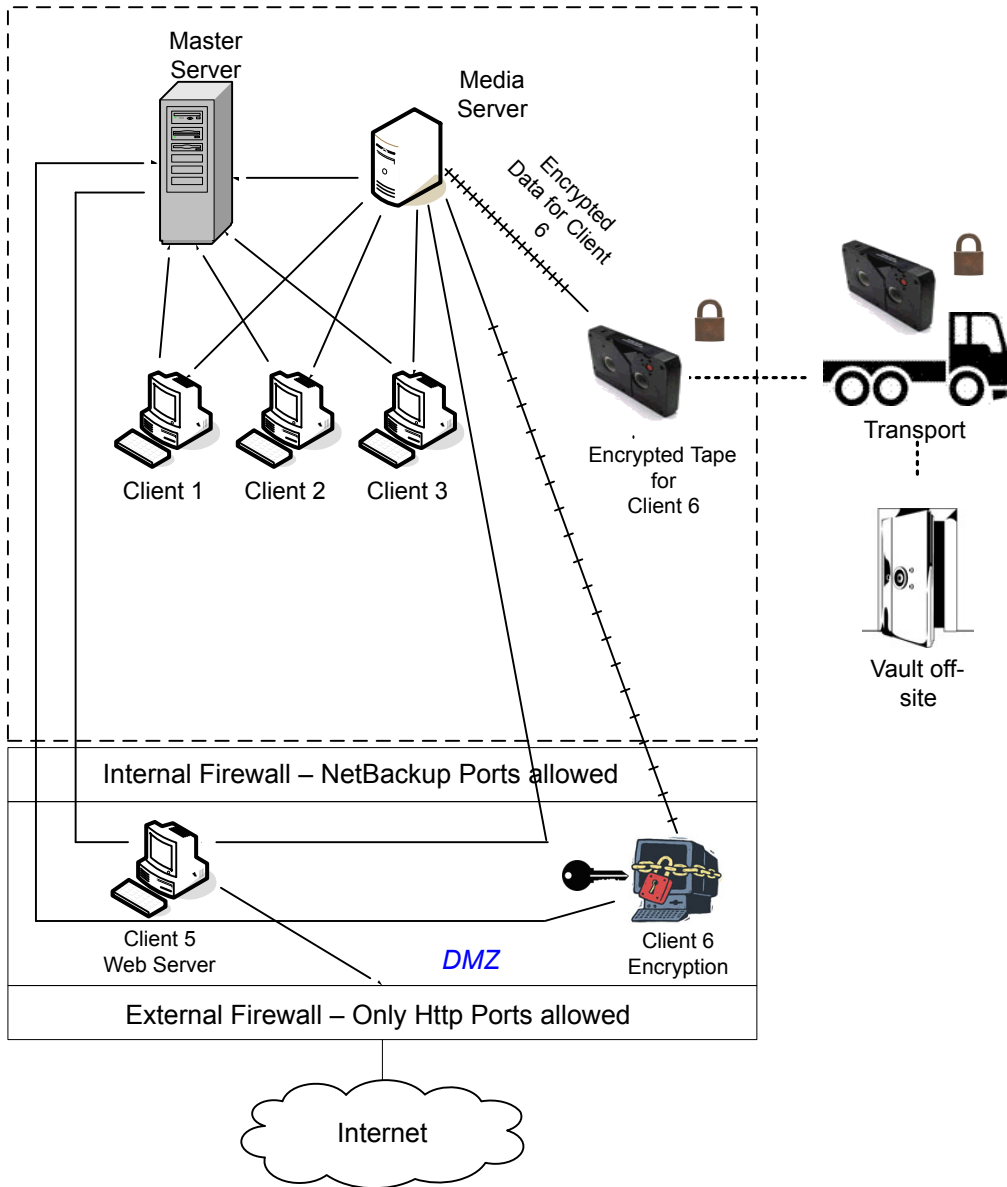
This single datacenter with client side encryption example uses the client side encryption to ensure data confidentiality across the wire as well as on tape. The client side encryption mitigates the risk of passive wire tapping within the organization. The risk of data exposure is reduced as tapes are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

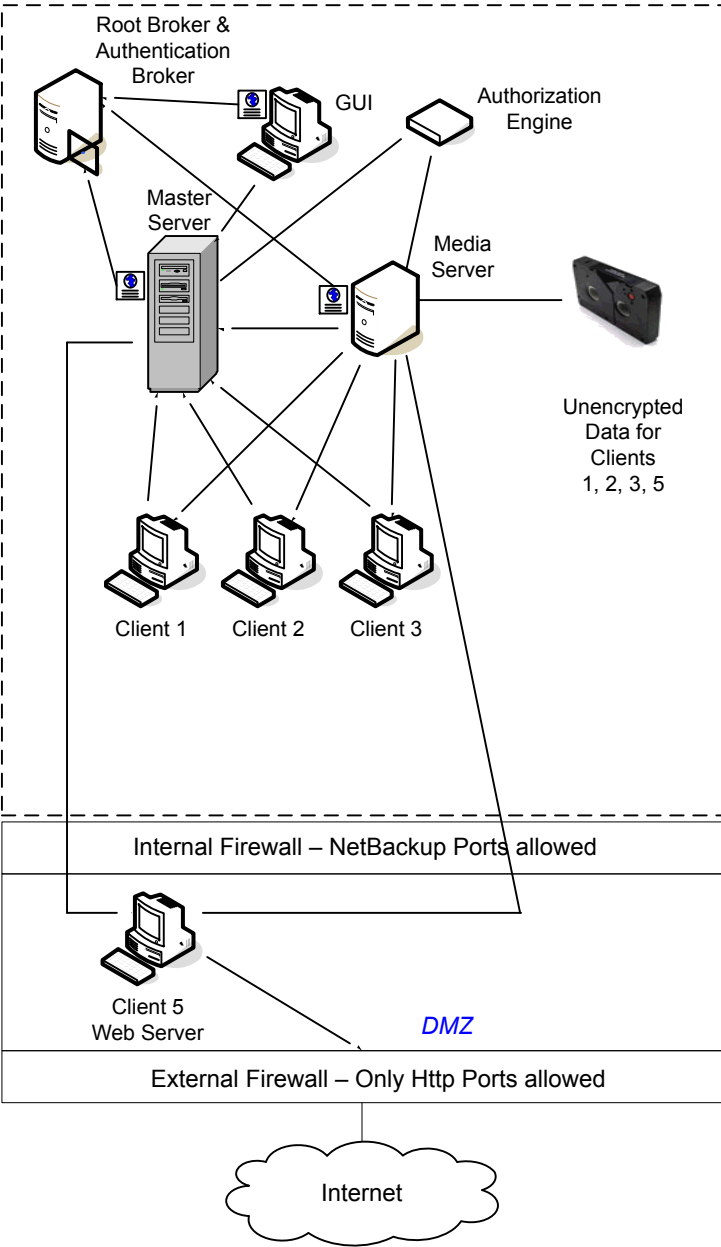
The single datacenter with NBAC on master and media servers includes the following highlights:

- 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	<p>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.</p> <p>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.</p>
Media server	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p>
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.

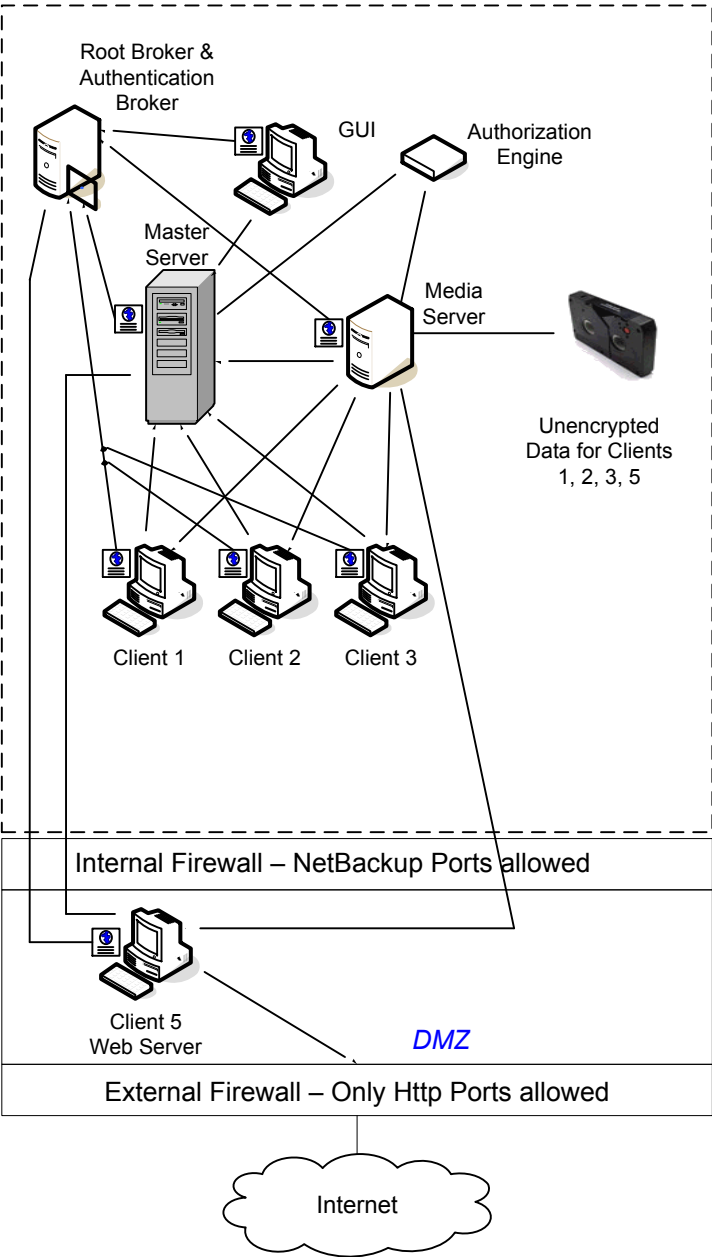
The single datacenter with NBAC complete includes the following highlights:

- 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	<p>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.</p> <p>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.</p>
Media server	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p>
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

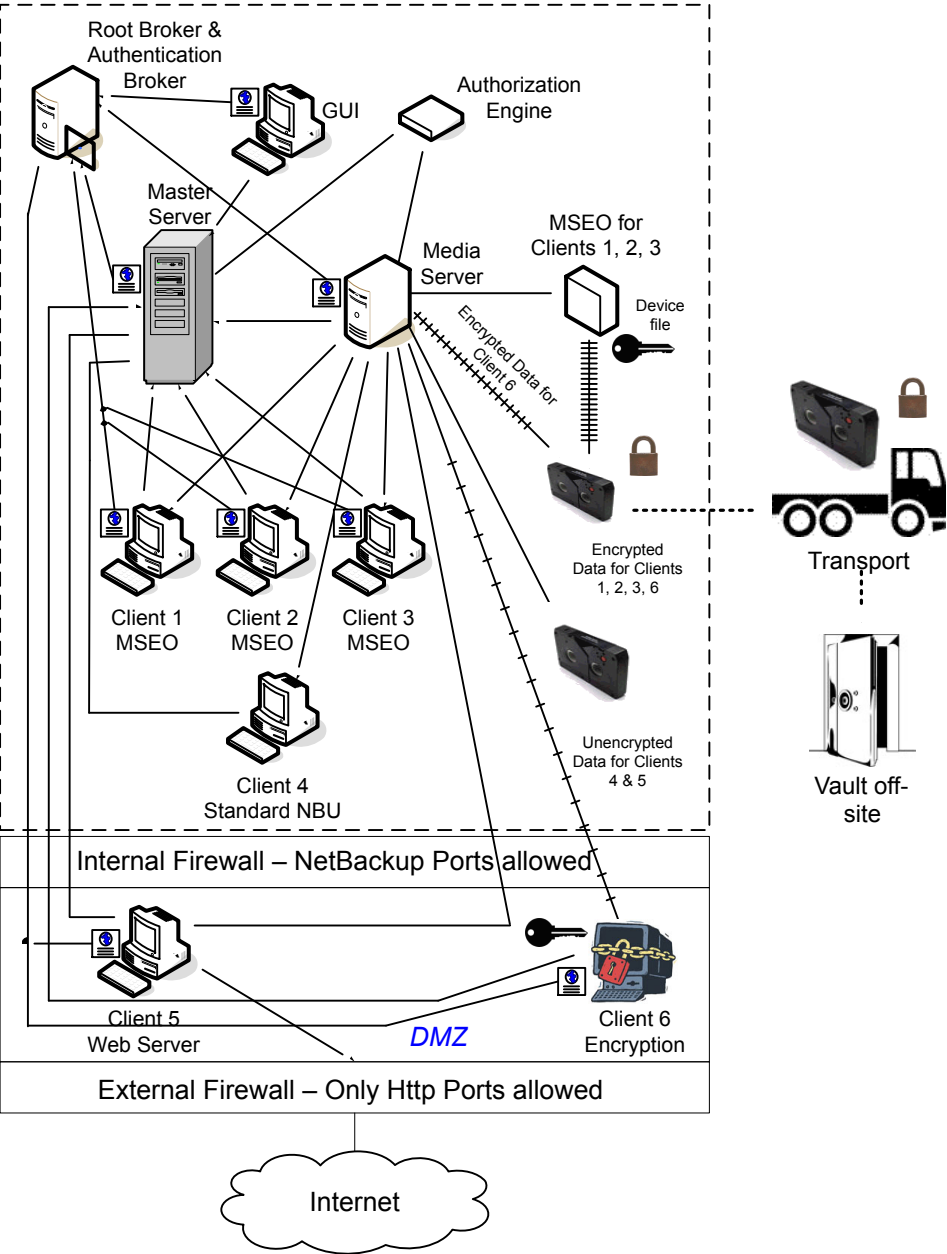
The example of a single datacenter with all security implemented combines all of the previous examples. It represents a very sophisticated environment in which there exists differing requirements for a variety of clients. Client requirements can necessitate using encryption off host (such as an underpowered 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	<p>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.</p> <p>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.</p>
Media server	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p>
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 from 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.

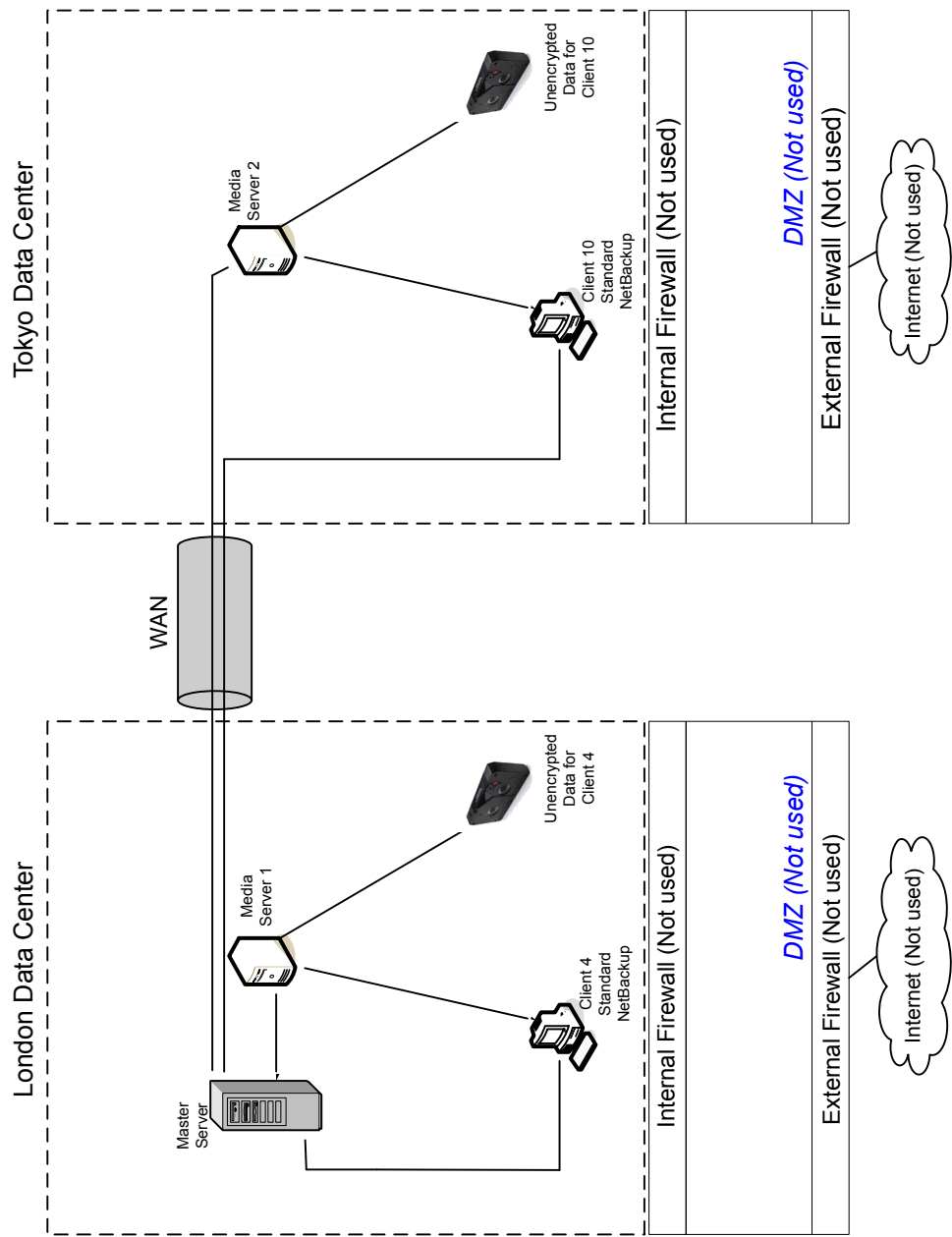
A multi-datacenter includes the hosts that are both internal only and those that expand through the DMZ to the Internet. This configuration typically has centralized naming service for hosts (such as DNS or WINS). It also has a centralized naming service for users (such as NIS or Active Directory).

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.

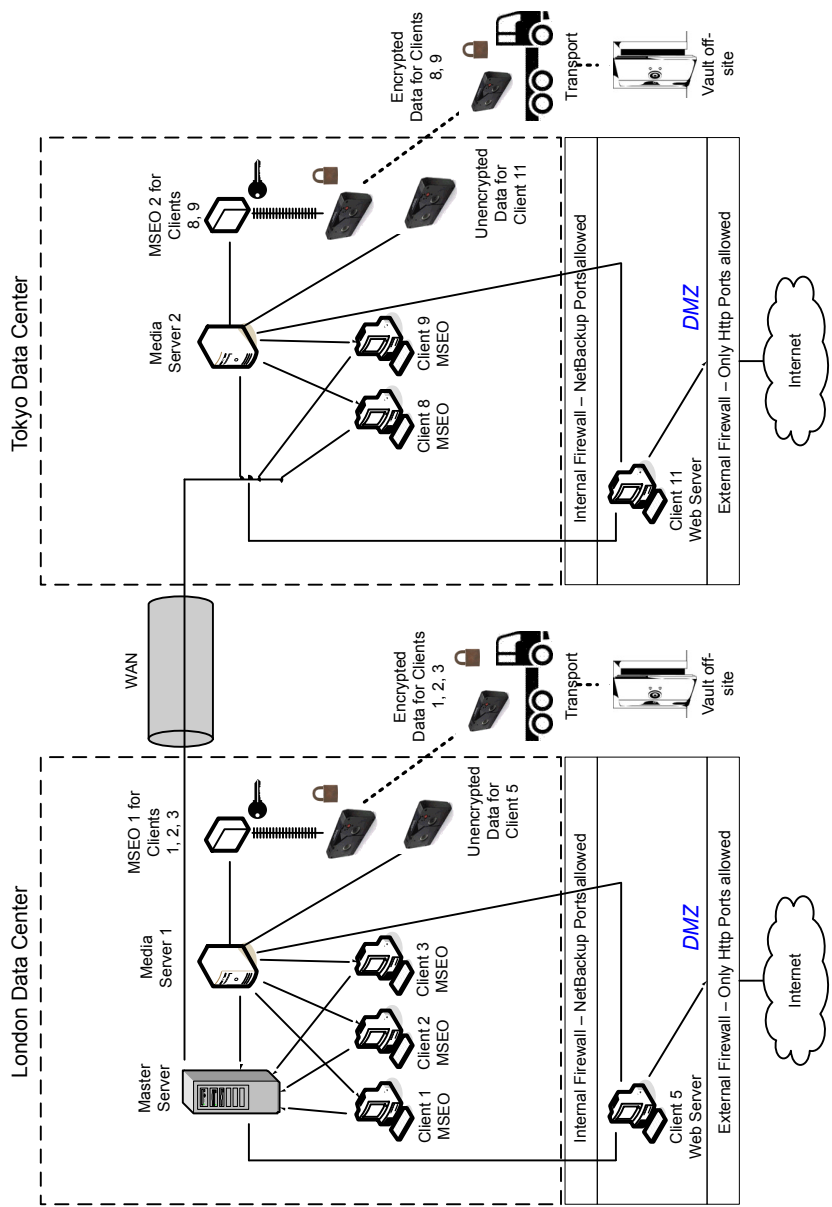
This multi-datacenter example can typically include more than 50 hosts. All externally facing hosts use the Media Server Encryption Option (MSEO). In this example, clients use both encrypted backups for some clients and the MSEO option for other hosts. Data that is too sensitive to be archived off-site 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	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p> <p>Note: To decrypt the data, the key(s) used to encrypt the data must be made available.</p>
Transports	<p>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.</p> <p>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.</p>
Vaults off-site	<p>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.</p> <p>Note: Good disaster recovery protection promotes having the encrypted tapes stored at locations separate from the datacenters.</p>
Clients	<p>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.</p> <p>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.</p>

Table 2-9

NetBackup parts for a multi-datacenter with MSEO implemented

(continued)

Part	Description
Internal firewalls	<p>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.</p>
Demilitarized Zones (DMZs)	<p>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.</p> <p>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.</p>
External firewalls	<p>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.</p> <p>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.</p>
Internet	<p>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.</p>

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.

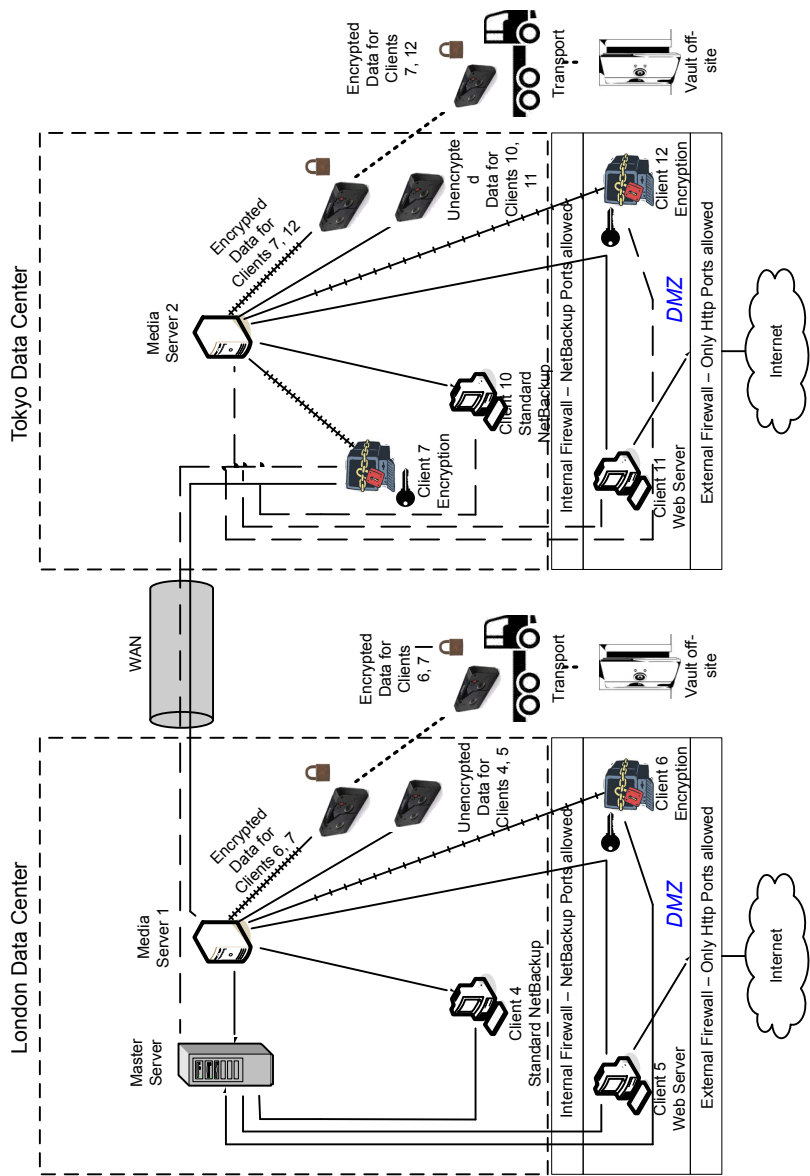
The example multi-datacenter can use client side encryption to ensure data confidentiality across the wire as well as on tape. This encryption helps to mitigate the risk of passive wire tapping within the organization. Risk of data exposure as the tapes are moved off site. This datacenter model assures 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	<p>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.</p> <p>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 7 and 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.</p>
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	<p>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.</p> <p>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.</p> <p>Note: To decrypt the data, the key(s) used to encrypt the data must be made available.</p>
Transports	<p>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.</p> <p>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.</p>
Vaults off-site	<p>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.</p> <p>Note: Storing the encrypted tapes at locations separate from the datacenters promotes good disaster recovery protection.</p>

Table 2-10 NetBackup parts for a multi-datacenter with client side encryption implemented (*continued*)

Part	Description
Clients	<p>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.</p> <p>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.</p>
Internal firewalls	<p>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.</p>
Demilitarized Zones (DMZs)	<p>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.</p> <p>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.</p>

Table 2-10

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

Part	Description
External firewalls	<p>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.</p> <p>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.</p>
Internet	<p>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.</p>

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

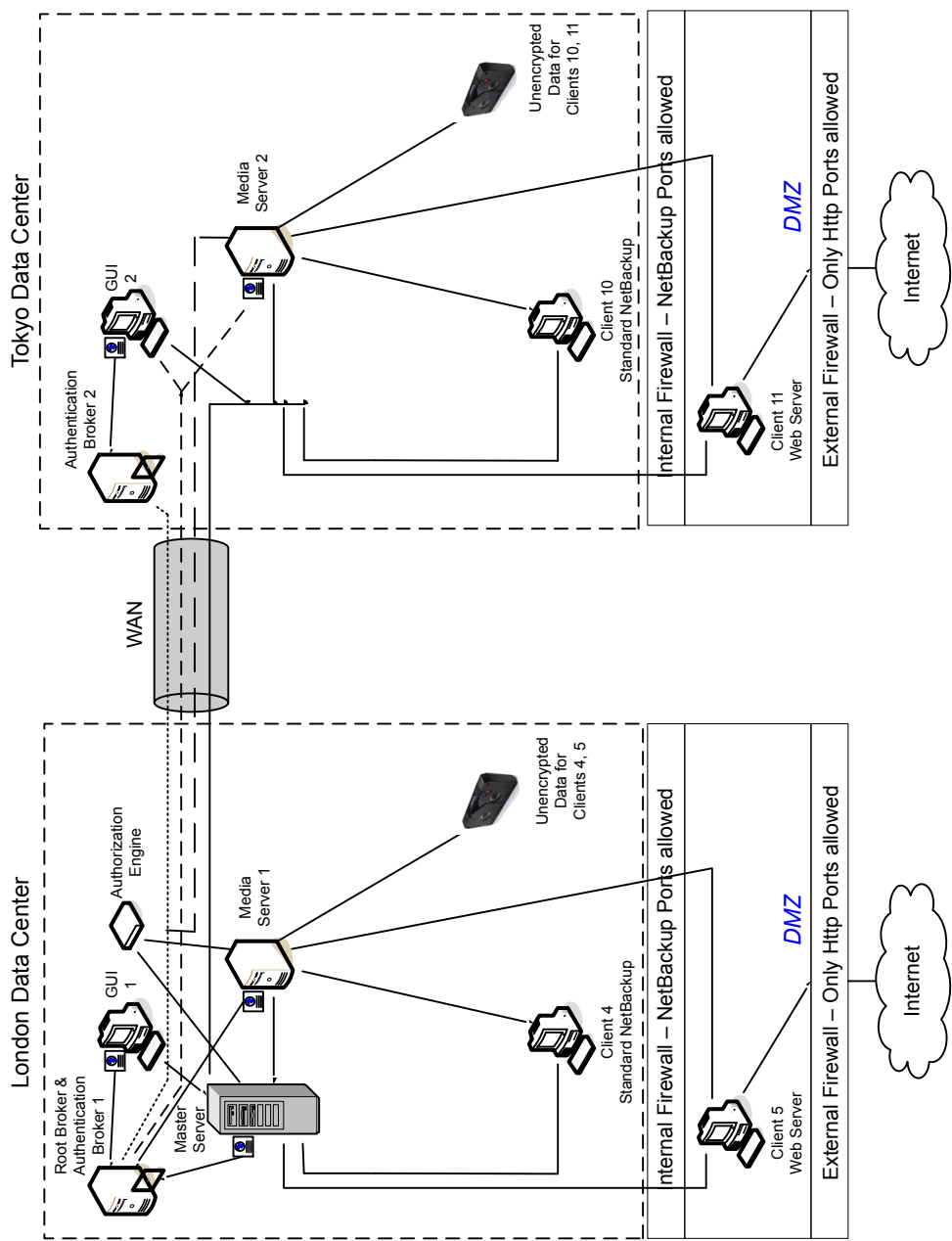
NetBackup. In addition, NBAC can be used to limit the level of access to NetBackup for certain individuals. For example, you can segregate day to day operational control from environmental configuration such as adding new policies, robots, etc.

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	<p>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.</p> <p>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.</p>

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	<p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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</p>
Internal firewalls	<p>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.</p>
Demilitarized Zones (DMZs)	<p>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.</p> <p>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.</p>

Table 2-11

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

Part	Description
External firewalls	<p>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.</p> <p>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.</p>
Internet	<p>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.</p>

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.

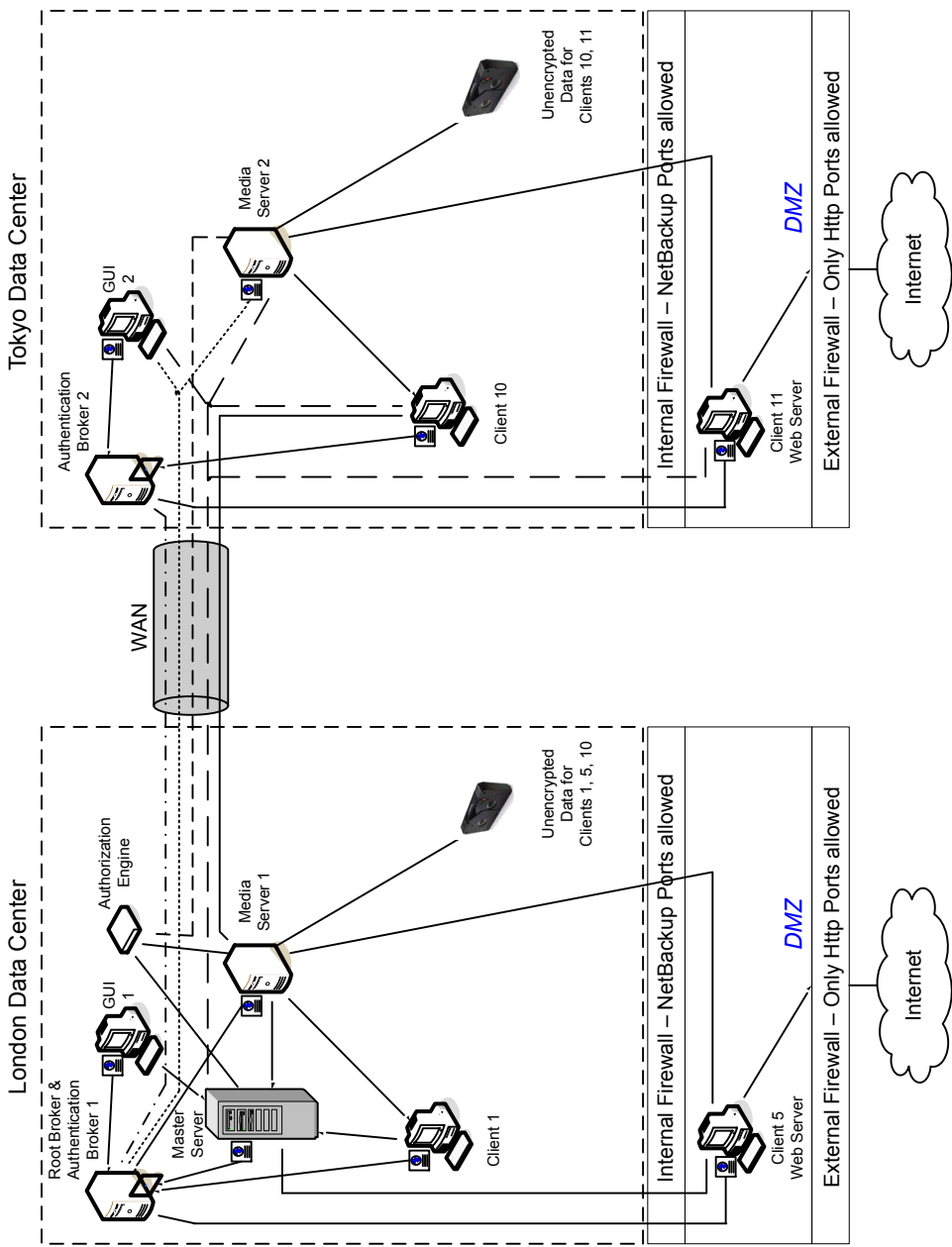
This environment is very similar to the multi-datacenter with NBAC master and media server. The main differences are that all hosts participating in the NetBackup environment are reliably identified using credentials and non-root administrators can manage the NetBackup clients based on configurable levels 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.

Table 2-12 NetBackup parts used for a multi-datacenter with NBAC complete implemented (*continued*)

Part	Description
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.
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	<p>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.</p> <p>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</p>
Internal firewalls	<p>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.</p>
Demilitarized Zones (DMZs)	<p>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.</p> <p>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.</p>

Table 2-12

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

Part	Description
External firewalls	<p>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.</p> <p>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.</p>
Internet	<p>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.</p>

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.

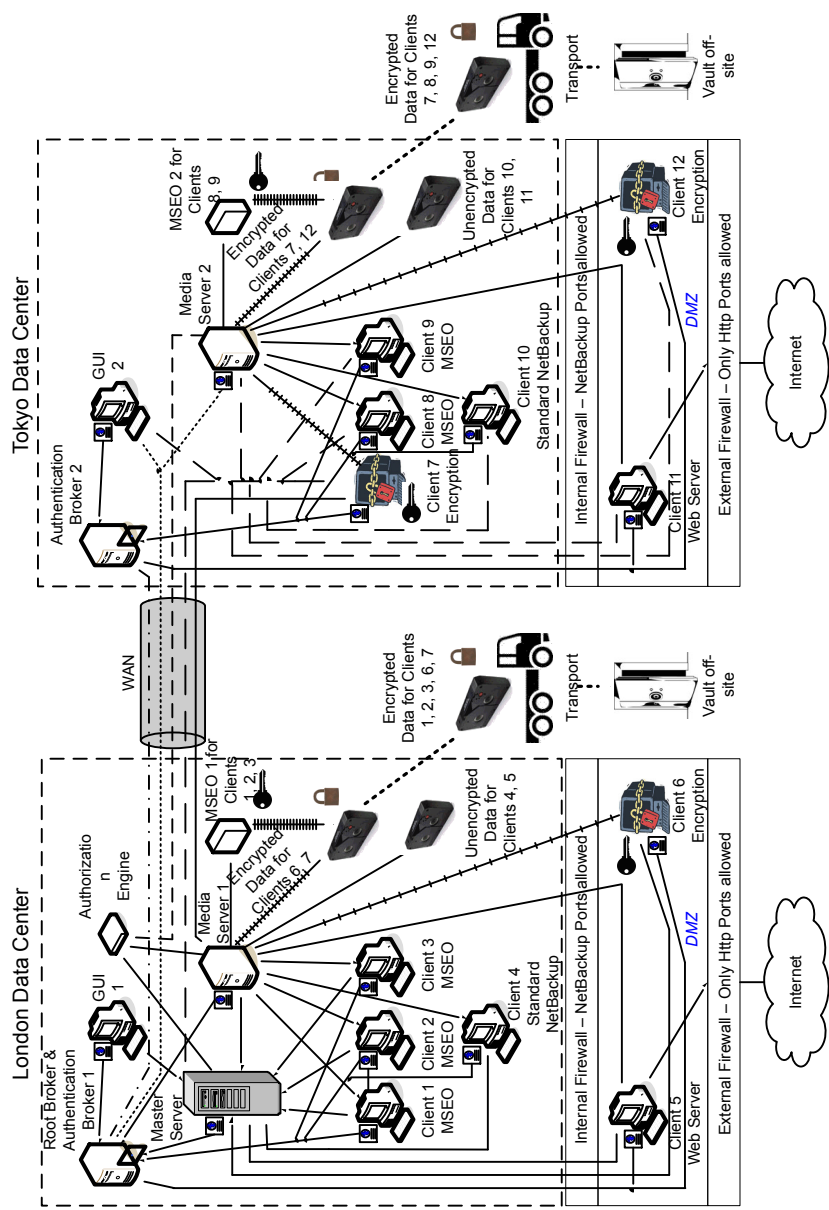
The multi-datacenter with all NetBackup security includes the following highlights:

- 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	<p>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.</p> <p>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.</p>

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	<p>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.</p> <p>Note: To decrypt the data, the key(s) used to encrypt the data must be made available.</p>
Transports	<p>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.</p> <p>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.</p>
Vaults off-site	<p>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.</p> <p>Note: Storing the encrypted tapes at a separate location from the datacenter promotes good disaster recovery protection.</p>
Clients	<p>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.</p> <p>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</p>

Table 2-13

NetBackup parts used for a multi-datacenter with all NetBackup security implemented (continued)

Part	Description
Internal firewalls	<p>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.</p>
Demilitarized Zones (DMZs)	<p>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.</p> <p>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.</p>
External firewalls	<p>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.</p> <p>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.</p>
Internet	<p>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.</p>

Port security

This chapter includes the following topics:

- [About ports](#)
- [NetBackup ports](#)
- [About overriding or modifying port numbers](#)
- [Default 7.5 NetBackup ports](#)
- [Default port numbers for NetBackup 7.5](#)
- [Master server outgoing ports](#)
- [Media server outgoing ports](#)
- [EMM server outgoing ports](#)
- [Client outgoing ports](#)
- [Windows administration console or Java server outgoing ports](#)
- [Java console outgoing ports](#)
- [About configuring ports](#)
- [About accepting remote connections from non-reserved ports](#)
- [Disabling random port assignments in the NetBackup configuration](#)
- [Random port assignments in the media manager configuration](#)
- [Specifying firewall connect options on a NetBackup server or client](#)
- [Ports options](#)
- [BPCD connect-back options](#)

- [Daemon connection port options](#)
- [Specifying firewall connect options for a source computer to apply to specific destination computers](#)
- [Firewall connection options on Media Manager](#)
- [About communication and firewall considerations](#)
- [Ports required to communicate with backup products](#)
- [Web browser to NetBackup Web GUI connection](#)
- [About NetBackup Web GUI to NetBackup server software communication](#)
- [About NetBackup server to NetBackup master server \(NBSL\) communication](#)
- [About SNMP traps](#)
- [Configuring the NetBackup master server to communicate with the OpsCenter server](#)
- [About NetBackup Web GUI/NetBackup server to Sybase database communication](#)
- [About NetBackup Web GUI to NetBackup server email communication](#)
- [About specifying NetBackup-Java connection options](#)
- [Specifying client attributes](#)
- [Specifying ports \(reserved or non-reserved\) that connect a master server or media server to a client](#)
- [Specifying a BPCD connect-back method that connects a master server or media server to a client](#)
- [Specifying a daemon connection port that connects a master server or media server to a client](#)
- [Specifying port ranges](#)
- [BPJAVA_PORT and VNETD_PORT ports](#)
- [Changing the ports for BPCD and BPRD on Windows](#)
- [Disabling the ping on the NetBackup Administration Console on Windows](#)
- [About ICMP pinging NDMP](#)
- [About NDMP in a firewall environment](#)

- [About the ACS storage server interface](#)
- [About known firewall problems when using NetBackup with other products](#)
- [About configuring port usage without a GUI](#)
- [About port usage settings in the NetBackup configuration - bp.conf](#)
- [Port usage-related NetBackup configuration settings](#)
- [About configuring port usage client attribute settings - bpclient command](#)
- [Specifying the bpclient command](#)
- [Port usage-related Media Manager configuration settings - vm.conf](#)

About ports

A modern computer system is capable of running multiple applications simultaneously. Any application may have the requirement to either send or receive one or more packets of data to and from the network.

To distinguish between application input and output flows of data, the operating system creates a separate input or output queue of data packets. These system queues are known within the TCP/IP terminology as ports.

NetBackup uses two classes of ports, commonly referred to as reserved ports and non-reserved ports. The following table describes the classes of security ports.

Table 3-1 Classes of security ports

Class	Description
Reserved ports	<p>Specifies the ports that are less than 1024 and are (normally) only accessible to operating system components.</p> <p>Note: Reserved ports are only used for back-rev connections.</p> <p>Note: Callback is only used for back-rev connections.</p>
Non-reserved ports	<p>Specifies the ports that are 1024 and greater and are accessible by user applications.</p>

NetBackup ports

NetBackup uses TCP/IP connections to communicate between one or more TCP/IP ports. Depending on the type of operation and configuration on the environment, different ports are required to enable the connections. NetBackup has different requirements for operations such as backup, restore, and administration.

The following table describes the ports that NetBackup uses to enable the TPC/IP connections.

Table 3-2 Ports that NetBackup uses to enable TPC/IP connections

Port	Description
Registered ports	<p>Specifies the 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, <code>bpcd</code>, is 13782. A system configuration file can be used to override the default port numbers for each daemon.</p> <p>These files are as follows:</p> <ul style="list-style-type: none">■ On UNIX systems, you can specify ports in the <code>/etc/services</code> file.■ On Windows systems, you can specify ports in the <code>%systemroot%\System32\drivers\etc\services</code> file.
Dynamically allocated ports	<p>Specifies the ports that are assigned from the ranges that you can specify on NetBackup clients and servers.</p> <p>In addition to the range of numbers, you can configure the following for dynamically allocated ports:</p> <ul style="list-style-type: none">■ NetBackup selects a port number at random from the allowed range. Or it starts at the top of the range and uses the first one available.

About overriding or modifying port numbers

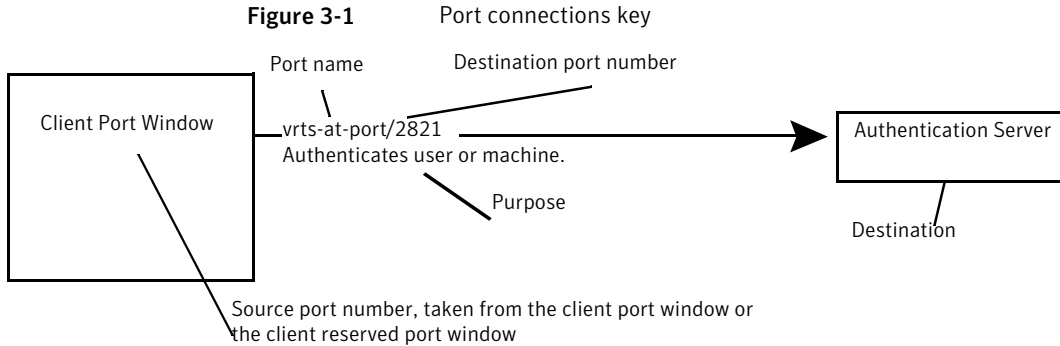
Symantec suggests that you use the default port number settings for NetBackup services and Internet service ports.

If you need to modify the port number for a daemon, make sure that you modify the port number. It must be the same for all NetBackup master servers, media servers, and client systems that communicate with each other. When necessary, you can log a support call to Symantec Technical Services. You should inform the technical support representative of non-standard ports throughout your NetBackup environment.

Default 7.5 NetBackup ports

This topic displays the NetBackup connections and ports that are used in NetBackup 7.5 systems.

The following figure shows an example port connection and explains how the port connections are represented.



Default port numbers for NetBackup 7.5

A base NetBackup installation may not have all of the daemons available. Some of the daemons are enabled or used by add-on products, and the right-most column of the following table indicates which product uses the daemon.

NetBackup 7.5 uses additional ports when connected to NetBackup 7.5 and earlier. See [“Default 7.5 NetBackup ports”](#) on page 104. for more details.

The following table lists the ports that are used within the NetBackup environment.

Table 3-3 Port numbers for NetBackup 7.5

Daemon or Process	Port number	Product	Purpose
VNETD	13724	NetBackup	Network daemon
VERITAS_PBX	1556	VxPBX	Symantec Private Branch Exchange Service
VRTS-AT-PORT	13783	VxAT	NetBackup authentication service . The <code>nbatd</code> process listens on port 13783 for back-level media servers and clients. The NetBackup 7.5 media servers and clients connect using the PBX port .
VRTS-AUTH-PORT	13722	VxAZ	NetBackup Authorization Service. The <code>nbazd</code> process listens on port 13722 for back level media servers and clients. The NetBackup 7.5 media servers and clients connects using the PBX port

Master server outgoing ports

The master server uses outgoing ports to the EMM server, media server, clients, and the NetBackup Product Authentication and Authorization Service (shown as vxss Server). The Java console and administration console or Java Server are also included.

The following figures show the port connections between various NetBackup components.

Note: In following figure showing part 2, the master server client port window connects to the authentication server using port 13783 only when using back-level media servers and clients.

Figure 3-2 indicates part one of the master server minimal outgoing port connections.

Figure 3-2 7.5 master server minimal outgoing port connections - part 1

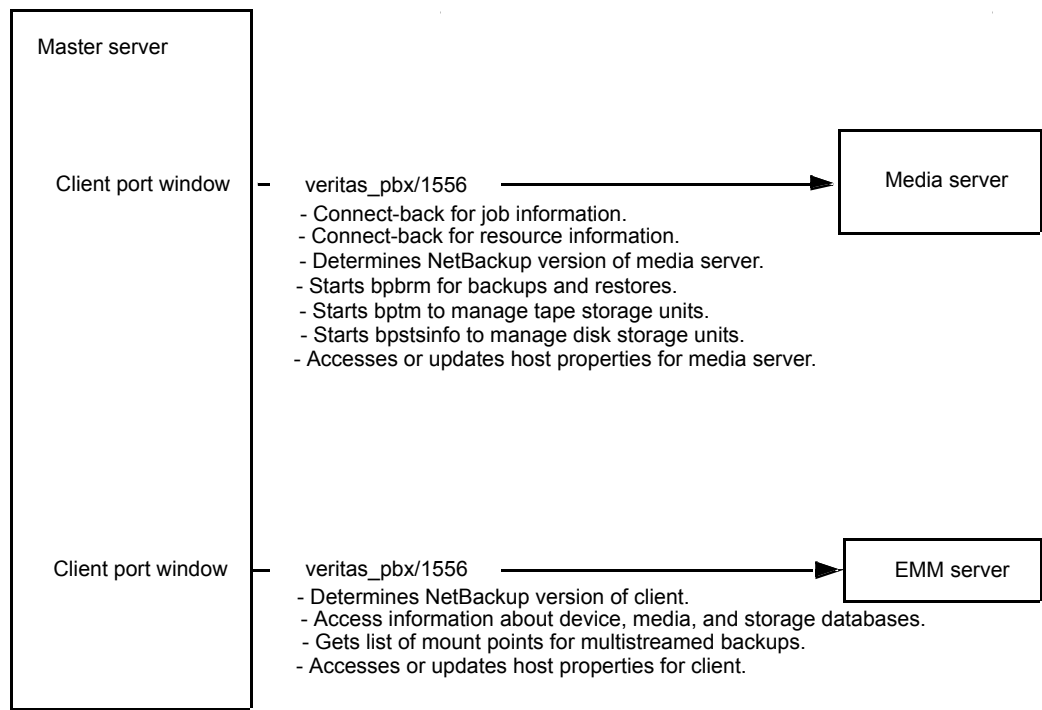
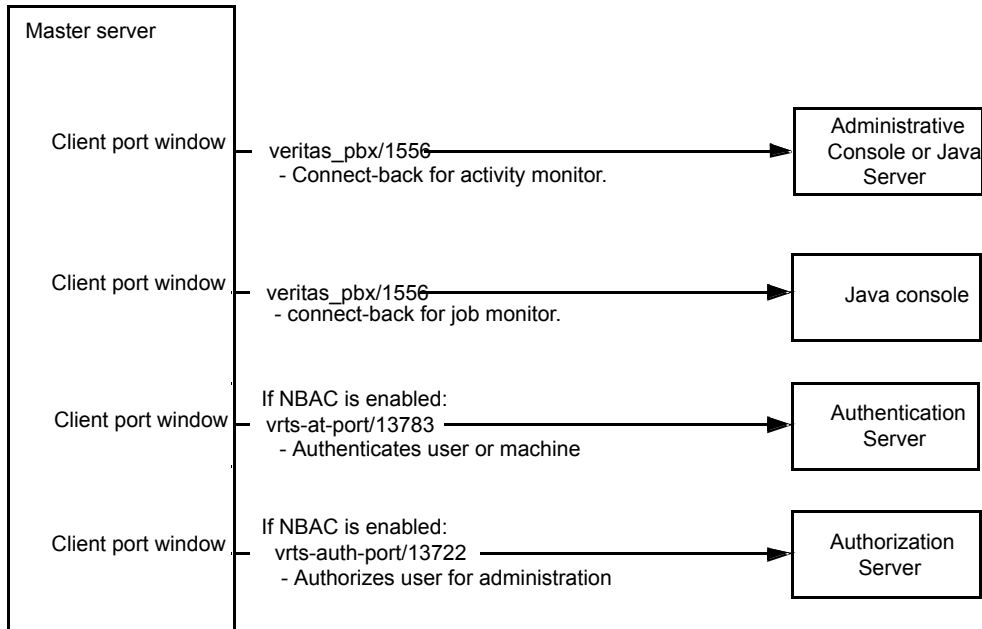


Figure 3-3 indicates part two of the master server minimal outgoing port connections.

Figure 3-3 7.5 master server minimal outgoing port connections - part 2



Media server outgoing ports

The media server uses outgoing ports to the EMM server, other media servers, clients, and the NetBackup Product Authentication and Authorization Service (shown as vxss Server). The media server also uses outgoing ports to the administration console or Java Server.

Figure 3-4 indicates part one of the 7.5 media server minimum outgoing port connections.

Figure 3-4 7.5 media server minimal outgoing port connections - part 1

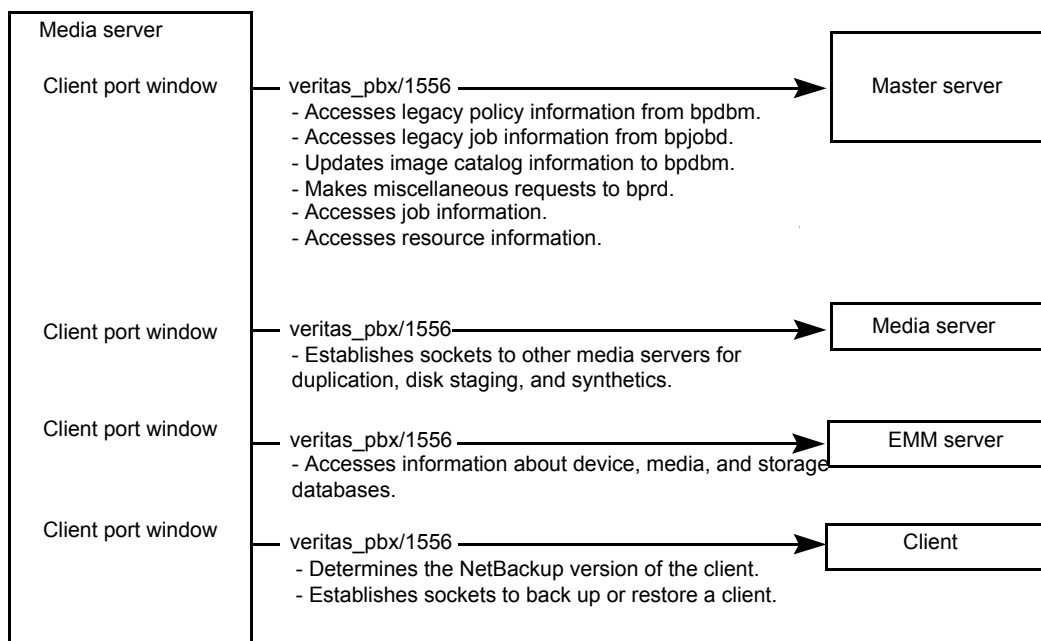
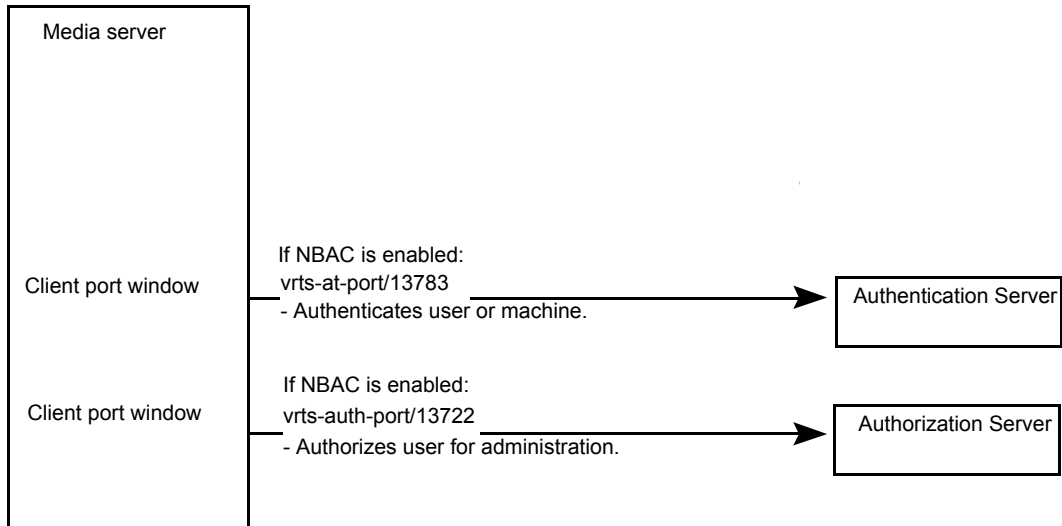


Figure 3-5 indicates part two of the 7.5 media server minimal outgoing port connections.

Figure 3-5 7.5 media server minimal outgoing port connections - part 2

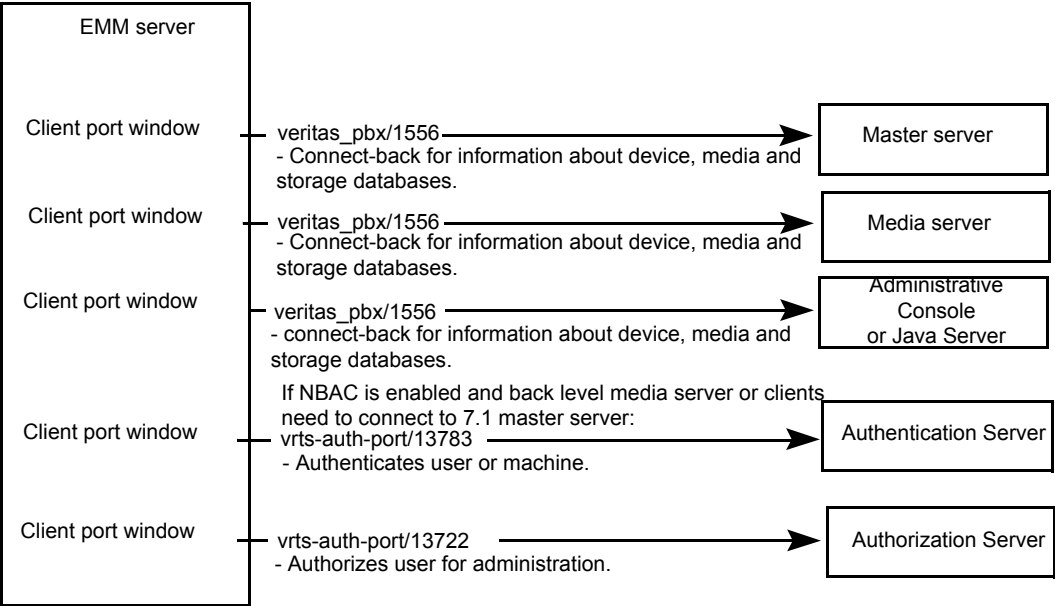


EMM server outgoing ports

The EMM server uses outgoing ports to the NetBackup Product Authentication and Authorization Service (shown as vxSS Server). The EMM server also uses outgoing ports to the media servers, master server, and the administration console or Java Server.

[Figure 3-6](#) indicates the Enterprise Media Manager (EMM) minimal outgoing port connections.

Figure 3-6 Enterprise Media Manager (EMM) minimal outgoing port connections

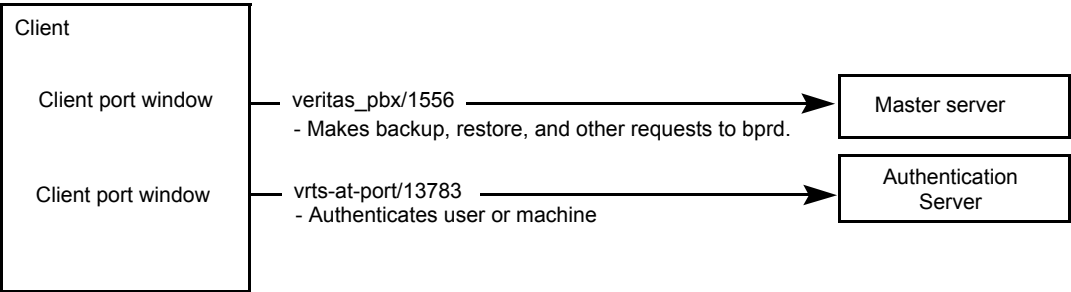


Client outgoing ports

The client uses outgoing ports to the NetBackup Product Authentication and Authorization Service (shown as vxss Server) and master server.

Figure 3-7 indicates the 7.5 client minimal outgoing port connections.

Figure 3-7 7.5 client minimal outgoing port connections

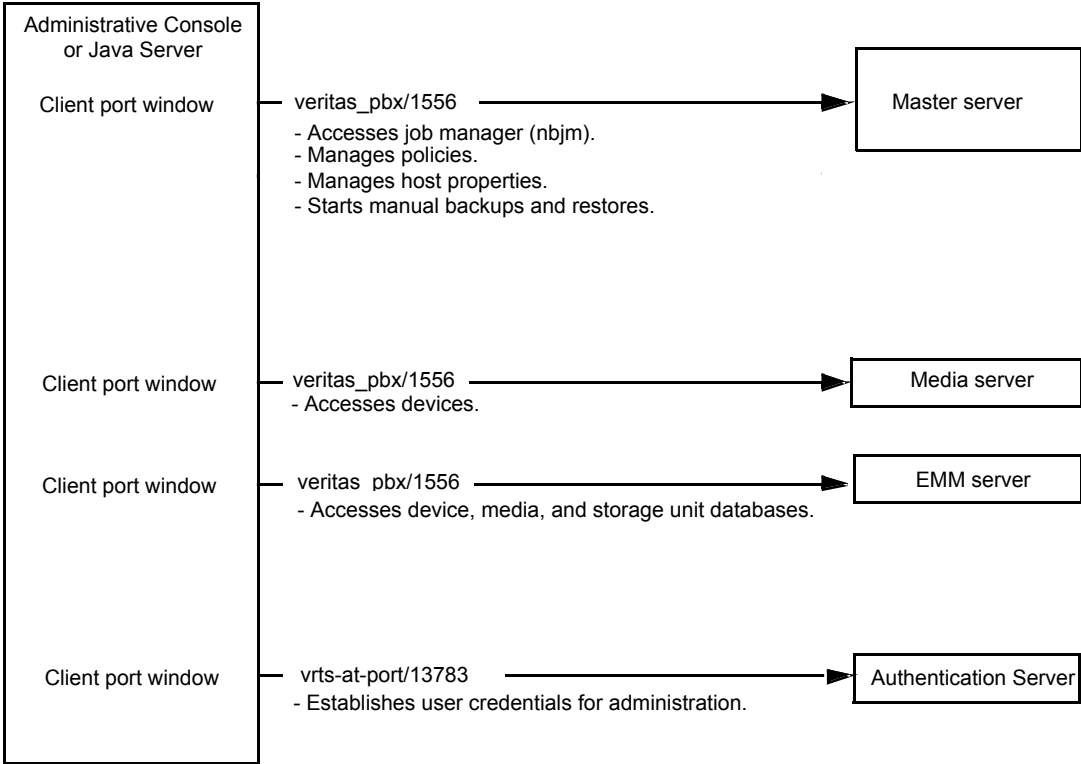


Windows administration console or Java server outgoing ports

The Windows administration console or Java Server uses outgoing ports to the EMM server, master server, and media server. The Windows administration console or Java Server also uses outgoing ports to the NetBackup Product Authentication and Authorization Service (shown as vxss Server).

Figure 3-8 indicates the Java server or Windows Administration Console minimal outgoing port connections.

Figure 3-8 Java server or Windows Administration Console minimal outgoing port connections



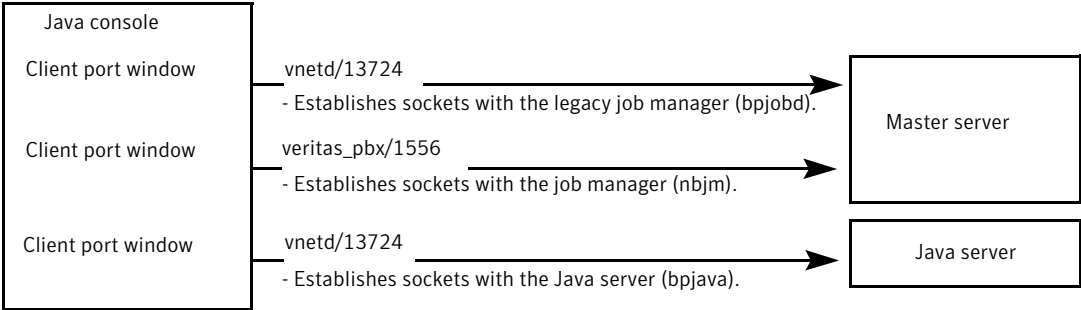
Java console outgoing ports

The Java console uses outgoing ports to the master server and administration console or Java Server.

Note: In the following figure the only the port used by the java console for NetBackup 7.5 is the `pbx` port 1556. The 13724 ports are used by back-level java consoles only.

Figure 3-9 indicates the Java console minimal outgoing port connections.

Figure 3-9 Java console minimal outgoing port connections



About configuring ports

You can configure the various non-default ports that you might need in your environment to support firewalls and other network features.

You can set the configuration options from both the graphical user interface (for Java or Windows) or from the command line (on UNIX or Windows). Unless otherwise specified, the procedures describe how to set the configuration options using the graphical user interface.

You can set configuration options from the command line. See [“About configuring port usage without a GUI”](#) on page 141.

About accepting remote connections from non-reserved ports

This property specifies whether the NetBackup client service (`bpcd`) can accept remote connections from non-reserved ports. (Non-reserved ports have port numbers of 1024 or greater.) The default is that this property is enabled.

This property no longer applies in NetBackup 7.5. For information about this property, see the documentation from a previous release.

Disabling random port assignments in the NetBackup configuration

The **Use random port assignments** setting specifies when NetBackup requires a port number to be used for communication with NetBackup on other computers. It can randomly choose a port from those that are free in the allowed range. This setting is the default behavior.

For example, if the range is from 1023 through 5000, it chooses randomly from the numbers in this range.

If this setting is changed from the default, 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. This setting is enabled by default.

The following procedure shows how to disable random port assignments from the Java or Windows interface.

To disable random port assignments from the Java or Windows interface

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.
- 2 Double click the host you want to configure.
- 3 Click **Port Ranges**.
- 4 Uncheck **Use random port assignments**.

Random port assignments in the media manager configuration

The random ports setting for the Media Manager works the same way that it does for the general NetBackup configuration.

The **Use random port assignments** setting specifies that the Media Manager requires a port number for communication with Media Manager on other computers. It can randomly choose one from those that are free in the allowed range. This setting is the default behavior.

For example, if the range is from 1023 through 5000, it chooses randomly from the numbers in this range.

If this setting is changed from the default, Media Manager 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, Media Manager chooses 5000, assuming that it is free. If 5000 is used, Media Manager chooses port 4999. This setting is enabled by default.

Note: Specify the same port selection for NetBackup as you do for Media Manager. That is, if you specify random ports in the NetBackup configuration, also specify random ports in the Media Manager configuration.

Specifying firewall connect options on a NetBackup server or client

The connect options specify how connections are made between computers. You can specify the settings on the computer that initiates the connection (source computer) for the server to which it connects (destination computer).

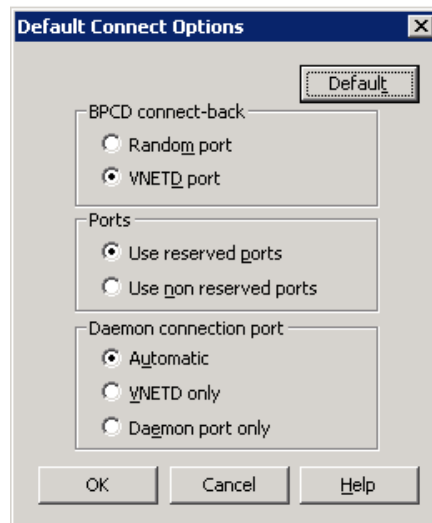
If there is a firewall between the master server and the media servers, you can specify the settings from the master server (source computer). The settings can be made for each of the media servers (destination computers) to which the master server connects.

You can define the connect options between the source computer and specific destination computers. If the source computer is running NetBackup 7.5 or later, you also can set the default connect options to apply to all of the other destination computers.

To specify Firewall default connect options for a NetBackup 7.5 or later source computer from the Java or Windows interface

- 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:



You can set the following connection options from the display:

- Ports (reserved versus non-reserved)
See [“Ports options”](#) on page 116.
- BPCD connect-back
See [“BPCD connect-back options”](#) on page 116.
- Daemon connection port
See [“Daemon connection port options”](#) on page 117.

If the source computer is a NetBackup client (not a server), only the Daemon connection port setting applies.

Ports options

In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**. After you have double clicked the host that you want to configure, click **Firewall** and **Change** in the **Default Connect Options** pane. Then, the **Use non-reserved ports** setting in the **Default Connect Options** window determines whether the source computer connects to `bpcd` on destination computers using a reserved or a non-reserved source port number.

By default, the **Use reserved ports** setting is specified. This means that the source computer connects to `bpcd` on the destination computers that use a reserved port number.

If you change the default, the **Use non-reserved ports** setting goes into effect. This means that the source computer connects to `bpcd` on destination computers using a non-reserved port number. In addition, if the **Use non-reserved ports** setting is specified, you must configure the host to allow connections on non-reserved ports.

Review the reconfiguration information. See [“About accepting remote connections from non-reserved ports”](#) on page 113.

Note: This setting generally has no effect if both the source and the destination computers are NetBackup 7.5 or later. By default, non-reserved ports are always used in that case. See the note in the Daemon connection port description.

See [“Daemon connection port options”](#) on page 117.

See [“Specifying firewall connect options on a NetBackup server or client”](#) on page 114.

BPCD connect-back options

In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**. After you have double clicked the host that you want to configure, click **Firewall** and **Change** in the **Default Connect Options** pane. The **BPCD connect-back** box in the **Default Connect Options** window specifies whether the host can be connected to by another computer using the legacy `bpcd` random port callback method or whether the host can be connected to by using the Veritas Network Daemon (`vnetd`). By default for NetBackup 5.1 or earlier, the BPCD connect-back option is **Random port**. This means that the connection uses the legacy random port callback method.

If the **VNETD port** option is selected in the **BPCD connect-back** box, other computers connect to the host using `vnetd`, which does not require random port callback. This setting is the default for NetBackup 7.5 and later.

Note: This setting generally has no effect if both the source and the destination computers are NetBackup 7.5 or later. By default, callback is not used in that case. See the note in the Daemon connection port description.

See [“Daemon connection port options”](#) on page 117.

Daemon connection port options

Note: This option only affects connections to NetBackup 7.5 and earlier. For connections to NetBackup 7.5 and later, the `veritas_pbx` port is used.

In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**. After you have double clicked the host that you want to configure, click **Firewall** and **Change** in the **Default Connect Options** pane. The **Daemon connection port** list box specifies one of the options in the following table for computers to use to connect to the host.

Table 3-4 Daemon connection port options

Option	Description
Automatic	(Default for NetBackup 6.0 and later). Specifies that connections to the daemons on the host be made using <code>vnetd</code> if possible. If it is not possible to use <code>vnetd</code> , the connection is made using the daemon's legacy port number.
VNETD only	Specifies that connections to the daemons on the host be made using <code>vnetd</code> only. If your firewall rules prevent connecting to the host using the legacy port number, make sure that <code>vnetd</code> is used.
Daemon port only	(Default for NetBackup 5.1 and earlier). Specifies that connections to the host are made using only the legacy port number.

Note: For NetBackup 5.1 and earlier, connections to `bpcd` are always made with the legacy `bpcd` port number. Connections to `bpcd` can be made with the `vnetd` port number if both the source and the destination computers are NetBackup 7.5 or later. When `bpcd` connections are made using the `vnetd` port number, the **Ports** and **BPCD connect-back** options are ignored. The default in that case is to use non-reserved source port numbers, the `vnetd` destination port number, and no callback.

Note: Connections to `veritas_pbx`, `veritas-at-port`, and `veritas-auth-port` are not affected by this setting. Those connections always use the legacy or IANA defined port numbers.

Specifying firewall connect options for a source computer to apply to specific destination computers

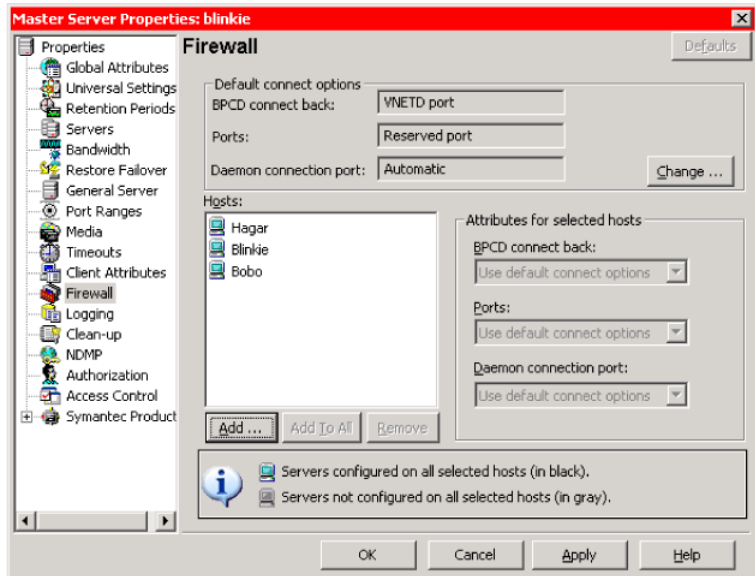
The following procedure describes how to specify Firewall connect options for a source computer to apply to specific destination computers from the Java or Windows interface.

To specify Firewall connect options for a source computer to apply to specific destination computers from the Java or Windows interface

- 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 Select the appropriate values from the **BPCD connect-back**, **Ports**, and **Daemon connection port** options. The values available in these menu items include the values available in the **Default Connect Options** window that are described previously. You can also specify the **Use default connect** options. This means that the value for the specified destination host uses the value from **Default Connect Options** window instead.

Firewall connection options on Media Manager

In NetBackup 7.5 and later, the Media Manager defaults to the NetBackup connection options that are described previously unless overridden by the `vm.conf` `CONNECT_OPTION` entries. For NetBackup 5.1 and earlier, Media Manager connection options must be specified in `vm.conf`.

Unlike the NetBackup master servers or clients, there is no graphical user interface to change the firewall connections for Media Manager.

You can review information on changing the `vm.conf` configuration file for Media Manager.

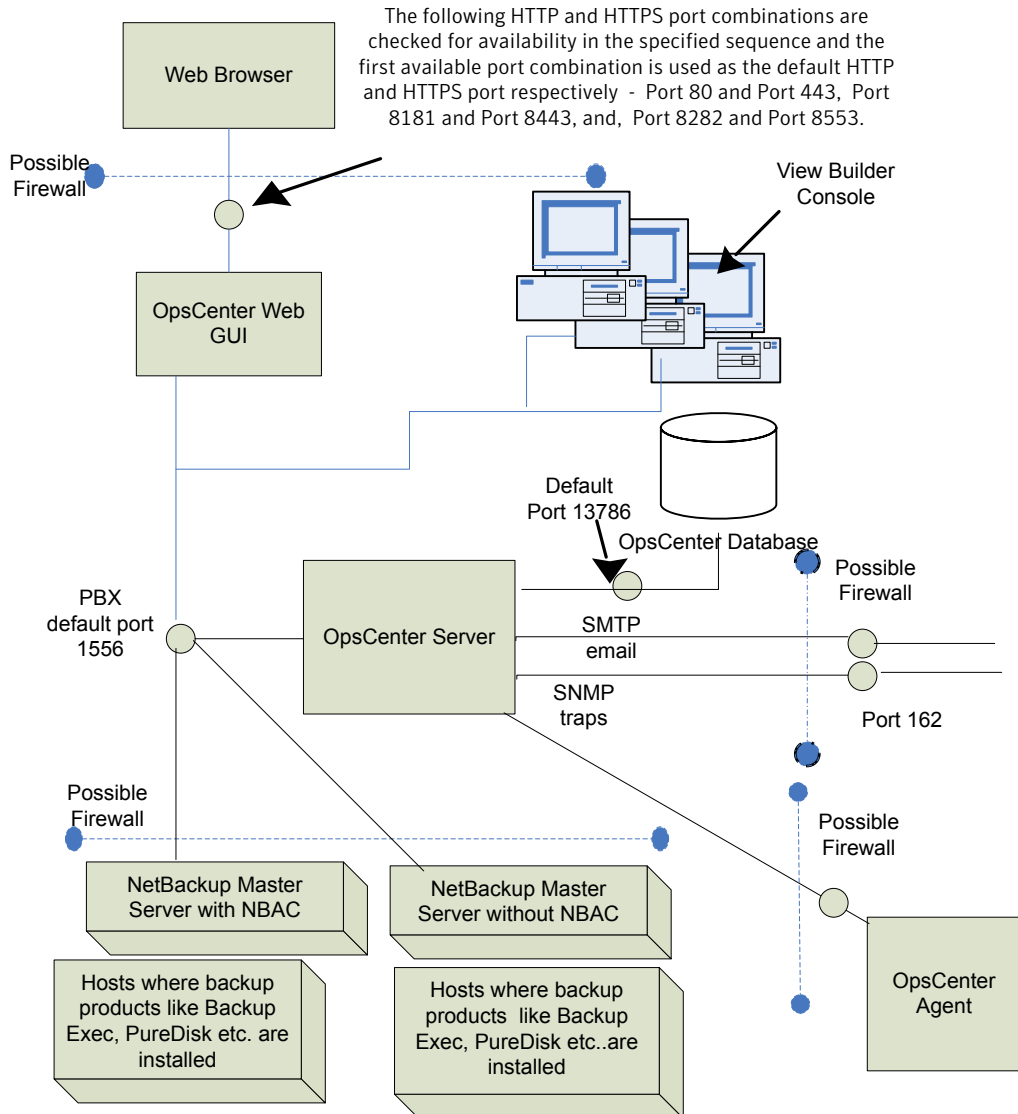
See [“Port usage-related Media Manager configuration settings - vm.conf”](#) on page 150. for more information about the `vm.conf` configuration file.

xSee [“About configuring port usage without a GUI”](#) on page 141.

About communication and firewall considerations

[Figure 3-10](#) shows the key NetBackup components and the communication ports that are used.

Figure 3-10 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 NetBackup, Backup Exec, PureDisk, TSM etc.

[Table 3-5](#) lists the ports that must be opened on NetBackup Agent to collect data from various backup products.

Table 3-5 Ports required to communicate with other backup product

Backup product	Communication	Port number
NetBackup	<p>NetBackup (NetBackup data collector) communicates with the NetBackup master server.</p> <p>13782 port should be used to connect to the NetBackup master server and 13724 port should be used to respond to the Agent host. The response is sent on a port in the reserved port range 512-1023 if not configured to use <code>vnetd</code></p> <p>The following processes are used for NetBackup data collection:</p> <ul style="list-style-type: none">■ <code>bpererror.exe</code>■ <code>bpretlevel.exe</code>■ <code>bpimagerlist.exe</code>	13782 & 13724
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 <code>atssl</code>	443 (HTTPS) 2821 (AT)
TSM	NetBackup (TSM data collector) communicates with TSM Server using TSM CLI <code>dsmadmc</code>	1500
EMC NetWorker	NetBackup (EMC data collector) communicates with EMC Server locally	A local host communication

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 3-6](#) lists how the default HTTP and HTTPS ports are selected.

Table 3-6 Default HTTP and HTTPS ports

Sr. No.	HTTP port number	HTTPS port number	Description
1.	80	443	<p>Port 80 and Port 443 are checked for availability.</p> <ul style="list-style-type: none"> ■ 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.
2.	8181	8443	<p>Port 8181 and Port 8443 are checked for availability.</p> <ul style="list-style-type: none"> ■ If port 8181 and 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	<p>Port 8282 and Port 8553 are checked for availability.</p>

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.

Configuring the NetBackup master server to communicate with the OpsCenter server

You can configure the NetBackup master server to communicate with the OpsCenter server.

Use the following steps to configure the NetBackup master server to communicate with the OpsCenter server.

- 1 Log into the master server as UNIX root or windows administrator.
- 2 Change directory to <NETBACKUP_INSTALL_PATH>/bin/admincmd.
- 3 Run the following CLI:

```
nbregopsc -add <OpsCenter server name>.
```

This CLI adds the OpsCenter server name to NetBackup and also the NetBackup master server name as a managed entity to the OpsCenter. It also establishes a trust relationship with OpsCenter server on the master server. Log in to the OpsCenter server and establish a trust relationship with the NetBackup master server. See the *NetBackup OpsCenter Administrator's Guide* for more details on adding the master server.

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 specifying NetBackup-Java connection options

There is no graphical user interface to use to change the NBJAVA_CONNECT_OPTION, unlike the NetBackup master servers or clients.

The /usr/opensv/java/nbj.conf file on UNIX and the nbjava_install_path\java\setconf.bat file on Windows contain the configuration settings that you might want to change if you configure ports. These options are as follows:

```
NBJAVA_CONNECT_OPTION=setting
```

```
NBJAVA_CLIENT_PORT_WINDOW=n m
```

For information on changing these settings, see one of the following manuals:

- *NetBackup Administrator's Guide for UNIX and Linux, Volume I*
- *NetBackup Administrator's Guide for Windows, Volume I*

Specifying client attributes

The **Client Attributes** tab lets you specify several connect options. These options all define how a master server or media server can connect to a client.

For example, you can specify reserved or non-reserved ports.

Note: If a master server or media server is configured to connect to a client using non-reserved ports, use the Specifying ports procedure that follows.

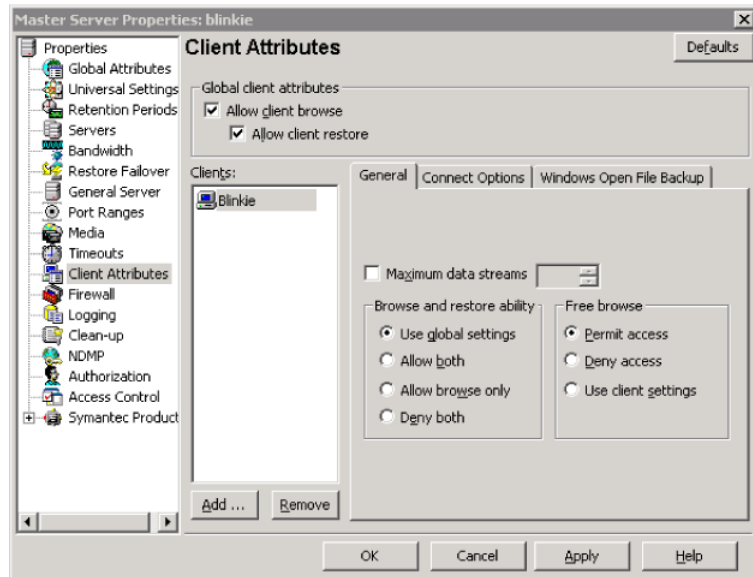
Refer to the See [“Specifying ports \(reserved or non-reserved\) that connect a master server or media server to a client”](#) on page 127., to configure that client to accept remote connections from non-reserved ports.

To specify client attributes from the Java or Windows interface

- 1 In the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Master Servers**.
- 2 Double click the host that you want to configure.
- 3 Click **Client Attributes**.

A display similar to the following appears:

Specifying ports (reserved or non-reserved) that connect a master server or media server to a client



The following topics describe how to enable or disable the following settings:

- Specifying ports (reserved or non-reserved ports)
See [“Specifying ports \(reserved or non-reserved\) that connect a master server or media server to a client”](#) on page 127.
- Specifying a BPCD connect-back method
See [“Specifying a BPCD connect-back method that connects a master server or media server to a client”](#) on page 130.
- Specifying a Daemon connection port
See [“Specifying a daemon connection port that connects a master server or media server to a client”](#) on page 132.

Specifying ports (reserved or non-reserved) that connect a master server or media server to a client

By default, a master server or media server uses a reserved port when it connects to `bpcd` on a client. This means that the **Reserved ports** connect option is in effect. You can use the following procedure to change this setting.

To specify reserved or non-reserved ports

- 1 Make sure that you are in the **Client Attributes** display.

For information on how to get to the **Client Attributes** display, see the following procedure:

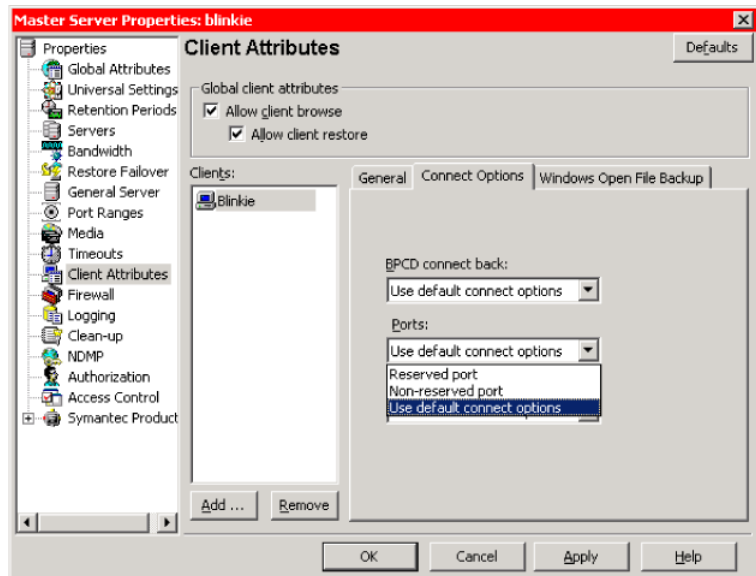
See [“To specify client attributes from the Java or Windows interface”](#) on page 126.

- 2 Make sure that the client(s) you want to configure show in the **Clients** pane.
To add a client, click **Add** and type the name of the client you want to add in the dialog box that appears. When you are finished adding clients, click **Close**.
- 3 Click the **Connect Options** tab.

Specifying ports (reserved or non-reserved) that connect a master server or media server to a client

- 4 In the **Ports** drop-down menu, select either **Reserved ports**, **Non-reserved ports**, or **Use default connect options**.

The display for these options is as follows:



The description for each option is as follows:

- | | |
|------------------------------------|---|
| Reserved port | Specifies that the master server and media server use a reserved port to connect to <code>bpcd</code> on this client. |
| Non-reserved port | Specifies that the master server and media servers use a non-reserved port to connect to <code>bpcd</code> on the client. |
| Use default connect options | Specifies that the master server and media servers use the <code>CONNECT_OPTIONS</code> or <code>DEFAULT_CONNECT_OPTIONS</code> . These options are defined on the master server or media server that connects to the client. |

- 5 Click **Apply** when you are finished specifying ports.
- 6 Click **OK** to exit from the **Client Attributes** interface.

By default, if both the server and the client are NetBackup 7.5 or later, this setting is not applicable. Non-reserved ports are always used in that case.

Note: This option only affects connections to NetBackup 7.5 and earlier. For connections to NetBackup 7.5 and later, the `veritas_pbx` port is used.

Specifying a BPCD connect-back method that connects a master server or media server to a client

The BPCD connect-back method specifies how the client responds when a master server or media server connects to `bpcd` on the client.

By default, the client connects back to the master server or media server on the VNETD port number. This means that the VNETD port selection is in effect. You can use the following procedure to change this setting.

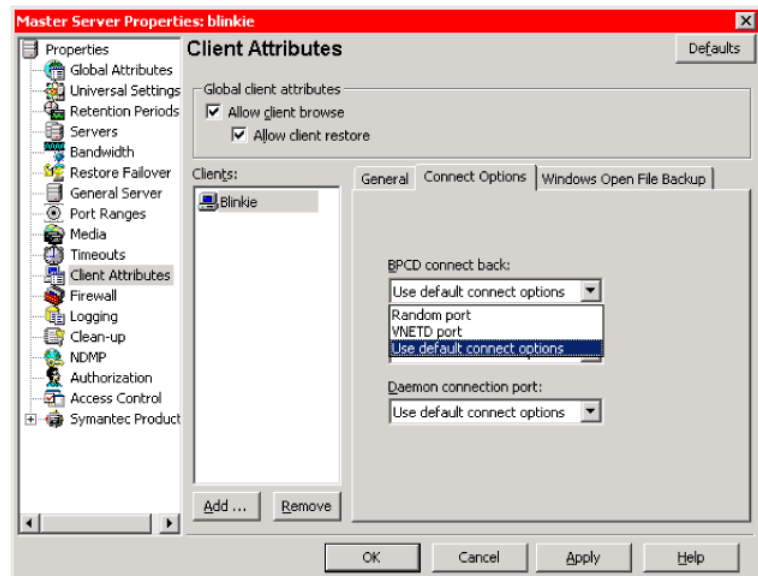
To specify a BPCD connect-back method

- 1 Make sure that you are in the **Client Attributes** display.
For information on how to get to the **Client Attributes** display, see the following procedure:
See [“To specify client attributes from the Java or Windows interface”](#) on page 126.
- 2 Make sure that the client(s) you want to configure show in the **Clients** pane.
To add a client, click **Add** and type the name of the client you want to add in the dialog box that appears. When you are finished adding clients, click **Close**.
- 3 Click the **Connect Options** tab.

Specifying a BPCD connect-back method that connects a master server or media server to a client

- 4 In the **BPCD connect back** drop-down menu, select either **Random port**, **VNETD port**, or **Use default connect options**.

This display is as follows:



The description for each option is as follows:

- | | |
|------------------------------------|--|
| Random port | Specifies that the client connects back to the master server and media server using a random port number. |
| VNETD port | Specifies that the client connects back to the master server and media server using the <code>vnetd</code> port number. |
| Use default connect options | Specifies that the client connects back to the master server and media server. The <code>CONNECT_OPTIONS</code> or <code>DEFAULT_CONNECT_OPTIONS</code> are defined on the master server or media server that connects to the client. Default. |

- 5 Click **Apply** when you are finished specifying a method.
- 6 Click **OK** to exit from the **Client Attributes** interface.

By default, if both the server and the client are NetBackup 6.0 or later, this setting is not applicable. Connect back is not used in that case.

Note: This option only affects connections to NetBackup 7.5 and earlier. For connections to NetBackup 7.5 and later, the `veritas_pbx` port is used.

Specifying a daemon connection port that connects a master server or media server to a client

Note: This option only affects connections to NetBackup 7.5 and earlier. For connections to NetBackup 7.5 and later, the `veritas_pbx` port is used.

The **Daemon connection port** connect option specifies which destination port the server uses to connect to the client. By default, if both server and client are NetBackup 6.0 or later, the connection can be on the `vnetd` port number. All other server to client `bpcd` connections are on the legacy `bpcd` port number. You can use the following procedure to change this setting.

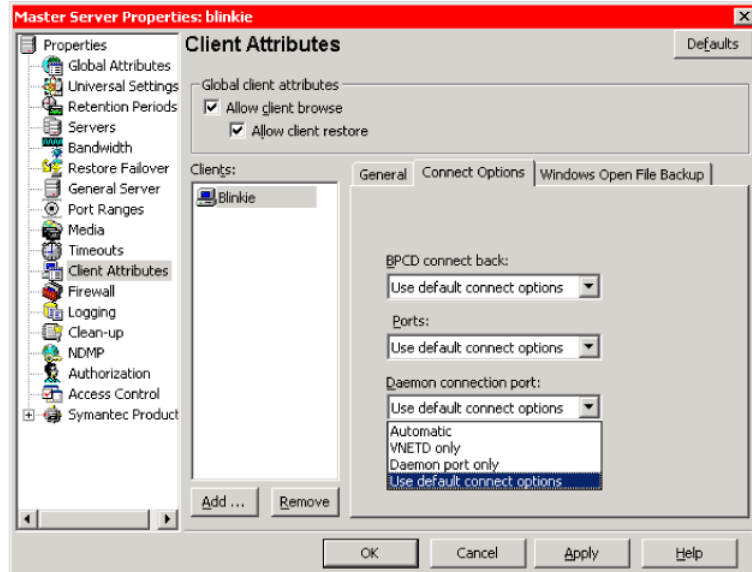
To specify a Daemon connection port

- 1 Make sure that you are in the **Client Attributes** display.
For information on how to get to the **Client Attributes** display, see the procedure:
See [“To specify client attributes from the Java or Windows interface”](#) on page 126.
- 2 Make sure that the client(s) that you want to configure show in the **Clients** pane. To add a client, click **Add...** and type the name of the client that you want to add in the dialog box that appears. When you are finished adding clients, click **Close**.
- 3 Click the **Connect Options** tab.

Specifying a daemon connection port that connects a master server or media server to a client

- 4 In the **Daemon connection port** drop-down menu, select either **Automatic**, **VNETD port only**, **Daemon port only**, or **Use default connect options**.

This display is as follows:



The description for each option is as follows:

Automatic

Specifies that the server attempts to connect to `bpcd` on the client using the `vnetd` port number. If that fails, the server attempts to connect to `bpcd` on the client using the legacy `bpcd` port number.

VNET only

Specifies that the server attempts to connect to `bpcd` on the client using the `vnetd` port number. Do not select this option if the client is NetBackup 5.1 or earlier.

Daemon port only

Specifies that the server attempts to connect to `bpcd` on the client using the legacy `bpcd` port number.

Use default connect options

Specifies the port number that is used by the server to connect to `bpcd` on the client using the `CONNECT_OPTIONS` or `DEFAULT_CONNECT_OPTIONS`. These options are defined on the master server or media server that connects to the client. Default.

- 5 Click **Apply** when you are finished specifying a method.
- 6 Click **OK** to exit from the **Client Attributes** interface.

For NetBackup 5.1 and earlier, connections to `bpcd` are always made with the legacy `bpcd` port number. Connections to `bpcd` can be made with the `vnetd` port number if both the server and client are NetBackup 7.5 or later. When the `bpcd` connections are made using the `vnetd` port number, the **Ports** and **BPCD connect back** options are ignored. The default in that case is to use non-reserved source port numbers, the `vnetd` destination port number, and no connect back.

Specifying port ranges

The following topic describes how to specify the numbers for the ranges of ports.

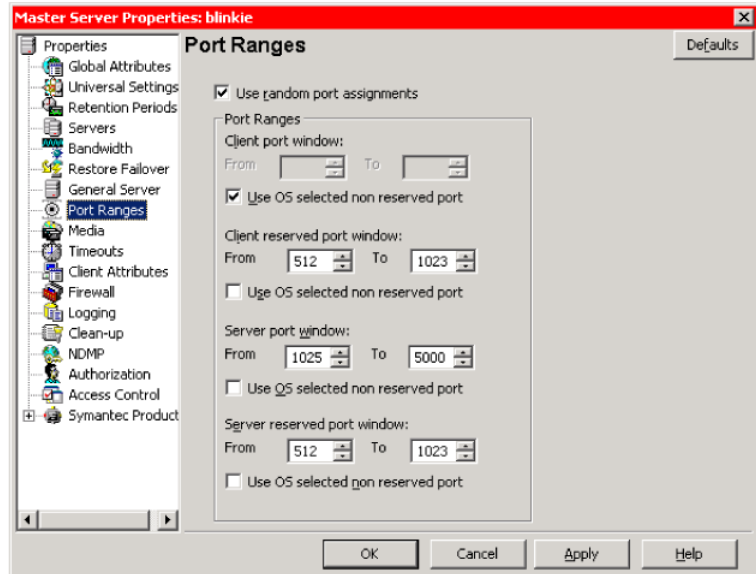
Note: For all port windows, if you specify a zero in the **From** box, the software uses a non-reserved port that the operating system chooses.

To specify port ranges

- 1 In the **NetBackup Administration Console**, expand **Host Properties > Master Servers**.
- 2 Double click the host that you want to configure.

3 Click **Port Ranges**.

A display similar to the following appears:



- 4 Click **Apply**
- 5 Click **OK**

The **Client reserved port window**, **Server port window**, and **Server reserved port window** options are not applicable to NetBackup clients.

By default, the **Server port window** and **Server reserved port window** options are not used for NetBackup 7.5 or later.

By default, the **Client reserved port window** option is not used for NetBackup 7.5 or later.

A description of the port, purpose, and default ranges is as follows:

Port	Purpose and default range
Client port window	Specifies the range of non-reserved source port numbers that this computer uses to connect to most NetBackup services. Default range is 0 to 0. The operating system chooses the port.
Client reserved port window	Specifies the range of reserved source port numbers that this computer uses to connect to <code>bpcd</code> with the legacy <code>bpcd</code> destination port number. The default range is 512 - 1023.
Server port window	Specifies the range of non-reserved destination port numbers that other computers use to connect to this computer for <code>bpcd</code> connect back. The default range is 1024 - 5000.
Server reserved port window	Specifies the range of reserved destination port numbers that other computers use to connect to this computer for <code>bpcd</code> connect back. The default range is 512 - 1023.

BPJAVA_PORT and VNETD_PORT ports

The BPJAVA_PORT port is the configured port for the `bpjava_msvc` daemon process. The VNETD_PORT port is the configured port for the `vnetd` daemon process. These ports are registered with IANA.

Caution: Symantec does not recommend changing these ports.

If the ports for these processes need to be changed, make the change on all NetBackup hosts in the relevant NetBackup cluster. This information is described in the *NetBackup Installation Guide for UNIX* or the *NetBackup Installation Guide for Windows*. In addition, specify the value in the corresponding `nbj.conf` option.

Changing the ports for BPCD and BPRD on Windows

The BPCD port is the configured port for the `bpcd` daemon process. The BPRD port is the configured port for the `bprd` daemon process. These ports are registered with IANA.

Caution: Symantec does not recommend changing these ports.

If the ports for these processes need to be changed, make the change on all NetBackup hosts.

On Windows hosts, use the following procedure to set the value for all Windows computers.

This procedure is used in addition to making the change in all the relevant services files:

To change the ports for BPCD and BPRD on Windows

- 1 On Windows, click through **Start > All Programs > Symantec NetBackup > Backup, Archive, and Restore**.
- 2 In the **Backup, Archive, and Restore** window, click **File > NetBackup Client Properties**.
- 3 Select the **Network** tab.
- 4 Change the values.
- 5 Click **OK**.

If the services file is not changed and the `bpcd` port is changed using the preceding procedure, the change is reflected in the NetBackup configuration. A difference exists between the value that is in the NetBackup configuration and the services file. The next time that the NetBackup Client Service is started on the computer, it automatically updates the services with the value that appears in the NetBackup configuration.

Disabling the ping on the NetBackup Administration Console on Windows

By default, the **NetBackup Administration Console** on Windows pings the computers that it communicates with to ensure that they are alive. The console performs this action before it connects to them. If the Internet Control Message Protocol (ICMP) protocol is blocked in a network, the **NetBackup Administration Console** may not function.

You can use the following procedure to disable the ping that the **NetBackup Administration Console** performs by default.

Note: For 7.5 release, ping by default is already disabled. For 5.x releases, use the following procedure to disable ping.

To disable the ping on the NetBackup Administration Console on Windows

- 1 In the **NetBackup Administration Console**, select the **View** menu.
- 2 Then, select the **Options** menu.
- 3 When the **Options** window appears, select the **Administration Console** tab.
- 4 On the **Administration Console** tab, select the **Disable "ping" connection checking** box.
- 5 Click **OK**.

About ICMP pinging NDMP

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.

About NDMP in a firewall environment

If you use an NDMP storage unit in a firewall environment, make sure that you know the different types of NDMP backups to be performed. The backup type determines which ports need to be opened in the firewall. These backup types include local, 3-way and remote NDMP, remote NDMP, and local and 3-way TIR.

The following table describes the types of NDMP backups and how they relate to firewall use.

Table 3-7 Types of NDMP backups

Backup type	Description
Local	For local operations, the DMA needs access to port 10,000 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 10,000 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.
Local and three-way TIR	For local and three-way TIR, the data requires an unlimited number of ports available because NetBackup has no control over the ports used.

About the ACS storage server interface

The following table describes the ACS robotic processes.

Table 3-8 ACS robotic processes

Robotic process	Description
ACSSEL	<p>Specifies the ACS SSI Event Logger. It is modeled after the <code>mini_el</code> event logger that is provided by StorageTek. Its functional model differs slightly from the other robotic test tools that are provided with the Media Manager.</p> <p>By default, ACSSEL listens on socket name (or IP port) 13740. If this entry is specified in <code>vm.conf</code>, you can change the default.</p> <p>This entry is read and interpreted where <code>acsd</code> is running, and the format for this entry is as follows:</p> <pre>ACS_SEL_SOCKET = socket_name</pre>

Table 3-8 ACS robotic processes (continued)

Robotic process	Description
ACSSSI	<p>By default, ACSSSI listens on unique, consecutive socket names starting as 13741. To specify socket names on an ACS library software host, add a configuration entry in vm.conf.</p> <p>This entry is read and interpreted on the host where <code>acsd</code> and <code>acsssi</code> are running, and the format for this entry is as follows:</p> <pre>ACS_SSI_SOCKET = ASC_library_software_host socket_name</pre> <p>For example: <code>ACS_SSI_SOCKET = Einstein 13750</code></p>

About known firewall problems when using NetBackup with other products

The following table describes the known firewall problems that you might have when using NetBackup with other products.

Table 3-9 Known firewall problems when using NetBackup with other products

Server	Firewall problem
ACS	Communication is required between the media server that has the ACS drives configured and the ACS server. But NetBackup has no control over the communication between these computers. The communication is handled by an RPC mechanism without a common port. You cannot define the ports that need to be open for a possible firewall between the media server and the ACS server.
LMF	Communication is required between the media server that has the robotic control and Fujitsu's LMF server. This communication is through an unknown network port, and NetBackup has no control over that port number. You cannot define the ports that would need to be open for a possible firewall between the media server and Fujitsu's LMF server.
TLH	Communication is required between the media server that has the robotic control and the server that has IBM's Library Manager. This communication is through an unknown network port, and NetBackup has no control over that port number. You cannot define the ports that would need to be open for a possible firewall between the media server and the IBM Library Manager server.

Table 3-9 Known firewall problems when using NetBackup with other products
(continued)

Server	Firewall problem
TLM	Communication is required between the media server that has the robotic control and ADICs DAS/SDLC server. NetBackup has no control over the communication mechanism and does not know which ports are used between the media server and ADICs DAS/SDLC server. You cannot define the ports that are needed to be open for a possible firewall between the media server and ADICs DAS/SDLC server.

About configuring port usage without a GUI

The following topics summarize how to configure port usage settings without a GUI. This appendix is not intended to provide details on using commands to change settings. For more information on any of these commands or files, see the following manuals:

- *NetBackup Administrator's Guide for UNIX and Linux, Volumes I and II*
- *NetBackup Administrator's Guide for Windows, Volumes I and II*
- *NetBackup Commands Reference Guide*

About port usage settings in the NetBackup configuration - bp.conf

This topic describes the NetBackup configuration settings that are related to port usage. All of the NetBackup configuration settings are described in *NetBackup Administrator's Guide for UNIX and Linux, Volume I*.

On UNIX or Linux systems, you can edit the `/usr/opensv/netbackup/bp.conf` file directly to update several port usage settings for the local computers NetBackup configuration. Typically, you would use a text editor such as vi(1) to read and update the file.

You can also use the `bpgetconfig` command and `bpsetconfig` command from UNIX, Linux, or Windows NetBackup servers to read and update NetBackup configuration. The configuration can be done for local or remote computers. The `bpgetconfig(1M)` and `bpsetconfig(1M)` commands are described in the *NetBackup Commands*.

You can read the configuration with the `bpgetconfig` command, copy it into a temporary file, and edit the configuration in the temporary file. Then, you can

use the `bpsetconfig` command to update the configuration from the temporary file.

You can use the following commands to update the NetBackup configuration of the computer client1:

```
bpgetconfig -M client1 > conf.txt

vi conf.txt # if UNIX or Linux

notepad conf.txt # if Windows

bpsetconfig -h client1 conf.txt
```

Port usage-related NetBackup configuration settings

The following table describes the port usage-related NetBackup configuration settings.

Table 3-10 Port usage-related NetBackup configuration settings

Setting	Description
ALLOW_NON_RESERVED_PORTS = YES NO	<p>Specifies if the NetBackup client daemon (<code>bpcd</code>) on the local computer can accept remote connections from non-reserved ports (port numbers 1024 or greater).</p> <p>Note: This option is not applicable to NetBackup 7.5 or later.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ NO (default for NetBackup 5.1 and earlier) means that <code>bpcd</code> requires remote connections to come from reserved ports (port numbers less than 1024).■ YES (default for NetBackup 6.0 and later) means that <code>bpcd</code> allows remote connections to come from non-reserved ports (port numbers less than 1024). <p>This option is useful when NetBackup clients and servers are on the opposite sides of a firewall.</p> <p>You should specify YES for this setting if NetBackup servers are configured by the <code>DEFAULT_CONNECT_OPTIONS</code> or <code>CONNECT_OPTIONS</code> settings. Or use the <code>bpclient</code> command line to connect to the local computers <code>bpcd</code> with non-reserved source port numbers.</p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Universal Settings and then click on the Accept connections on nonreserved ports check box.</p>

Table 3-10 Port usage-related NetBackup configuration settings (*continued*)

Setting	Description
RANDOM_PORT = YES NO	<p>Specifies whether NetBackup chooses source port numbers randomly or sequentially when it requires one for communication with NetBackup on other computers.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none"> ■ YES (the default) means that NetBackup chooses port numbers randomly from those that are free in the allowed range. For example, if the range is from 1024 through 5000, it chooses randomly from the numbers in this range. ■ NO means that NetBackup chooses numbers sequentially, starting with the highest number that is available in the allowed range. For example, if the range is from 1024 through 5000, NetBackup chooses 5000 (assuming that it is free). If 5000 is used, port 4999 is chosen. <p>The allowed port ranges can be determined by the CLIENT_PORT_WINDOW and CLIENT_RESERVED_PORT_WINDOW settings.</p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Port ranges and then click on the Use random port assignments check box.</p>
CLIENT_PORT_WINDOW = min max	<p>Specifies the range of non-reserved source ports on this computer that are used to connect to NetBackup on other computers. This setting applies to most NetBackup connections. The CLIENT_RESERVED_PORT_WINDOW setting is applicable to connect to bpcd with the legacy bpcd destination port number with reserved source port numbers.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none"> ■ min is the minimum port number in the range. It should be 0 (zero) or a number between 1024 and 65535. ■ max is the maximum port number in the range. It should be a number between min and 65535. <p>If min is 0 (zero), the operating system determines the source port number and max is ignored. The default is 0 0.</p> <p>For example, the following command permits ports from 4800 through 5000: CLIENT_PORT_WINDOW = 4800 5000.</p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Port ranges and then enter the range in the Client reserved port window.</p>

Table 3-10

Port usage-related NetBackup configuration settings *(continued)*

Setting	Description
CLIENT_RESERVED_PORT_WINDOW = min max	<p>Specifies the range of reserved source ports on this computer that are used to connect to <code>bpcd</code> on other computers. This setting is applicable to connect to <code>bpcd</code> with the legacy <code>bpcd</code> destination port number with reserved source port numbers.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ min is the minimum port number in the range. It should be 0 (zero) or a number between 1 and 1023.■ max is the maximum port number in the range. It should be a number between min and 1023. <p>If min is 0 (zero), the operating system determines the source port number and max is ignored. The default is 512 1023.</p> <p>For example, the following command permits ports from 700 through 980: <code>CLIENT_RESERVED_PORT_WINDOW = 700 980.</code></p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Port Ranges and then enter the range in the Client reserved port window.</p>
SERVER_PORT_WINDOW = min max	<p>Specifies the range of reserved destination ports on this computer that can be used by <code>bpcd</code> on other computers. It is used to connect back to this computer. This setting is applicable to connect to <code>bpcd</code> with the legacy <code>bpcd</code> destination port number. It can be used with non-reserved source port numbers with random port <code>bpcd</code> connect back.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ min is the minimum port number in the range. It should be 0 (zero) or a number between 1024 and 65535.■ max is the maximum port number in the range. It should be a number between min and 65535. <p>If min is 0 (zero), the operating system determines the source port number and max is ignored. The default is 1025 5000.</p> <p>For example, the following command permits ports from 3000 through 7500: <code>SERVER_PORT_WINDOW = 3000 7500.</code></p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Port Ranges and then enter the range in the Server port window.</p>

Table 3-10

Port usage-related NetBackup configuration settings (continued)

Setting	Description
SERVER_RESERVED_PORT_WINDOW = min max	<p>Specifies the range of reserved destination ports on this computer that can be used by <code>bpcd</code> on other computers to connect back to this computer. This setting is applicable to connect to <code>bpcd</code> with the legacy <code>bpcd</code> destination port number. It is used with reserved source port numbers with random port <code>bpcd</code> connect back.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ min is the minimum port number in the range. Should be 0 (zero) or a number between 1 and 1023.■ max is the maximum port number in the range. Should be a number between min and 1023. <p>If min is 0 (zero), the operating system determines the source port number and max is ignored. The default is 512 1023.</p> <p>For example, the following command permits ports from 700 through 980: <code>SERVER_RESERVED_PORT_WINDOW = 700 980.</code></p> <p>This setting can also be configured in the NetBackup Administration Console by expanding Host Properties > Port Ranges and then enter the range in the Server reserved port window.</p>

Table 3-10

Port usage-related NetBackup configuration settings *(continued)*

Setting	Description
CONNECT_OPTIONS = host 0 1 2 0 1 2 0 1 2 3 and DEFAULT_CONNECT_OPTIONS = 0 1 0 1 0 1 2	<p>The CONNECT_OPTIONS and DEFAULT_CONNECT_OPTIONS configuration values specify how the local computer connects to services on other NetBackup systems. DEFAULT_CONNECT_OPTIONS is only available for NetBackup 6.0 and later. The values for CONNECT_OPTIONS are a host name followed by three digits. The values for DEFAULT_CONNECT_OPTIONS are three digits.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ Host is a remote NetBackup system that the local computer connects to. You may have multiple CONNECT_OPTIONS entries in the configuration. If a host is not specified in any CONNECT_OPTIONS entries, the values from the DEFAULT_CONNECT_OPTIONS entry are used.■ The first digit is the reserved versus non-reserved source port as follows:<ul style="list-style-type: none">■ 0 means that connections to <code>bpcd</code> from the local computer should use a reserved source port number. It is selected from the <code>CLIENT_RESERVED_PORT_WINDOW</code> range. (Default.)■ 1 means that connections to <code>bpcd</code> from the local computer should use a non-reserved source port number that is selected from the <code>CLIENT_PORT_WINDOW</code> range. Be sure <code>ALLOW_NON_RESERVED_PORTS = YES</code> is set on the remote hosts that the local computer may connect to.■ 2 when specified in <code>CONNECT_OPTIONS</code> means that the value from <code>DEFAULT_CONNECT_OPTIONS</code> should be used instead.■ The second digit is <code>bpcd</code> callback method as follows:<ul style="list-style-type: none">■ 0 means that connections to <code>bpcd</code> from the local computer, <code>bpcd</code> connects back to a random port number on the local computer that is selected from the <code>SERVER_RESERVED_PORT_WINDOW</code> range, or <code>SERVER_PORT_WINDOW</code> range on the server. (Default for 5.1 and earlier.)■ 1 means that connections to <code>bpcd</code> from the local computer, <code>bpcd</code> connects back to the <code>vnetd</code> port number on the server. (Default for 6.0 and later.)■ 2 when specified in <code>CONNECT_OPTIONS</code> means that the value from <code>DEFAULT_CONNECT_OPTIONS</code> should be used instead.

Table 3-10 Port usage-related NetBackup configuration settings (*continued*)

Setting	Description
CONNECT_OPTIONS = host 0 1 2 0 1 2 0 1 2 3 and DEFAULT_CONNECT_OPTIONS = 0 1 0 1 0 1 2 (continued)	<div> <div> <ul style="list-style-type: none"> ■ The third digit is the legacy versus vnetd destination port as follows: <ul style="list-style-type: none"> ■ 0 means that the local computer first attempts to connect to a NetBackup service using the <code>vnetd</code> destination port number. If that fails, the local computer can attempt to connect to the NetBackup service using the legacy destination port number for that service. (Default for 6.0 and later.) ■ 1 means that connections to a NetBackup service from the local computer use the <code>vnetd</code> destination port number. ■ 2 means that connections to a NetBackup service from the local computer use the legacy destination port number for the service. ■ 3 when specified in <code>CONNECT_OPTIONS</code> means that the value from <code>DEFAULT_CONNECT_OPTIONS</code> should be used instead. </div> <div> <p>Note: The third digit is not applicable when connecting to NetBackup 7.5 or later. When connecting to NetBackup 7.5 or later, the <code>veritas_pbx</code> port is used.</p> <p>Note: <code>vnetd</code> can only be used as the destination port if the remote host is NetBackup 6.0 or later. If <code>vnetd</code> is used as the destination port, the settings from the first two digits are not applicable. In that case, the source port is from the non-reserved <code>CLIENT_PORT_WINDOW</code> range and no connect back is used.</p> <p>For example, the connection options to most remote hosts from the local computer can use the NetBackup 5.1 defaults.</p> <p>However, connections to host servers use the NetBackup 7.5 defaults:</p> <pre>CONNECT_OPTIONS = servers 0 1 0 DEFAULT_CONNECT_OPTIONS = 0 0 2</pre> <p>For example The <code>DEFAULT_CONNECT_OPTIONS</code> is restored to the defaults for NetBackup 7.5 and later:</p> <pre>DEFAULT_CONNECT_OPTIONS = 0 1 0</pre> <p>These settings can also be configured in the NetBackup Administration Console by expanding Host Properties > Firewall.</p> </div> </div>

About configuring port usage client attribute settings - bpclient command

The `bpclient` command is used to update a variety of client attributes in a database on the NetBackup master server.

The `bpcient (1M)` command is described in the *NetBackup Commands*.

The `-connect_options` argument to `bpcient` sets three port usage attributes that NetBackup servers use to connect to `bpcd` on the specified NetBackup client.

To specify connection options to a client, first make sure that the client is in the master servers database:

```
bpcient -client name -add
```

where *name* is the name of the client.

Specifying the `bpcient` command

The `bpcient` command updates the client connection attributes. The format of the `bpcient` command is as follows:

```
bpcient -client_name -update -connect_options 0|1|2 0|1|2 0|1|2|3
```

The `-connect_options` option can be followed by three digits.

The option digits are as follows:

- The first digit is the reserved versus non-reserved source port and is specified as follows:
 - 0 means that the connections to `bpcd` from the servers to the specified client should use a reserved source port number. The number is selected from the `CLIENT_RESERVED_PORT_WINDOW` range on the server. (Default for 5.1 and earlier servers.)
 - 1 means that the connections to `bpcd` from the servers to the specified client should use a non-reserved source port number. The number is selected from the `CLIENT_PORT_WINDOW` range on the server. Be sure that `ALLOW_NON_RESERVED_PORTS = YES` is set on the client.
 - 2 means that the reserved versus non-reserved source port setting can be determined by the `CONNECT_OPTIONS` and `DEFAULT_CONNECT_OPTIONS` on the server. (Default for 6.0 and later servers.)
- The second digit is the BPCD callback method and is specified as follows:
 - 0 means that for connections to `bpcd` from the servers to the specified client, the client connects back to a random port number of the server. That server is selected from the `SERVER_RESERVED_PORT_WINDOW` range or `SERVER_PORT_WINDOW` range on the server. (Default for 5.1 and earlier servers.)

- 1 means that for connections to `bpcd` from the servers to the specified client, the client connects back to the `vnetd` port number on the server.
- 2 means that the random port versus the `vnetd` port setting can be determined by the `CONNECT_OPTIONS` and `DEFAULT_CONNECT_OPTIONS` on the server. (Default for 6.0 and later servers.)
- The third digit is the legacy `bpcd` versus `vnetd` destination port, and is specified as follows:
 - 0 is the servers first attempt to connect to `bpcd` on the specified client using the `vnetd` destination port number. If that fails, the servers then try to connect to `bpcd` on the specified client using the legacy `bpcd` destination port number.
 - 1 means that the connections to `bpcd` from servers to the specified client use the `vnetd` destination port number.
 - 2 means that the connections to `bpcd` from the servers to the specified client use the legacy `bpcd` destination port number. (Default for 5.1 and earlier servers.)
 - 3 means that the legacy `bpcd` versus the `vnetd` destination port setting can be determined by the `CONNECT_OPTIONS` and `DEFAULT_CONNECT_OPTIONS` on the server. (Default for 6.0 and later servers.)

Note: The third digit is not applicable for NetBackup 7.5 or later clients. When connecting to NetBackup 7.5, the `veritas_pbx` port is used.

Note: `vnetd` can only be used as the destination port if the client is NetBackup 7.5 or later. If `vnetd` is used as the destination port, the settings from the first two digits are not applicable. In that case, the source port is from the non-reserved `CLIENT_PORT_WINDOW` range and no connect back is used.

For example, the following commands set the legacy (before NetBackup 7.5) client connect options for connections to `client1`.

The following commands are useful for older clients:

```
bpclient -add -client client1
```

```
bpclient -update -client client1 -connect_options 0 0 2
```

For example, the following command restores the NetBackup 6.5 or later client connect option defaults.

This command is useful after you upgrade the client to 6.5 or later:

```
bpclient -update -client client1 -connect_options 2 2 3
```

These settings can also be configured in the **NetBackup Administration Console** by expanding **Host Properties > Master Servers > Client Attributes > Connect Options** tab.

Port usage-related Media Manager configuration settings - vm.conf

For the Media Manager, update the port usage settings by editing the `/usr/opensv/volmgr/vm.conf` file (UNIX or Linux) or the `install_path\volmgr\vm.conf` file (Windows). There is no GUI available to change these settings.

The following table describes the port usage-related Media Manager configuration settings.

Table 3-11 Port usage-related Media Manager configuration settings

Setting	Description
RANDOM_PORTS = YES NO	<p>Specifies how Media Manager chooses a source port. The port is used when the Media Manager software on one computer needs to communicate with the Media Manager software on another computer. The default is YES.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ YES specifies that the source port number is selected randomly from the range that is defined by the CLIENT_PORT_WINDOW setting.■ NO specifies that the source port number is selected sequentially and randomly from the range that is defined by the CLIENT_PORT_WINDOW setting. The Media Manager attempts the connection with the highest source port number in the range. If the source port does not work, the Media Manager tries the next highest source port number. The port number is chosen from the list until it finds a source port number that works.

Table 3-11

Port usage-related Media Manager configuration settings (continued)

Setting	Description
<code>CLIENT_PORT_WINDOW</code> <code>= min max</code>	<p>Specifies the range of source ports that can be used on outgoing Media Manager connections. Min defines the lowest source port number and max defines the highest source port number, where min and max are integers from 1024 to 65535 or 0 (zero). If min is 0 or if max is less than min, then the Media Manager can let the operating system determine the source port number. The default is 0 0.</p> <p>For example, this setting defines a source port range from 3000 to 8000:</p> <pre>CLIENT_PORT_WINDOW = 3000 8000</pre>

Table 3-11 Port usage-related Media Manager configuration settings (continued)

Setting	Description
<code>CONNECT_OPTIONS = host 0 0 0 1 2</code>	<p>Specifies the destination port number that can be used to connect to the Media Manager services. You can specify multiple <code>CONNECT_OPTIONS</code> settings in the <code>vm.conf</code> file.</p> <p>Note: This setting is not applicable when connecting to NetBackup 7.5 or later. When connecting to NetBackup 7.5 or later, the <code>veritas_pbx</code> port is used.</p> <p>The option choices are as follows:</p> <ul style="list-style-type: none">■ <code>Host</code> specifies the host name of a computer with Media Manager services such as <code>vmd</code>.■ The first two digits are ignored.■ The third digit is the legacy Media Manager ports versus the <code>vnetd</code> destination port as follows:<ul style="list-style-type: none">■ 0 means that the local computer first attempts to connect to the Media Manager service on the specified host using the <code>vnetd</code> destination port number. If that attempt fails, servers then attempt to connect to the Media Manager service on the specified host. The server uses the legacy Media Manager destination port number.■ 1 means that connections to the Media Manager service on from the local computer to the specified host use the <code>vnetd</code> destination port number.■ 2 means that connections to the Media Manager service from the local computer to the specified host use the legacy Media Manager destination port number. (Default for 5.1 and earlier servers.) <p>For NetBackup 6.0 and later, if no <code>CONNECT_OPTIONS</code> settings are specified in the <code>vm.conf</code> file, the Media Manager sets defaults to the <code>DEFAULT_CONNECT_OPTIONS</code> and <code>CONNECT_OPTIONS</code> settings. Both settings are defined in the NetBackup configuration.</p> <p>For example, the following settings force the Media Manager connections to <code>server3</code> to use <code>vnetd</code> as the destination port:</p> <pre>CONNECT_OPTIONS = server3 0 0 1</pre>

Access control security

This chapter includes the following topics:

- [About using NetBackup Access Control \(NBAC\)](#)
- [NetBackup access management administration](#)
- [About NetBackup Access Control \(NBAC\) configuration](#)
- [Configuring NetBackup Access Control \(NBAC\)](#)
- [NBAC configuration overview](#)
- [Configuring NetBackup Access Control \(NBAC\) on standalone master servers](#)
- [Installing the NetBackup 7.5 master server highly available on a cluster](#)
- [Configuring NetBackup Access Control \(NBAC\) on a clustered master server](#)
- [Configuring NetBackup Access Control \(NBAC\) on media servers](#)
- [Installing and configuring NetBackup Access Control \(NBAC\) on clients](#)
- [Establishing a trust relationship between the broker and the Windows remote console](#)
- [NBAC configure commands summary](#)
- [Upgrading NetBackup Access Control \(NBAC\)](#)
- [About including authentication and authorization databases in the NetBackup hot catalog backups](#)
- [Upgrading NetBackup 7.5 when an older version of NetBackup is using a root broker installed on a remote machine](#)
- [Configuring NetBackup Access Control \(NBAC\) for NetBackup pre-7.0 media server and client computers](#)

- [Manually configuring the Access Control host properties](#)
- [Unifying NetBackup Management infrastructures with the setuptrust command](#)
- [Using the setuptrust command](#)
- [Accessing the master server and media server host properties](#)
- [Access control host properties](#)
- [Network Settings tab](#)
- [Authentication Domain tab](#)
- [Authorization Service tab](#)
- [Accessing the client host properties](#)
- [Access control host properties dialog for the client](#)
- [Authentication Domain tab for the client](#)
- [Network Settings tab for the client](#)
- [Access management troubleshooting guidelines](#)
- [Troubleshooting topics for NetBackup Authentication and Authorization](#)
- [About the UNIX verification procedures](#)
- [UNIX master server verification](#)
- [UNIX media server verification](#)
- [UNIX client verification](#)
- [Verification points in a mixed environment with a UNIX master server](#)
- [Master server verification points for a mixed UNIX master server](#)
- [Media server verification points for a mixed UNIX master server](#)
- [Client verification points for a mixed UNIX master server](#)
- [Verification points in a mixed environment with a Windows master server](#)
- [Master server verification points for a mixed Windows master server](#)
- [Media server verification points for a mixed Windows master server](#)
- [Client verification points for a mixed Windows master server](#)
- [Windows verification points](#)

- Master server verification points for Windows
- Media server verification points for Windows
- Client verification points for Windows
- Using the Access Management utility
- About determining who can access NetBackup
- Individual users
- User groups
- NetBackup default user groups
- Configuring user groups
- Creating a new user group
- Creating a new user group by copying an existing user group
- Renaming a user group
- General tab
- Users tab
- Defined Users pane on the Users tab
- Assigned Users pane on the Users tab
- Adding a new user to the user group
- About defining a user group and users
- Logging on as a new user
- Assigning a user to a user group
- Permissions tab
- About authorization objects and permissions
- Granting permissions
- Viewing specific user permissions for NetBackup user groups
- Authorization objects
- Media authorization object permissions
- Policy authorization object permissions

- Drive authorization object permissions
- Report authorization object permissions
- NBU_Catalog authorization object permissions
- Robot authorization object permissions
- Storage unit authorization object permissions
- DiskPool authorization object permissions
- BUAndRest authorization object permissions
- Job authorization object permissions
- Service authorization object permissions
- HostProperties authorization object permissions
- License authorization object permissions
- Volume group authorization object permissions
- VolumePool authorization object permissions
- DevHost authorization object permissions
- Security authorization object permissions
- Fat server authorization object permissions
- Fat client authorization object permissions
- Vault authorization object permissions
- Server group authorization object permissions
- Key management system (kms) group authorization object permissions

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.

Note: It has been found that NBAC running on NetBackup 6.5 (AZ version 4.3.19.2) cannot be upgraded to NetBackup 7.5. It is important that you upgrade to AZ version 6.5.4 (4.3.24.4) before the NBAC upgrade from NetBackup 6.5 to NetBackup 7.5 is successful.

The following table lists the NBAC considerations.

Table 4-1 NBAC Considerations

Consideration or issue	Description or resolution
Prerequisites before you configure NBAC	<p>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:</p> <ul style="list-style-type: none"> ■ 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 <p>Note: Host names should be resolvable to a valid IP address.</p> <ul style="list-style-type: none"> ■ Use the <code>ping</code> or <code>tracert</code> 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 4-1 NBAC Considerations (*continued*)

Consideration or issue	Description or resolution
Determine if the master server, media server, or client is to be upgraded	<p>Determine if the master server, media server, or client is to be upgraded as follows:</p> <ul style="list-style-type: none"> ■ 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	<p>Determine the roles in the configuration as follows:</p> <ul style="list-style-type: none"> ■ Who administers the hosts (root permission on master server equals head administrator). ■ Determine roles to start and then add on 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 the <code>Setupmaster</code> command is run, the NetBackup related group permissions (for example, <code>NBU_Admin</code> and <code>KMS_Admin</code>) 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 6.5.x to 7.0 or from 7.0 to 7.0.1. The solution is to grant the root and administrator users <code>NBU_Admin</code> and <code>KMS_Admin</code> permissions manually.
MSCS Error messages while unhooking shared security services from PBX	In MSCS environments running the <code>bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname></code> 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 <code>bpnbaz -setupmaster</code> is run in the context of local Administrator the <code>AUTHENTICATION_DOMAIN</code> entries may not contain the other cluster node entries. In such case these entries must be manually added from Host Properties into the <code>bp.conf</code> file.
Catalog recovery fails when NBAC is set to REQUIRED mode	If NBAC is running in REQUIRED mode and a catalog recovery was preformed, NBAC needs to be reset back from PROHIBITED mode to REQUIRED mode.

Table 4-1 NBAC Considerations (*continued*)

Consideration or issue	Description or resolution
Policy validation fails in NBAC mode (i.e. USE_VXSS = REQUIRED)	<p>Back up, restore, and verification of policy for snapshot can fail in NBAC enabled mode if one of the following has been done.</p> <ul style="list-style-type: none">■ Authenticated Principle is removed from the NBAC group: NBU_Users group■ Back up and restore permissions of NBU_User group have been removed

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 160. for the NBAC configuration sequence.

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 161.

Note: The master server can be installed in a stand-alone 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 164.

- 3 Configure clients for NBAC.

See [“Installing and configuring NetBackup Access Control \(NBAC\) on clients”](#) on page 166.

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 [“NBAC configure commands summary”](#) on page 169. for a

summary reference of the `bpnbaz` command. 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. See [“About using NetBackup Access Control \(NBAC\)”](#) on page 156. to review the prerequisites list. Review the list to ensure that you have noted all the associated media servers, clients, and the addresses to communicate with them.

See [“Troubleshooting topics for NetBackup Authentication and Authorization”](#) on page 191. for troubleshooting information. A set of OS commands and one NetBackup command is useful for the first level of troubleshooting. The OS commands are `ping`, `tracert` and `telnet`. The NetBackup command is `bpcintcmd`. 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 4-2 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 164.

Installing the NetBackup 7.5 master server highly available on a cluster

You can use the following procedure to install the NetBackup 7.5 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 7.5 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 fail over 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 fail over). 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 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 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 169.

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 NetBackup Access Control \(NBAC\) on clients”](#) on page 166.

Installing and configuring NetBackup Access Control (NBAC) on clients

The following procedure describes how to install and configure NetBackup Access Control (NBAC) on clients in a NetBackup configuration. The target client should be running the NetBackup client software version 7.5 or higher.

Installing and configuring NetBackup Access Control (NBAC) on clients

- 1 Make sure that no backups are currently running for the client computer.
- 2 Log on to the master server computer as the UNIX root or the Windows administrator.
- 3 Check that authentication daemon (`nbatd`) is running. If not, start the authentication daemon.
- 4 Go to the `NBU_INSTALL_PATH/bin` directory.

- 5 Log on as the NetBackup security administrator by using the following command:

Note: The UNIX root user and the Windows administrator on the master server are the default NetBackup security administrators.

```
bpbnet -Login
```

The following information is displayed.

```
Authentication Broker [master.server.com is default]:
Authentication port [0 is default]:
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd)
[unixpwd is default]:
Domain [master.server.com is default]:
Login Name [root is default]:
Password:
Operation completed successfully.
```

6 Run `bpbaz -SetupClient` with the described options.

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

See [“NBAC configure commands summary”](#) on page 169.

First do a dry run to see all of the clients that are visible to the master server. Use this process for the companies that have a large number of clients (greater than 250). The `-dryrun` option can be used with both the `-all` and single client configuration. By default, the discovered host list is written to the file `SetupClient.nbac` in the same directory. You can also provide your own output file name using `-out <output file>` option. If you use your own output file, then it should be passed for the subsequent runs with `-file` option. For example, you can use the following command:

```
bpbaz -SetupClient -all -dryrun [-out <outfile>] or
```

```
bpbaz -SetupClient <client.host.com> -dryrun [-out <outfile>].
```

After the dry run, check the client host names and run the same command without the `-dryrun` option. For example, use the following command:

```
bpbaz -SetupClient -all or
```

```
bpbaz -SetupClient -file SetupClient.nbac or bpbaz -SetupClient  
<client.host.com>.
```

The `-all` option runs with the clients known to the master server. It can take time to address all the clients in a large environment(greater than 250).

The `-all` client listing updates the credentials on all clients. It can take some time and resources; instead, use the `-file` option to update a subset of the clients. You can run the same command multiple times, until all the clients in the progress file are successfully configured. The status for each client is updated in the input file. The ones that succeeded in each run are commented out for the subsequent runs. A smaller subset is left for each successive run. Use this option if you have added a number of clients (greater than 250). Target the ones you want to update at that time.

The `-images` option with `-all` looks for client host names in the image catalogs. It can return decommissioned hosts in larger environments. Run the `-all -dryrun` options with the `-images` option to determine which hosts should be updated

7 Restart the client services on the specific clients once the installation is finished.

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 4-3

NBAC configure commands summary

Command	Description
<code>bpbaz -GetConfiguredHosts [target.server.com [-out file] -all [-outfile] -file progress.file]</code>	<p>The <code>bpbaz -GetConfiguredHosts</code> command is used to obtain NBAC status on the host. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command.</p> <p>The syntax is:</p> <ul style="list-style-type: none">■ <code>target.server.com</code> 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.■ <code>-out</code> option is used to specify a custom output file name. By default, the output is written to the <code>SetupMedia.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options.■ <code>-all</code> 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 <code>ConfiguredHosts.nbac</code> file.■ <code>-file progress.file</code> is an option used to specify host name(s) to be read from <code>progress_file</code>. This option expects one host name per line in the <code>progress_file</code>. CLI updates the <code>progress_file</code> with the host's NBAC status. It appends <code>#</code> after <code>hostname</code> followed by the NBAC status.■ When used with <code>target.server.com</code> or <code>-all</code> option, status of the host(s) is captured in the <code>ConfiguredHosts.nbac</code> file.

Table 4-3 NBAC configure commands summary (*continued*)

Command	Description
<pre>bpnbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]</pre>	<p>The <code>bpnbaz -SetupMaster</code> 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.</p> <p>Use the <code>bpnbaz -SetupMaster -fsa</code> command with the First Security Administrator option to provision a particular OS user as NBU Administrator.</p> <p>The syntax is:</p> <ul style="list-style-type: none"> ■ <code>-fsa</code> 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. ■ <i>domain type</i> is the type of network domain you are using. For example the <code>bpnbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe</code> command provisions the Windows enterprise domain user <code>jdoe</code> as NBU Administer. ■ <i>domain name</i> is the name of the particular domain you are using. For example the <code>bpnbaz -SetupMaster -fsa jdoe</code> command takes the current logged on user domain type (Windows/UNIXPWD), domain name, and provisions <code>jdoe</code> user in that domain. ■ <i>user name</i> is the particular OS user name you are designating as an NBU Administrator. <p>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.</p>

Table 4-3

NBAC configure commands summary (continued)

Command	Description
<code>bpbaz -SetupMedia [media.server.com [-out file] -all [-out file] -file progress.file] [-dryrun] [-disable]</code>	<p>The <code>bpbaz -SetupMedia</code> command is run by an NBU_Administrator group member on the master server. It should not be run until a <code>bpbaz -SetupMaster</code> has been completed successfully. It expects connectivity between the master server and target media server systems. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command.</p> <p>The syntax is:</p> <ul style="list-style-type: none">■ <code>media.server.com</code> is the name of a single target host. Use this option to add a single additional host for use with NBAC.■ <code>-out</code> option is used to specify a custom output file name. By default, the output is written to the <code>SetupMedia.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options.■ <code>-all</code> 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.■ <code>-file progress_file</code> 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.■ <code>-dryrun</code> can generate the list of media server names and write them to the log. This option can work with <code>media.server.com</code> but it is intended to be used with the <code>-all</code> option.■ <code>-disable</code> option can disable NBAC (USE_VXSS = PROHIBITED) on targeted hosts.

Table 4-3

NBAC configure commands summary (*continued*)

Command	Description
<pre>bpnbaz -SetupClient [client.server.com [-out file] -all [-images] [-out file] -file progress.file] [-dryrun] [-disable]</pre>	<p>The <code>bpnbaz -SetupClient</code> command is used for setting up NBAC on the clients. It should not be run until the <code>bpnbaz -SetupMaster</code> command has been completed successfully. The <code>bpnbaz -SetupClient</code> needs to run from the master server. It expects connectivity between the master server and target client systems. Either the <code>-all</code> or <code>target.server.com</code> options are required for this command.</p> <p>The syntax is:</p> <ul style="list-style-type: none">■ <code>client.server.com</code> 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.■ <code>-out</code> is an option that is used to specify a custom output file name. By default, the output is written to the <code>SetupClient.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options. The <code>-out</code> option is used to specify a custom output file name. By default, the output is written to the <code>SetupClient.nbac</code> file. This option can be used with <code>-all</code> and the single host configuration options.■ <code>-all</code> 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.■ <code>-images</code> is an option that searches all images for unique host names. This option cannot be recommend for customers with large catalogs unless they add the <code>-dryrun</code> 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.■ <code>-dryrun</code> 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.■ <code>-disable</code> is an option that disables NBAC (<code>USE_VXSS = PROHIBITED</code>) on targeted hosts.■ <code>-file progress.file</code> is an option used to specify a different file name for the progress log. The CLI reads the host names from the <code>progress_file</code>. The status is appended next to each host name with a <code>[# separated value]</code>. Successfully completed ones are commented out. This command can be run multiple times until all the clients in the <code>progress_file</code> 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 Install and 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 is using 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 7.5 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 7.5 when an older version of NetBackup is using a root broker installed on a remote machine.

Upgrading NetBackup 7.5 when an older version of NetBackup is using a root broker installed on a remote machine

- 1 Before upgrading to NetBackup 7.5, 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 7.5 upgrade.

On UNIX platforms, use

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

On Windows, use

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

- 2 Once the NetBackup 7.5 upgrade is completed then migrates the remote root broker (RB) and local shared authentication broker (AB) into NetBackup 7.5 by using the `atutil` tool which is shipped with NetBackup 7.5.
- 3 Copy the `atutil` utility from the NetBackup computer to the root broker computer.

On UNIX Platforms, copy the `/usr/opensv/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/opensv/netbackup/sec/at/bin/atutil import -z /usr/opensv/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/opensv/netbackup/sec/at/bin/vssregctl -s -f /usr/opensv/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/opensv/netbackup/bin/admincmd/bpsetconfig
bpsetconfig> USE_VXSS=AUTOMATIC
bpsetconfig> Ctrl + D (to save and quit).
```

On Windows,

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


- 9 Start the NetBackup 7.5 authentication service by running the following command.

On UNIX platforms, run `/usr/opensv/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/opensv/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 7.5 by running the following command.

On UNIX platforms, execute the following commands in sequence.

```
/usr/opensv/netbackup/sec/at/bin/atutil export -t ab -f
<AB output xml file> -p <password>
/usr/opensv/netbackup/sec/at/bin/atutil import -z
/usr/opensv/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 7.5 authorization service by executing the following commands.

On UNIX platforms, run `/usr/opensv/netbackup/bin/nbzd -f`.

On Windows, run `net start nbzd`.

13 Logon into 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 Logout 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 Logon to NetBackup 7.5 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 7.5 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 7.5 may not be compatible with the older NetBackup media servers or clients.

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

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

Please 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.

See [“Accessing the master server and media server host properties”](#) on page 183. for the media servers. See [“Accessing the client host properties”](#) on page 187. for the clients.

- 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 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 7.5 and OpsCenter 7.5 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 7.5 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 182. for a summary of the `setuptrust` command.

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 will be prompted to verify the hash.
- Medium security (1): The first authentication broker will be trusted without prompting. Any attempts to trust subsequent authentication brokers will cause 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

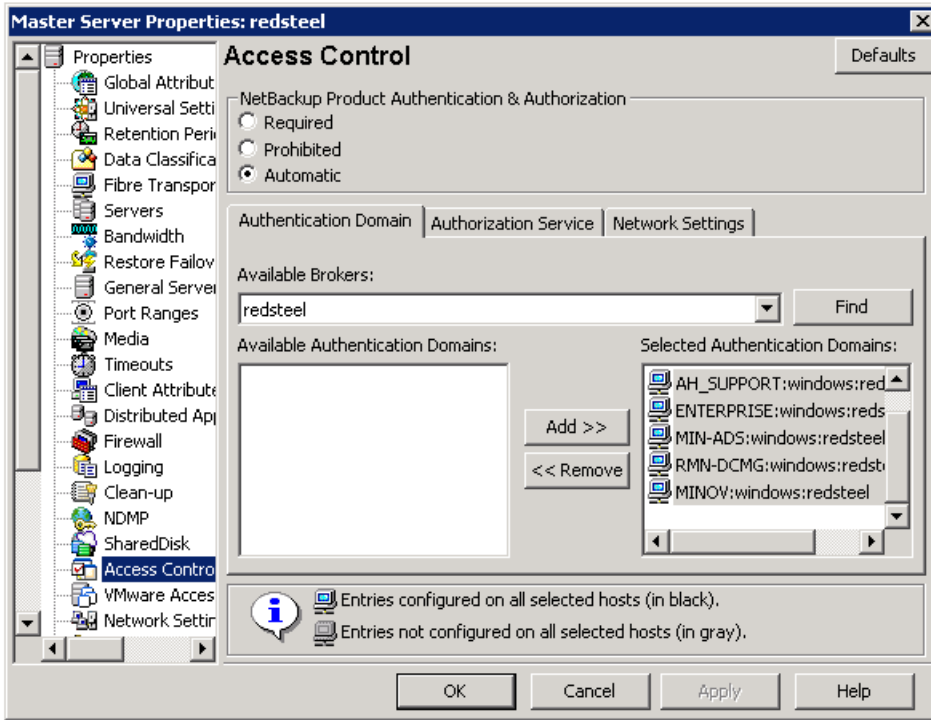
To access the master server and media server host properties in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > master server or media server > *Select server* > Access Control**.

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 4-1](#) shows the **Access Control** host properties dialog box.

Figure 4-1 Access control host properties dialog box



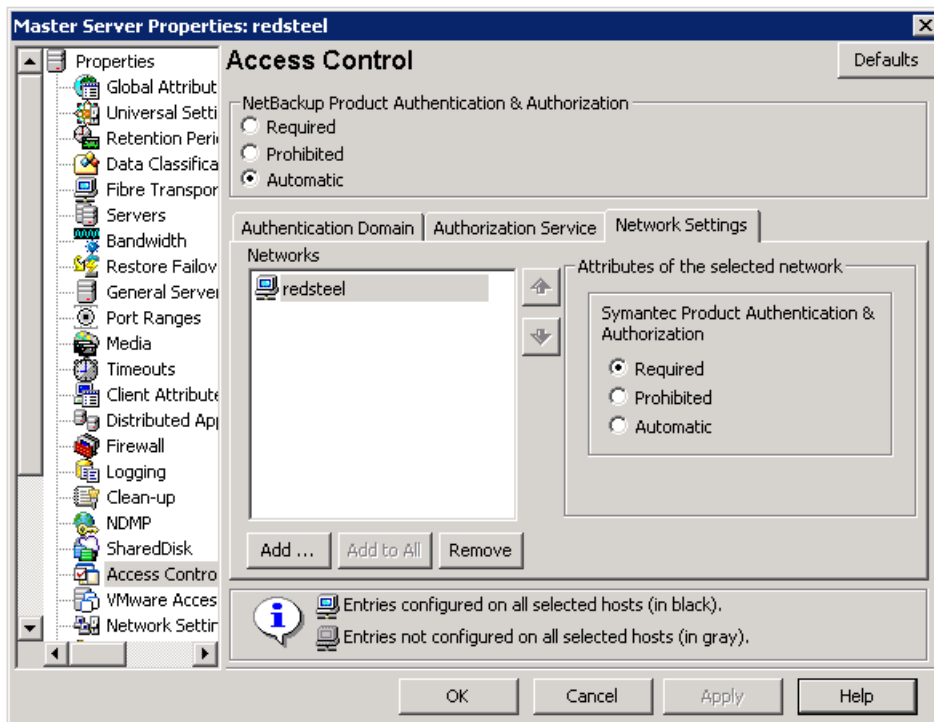
When **Automatic** is selected, you can specify computers or domains required to use **NetBackup Product Authentication and Authorization**. Otherwise you can specify computers that are prohibited from using the **NetBackup Product Authentication and Authorization**.

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 4-2 shows the **Network Settings** tab.

Figure 4-2 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:

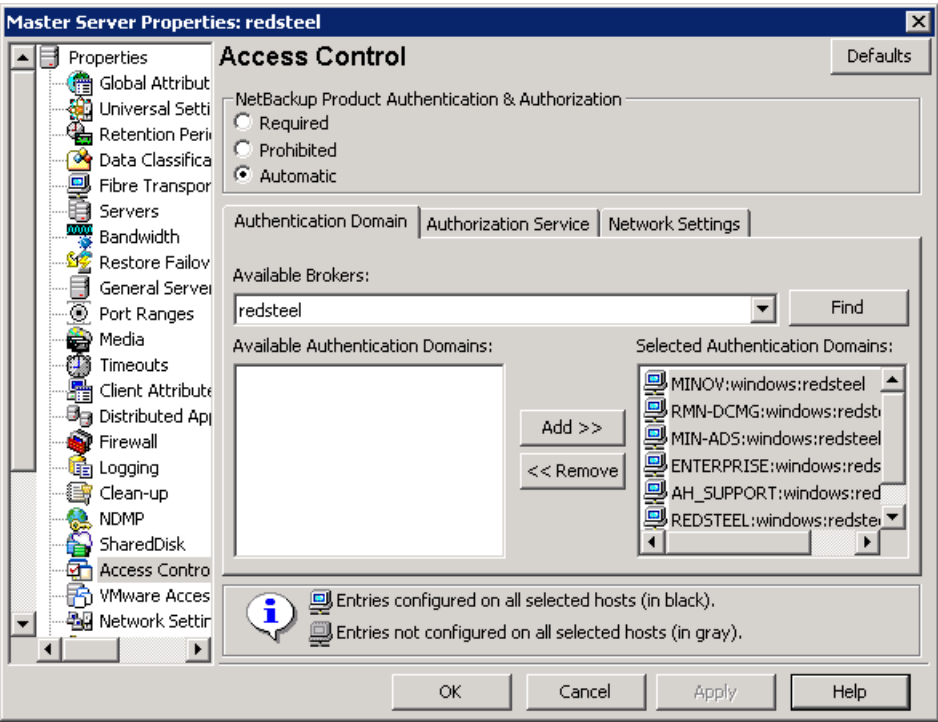
- Which authentication servers support which authentication mechanisms
- What domains each supports.

Add the domain that you want users to authenticate against.

The following examples contain six authentication domains.

Figure 4-3 shows the **Authentication Domain** tab.

Figure 4-3 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).

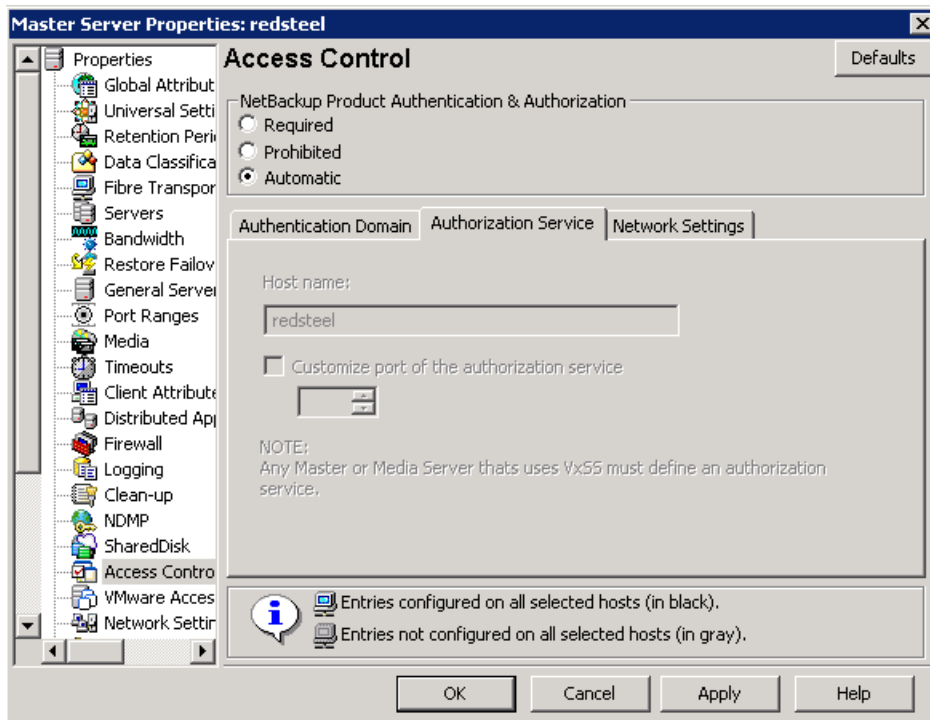
Authorization Service tab

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 4-4 shows the authorization service tab.

Figure 4-4 Authorization Service tab



Accessing the client host properties

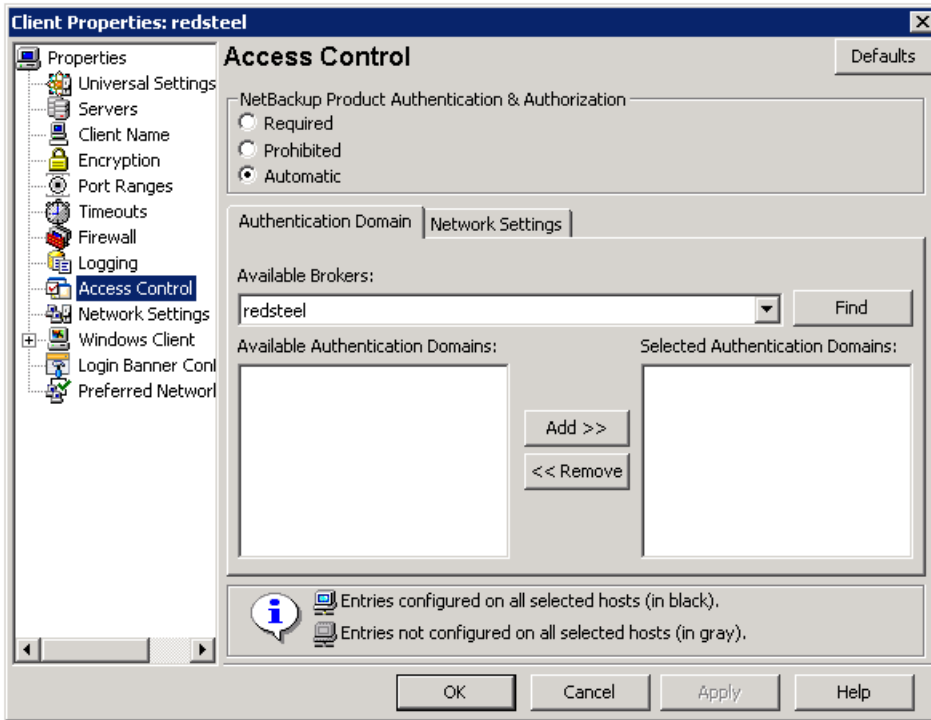
To access the client host properties in the **NetBackup Administration Console**, expand **NetBackup Management > Host Properties > Clients > *Select client(s)* > Access Control**.

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 4-5 Access control host properties for the client



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

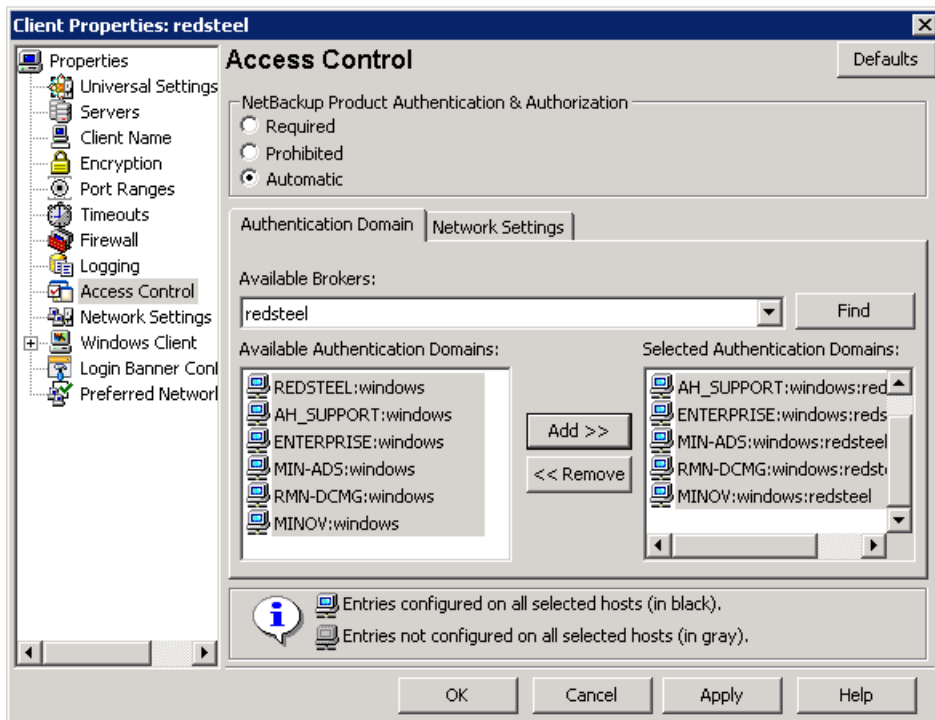
Authentication Domain tab for the client

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 4-6 shows the **Authentication Domain** tab and the selected authentication domains.

Figure 4-6 Authentication Domain tab for client

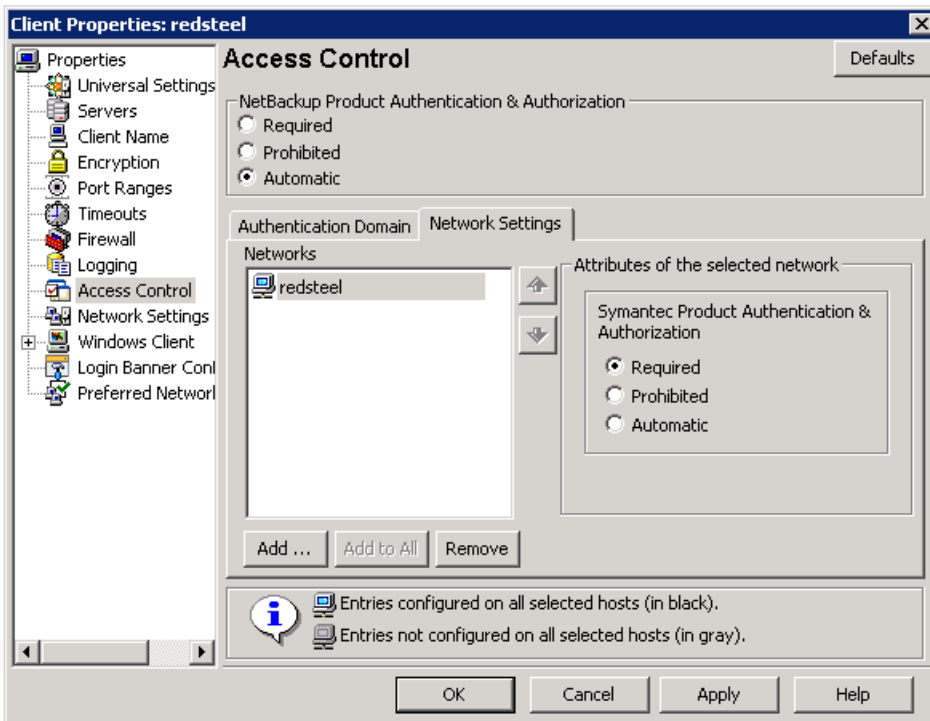


Network Settings tab for the client

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

[Figure 4-7](#) shows the **Network Settings** tab for the client.

Figure 4-7 Network Settings tab for the client



Access management troubleshooting guidelines

See [“Troubleshooting topics for NetBackup Authentication and Authorization”](#) on page 191. to troubleshoot access management and use the following verification points to determine if certain processes and functionality are operating correctly.

These verification points include:

- Windows verification points
See [“Windows verification points”](#) on page 219.
- UNIX verification points
See [“About the UNIX verification procedures”](#) on page 199.
- 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 207.
- 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 212.

Note that while possible to share the Enterprise Media Manager (EMM) server between multiple master servers, this configuration is not supported when using access control. The EMM server must be bound to one master server.

Troubleshooting topics for NetBackup Authentication and Authorization

The following topics describe helpful tips to configure **NetBackup Authentication and Authorization** with NetBackup:

- Verifying master server settings
- Establishing root credentials
- Expired credentials message
- Useful debug logs
- Uninstalling NetBackup Authentication and Authorization Shared Services
- Unhooking Shared AT from PBX
- Where credentials are stored
- How system time affects access control
- NetBackup Authentication and Authorization ports
- Stopping NetBackup Authentication and Authorization daemons
- If you lock yourself out of NetBackup
- Backups of storage units on media servers might not work in an NBAC environment
- Using the `nbac_cron` utility
- Enabling NBAC after a recovery on Windows
- In cluster installations the `setupmaster` might fail
- Known issue on a cluster if shared security services (`vxatd` or `vxazd`) are clustered along with the master server
- 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
- Known issue that `nbazd` fails with an error on Solaris x64

- Known issue on Windows 2003 dual stack computers
- Known issue relating to access control failures and short and long host names
- Known issue relating to AZ when upgrading from NetBackup 6.5 to NetBackup 7.5
- Known issue in a cluster upgrade with NBAC when the broker profile has `ClusterName` set to the virtual name of AT
- Known issue of multiple instances of `bpcd` causing a possible error
- Known issue with clusters using shared AT with configuration files on the shared drive
- Known issue relating to database utilities supporting `NBAZDB`

The following table describes the troubleshooting topics for **NetBackup Authentication and Authorization** and their configuration tips.

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization

Topic	Configuration tips
Verifying master server settings	<p>Running <code>bpnbat -whoami</code> and specifying the computer credentials, tells in what domain a host is registered and the name of the computer the certificate represents.</p> <pre>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.</pre> <p>If the domain listed is not <code>NBU_Machines@master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (master). The command is run on the computer that serves the <code>NBU_Machines</code> domain (master).</p> <p>Then, on the computer where you want to place the credentials, run: <code>bpnbat -loginmachine</code></p>

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Establishing root credentials	<p>If you have problems setting up either the authentication server or authorization server, and the application complains about your credentials as <code>root</code>: ensure that the <code>\$HOME</code> environmental variable is correct for <code>root</code>.</p> <p>Use the following command to detect the current value:</p> <pre>echo \$HOME</pre> <p>This value should agree with <code>root</code>'s home directory, which can be typically found in the <code>/etc/passwd</code> file.</p> <p>Note that when switching to <code>root</code>, you may need to use:</p> <pre>su -</pre> <p>instead of only <code>su</code> to correctly condition the <code>root</code> environment variables.</p>
Expired credentials message	<p>If your credential has expired or is incorrect, you may receive the following message while running a <code>bpnbaz</code> or <code>bpnbat</code> command:</p> <pre>Supplied credential is expired or incorrect. Please reauthenticate and try again.</pre> <p>Run <code>bpnbat -Login</code> to update an expired credential.</p>
Useful debug logs	<p>The following logs are useful to debug NetBackup Access Control:</p> <p>On the master: <code>admin</code>, <code>bpcd</code>, <code>bprd</code>, <code>bpdgm</code>, <code>bpjobd</code>, <code>bpsched</code></p> <p>On the client: <code>admin</code>, <code>bpcd</code></p> <p>Access control: <code>nbatd</code>, <code>nbazd</code>.</p> <p>See the <i>NetBackup Troubleshooting Guide</i> for instructions on proper logging.</p>

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Uninstalling NetBackup Authentication and Authorization Shared Services	<p>On UNIX:</p> <p>Using <code>installics</code>, select the option for uninstalling authentication and authorization. The following directories should be empty after uninstalling:</p> <p><code>/opt/VRTSat</code> and <code>/opt/VRTSaz</code></p> <p><code>/etc/vx/vss</code></p> <p><code>/var/VRTSat</code> and <code>/var/VRTSaz</code></p> <p>On Windows:</p> <p>Use the Windows Add/Remove Programs panel from the Control Menu to uninstall authentication and authorization. The <code>\Veritas\Security</code> directory should be empty after uninstalling.</p>
Unhooking Shared AT from PBX	<p>When NetBackup 7.5 is upgraded and NBAC was already enabled in a previous setup, the old Shared AT should be unhooked from PBX.</p> <p>To unhook shared AT, run following command.</p> <p>On UNIX platforms, run <code>/opt/VRTSat/bin/vssat setispbxexchflag --disable</code>.</p> <p>On Windows x86, run <code>C:\Program Files\VERITAS\Security\Authentication\bin\vssat setispbxexchflag --disable</code>.</p> <p>On Windows x64, run <code>C:\Program Files(x86)\VERITAS\Security\Authentication\bin\vssat setispbxexchflag --disable</code>.</p>
Where credentials are stored	<p>The NetBackup Authentication and Authorization credentials are stored in the following directories:</p> <p>UNIX:</p> <p>User credentials: <code>\$HOME/.vxss</code></p> <p>Computer credentials: <code>/usr/opensv/var/vxss/credentials/</code></p> <p>Windows:</p> <p><code><user_home_dir>\Application Data\VERITAS\VSS</code></p>
How system time affects access control	<p>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.</p>

Table 4-4

Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization *(continued)*

Topic	Configuration tips
NetBackup Authentication and Authorization ports	<p>The NetBackup Authentication and Authorization daemon services use ports 13783 and 13722 for back-level media server and clients. For 7.5 versions it uses PBX connections.</p> <p>You can verify that the processes are listening with the following commands:</p> <p>Authentication:</p> <p>UNIX</p> <pre>netstat -an grep 13783</pre> <p>Windows</p> <pre>netstat -a -n find "13783"</pre> <p>Authorization:</p> <p>UNIX</p> <pre>netstat -an grep 13722</pre> <p>Windows</p> <pre>netstat -a -n find "13722"</pre>

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Stopping NetBackup Authentication and Authorization daemons for Shared Services	<p>When the NetBackup Authentication and Authorization services are stopped, stop authorization first, then stop authentication.</p> <p>UNIX -Use the following commands.</p> <p>To stop authorization use the term signal as shown in the example:</p> <pre># 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</pre> <p>To stop authentication use the term signal as shown in the example:</p> <pre># 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</pre> <p>Windows</p> <p>Use the Services utility that Windows provides, since these services do not appear in the NetBackup Activity Monitor.</p>
If you lock yourself out of NetBackup	<p>You can lock yourself out of the NetBackup Administration Console if access control is incorrectly configured.</p> <p>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:</p> <pre>HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\ CurrentVersion\config</pre> <p>You can look to see if the following entries are set correctly: AUTHORIZATION_SERVICE, AUTHENTICATION_DOMAIN, and USE_VXSS.</p> <p>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.</p>
Backups of storage units on media servers might not work in an NBAC environment	<p>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.</p>

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Using the nbac_cron utility	<p>Use the <code>nbac_cron.exe</code> utility to create identities under which to run cron or at jobs.</p> <p><code>nbac_cron.exe</code> is found in the following location:</p> <p>UNIX <code>-/opt/opensv/netbackup/bin/goodies/nbac_cron</code></p> <p>Windows <code>-Install_path\Veritas\netbackup\bin\goodies\nbac_cron.exe</code></p> <p><code>nbac_cron</code> options:</p> <ul style="list-style-type: none"> ■ <code>-SetupAt [-Port #]</code> ■ <code>-SetupCron [-Port #]</code> <p>Either option sets up an authentication account. Optionally, specify a port number to use for authentication.</p> <ul style="list-style-type: none"> ■ <code>-AddAt</code> <p>Create an authorization account for a user.</p> <ul style="list-style-type: none"> ■ <code>-AddCron</code> <p>Create a cron account for a user.</p>
Enabling NBAC after a recovery on Windows	<p>Use the following procedure to manually enable NBAC after a recovery on Windows.</p> <ul style="list-style-type: none"> ■ Add <code>AUTHENTICATION_DOMAIN</code>, <code>AUTHORIZATION_SERVICE</code> and <code>USE_VXSS</code> entries in Registry. ■ Change the service type of NetBackup Authentication and Authorization services to <code>AUTOMATIC</code>. ■ Restart the NetBackup services. ■ Verify that the <code>nbatd</code> and <code>nbazd</code> services are running. <p>Note: On a cluster run the <code>bpclusterutil -enableSvc nbatd</code> and <code>bpclusterutil -enable nbazd</code> commands.</p>
In cluster installations the <code>setupmaster</code> might fail	<p>There is a known issue that in the case of cluster installations, where the configuration file is on a shared disk, the <code>setupmaster</code> might fail.</p>
Known issue on a cluster if shared security services (<code>vxatd</code> or <code>vxazd</code>) are clustered along with the master server	<p>There is a known issue on a cluster if shared security services (<code>vxatd</code> or <code>vxazd</code>) are clustered along with the master server. When executing the <code>bpbaz -SetupMaster</code> 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 <code>setupmaster</code> command.</p>

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Known issue in a clustered master server upgrade with NBAC, that all the <code>AUTHENTICATION_DOMAIN</code> entries in the <code>bp.conf</code> file are updated with the master server virtual name as the authentication broker	There is a known issue that in a clustered master server upgrade with NBAC, all the <code>AUTHENTICATION_DOMAIN</code> entries in the <code>bp.conf</code> 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 <code>bp.conf</code> file.
Known issue that <code>nbazd</code> fails with an error on Solaris x64	<p>There is a known issue that <code>nbazd</code> fails with the following error on Solaris x64.</p> <pre>ld.so.1: nbazd: fatal: relocation error: R_AMD64_PC32: file /usr/lib/64/libCrun.so.1: symbol __libc__CimplMex_terminate6F_v_: value 0x28001a4b2ba does not fit</pre> <p>To resolve the issue install patch 119964-*. </p>
Known issue on Windows 2003 dual stack computers	There is a known issue that 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	There is a known issue that if you see 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 relating to AZ when upgrading from NetBackup 6.5 to NetBackup 7.5	There is a known issue that NetBackup 6.5 with AZ version 4.3.19.2 fails to upgrade to NetBackup 7.5. Commands needed to migrate the shared AZ data are not supported in this version. The work-arounds are to upgrade AZ to version 4.3.24.4 or higher and then run the NetBackup 7.5 upgrade.
Known issue in a cluster upgrade with NBAC when the broker profile has <code>ClusterName</code> set to the virtual name of AT	There is a known issue that in a cluster upgrade with NBAC when the broker profile has <code>ClusterName</code> set to the virtual name of AT. This is migrated as is to the embedded broker. The embedded broker has <code>UseClusterNameAsBrokerName</code> in its profile set to 1. When a request is sent for broker domain maps, it uses the virtual name of shared AT as the broker name. The <code>bpbaz -GetDomainInfosFromAuthBroker</code> returns none. This work around should work fine because in the upgrade the <code>bp.conf</code> file is updated to have the NetBackup virtual name.

Table 4-4 Troubleshooting topics and configuration tips for NetBackup Authentication and Authorization (*continued*)

Topic	Configuration tips
Known issue of multiple instances of <code>bpcd</code> causing a possible error	There is a known issue that in the <code>bpbaz -SetupMedia</code> command, <code>bprd</code> uses the <code>AT_LOGINMACHINE_RQST</code> protocol to talk with <code>bpcd</code> on the destination box. A new instance of <code>bpcd</code> is spawned. After the command completes it tries to free a <code>char</code> array as a regular pointer possibly causing <code>bpcd</code> to core dump on the client side. Functionality should not be lost as this <code>bpcd</code> instance is only created temporarily and exits normally. The parent <code>bpcd</code> is unaffected.
Known issue with clusters using shared AT with configuration files on the shared drive	There is a known issue with clusters using 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 <code>bpbaz -SetupMaster</code> to manage remote broker parts fail. You will have to manually configure passive nodes. Run <code>bpbaz -SetupMedia</code> for each passive node.
Known issue relating to database utilities supporting NBAZDB	<p>There is a known issue that some database utilities support NBAZDB and other database utilities do not.</p> <p>The following database utilities support NBAZDB: <code>nbdb_backup</code>, <code>nbdb_move</code>, <code>nbdb_ping</code>, <code>nbdb_restore</code>, and <code>nbdb_admin</code>.</p> <p>The following utilities do not support NBAZDB: <code>nbdb_unload</code> and <code>dbadm</code>.</p>

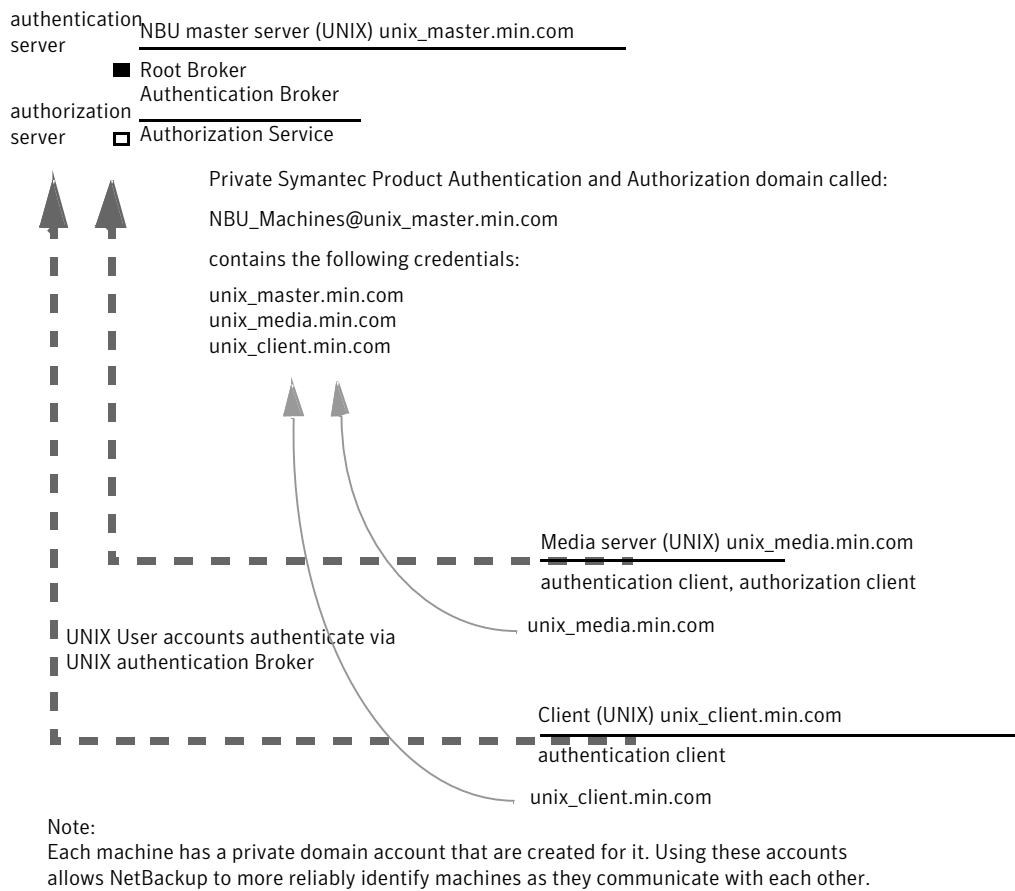
About the UNIX verification procedures

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 200.
- UNIX media server verification
See “[UNIX media server verification](#)” on page 203.
- UNIX client verification
See “[UNIX client verification](#)” on page 205.

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

Figure 4-8 Example configuration containing UNIX systems only



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 4-5 Verification process for the UNIX master server

Process	Description
Verify UNIX master server settings	<p>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 <code>bpnbat</code> with <code>-whoami</code> with <code>-cf</code> for the master server's credential file. The server credentials are located in the <code>/usr/opensv/var/vxss/credentials/</code> directory.</p> <p>For example:</p> <pre>bpnbat -whoami -cf /usr/opensv/var/vxss/credentials/unix_master.company.com Name: unix_master.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master/O=vx Expiry Date: Oct 31 15:44:30 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> <p>If the domain listed is not <code>NBU_Machines@unix_master.company.com</code>, or the file does not exist, consider running <code>bpnbat -addmachine</code> for the name in question (<code>unix_master</code>). Run this command on the computer that serves the <code>NBU_Machines</code> domain (<code>unix_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>unix_master</code>), run: <code>bpnbat -loginmachine</code></p> <p>Note: When determining if a credential has expired, remember that the output displays the expiration time in GMT, not local time.</p> <p>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 <code>bpnbat -login</code> using an identity that is a member of <code>NBU_Security Admin</code>. This identity is usually the first identity with which the security was set up.</p>
Verify which computers are present in the authentication broker	<p>To verify which computers are present in the authentication broker, log on as a member of the Administrators group and run the following command:</p> <pre>bpnbat -ShowMachines</pre> <p>The following command shows which computers you have run:</p> <pre>bpnbat -AddMachine</pre>

Table 4-5 Verification process for the UNIX master server (continued)

Process	Description
Verify which computers are permitted to perform authorization lookups	<p>To verify which computers can perform authorization lookups, log on as root on the authorization broker and run the following command:</p> <pre>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.</pre> <p>This command shows that <code>unix_master</code> and <code>unix_media</code> are permitted to perform authorization lookups. Note that both servers are authenticated against the same vx (Veritas Private Domain) Domain, <code>NBU_Machines@unix_master.company.com</code>.</p> <p>If a master server or media server is not part of the list of authorized computers, run <code>bpnbaz -allowauthorization <server_name></code> to add the missing computer.</p>
Verify that the database is configured correctly	<p>To make sure that the database is configured correctly, run <code>bpnbaz -listgroups</code>:</p> <pre>bpnbaz -listgroups NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If the groups do not appear, or if <code>bpnbaz -listmainobjects</code> does not return data, run <code>bpnbaz -SetupSecurity</code>.</p>

Table 4-5 Verification process for the UNIX master server (*continued*)

Process	Description
Verify that the nbatd and nbazd processes are running	<p>Run the <code>ps</code> command to ensure that the <code>nbatd</code> and <code>nbazd</code> processes are running on the designated host. If necessary, start them.</p> <p>For example:</p> <pre>ps -fed grep vx root 10716 1 0 Dec 14 ? 0:02 /usr/opensv/netbackup/bin/private/nbatd root 10721 1 0 Dec 14 ? 4:17 /usr/opensv/netbackup/bin/private/nbazd</pre>
Verify that the host properties are configured correctly	<p>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.)</p> <p>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.</p> <p>This process can also be verified in <code>bp.conf</code> using <code>cat</code>.</p> <pre>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 #</pre>

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 4-6 Verification process for the UNIX media server

Process	Description
Verify the media server	<p>To determine which authentication broker the media server is authenticated against, run <code>bpnbat -whoami -cf</code> for the media server's credential file. The server credentials are located in the <code>/usr/openv/var/vxss/credentials/</code> directory.</p> <p>For example:</p> <pre>bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com Name: unix_media.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master.company.com/ O=vx Expiry Date: Oct 31 14:48:08 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> <p>If the domain listed is not <code>NBU_Machines@unix_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>unix_media</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>unix_master</code>).</p> <p>Then, on the computer where we want to place the certificate, run (<code>unix_master</code>):</p> <pre>bpnbat -loginmachine</pre>
Verify that the server has access to the authorization database	<p>To make sure that the media server is able to access the authorization database as it needs, run <code>bpnbaz -ListGroup</code></p> <p>"machine_credential_file"</p> <p>For example:</p> <pre>bpnbaz -ListGroup -CredFile /usr/openv/var/vxss/credentials/unix_media.company.com NBU_User NBU_Operator NBU_Admin NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If this command fails, run <code>bpnbaz -AllowAuthorization</code> on the master server that is the authorization server (<code>unix_master</code>). Note that you need to run as root or administrator.</p>

Table 4-6 Verification process for the UNIX media server (*continued*)

Process	Description
Unable to load library message	<p>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.</p> <p>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 <code>cat(1)</code>ing the <code>bp.conf</code> file.</p>

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 4-7 Verification procedures for the UNIX client

Procedures	Description
Verify the credential for the UNIX client	<p>Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre>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.</pre> <p>If the domain listed is not <code>NBU_Machines@unix_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>unix_client</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>unix_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>unix_client</code>), run: <code>bpnbat -loginmachine</code></p>
Verify that the authentication client libraries are installed	<p>Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre>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.</pre>

Table 4-7 Verification procedures for the UNIX client (continued)

Procedures	Description
Verify correct authentication domains	<p>Check that any defined authentication domains for the client are correct in the Access Control host properties or by using <code>cat (1)</code>. 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.</p> <p>This process can also be verified in <code>bp.conf</code> using <code>cat (1)</code>.</p> <pre>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</pre>

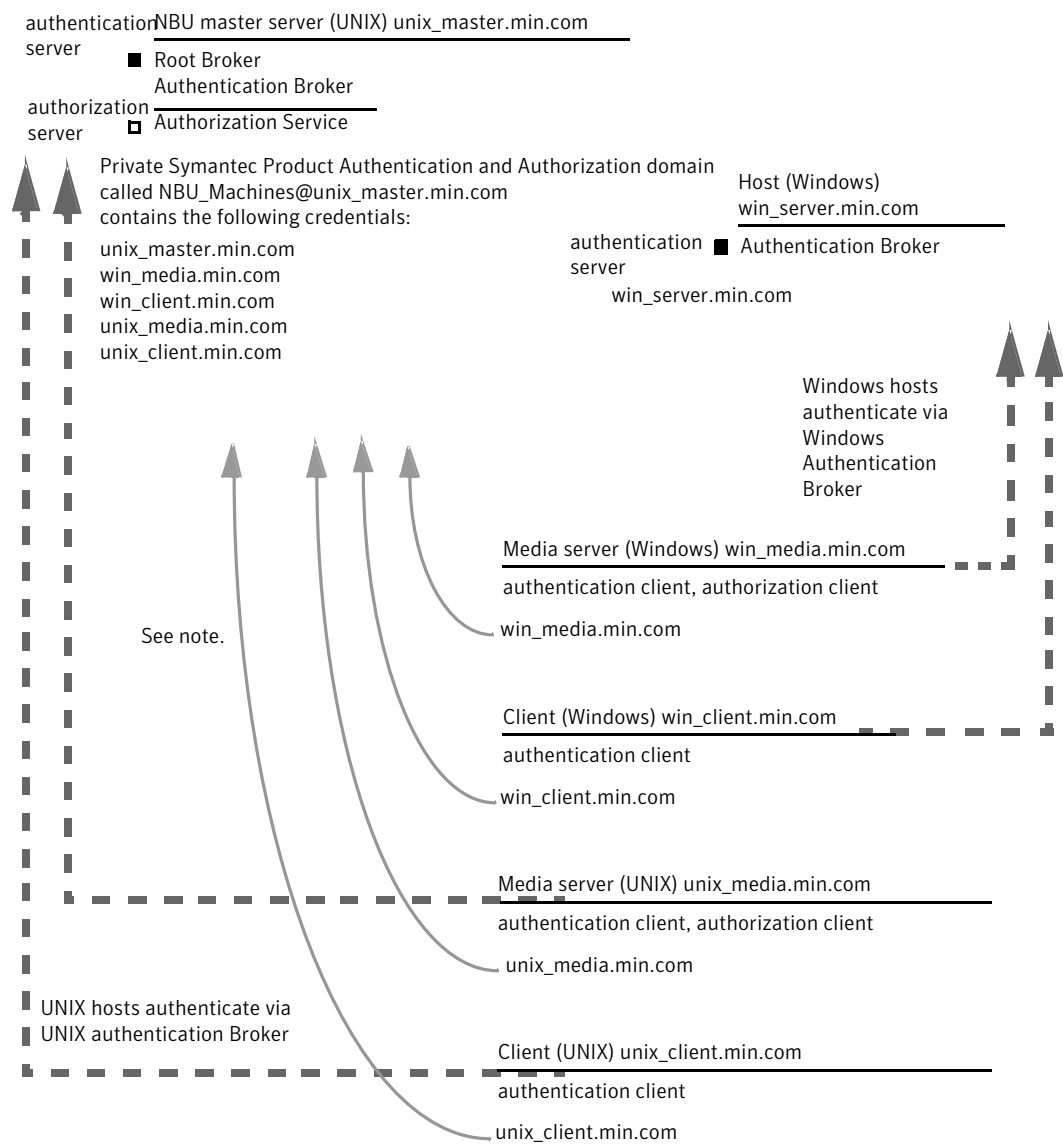
Verification points in a mixed environment with a UNIX master server

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

See [Figure 4-9](#) on page 208. for an example of a mixed configuration that contains a UNIX master server.

Figure 4-9 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 “UNIX master server verification” on page 200. for the verification procedure for a UNIX master server.

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.

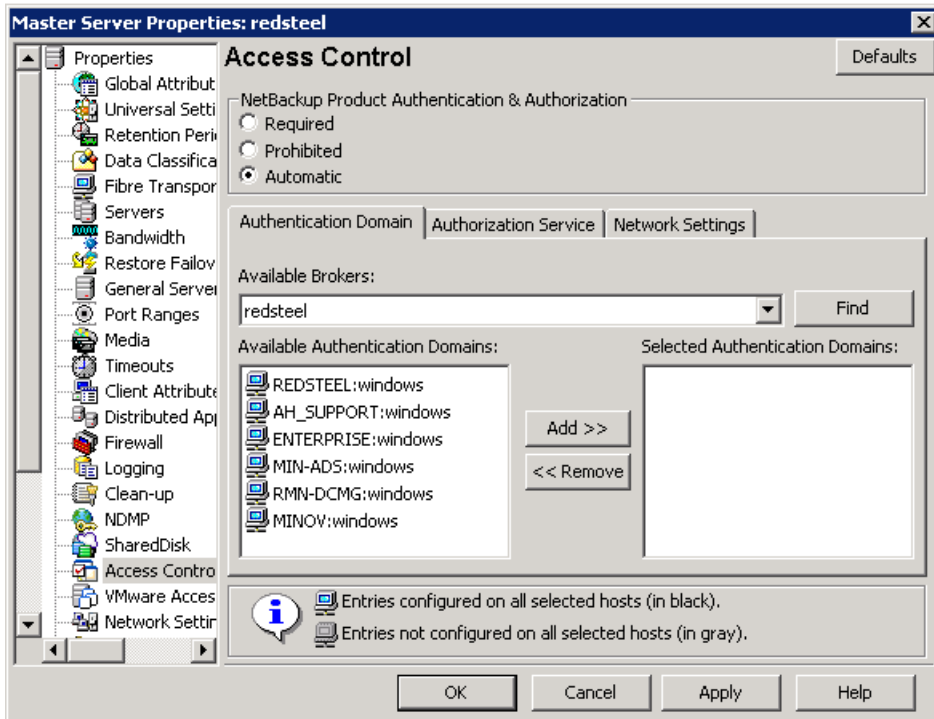
Table 4-8 Verification procedures for a mixed UNIX master server

Procedure	Description
Verify the UNIX media server	See “UNIX media server verification” on page 203. for the verification procedure for a UNIX media server.
Verify the Windows media server	<p>Check that the computer certificate comes from the root authentication broker, which is found on the UNIX master server (unix_master).</p> <p>If there is a missing certificate, run the following commands to correct the problem:</p> <ul style="list-style-type: none">■ bpnbat -addmachine on the root authentication broker (in this example, unix_master)■ bpnbat -loginmachine (in this example, win_media) <p>For example:</p> <pre>bpnbat -whoami -cf "C:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@ unix_master.company.com/O=vx Expiry Date: Oct 31 20:11:04 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>

Table 4-8 Verification procedures for a mixed UNIX master server (continued)

Procedure	Description
Verify that a media server is permitted to perform authorization lookups	<p>Ensure that the media server is allowed to perform authorization checks by running <code>bpnbaz -listgroups -CredFile</code>.</p> <p>For example:</p> <pre>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.</pre> <p>If the media server is not allowed to perform authorization checks, run <code>bpnbaz -allowauthorization</code> on the master server for the media server name in question.</p>
Unable to load library message	<p>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.</p>
Verify authentication domains	<p>Verify that the authentication domains are correct by viewing the access control host properties for this media server.</p> <p>You can also use <code>regedit</code> (or <code>regedit32</code>) directly on the media server in the following location:</p> <pre>HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\ CurrentVersion\config\AUTHENTICATION_DOMAIN</pre>
Cross platform authentication domains	<p>Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers.</p> <p>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.</p> <p>See Figure 4-10 on page 211. for a display on how to match the platform to the most useful authentication domains.</p>

Cross platform authentication domains



Client verification points for a mixed UNIX master server

See “[UNIX client verification](#)” on page 205. for the procedures to verify the UNIX client computers.

The following table describes the procedures to verify Windows clients.

Table 4-9 Procedures to verify Windows clients

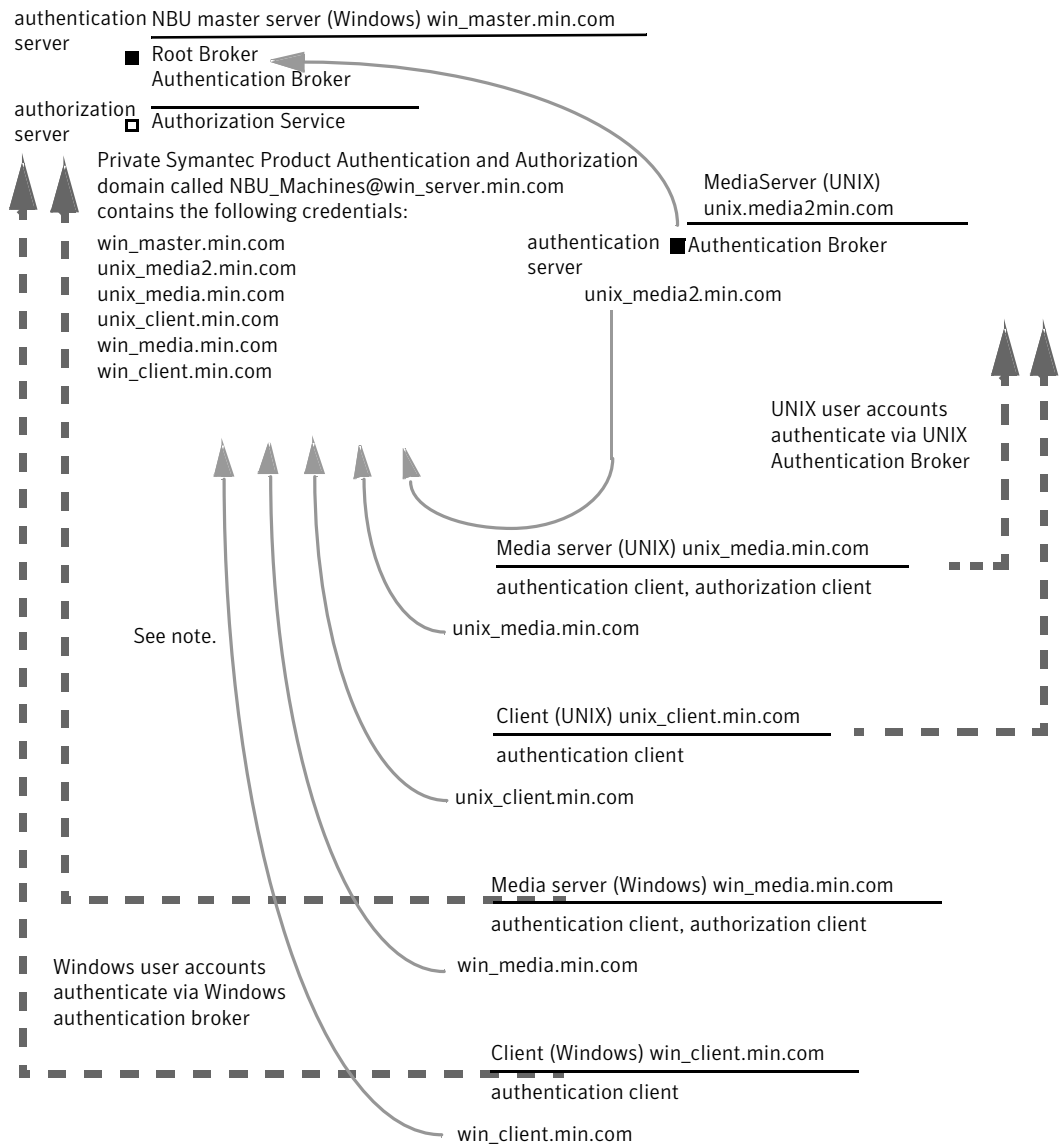
Procedures	Description
Verify the credential for the Windows client	<p>Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre>bpnbat -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.</pre>
Verify that the authentication client libraries are installed	<p>Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <p>For example:</p> <pre>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.</pre>
Verify the Windows authentication broker	<p>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.</p>

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 215.
- Media server verification points for mixed Windows master
See [“Media server verification points for a mixed Windows master server”](#) on page 215.
- Client verification points for mixed Windows master
See [“Client verification points for a mixed Windows master server”](#) on page 217.
See [Figure 4-11](#) on page 214. for an example configuration that contains a Windows master server.

Figure 4-11 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 “[Master server verification points for Windows](#)” on page 220. for the verification procedures for a mixed Windows master server.

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 4-10 Media server verification procedures for a mixed Windows master server

Procedure	Description
Verify the Windows media server for a mixed Windows master server	See “ Media server verification points for Windows ” on page 224. for the verification procedures for a Windows media server.
Verify the UNIX media server	<p>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 <code>bpnbat -whoami</code> with <code>-cf</code> for the media server's credential file.</p> <p>For example:</p> <pre>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.</pre>

Table 4-10

Media server verification procedures for a mixed Windows master server (continued)

Procedure	Description
Verify that the server has access to the authorization database	<p>To make sure that the media server is able to access the authorization database it needs to perform authorization checks. Run <code>bpbaz -ListGroup -CredFile "/usr/opensv/var/vxss/credentials/<hostname>"</code></p> <p>For example:</p> <pre>bpbaz -ListGroup -CredFile\ /usr/opensv/var/vxss/credentials/unix_media.company.com NBU_Operator NBU_AdminNBU_SAN Admin NBU_UserNBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If the media server is not allowed to perform authorization checks, run <code>bpbaz -allowauthorization</code> on the master server for the media server name in question.</p>
Unable to load library message	<p>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.</p>

Table 4-10

Media server verification procedures for a mixed Windows master server *(continued)*

Procedure	Description
Cross platform authentication domains	<p>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 <code>cat (1)</code> ing the <code>bp.conf</code> file.</p> <p>Take extra care in mixed environments to ensure that the appropriate domain types point to the correct authentication brokers.</p> <p>In the example, note that the <code>PASSWD</code> domains and <code>NIS</code> domains point to <code>unix_media2.company.com</code>, which, in this example, is the UNIX authentication broker:</p> <pre>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</pre>

Client verification points for a mixed Windows master server

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

Table 4-11

Verification procedures for a mixed Windows master server

Procedure	Description
Verify the credential for the Windows client	See “Client verification points for Windows” on page 226. for the verification procedures for Windows clients.

Table 4-11

Verification procedures for a mixed Windows master server

(continued)

Procedure	Description
Verify the credential for the UNIX client	<p>Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre>bpnbat -whoami -cf \ "/usr/opensv/var/vxss/credentials/ unix_client.company.com" Name: unix_client.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@ win_master.company.com/O=vx Expiry Date: Oct 31 21:16:01 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre>
Verify that the authentication client libraries are installed	<p>Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre>bpnbat -login Authentication Broker: unix_media2.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : NIS Domain: min.com Name: Smith Password: You do not currently trust the server: unix_media.company.com, do you wish to tr ust it? (y/n): y Operation completed successfully.</pre>
Verify the UNIX authentication broker	<p>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.</p>

Windows verification points

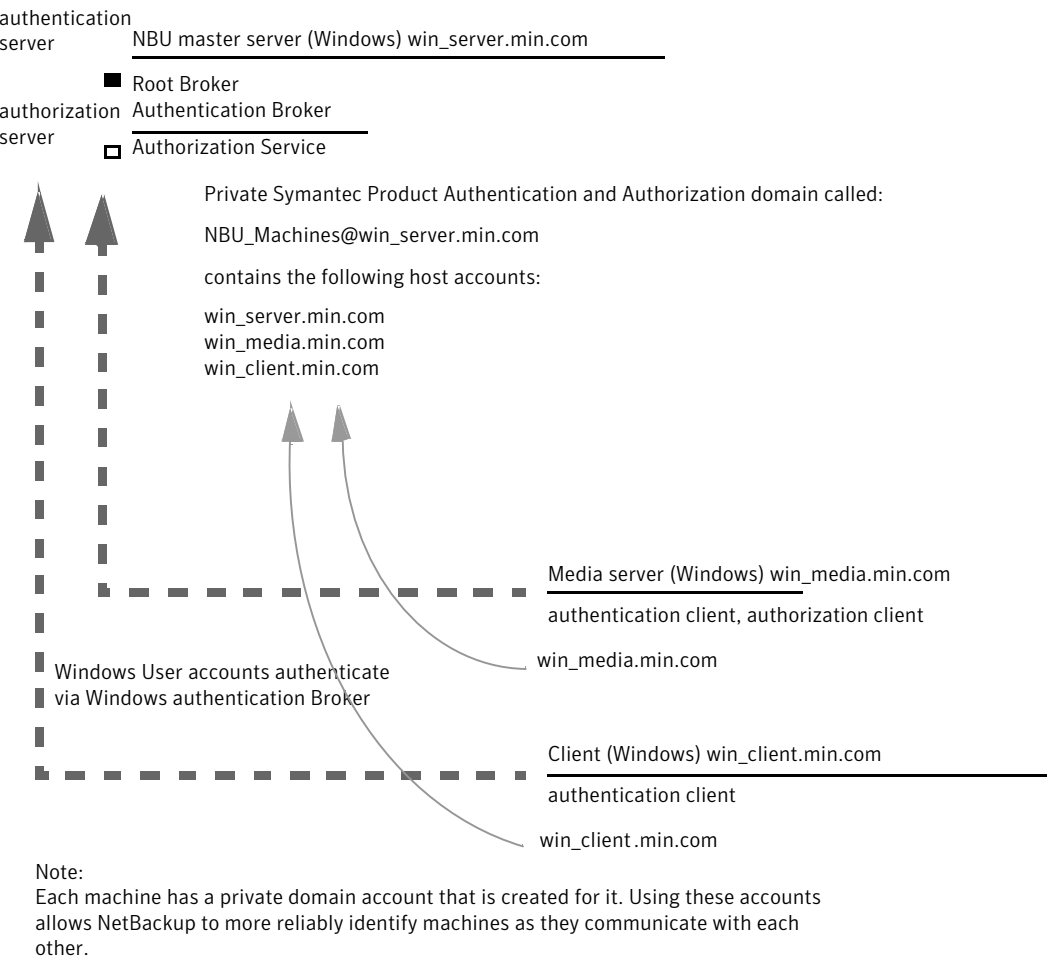
The following configuration procedures can help you verify that the master server, media server, and client are configured correctly for access control.

These Windows verification points include:

- See [“Master server verification points for Windows”](#) on page 220.
- See [“Media server verification points for Windows”](#) on page 224.
- See [“Client verification points for Windows”](#) on page 226.

[Figure 4-12](#) shows an example configuration containing Windows systems only.

Figure 4-12 Example configuration containing Windows systems only



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 4-12 Master server verification procedures for Windows

Procedure	Description
Verify Windows master server settings	<p>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 <code>bpnbat</code> with <code>-whoami</code> and specify the host credential file. The server credentials are located in the <code>c:\Program Files\Veritas\Netbackup\var\vxss\credentials\...</code> directory.</p> <p>For example:</p> <pre>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.</pre> <p>If the domain listed is not <code>NBU_Machines@win_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>win_master</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>win_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>win_master</code>), run:</p> <pre>bpnbat -loginmachine</pre> <p>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.</p> <p>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 <code>bpnbat -login</code> from that window. The user is an identity that is a member of <code>NBU_Security Admin</code>. This identity is usually the first identity with which the security was set up.</p>

Table 4-12 Master server verification procedures for Windows (continued)

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

Table 4-12 Master server verification procedures for Windows (*continued*)

Procedure	Description
Verify that the database is configured correctly	<p>To make sure that the database is configured correctly, run <code>bpnbaz -listgroups</code>:</p> <pre>bpnbaz -listgroups NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If the groups do not appear, or if <code>bpnbaz -listmainobjects</code> does not return data, you may need to run <code>bpnbaz -SetupSecurity</code>.</p>
Verify that the <code>nbatd</code> and <code>nbazd</code> processes are running	Use the Windows Task Manager to make sure that <code>nbatd.exe</code> and <code>nbazd.exe</code> are running on the designated host. If necessary, start them.
Verify that the host properties are configured correctly	<p>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.</p> <p>The host properties can also be verified by looking at <code>USE_VXSS</code> in the registry at:</p> <pre>HKEY_LOCAL_MACHINE\Software\Veritas\NetBackup\ CurrentVersion\config.</pre> <p>See Figure 4-13 on page 224. for an example of the host properties settings on the Authentication domain tab.</p> <p>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.</p>

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

Figure 4-13 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 4-13 Media server verification procedures for Windows

Procedure	Description
Verify the media server	<p>To determine which authentication broker the media server is authenticated against, run <code>bpnbat -whoami -cf</code> for the media server's credential file. The server credentials are located in the <code>c:\Program Files\Veritas\Netbackup\var\vxss\credentials\...</code> directory.</p> <p>For example:</p> <pre>bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:11:40 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> <p>If the domain listed is not <code>NBU_Machines@win_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>win_media</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>win_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>win_media</code>), run:</p> <pre>bpnbat -loginmachine</pre>

Table 4-13 Media server verification procedures for Windows (continued)

Procedure	Description
Verify that the server has access to the authorization database	<p>To make sure that the media server is able to access the authorization database as it needs, run <code>bpnbaz -ListGroup -CredFile "machine_credential_file"</code></p> <p>For example:</p> <pre>bpnbaz -ListGroup -CredFile "C:\Program Files\Veritas\NetBackup\var\vxss\credentials\ win_media.company.com" NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully.</pre> <p>If this command fails, run <code>bpnbaz -AllowAuthorization</code> on the master server that is the authorization server (<code>win_master.company.com</code>).</p>
Unable to load library message	<p>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.</p> <p>You may also verify that the authentication domains are correct by viewing the access control host properties for this media server.</p>

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 4-14 Client verification procedures for Windows

Procedure	Description
Verify the credential for the client	<p>Check that the credential for the client is indeed for the correct client and comes from the correct domain. Run <code>bpnbat -whoami</code> with <code>-cf</code> for the client's credential file.</p> <p>For example:</p> <pre>bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_client.company.com " Name: win_client.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:11:45 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.</pre> <p>If the domain listed is not <code>NBU_Machines@win_master.company.com</code>, consider running <code>bpnbat -addmachine</code> for the name in question (<code>win_client</code>). This command is run on the computer with the authentication broker that serves the <code>NBU_Machines</code> domain (<code>win_master</code>).</p> <p>Then, on the computer where we want to place the certificate (<code>win_client</code>), run:</p> <pre>bpnbat -loginmachine</pre>
Verify that the authentication client libraries are installed	<p>Note:</p> <p>Run <code>bpnbat -login</code> on the client to verify that the authentication client libraries are installed.</p> <pre>bpnbat -login Authentication Broker: win_master Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : WINDOWS Domain: ENTERPRISE Name: Smith Password: Operation completed successfully.</pre> <p>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.</p>

Table 4-14 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 <code>regedit</code> . 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** mode in the GUI. 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/opensv/netbackup/bin/admincmd`

Windows

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

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

```
bpnbaz -ListGroups
NBU_User
NBU_Operator
NBU_Admin
NBU_Security Admin
Vault_Operator
NBU_SAN Admin
NBU_KMS Admin
Operation completed successfully.
```

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

About determining who can access NetBackup

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

- The permissions of individual users.
See [“Individual users”](#) on page 229.
- The creation of user groups.
See [“User groups”](#) on page 230.

First, determine which NetBackup resources your users need to access.

See [“Viewing specific user permissions for NetBackup user groups”](#) on page 243. for resources and associated permissions.

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.

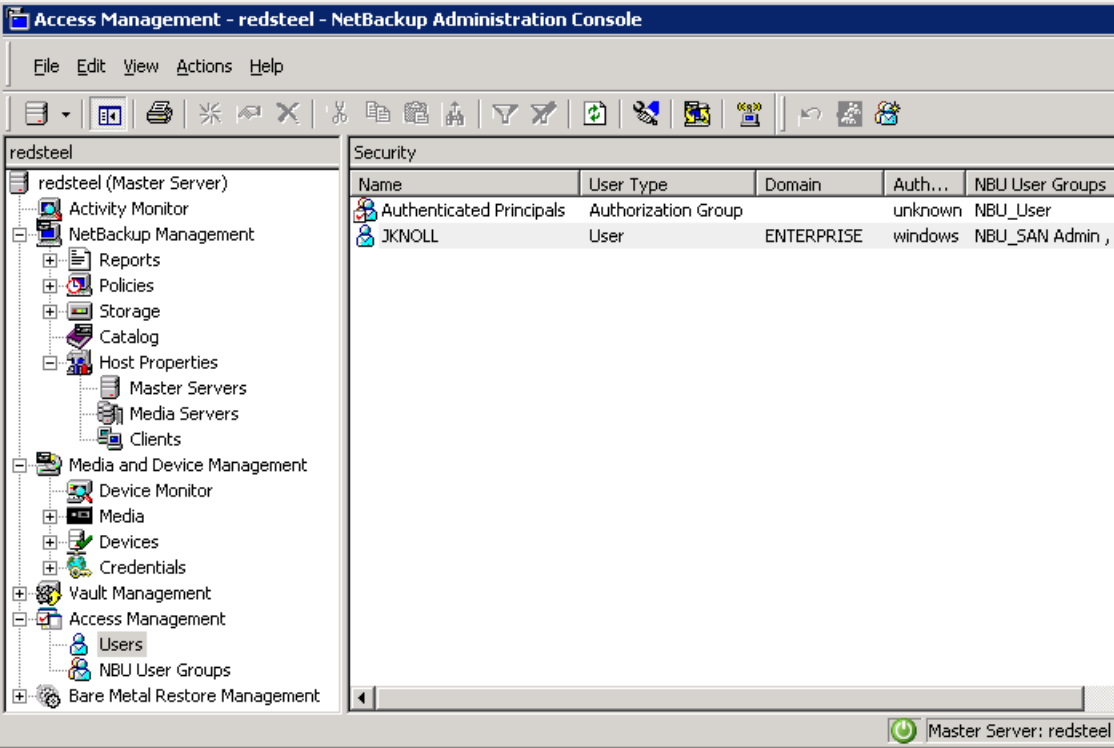
Individual users

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.

See [Figure 4-14](#) on page 230. for a display of the individual authenticated users.

Figure 4-14 Individual users



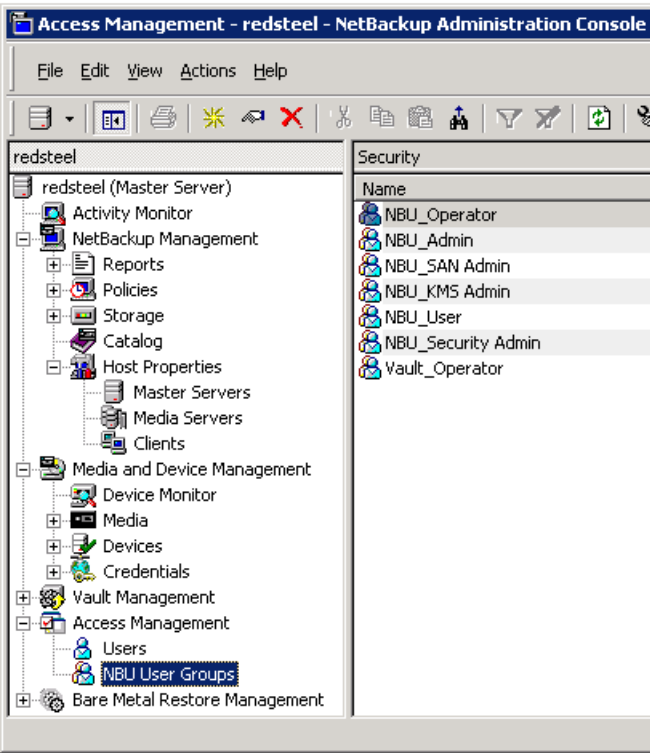
All authenticated users are implicit members of the NBU_Users user group. All other groups must have members defined explicitly. The NetBackup Security Administrator can delete a manually added member to other groups. However, the Security Administrator may not delete the predefined implicit members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

See [Figure 4-15](#) on page 231. for a display of the user groups.

Figure 4-15 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 4-15

NetBackup default user groups

Default user group	Description
Operator (NBU_Operator)	<p>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.</p> <p>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.</p>
Administrator (NBU_Admin)	<p>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.</p> <p>Note: Members of the NBU_Admin user group cannot see the contents of Access Management, and therefore, cannot ascribe permissions to other user groups.</p>
SAN Administrator (NBU_SAN Admin)	<p>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.</p>
User (NBU_User)	<p>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).</p>
Security administrator (NBU_Security Admin)	<p>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:</p> <ul style="list-style-type: none">■ 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 4-15 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. They can be created by expanding **Access Management > Actions > New Group** or by selecting an existing user group and expanding **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 235. for more information on users.
- 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 240.

- 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

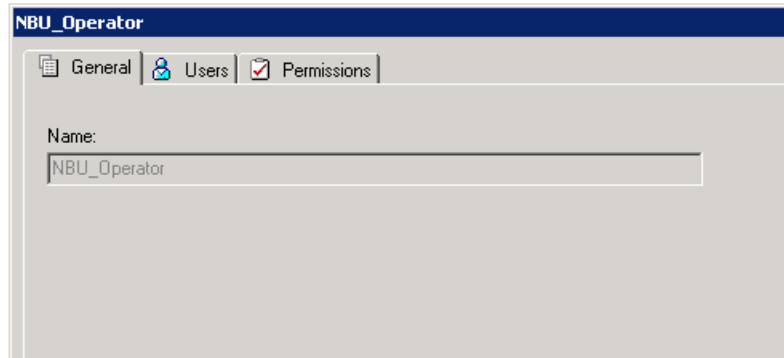
Once a NetBackup user group has been created, the user group cannot be renamed. The alternative to directly renaming a user group is to follow these steps: copy the user group, give the copy a new name, ensure the same membership as the original, then delete the original NetBackup user group.

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 4-16 General tab

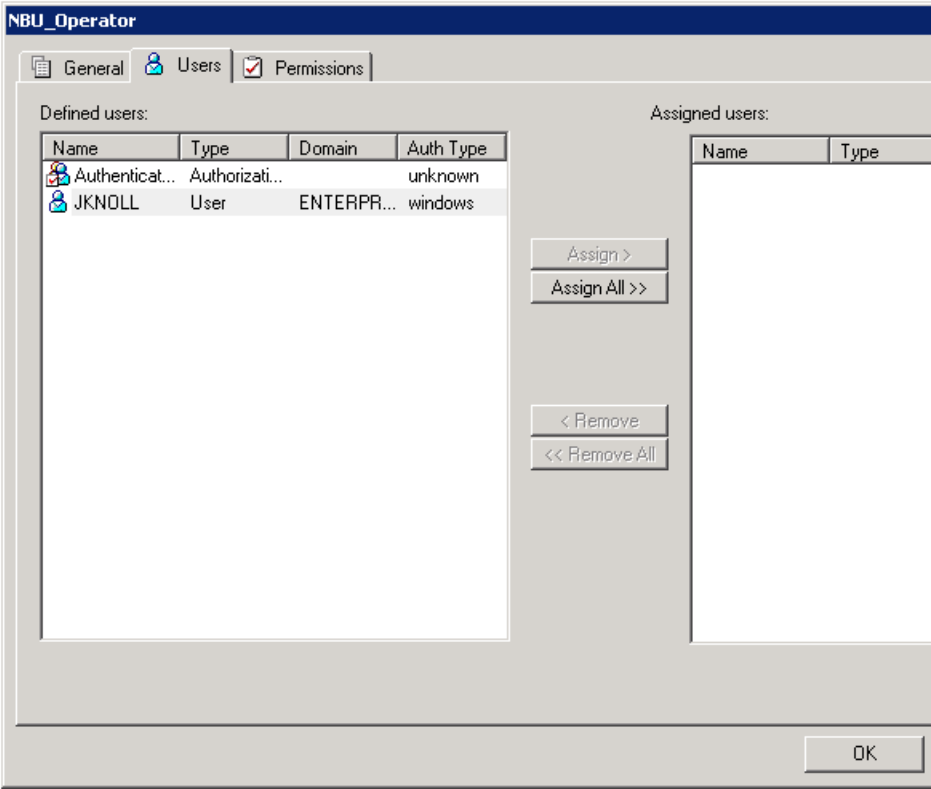


Users tab

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

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

Figure 4-17 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 239.

About defining a user group and users

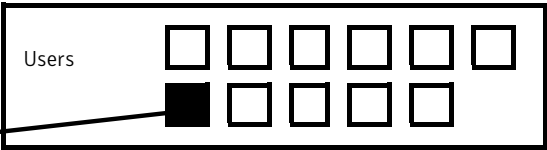
NetBackup authenticates existing users of the operating system instead of requiring that NetBackup users be created with a NetBackup password and profile.

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

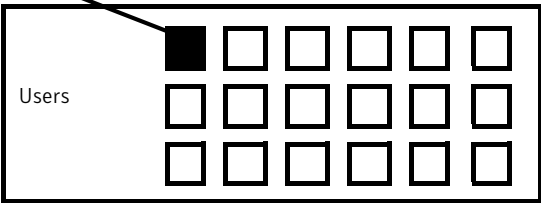
[Figure 4-18](#) shows defining a user group.

Figure 4-18 Defining a user group

User_Group_1



User_Group_2

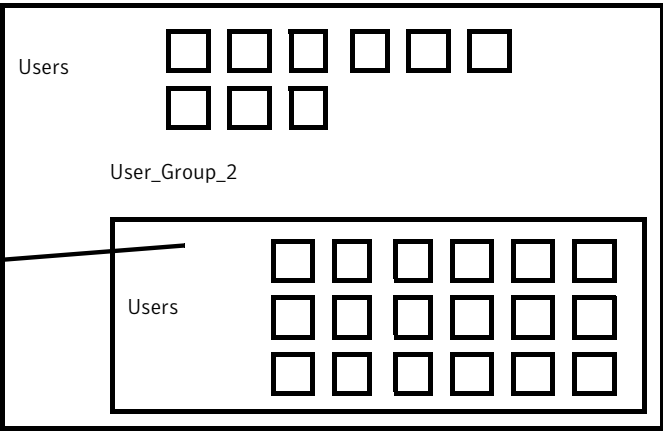


Users can be members of multiple user groups simultaneously, but NetBackup does not allow user groups to be nested. For example, members of a user group can belong to more than one user group, but a user group cannot belong to another user group.

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

Figure 4-19 Nested user groups are not allowed

User_Group_1



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 systems 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.

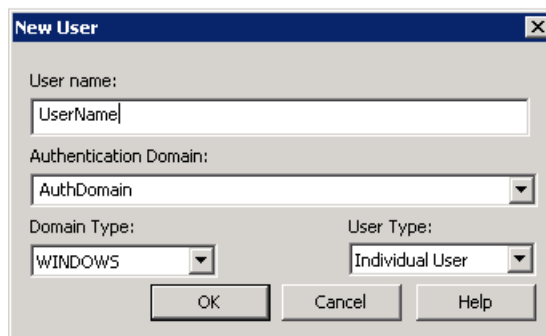
Assigning a user to a user group

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 being 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:

A screenshot of a 'New User' dialog box. It has a title bar with 'New User' and a close button. The dialog contains four input fields: 'User name:' with a text box containing 'UserName'; 'Authentication Domain:' with a dropdown menu showing 'AuthDomain'; 'Domain Type:' with a dropdown menu showing 'WINDOWS'; and 'User Type:' with a dropdown menu showing 'Individual User'. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

- 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

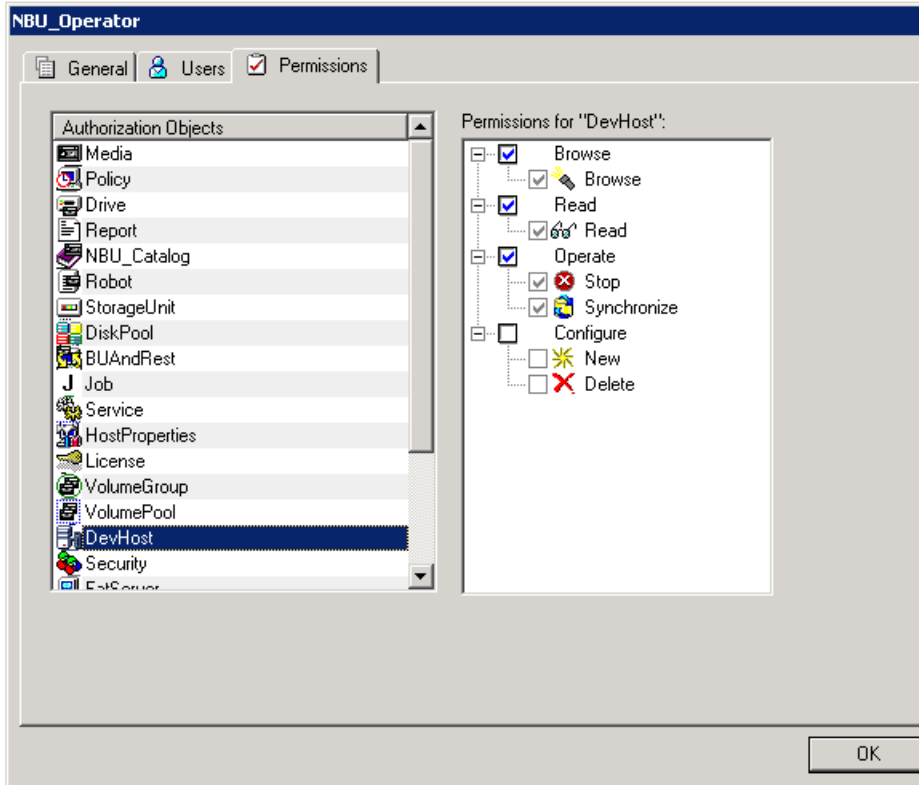
The **Permissions** tab contains a list of the NetBackup authorization objects and configurable permissions that are associated with each object.

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 4-20 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.

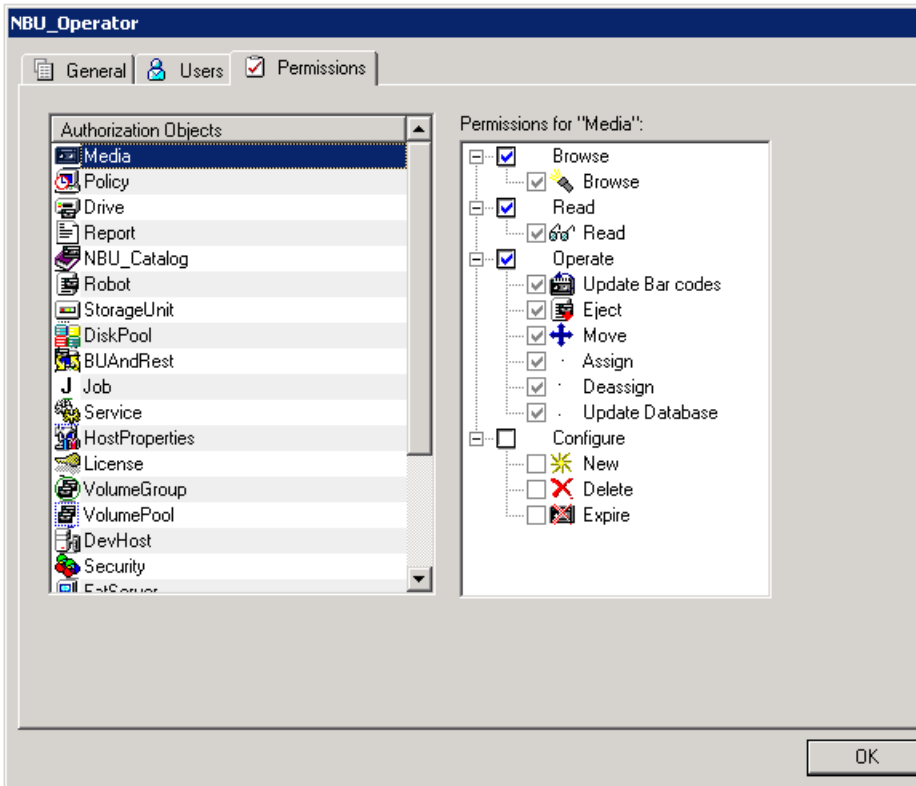
To grant a permission to the members of a user group

- 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 4-21 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 [“Media authorization object permissions”](#) on page 245.
- See [“Policy authorization object permissions”](#) on page 245.
- See [“Drive authorization object permissions”](#) on page 246.
- See [“Report authorization object permissions”](#) on page 247.
- See [“NBU_Catalog authorization object permissions”](#) on page 247.
- See [“Robot authorization object permissions”](#) on page 248.
- See [“Storage unit authorization object permissions”](#) on page 248.
- See [“DiskPool authorization object permissions”](#) on page 249.
- See [“BUAndRest authorization object permissions”](#) on page 250.
- See [“Job authorization object permissions”](#) on page 250.
- See [“Service authorization object permissions”](#) on page 251.
- See [“HostProperties authorization object permissions”](#) on page 252.
- See [“License authorization object permissions”](#) on page 252.
- See [“Volume group authorization object permissions”](#) on page 253.
- See [“VolumePool authorization object permissions”](#) on page 253.
- See [“DevHost authorization object permissions”](#) on page 254.
- See [“Security authorization object permissions”](#) on page 254.
- See [“Fat server authorization object permissions”](#) on page 255.
- See [“Fat client authorization object permissions”](#) on page 255.
- See [“Vault authorization object permissions”](#) on page 256.
- See [“Server group authorization object permissions”](#) on page 256.

- See “[Key management system \(kms\) group authorization object permissions](#)” on page 257.

Media authorization object permissions

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

Table 4-16 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							
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 4-17 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 4-17 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 4-18 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 4-19 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 4-20 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 4-20 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	---	X	---	---	---	---	---
	Configuration	---	X	---	---	---	---	---
	Set Configuration							

Robot authorization object permissions

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

Table 4-21 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 4-22 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 4-23 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	---	---	---	---
		---	---	X	---	---	---	---
	Set Configuration							

BUAndRest authorization object permissions

The following table shows the permissions that are associated with the backup and restore authorization object.

Table 4-24BUAndRest authorization object permissions

Set	Activity	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Browse	Browse	X	X	X	X	---	---	X
Read	Read	X	X	X	X	---	---	X
Operate	Back up	X	X	X	X	---	---	X
	Restore	X	X	X	X	---	---	X
	Alternate Client	X	X	---	---	---	---	---
	Alternate Server	X	X	---	---	---	---	---
	Admin Access	X	X	---	---	---	---	---
	Database Agent	X	X	X	X	---	---	X
	List							

Job authorization object permissions

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

Table 4-25Job 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 4-25 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 4-26 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 4-27 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 4-28 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 4-29 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 4-30 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 4-30 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: Access to the "Media and Device Management --> Credentials" node in the GUI is controlled by the DevHost object.

Table 4-31 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 4-32 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 4-33 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 4-34 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 4-34 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 4-35 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 4-36 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 4-36 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 managment system (kms) group authorization object permissions

The following table shows the permissions that are associated with the Key management system group authorization object.

Table 4-37 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

Data at rest encryption security

This chapter includes the following topics:

- [Data at rest encryption terminology](#)
- [Data at rest encryption limitations](#)
- [Encryption security questions to consider](#)
- [NetBackup data at rest encryption options](#)
- [Encryption options comparison](#)
- [Option 1 - NetBackup client encryption](#)
- [About running an encryption backup](#)
- [About choosing encryption for a backup](#)
- [Standard encryption backup process](#)
- [Legacy encryption backup process](#)
- [NetBackup standard encryption restore process](#)
- [NetBackup legacy encryption restore process](#)
- [Installation prerequisites for encryption security](#)
- [Installing encryption on a UNIX NetBackup server](#)
- [Installing encryption on a Windows NetBackup server](#)
- [About installing encryption locally on a NetBackup UNIX client](#)

- [About installing encryption locally on a NetBackup Windows client](#)
- [About configuring standard encryption on clients](#)
- [Managing standard encryption configuration options](#)
- [Managing the NetBackup encryption key file](#)
- [About configuring standard encryption from the server](#)
- [About creating encryption key files on clients notes](#)
- [Creating the key files](#)
- [Best practices for key file restoration](#)
- [Manual retention to protect key file pass phrases](#)
- [Automatic backup of the key file](#)
- [Restoring an encrypted backup file to another client](#)
- [About configuring standard encryption directly on clients](#)
- [Setting standard encryption attribute in policies](#)
- [Changing the client encryption settings from the NetBackup server](#)
- [About configuring legacy encryption](#)
- [About configuring legacy encryption from the server](#)
- [Legacy encryption configuration options](#)
- [About pushing the legacy encryption configuration to clients](#)
- [About pushing the legacy encryption pass phrases to clients](#)
- [Managing legacy encryption key files](#)
- [Restoring a legacy encrypted backup created on another client](#)
- [About setting legacy encryption attribute in policies](#)
- [Changing client legacy encryption settings from the server](#)
- [Additional legacy key file security for UNIX clients](#)
- [Running the bpcd -keyfile command](#)
- [Terminating bpcd on UNIX clients](#)
- [Option 2 - Media server encryption](#)

■ [Media server encryption option administration](#)

Data at rest encryption terminology

The following table describes the data at rest encryption terminology.

Table 5-1 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 5-2 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 5-2 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	<p>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 five 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.</p> <p>"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."</p> <p>For more information, refer to this Web site : http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf.</p>
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 5-2 Data at rest encryption limitations (*continued*)

Limitation	Description
FIPS certification for my encryption solution	<p>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.</p> <p>Other considerations should be part of any decision making process as follows:</p> <ul style="list-style-type: none"> ■ 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 exists 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 / 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. <p>Usability considerations include the following:</p> <ul style="list-style-type: none"> ■ Encryption integration with the product ■ Encryption integration with business processes. ■ Appropriate encryption key granularity ■ Recoverability
Appropriate encryption key granularity	<p>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.</p> <p>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.</p>

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

See [Table 5-3](#) on page 265. for a comparison of the following three NetBackup data at rest encryption options.

- Option 1 - NetBackup client encryption
See “[Option 1 - NetBackup client encryption](#)” on page 265.
- Option 2 - Media server encryption
See “[Option 2 - Media server encryption](#)” on page 290.
- 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 5-3 Encryption options comparison

Encryption option	Potential advantages	Potential disadvantages
See “ Option 1 - NetBackup client encryption ” on page 265.	<ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ 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 290.	<ul style="list-style-type: none"> ■ Will not affect client computer performance ■ Master / Media server centralized keys 	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Generally little (or no performance) affect due to added hardware. ■ Generally NIST FIPS 140 certified. 	<ul style="list-style-type: none"> ■ 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 266.
- Standard encryption backup process
See “[Standard encryption backup process](#)” on page 267.
- Legacy encryption backup process
See “[Legacy encryption backup process](#)” on page 267.

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 5-4 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 267. for a description of the backup process for standard encryption. See “[NetBackup standard encryption restore process](#)” on page 268. for a description of the restore process for standard encryption.

See “[Legacy encryption backup process](#)” on page 267. for a description of the backup process for legacy encryption. See “[NetBackup legacy encryption restore process](#)” on page 269. for a description of the restore process for legacy encryption.

Standard encryption backup process

The prerequisites for encrypting a standard backup are as follows:

- **Note:** In NetBackup 7.5 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 `bkeyutil` 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 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 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 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 7.5 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 272. for information on how to configure the client encryption settings.

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 272. for information on how to configure the client encryption settings.

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, Vol. 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 5-5 Three encryption-related configuration options

Option	Value	Description
CRYPT_OPTION = <i>option</i>		Defines the encryption options on NetBackup clients. The possible values for <i>option</i> 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.

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

Option	Value	Description
<code>CRYPT_KIND = kind</code>		Defines the encryption kind on NetBackup clients. The <i>kind</i> 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.
<code>CRYPT_CIPHER = cipher</code>		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 6.0 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/opensv/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* 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 278.
- Changing client encryption settings from the server
See [“Changing the client encryption settings from the NetBackup server”](#) on page 278.

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 [“Managing standard encryption configuration options”](#) on page 272. for the configuration options that correspond to the settings in the **Encryption** pane.

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 for UNIX and Linux, Vol. 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 6.0 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 on the options that are available with the `bpinst` command. See [“About pushing the legacy encryption configuration to clients”](#) on page 282. and See [“About pushing the legacy encryption pass phrases to clients”](#) on page 282. for examples of how to use `bpinst`.

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 5-6 Legacy encryption configuration options

Option	Value	Description
<code>CRYPT_OPTION = option</code>		Defines the encryption options on NetBackup clients. The possible values for <i>option</i> follow:
	<code>denied DENIED</code>	Specifies that the client does not permit encrypted backups. If the server requests an encrypted backup, it is considered an error.
	<code>allowed ALLOWED</code>	(The default value) Specifies that the client allows either encrypted or unencrypted backups.

Table 5-6 Legacy encryption configuration options (*continued*)

Option	Value	Description
	required REQUIRED	Specifies that the client requires encrypted backups. If the server requests an unencrypted backup, it is considered an error.
CRYPT_KIND = <i>kind</i>		Defines the encryption type on NetBackup clients. The possible values for <i>kind</i> 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.
CRYPT_STRENGTH = <i>strength</i>		Defines the encryption strength on NetBackup clients. The possible values for <i>strength</i> 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 = <i>directory_path</i>		Defines the directory that contains the encryption libraries on NetBackup clients. The <i>install_path</i> is the directory where NetBackup is installed and by default is C:\VERITAS.
	/usr/opensv/lib/	The default value on UNIX systems.
	<i>install_path</i> \NetBackup\bin\	The default value on Windows systems
CRYPT_KEYFILE = <i>file_path</i>		Defines the file that contains the encryption keys on NetBackup clients.
	/usr/opensv/netbackup/keyfile	The default value on UNIX systems.
	<i>install_path</i> \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/opensv/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 288. for more details.

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/opensv/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.

Suppose you want to enter a new NetBackup pass phrase on a Windows client.

You would enter a command like the following:

```
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* 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 289., for more information about this parameter.

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/opensv/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
- Each device

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

Data at rest key management

This chapter includes the following topics:

- [About the Key Management Service \(KMS\)](#)
- [KMS considerations](#)
- [KMS principles of operation](#)
- [About writing an encrypted tape](#)
- [About reading an encrypted tape](#)
- [KMS terminology](#)
- [Installing KMS](#)
- [Using KMS with NBAC](#)
- [About installing KMS with HA clustering](#)
- [Enabling cluster use with the KMS service](#)
- [Enabling the monitoring of the KMS service](#)
- [Disabling the monitoring of the KMS service](#)
- [Removing the KMS service from monitored list](#)
- [Configuring KMS](#)
- [Creating the key database](#)
- [About key groups and key records](#)

- [About creating key groups](#)
- [About creating key records](#)
- [Overview of key record states](#)
- [Key record state considerations](#)
- [Prelive key record state](#)
- [Active key record state](#)
- [Inactive key record state](#)
- [Deprecated key record state](#)
- [Terminated key record state](#)
- [About backing up the KMS database files](#)
- [About recovering KMS by restoring all data files](#)
- [Recovering KMS by restoring only the KMS data file](#)
- [Recovering KMS by regenerating the data encryption key](#)
- [Problems backing up the KMS data files](#)
- [Solutions for backing up the KMS data files](#)
- [Creating a key record](#)
- [Listing keys](#)
- [Configuring NetBackup to work with KMS](#)
- [NetBackup and key records from KMS](#)
- [Example of setting up NetBackup to use tape encryption](#)
- [About using KMS for encryption](#)
- [Example of running an encrypted tape backup](#)
- [Example of verifying an encryption backup](#)
- [About importing KMS encrypted images](#)
- [KMS database constituents](#)
- [Creating an empty KMS database](#)
- [Importance of the KPK ID and HMK ID](#)

- [About periodically updating the HMK and KPK](#)
- [Backing up the KMS keystore and administrator keys](#)
- [Command line interface \(CLI\) commands](#)
- [CLI usage help](#)
- [Create a new key group](#)
- [Create a new key](#)
- [Modify key group attributes](#)
- [Modify key attributes](#)
- [Get details of key groups](#)
- [Get details of keys](#)
- [Delete a key group](#)
- [Delete a key](#)
- [Recover a key](#)
- [Modify host master key \(HMK\)](#)
- [Get host master key \(HMK\) ID](#)
- [Get key protection key \(KPK\) ID](#)
- [Modify key protection key \(KPK\)](#)
- [Get keystore statistics](#)
- [Quiesce KMS database](#)
- [Unquiesce KMS database](#)
- [Key creation options](#)
- [Troubleshooting KMS](#)
- [Solution for backups not encrypting](#)
- [Solution for restores not decrypting](#)
- [Troubleshooting example - backup with no active key record](#)
- [Troubleshooting example - restore with an improper key record state](#)

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 (LTO4). 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 `bmksutil`.

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 6-1 Considerations that relate to the functionality and use of KMS

Consideration	Description
New NBKMS service	The <code>nbkms</code> service is a master-server-based service that provides encryption keys to the media server BPTM processes.
New <code>nbkmsutil</code> KMS configuration utility	For security reasons, the KMS configuration utility can only be run from the master server as root or administrator.

Table 6-1 Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
NetBackup wide changes	<p>Changes were necessary throughout NetBackup for the following:</p> <ul style="list-style-type: none">■ 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 (LT04 and equivalent) encryption.■ NetBackup GUI and CLI changes to report the encryption key tag addition to the NetBackup image information The <code>bpimmedia</code> and <code>bpimagelist</code> 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 passphrases. You type in a passphrase and the key management system creates a reproducible encryption key from that passphrase.
KMS installation and deployment decisions	<p>Following are decisions you must make for KMS deployment:</p> <ul style="list-style-type: none">■ Whether to choose KMS random generated keys or passphrase generated keys■ Whether to include NBAC deployment
KMS security	<p>No burden is placed on existing NetBackup services with additional security concerns.</p>
Cipher types	<p>The following cipher types are supported in KMS:</p> <ul style="list-style-type: none">■ AES_128■ AES_192■ AES_256 (default cipher)
KMS recoverability	<p>You can use KMS in such a way where all of the encryption keys are generated from passphrases. You can record these passphrases and then use them at a later time to recreate the entire KMS for NetBackup.</p>

Table 6-1

Considerations that relate to the functionality and use of KMS

(continued)

Consideration	Description
KMS files	<p>KMS files associated with it where information on the keys is kept, as follows:</p> <ul style="list-style-type: none">■ Key file or key database Contains the data encryption keys. The key file is located at /opt/opensw/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/opensw/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/opensw/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 passphrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by passphrases. If you have recorded all of the encryption key passphrases 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 6-1 Considerations that relate to the functionality and use of KMS
(continued)

Consideration	Description
Key records	<p>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.</p> <p>These key records are defined as follows:</p> <ul style="list-style-type: none"> ■ 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	<p>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 and NetBackup 6.5.2 supported two key groups. Only 10 encryption keys are allowed per key group.</p>
Tape drives and media capabilities	<p>Drive, tape, and NetBackup capabilities must all match for drive encryption to be successful. A number of drives adhere to the standard. The LT04 is a typical type. Currently only LT04 drives and LT04 media can be encrypted or decrypted. You can still run LT03 media in LT04 drives for reading and writing but you cannot encrypt the data. If you use LT02 media, that data can be read in LT04 drives but they cannot be written in either unencrypted or encrypted format.</p> <p>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.</p> <p>Following is the interoperability matrix for the tape drives and media:</p> <ul style="list-style-type: none"> ■ LTO4 drives can read LTO2, LTO3, and LTO4 media ■ LTO4 drives can write LTO3 and LTO4 media ■ LTO4 drives can only encrypt LTO4 media ■ LTO4 encrypted and decrypted media only works in LTO4 drives

Table 6-1

Considerations that relate to the functionality and use of KMS

(continued)

Consideration	Description
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.
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 <code>nbkmsutil</code> command uses traditional logging and its logs can be found in the file <code>/usr/opensv/netbackup/logs/admin/*.log</code> .
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 <i>Symantec NetBackup Cloud Administrator's Guide</i> .
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 <i>Symantec NetBackup AdvancedDisk Storage Solutions Guide</i> .
NBAC and KMS permissions	Typically when using NBAC and the <code>Setupmaster</code> command is run, the NetBackup related group permissions (for example, <code>NBU_Admin</code> and <code>KMS_Admin</code>) 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 6.5.x to 7.0 or from 7.0 to 7.0.1. The solution is to grant the root and administrator users <code>NBU_Admin</code> and <code>KMS_Admin</code> permissions manually.

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.

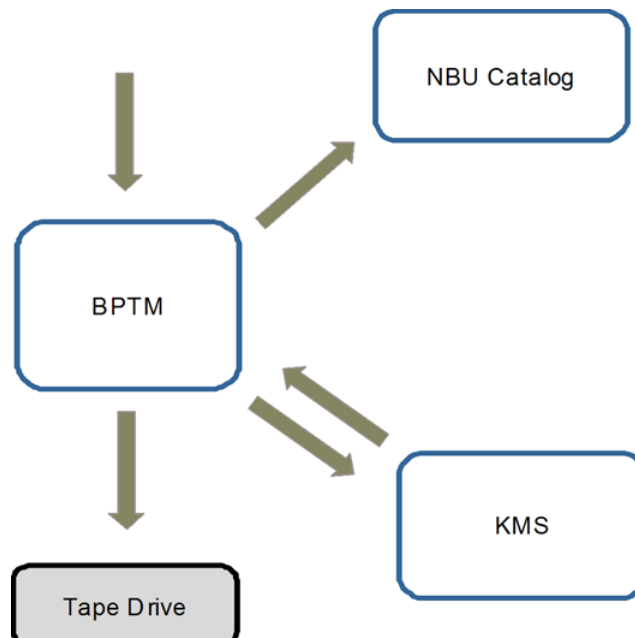
The backup then proceeds as normal.

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 6-1 shows how the process flows.

Figure 6-1 Process flow for writing an encrypted tape



About reading an encrypted tape

When a tape is read and an area of the tape is 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 6-2 defines the terms that are associated with KMS.

Table 6-2 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 <code>nbkmsutil</code> 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 <code>KMS_DATA.dat</code> key file using AES 256. The host master key is located at <code>/opt/opensv/kms/key/KMS_HMKF.dat</code> .
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 <code>/usr/opensv/netbackup/bin/nbkms</code> .
Key record (KR)	A key record contains the details of an encryption key.
KMS database	The KMS database contains the data encryption keys.

Table 6-2 Definitions for common KMS terms (*continued*)

Term	Definition
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 <code>kms/key/KMS_KPKF.dat</code> . 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 <code>/opt/opensv/kms/db/KMS_DATA.dat</code> .
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.
Key record states	<p>Key record states are as follows:</p> <ul style="list-style-type: none"> ■ 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. ■ Passphrase, which means that the passphrase 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 passphrase. <p>Note: Keep track of all passphrases by recording them and storing them in a safe place for future use.</p> <p>Using a passphrase has definite benefits. It results in keys with better security strength. And if keys are lost, you can regenerate them by providing the passphrase that was used to create the original key.</p>

Table 6-2 Definitions for common KMS terms (*continued*)

Term	Definition
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 passphrase 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 passphrase 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 | grepnbkms
```


- 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 passphrase 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.

```
fel (root) [331]: nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name      : ENCR_pool1
Supported Cipher    : AES_256
Number of Keys      : 2
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
Number of Keys: 2
```

See [“About installing KMS with HA clustering”](#) on page 307.

See [“Using KMS with NBAC”](#) on page 307.

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 6-3](#) shows the default KMS permissions for each of the NetBackup user groups.

Table 6-3 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/opensv/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/opensv/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/opensv/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/opensv/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 passphrases
- Randomly generated passphrases

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/opensv/kms/db/KMS_DATA.dat  
/opt/opensv/kms/key/KMS_HMKF.dat  
/opt/opensv/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 passphrase for the Host Master Key, or press Enter to use a randomly generated key. Re-enter the passphrase 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 passphrase for the Key Protection Key, or press Enter to use a randomly generated key. Re-enter the passphrase 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

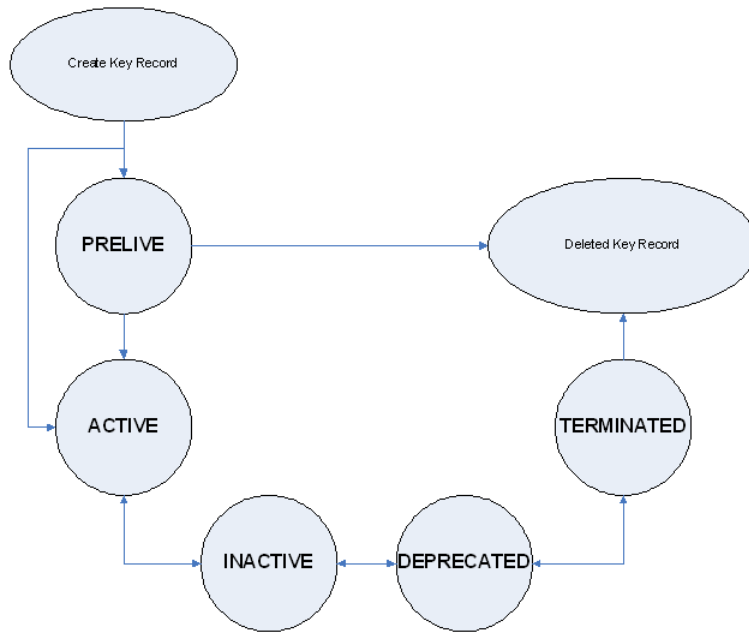
The key record states include the prelive, active, inactive, deprecated, and terminated. Key record states adhere to a key record life cycle. Once a key has entered the active state (that is set up for encryption), the key must progress in proper order through the lifecycle. The proper order includes 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 passphrase), 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 6-2 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 passphrase 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 commands that could 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 start up 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 passphrases. So, if you have written down passphrases for the host master key and key protection key, you can run a command to regenerate those files. The system will prompt you for the passphrase and if the passphrase you now enter matches the passphrase 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 Start up 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 could 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 will need to enter all 64 characters manually.

- 3 Enter the passphrase at the prompt. It must be an exact match with the original passphrase you previously provided.

Note: If the tag you enter already exists in the KMS database, then you will not be able to 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 say on the same transport truck. If both tapes are lost together then that situation would 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 passphrase generated encryption keys to manually rebuild KMS. All of the keys can be generated by passphrases. So if you have recorded all of the passphrases, 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 passphrase 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 passphrase.

Listing keys

Use the following procedure to list the 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 1342205038600000000  
  
1342205038600000000 -  
KR my_latest_key Active 134220507320000000 134220507320000000  
key for Jan, Feb, March data  
Number of keys: 1
```

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 320.
- Setting up NetBackup to use encryption
See [“Example of setting up NetBackup to use tape encryption”](#) on page 321.

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 6-3 NetBackup Administration Console with two volume pools set up to use KMS

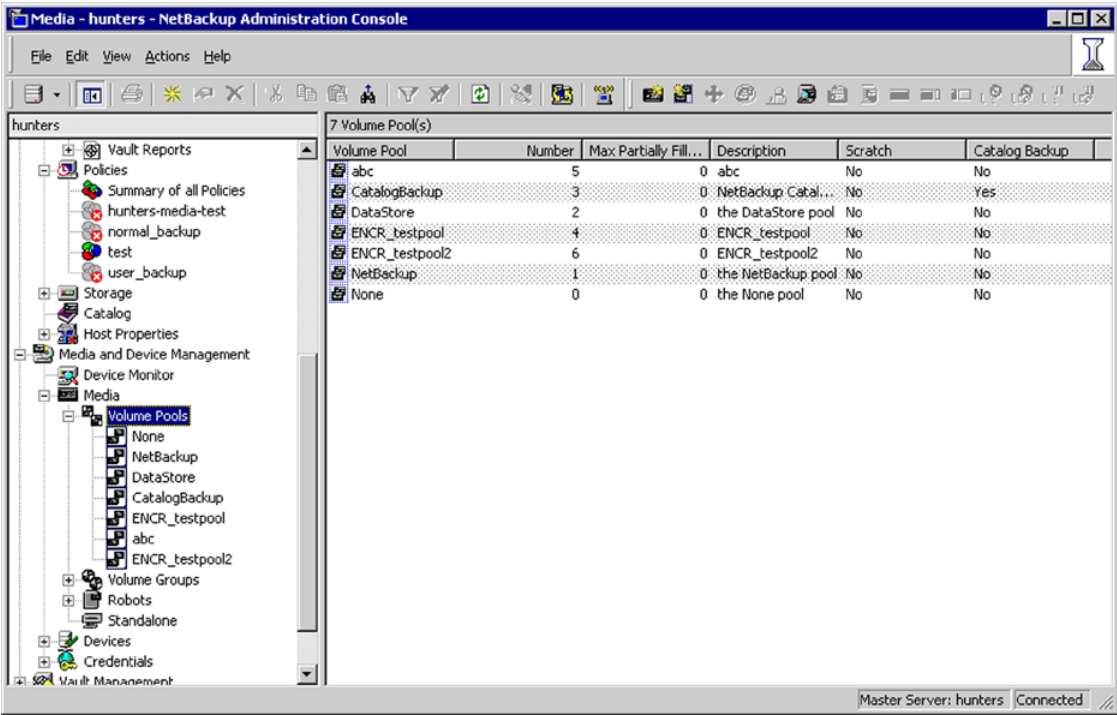
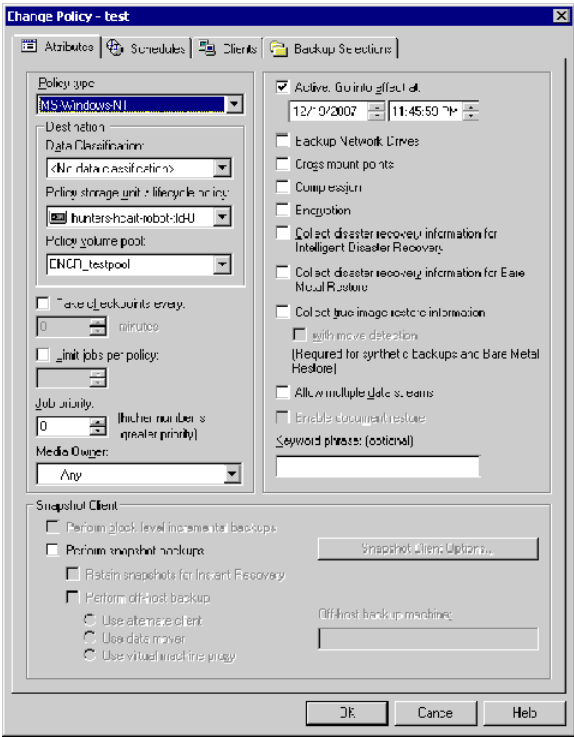


Figure 6-4 shows a NetBackup Policy that is configured to use the volume pool ENCR_testpool1, which is the same name as the key group that you configured earlier.

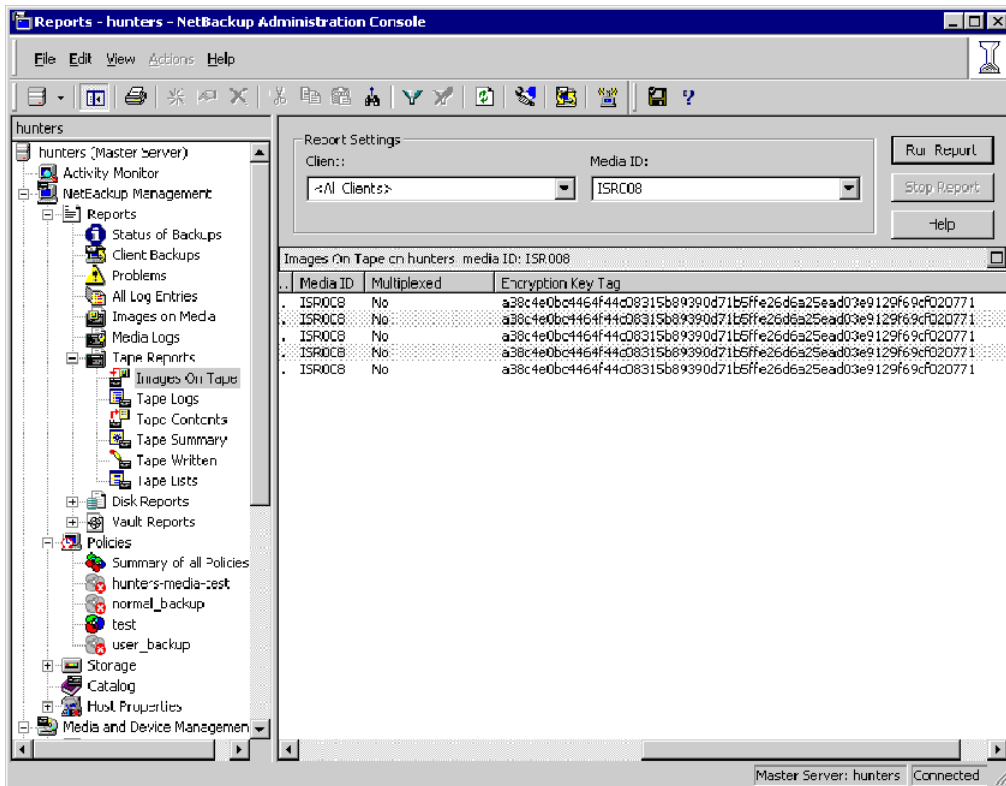
Figure 6-4 NetBackup Change Policy dialog box with KMS volume pool



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 6-5 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 324.
- Example of verifying an encryption backup
See [“Example of verifying an encryption backup”](#) on page 324.
- About importing KMS encrypted images
See [“About importing KMS encrypted images”](#) on page 325.

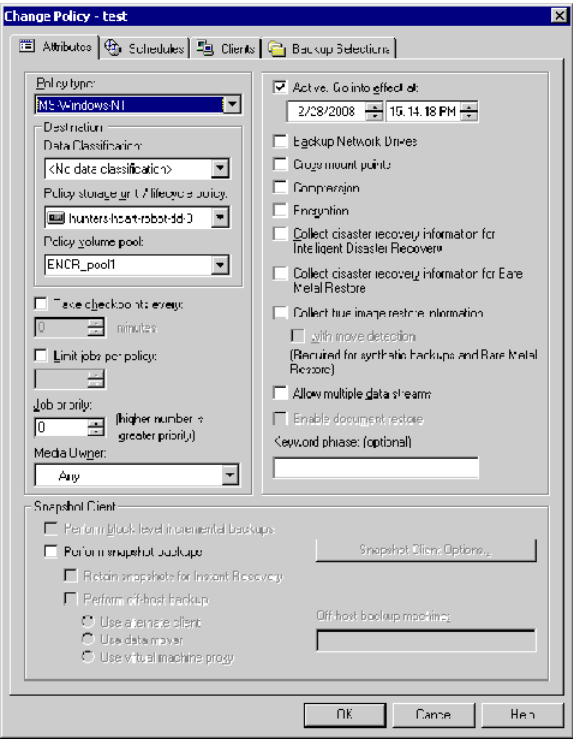
Example of running an encrypted tape backup

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

Figure 6-6

NetBackup Change Policy dialog box with KMS volume pool ENCR_pool1



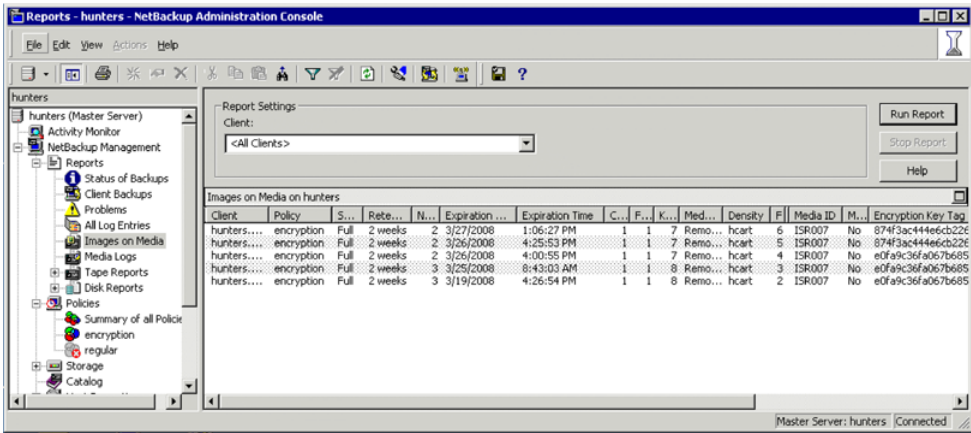
Example of verifying an encryption backup

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.

Images on Tape with tape encryption keys shows an Images on Media report that has encryption key tags displayed.

See [Figure 6-5](#) on page 323.

Figure 6-7 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 .*ef* 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 passphrase (leave empty for a random HMK)
- HMK ID
- KPK passphrase (leave empty for a random KPK)
- KPK ID

The KMS database backup and disaster recovery procedures will vary for random and passphrase 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 passphrases 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 passphrase and ID and then update the KPK/HMK. You can choose either random or passphrase based KPK/HKM at each such invocation.

Note: It is a best practice to use the `-usephrase` option when modifying the HMK and KPK so that you are required to use a known passphrase for future recovery. With the `-nopphrase` option, KMS generates a random passphrase 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/opensv/kms/db/KMS_DATA.dat
/opt/opensv/kms/key/KMS_HMKF.dat
/opt/opensv/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 328.
- Create a new key group
See [“Create a new key group”](#) on page 329.
- Create a new key
See [“Create a new key”](#) on page 329.
- Modify key group attributes
See [“Modify key group attributes”](#) on page 330.

- Modify key attributes
See [“Modify key attributes”](#) on page 330.
- Get details of key groups
See [“Get details of key groups”](#) on page 331.
- Get details of keys
See [“Get details of keys”](#) on page 331.
- Delete a key group
See [“Delete a key group”](#) on page 332.
- Delete a key
See [“Delete a key”](#) on page 332.
- Recover a key
See [“Recover a key”](#) on page 333.
- Modify host master key (HMK)
See [“Modify host master key \(HMK\)”](#) on page 333.
- Get host master key (HMK) ID
See [“Get host master key \(HMK\) ID”](#) on page 334.
- Modify key protection key (KPK)
See [“Modify key protection key \(KPK\)”](#) on page 334.
- Get key protection key (KPK) ID
See [“Get key protection key \(KPK\) ID”](#) on page 334.
- Get keystore statistics
See [“Get keystore statistics”](#) on page 334.
- Quiesce KMS database
See [“Quiesce KMS database”](#) on page 335.
- Unquiesce KMS database
See [“Unquiesce KMS database”](#) on page 335.

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.

<code>-kgname</code>	Specifies the name of the new key group (it has to be unique within the keystore).
<code>-cipher</code>	Specifies the type of cipher 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.

<code>-nopphrase</code>	Creates the key without using a passphrase. If this option is not specified, the user is prompted for a passphrase.
<code>-keyname</code>	Specifies the name of the new key (it should be unique within the key group to which it belongs).
<code>-kgname</code>	Specifies the name of an existing key group to which the new key should be added.
<code>-activate</code>	Sets the key state to active (default key state is prelive).

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> ]
```

<code>-kgname</code>	Specifies the name of the key group to be modified.
<code>-name</code>	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>
-kgroup <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
```

Note: `-state` and `-activate` are mutually exclusive

<code>-keyname</code>	Specifies the name of the key to be modified.
-----------------------	---

<code>-kgname</code>	Specifies the name of the key group to which this key belongs.
<code>-name</code>	Specifies the new name of the key (it should be unique within the key group).
<code>-state</code>	Specifies the new state of the key (see valid key state transition order).
<code>-activate</code>	Sets the key state to active.

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 would be listed. If no option is specified, the details of all of the key groups are returned.

<code>-kgname</code>	Specifies the name of a key group.
<code>-cipher</code>	Gets the details of all the key groups which supports specific cipher type.
<code>-emptykgs</code>	Gets the details of all the key groups with zero keys in it.
<code>-noactive</code>	Gets the details of all the key groups in which there is no active key.
<code>-noverbose</code>	Prints the details in formatted form (non-readable) format. The default is verbose. The output is displayed in a human readable form.

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 ]
```

<code>-kgname</code>	Specifies the key group name. The details of all of the keys belonging to a key group are returned.
<code>-keyname</code>	Gets the details of the specific key which belongs to a specific key group.
<code>-activekey</code>	Gets the details of a specific key group's active key.
<code>-noverbose</code>	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>
```

<code>-kgname</code>	Specifies the name of the key group to be deleted. Only empty key groups can be deleted.
----------------------	--

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.

<code>-keyname</code>	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>
-kname <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 passphrase)

<code>-keyname</code>	Specifies the name of the key to be recovered (re-created).
<code>-kgname</code>	Specifies the name of the key group to which this key should belong.
<code>-tag</code>	Specifies the tag that identifies the original key (we need to use the same tag).

Note: The user is prompted to enter the correct passphrase to get the right key (the system does not verify the validity of entered passphrases).

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 passphrase. An ID (HMK ID) should also be provided that can remind them of the specified passphrase. Both the passphrase 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 passphrase. Also, provide an ID (KPK ID) that can remind us of the specified passphrase. Both the passphrase 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 passphrases. 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 passphrases 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 is not affecting 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 not decrypting

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 6-8](#) 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 6-8 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 6-9 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 6-9 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 6-10 shows the BPTM log output. It logs the message within the 1227 error code in the BPTM log.

Figure 6-10 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 statÜs: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decrypt 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 kmScLiB with: kmScLiB -ORBSvcConfDirective "-
ORBDDottedDecimalAddresses 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 kmScLiB'" -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: dberorr.c.cmdnrite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBRMS 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 6-11 shows that a status code 83 - media open error message returned.

Figure 6-11 Activity monitor with status code 83

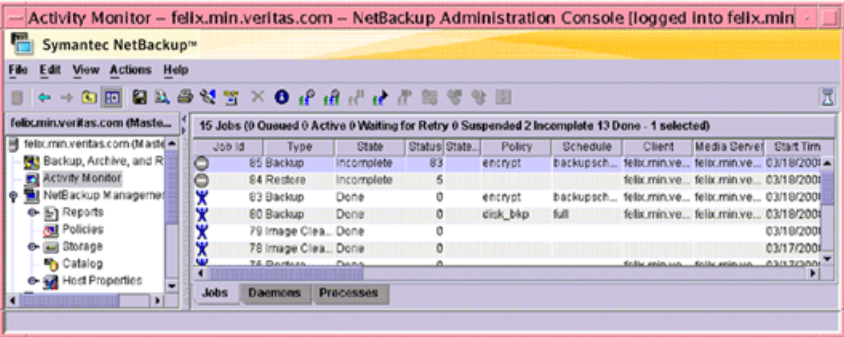


Figure 6-12 shows the detailed status. You can see a message stating that nbksm failed with error status key group does not have and active key (1227). With the information in the previous diagnostics, you can determine the particular problem or to identify what a given problem is related to.

Figure 6-12 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 6-13 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 6-13 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
```

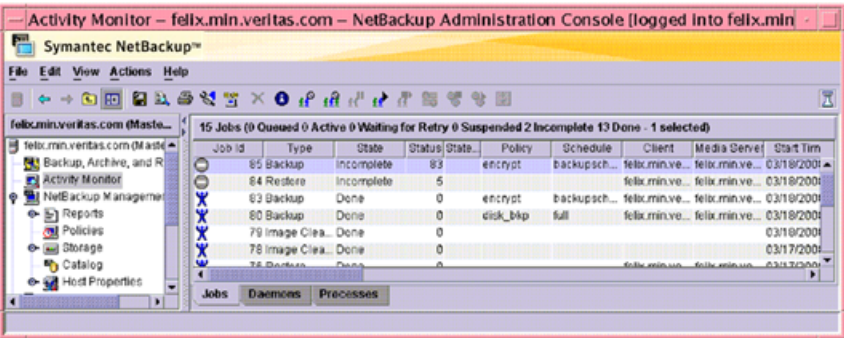
Figure 6-14 shows the `bptm` log output with the 1242 error returned.

Figure 6-14 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
[cf7ac430d8795a9b39e70382137led10be6ec80eab72d89aef6f8a791fc2460d]
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 "-
ORBDDottedDecimalAddresses 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: dberror.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 6-15 shows a status code 5 - restore failed to recover the requested files.

Figure 6-15 Activity monitor with status code 5



Index

Symbols

- 40-bit DES key
 - library 268–269
- 56-bit DES key
 - library 270
- 7.5 NetBackup ports
 - default 104

A

- About
 - KMS 296
- about
 - ports 103
- Access Control
 - nbac_cron.exe 197
- access control
 - host properties 183
 - individual users
 - description 229
 - nbac_cron utility 197
 - user groups
 - Administrator 232
 - configuring 233
 - Default User 232
 - description 230
 - KMS Administrator 233
 - Operator 232
 - renaming user groups 234
 - SAN Administrator 232
 - Security Administrator 232
 - Vault Operator 233
- access control host properties dialog
 - for client 187
- Access Management
 - utility 228
- access management
 - troubleshooting guidelines 190
- accessing
 - client host properties 187
- ACS
 - storage server interface 139

- active
 - key record state 315
- adding a new user
 - to the user group 237
- administration
 - media server encryption 291
 - NetBackup access management 159
- Administrator Access Control user group 232
- all NetBackup security
 - multi-datacenter 94
- all security implemented
 - single datacenter 64
- ALLOWED (encryption option) 272, 280
- alternate client restore (see redirected restore) 277, 286
- Assigned Users pane
 - on the Users tab 237
- assigning a user
 - to a user group 239
- attribute for encryption 266, 278, 287
- authentication
 - port 195
- Authentication Domain
 - tab 185
 - tab for client 188
- authorization objects
 - in NetBackup Administration Console 244
- authorization objects and permissions
 - in the NetBackup Administration Console 240
- authorization port 195
- Authorization Service
 - tab 186
- automatic backup
 - key file 277

B

- backing up
 - KMS database files 316
- backing up problems
 - KMS data files 318

- backup
 - choosing encryption 266
- backup with no active key record
 - troubleshooting example 337
- backups
 - KMS keystore and administrator keys 327
- backups not encrypting
 - solution 337
- best practices
 - for key file restoration 276
- bp.conf
 - port usage settings in the NetBackup configuration 141
- bpcd 269–270
 - terminating 290
- BPCD and BPRD ports on Windows
 - changing 137
- BPCD connect-back
 - options 116
- BPCD connect-back method
 - specifying
 - that connects a master server or media server to a client 130
- bpclient command
 - configuring port usage client attribute settings 147
 - specifying 148
- bpinst command 268–269
 - for setting encryption attribute (legacy) 287
 - pushing configuration to clients (legacy) 282
- BPJAVA_PORT and VNETD_PORT
 - ports 136
- bpkeyfile command
 - change_netbackup_pass_phrase option 285
 - changing key file pass phrase 290
 - introduction (standard) 268–269
 - managing the key file (legacy) 284
- bpkeyutil command
 - adding pass phrases 273
 - creating the key file 275
 - introduction 267
 - managing the key file 273
 - redirected restore 277, 287
 - standard restore introduction 269
- BUAndRest authorization object
 - permissions 250

C

- changing
 - client encryption settings from the server 278
 - client legacy encryption settings 288
- changing ports
 - for BPCD and BPRD on Windows 137
- checksum of DES key
 - explanation
 - legacy encryption 268
 - legacy restore 270
 - standard encryption 267
 - standard restore 269
- choosing encryption
 - for a backup 266
- cipher types 297
- class
 - see policy 278, 287
- CLI
 - usage help 328
- client
 - access control host properties dialog 187
 - outgoing ports 110
- client attributes
 - specifying 126
- client encryption settings
 - changing 278
- client legacy encryption settings
 - changing 288
- client side encryption
 - multi-datacenter 77
 - security 36
 - single datacenter 54
- client verification points
 - for a mixed Windows master server 217
 - for Windows 226
- clients
 - configuring standard encryption 272
- clustered environments
 - additional key file security (legacy) 289
 - managing the key file (legacy) 284
 - managing the key file (standard) 273
 - pushing configuration (legacy) 282
 - pushing software (standard) 284
- cnpp option 285
- Combined world, enterprise, and data center levels 30
- command line interface (CLI)
 - commands 327
- command usage
 - conventions 169

- commands
 - command line interface (CLI) 327
 - comparison
 - encryption options 264
 - configuration
 - and clustering (legacy) 280
 - and clustering (standard) 275
 - options (legacy) 280
 - pushing to clients (legacy) 282
 - configuring
 - clients for encryption
 - from client (standard) 278
 - from server (legacy) 282
 - from server (standard) 274
 - KMS 309
 - legacy encryption 279
 - legacy encryption from the server 279
 - NetBackup master server
 - to communicate with the OpsCenter server 124
 - ports 112
 - standard encryption
 - on clients 272
 - standard encryption from the server 274
 - configuring access control
 - for NetBackup pre-7.0 media server and client machines 179
 - on clients 166
 - configuring access control host properties
 - manually 180
 - configuring NetBackup
 - to work with KMS 320
 - configuring port usage client attribute settings
 - bpclient command 147
 - configuring port usage without a GUI
 - port usage 141
 - connect a master server or media server to a client
 - specifying ports 127
 - considerations
 - key record state 314
 - controls users in user groups
 - Users tab 235
 - create
 - new key 329
 - new key group 329
 - creating
 - empty KMS database 326
 - encryption key files
 - on clients notes 275
 - creating *(continued)*
 - key database 310
 - key file 275
 - key groups 312
 - key record 319
 - key records 312
 - new user group 233
 - by copying an existing user group 234
 - CRYPT option 287
 - CRYPT_CIPHER option 273
 - CRYPT_KEYFILE option 268–269, 281, 284
 - CRYPT_KIND option 273, 281
 - CRYPT_LIBPATH option 281
 - CRYPT_OPTION 266, 272, 280, 282
 - CRYPT_STRENGTH option 269, 281–282
- ## D
- Daemon connection port
 - options 117
 - daemon connection port
 - that connects a master server or media server to a client 132
 - data at rest encryption
 - limitations 261
 - options 264
 - terminology 261
 - database constituents
 - KMS 325
 - datacenter
 - multi 44
 - single 44
 - datacenter level
 - security 23
 - decryption
 - of key file (legacy) 289
 - overview (legacy) 270
 - overview (standard) 268
 - default
 - port numbers
 - NetBackup 7.5 105
 - default ports
 - 7.5 NetBackup 104
 - Default User Access Control user group 232
 - default user groups
 - NetBackup 231
 - Defined Users pane
 - on the Users tab 236
 - defining
 - user group and users 237

definition

- key groups and key records 311

delete

- key 332
- key group 332

DENIED (encryption option) 272, 280

deprecated

- key record state 315

DES

- key checksum 268–270
- key checksum for standard encryption 267

details

- key groups 331
- keys 331

DevHost authorization object

- permissions 254

disable

- random port assignments 113

disabling the monitoring

- KMS service 309

disabling the ping

- on the NetBackup Administration Console on Windows 137

DiskPool authorization object

- permissions 249

display

- HMK ID 334
- KPK ID 334

documentation

- HTTP and HTTPS ports 124

drive authorization object

- permissions 246

E

EMM server 191

- outgoing ports 109

enabling cluster use

- KMS service 308

enabling the monitoring

- KMS service 308

encrypted backup

- restoring (legacy) 286
- restoring (standard) 277

encrypted backup file

- restoring to another client 277

encrypted tape

- reading 302
- writing 301

encryption

allow

- deny. *See* require

attribute

- setting 278

configuration options (legacy) 280

configuring from client (standard) 278

file containing keys for (legacy) 281

kind

- defining (legacy) 281
- defining (standard) 273

legacy

- prerequisites 267
- prerequisites for restoring 269
- tar header 270

libraries

- defining (legacy) 281
- managing from client (standard) 272

of key file (legacy) 289

overview (legacy) 270

overview (standard) 268

policy attribute for

- how to set 266, 278, 287

security questions 264

standard

- prerequisites for restoring 268
- tar header 269

strength

- defining (legacy) 281

tar header

- legacy 268
- standard 267

using KMS 323

what is and isn't encrypted (legacy) 268

what is and isn't encrypted (standard) 267

Encryption attribute

- in policies 287

encryption backup

- running 266

encryption options

- comparison 264

encryption security

- installation prerequisites 270

enterprise level

- security 21

Enterprise Media Manager server 191

example

- running an encrypted tape backup 324

- setting up NetBackup to use tape encryption 321

example (*continued*)
 verifying an encryption backup 324

F

fat client authorization object
 permissions 255
 fat server authorization object
 permissions 255
 firewall connect options
 on a NetBackup server or client 114
 specifying for a source computer to apply to
 specific destination computers 118
 firewall connection options
 on Media Manager 119
 firewall considerations 120
 firewall environment
 NDMP 138
 firewall problems
 when using NetBackup with other products 140

G

General tab
 contains name of user group 235
 granting
 permissions 242

H

HMK and KPK
 updating 327
 HMK ID
 display 334
 host master key (HMK)
 modify 333
 host properties
 access control 183
 client
 accessing 187
 master server and media server 183
 HostProperties authorization object
 permissions 252

I

ICMP
 pinging NDMP 138
 identify
 KPK and HMK 326
 importing
 KMS encrypted images 325

inactive
 key record state 315
 individual users
 description 229
 installation
 on server for push to client 270
 pushing configuration to clients (legacy) 282
 pushing pass phrases to clients (legacy) 282
 installation prerequisites
 for encryption security 270
 installing
 KMS 304
 with HA clustering 307
 installing access control
 on clients 166
 installing encryption
 locally on a NetBackup UNIX client 271
 locally on a NetBackup Windows client 271
 on a UNIX NetBackup server 270
 on a Windows NetBackup server 271

J

Java console
 outgoing ports 112
 job authorization object
 permissions 250

K

key
 delete 332
 recover 333
 key attributes
 modify 330
 key creation
 options 335
 key database
 creating 310
 key file 267, 269
 automatic backup 277
 backing up (legacy) 286
 bpkeyutil command 273
 creating (legacy) 284
 creating (standard) 275
 defining (legacy) 281
 encrypting (legacy) 284
 encrypting with admin's pass phrase
 (legacy) 289

key file (*continued*)

- encrypting with admin's pass phrase
 - (standard) 274
- explanation (legacy) 282
- for redirected restore (standard) 277, 287
- in a cluster (legacy) 284, 288–289
- in a cluster (standard) 273
- legacy 268
- managing (standard) 273
- pass phrase (legacy) 290
- key file pass phrase protection
 - manual retention 276
- key file restoration
 - best practices 276
- key files
 - creating
 - on clients notes 275
- key group
 - delete 332
- key group attributes
 - modify 330
- key groups
 - creating 312
 - details 331
- key groups and key records
 - definition 311
- Key Management Service (KMS)
 - about 296
- key protection key (KPK)
 - modify 334
- key record
 - creating 319
- key record state
 - active 315
 - considerations 314
 - deprecated 315
 - inactive 315
 - prelive 315
 - terminated 316
- key record states
 - overview 313
- key records
 - creating 312
- keys
 - details 331
 - listing 320
- keystore
 - statistics 334

KMS

- configuring 309
- configuring NetBackup to work with 320
- considerations 296
- database constituents 325
- installing 304
 - with HA clustering 307
- NetBackup and key records 320
- principles of operation 300
- recovering
 - by restoring all data files 317
 - by restoring only KMS data file 317
 - regenerating the data encryption key 317
- terminology 302
- troubleshooting 336
- using for encryption 323
- with NBAC 307
- KMS Administrator Access Control user group 233
- KMS data files
 - problems backing up 318
 - solutions for backing up 319
- KMS database
 - creating an empty one 326
 - quiesce 335
 - unquiesce 335
- KMS database files
 - backing up 316
- KMS encrypted images
 - importing 325
- Kms group authorization object
 - permissions 257
- KMS keystore and administrator keys
 - backups 327
- KMS service
 - disabling the monitoring 309
 - enabling cluster use 308
 - enabling the monitoring 308
 - removing from monitored list 309
- KPK ID
 - display 334
- KPK ID and HMK ID
 - importance 326

L

- legacy encrypted backup created on another client
 - restoring 286
- legacy encryption
 - backup process 267
 - configuring 279

- legacy encryption (*continued*)
 - managing 284
- legacy encryption attribute
 - setting in policies 287
- legacy encryption configuration
 - pushing to clients 282
- legacy encryption configuration options
 - managing 280
- legacy encryption from the server
 - configuring 279
- legacy encryption pass phrases
 - pushing to clients 282
- legacy key file security
 - for UNIX clients 288
- libraries
 - defining for encryption (legacy) 281
- license authorization object
 - permissions 252
- limitations
 - data at rest encryption 261
- list of NetBackup authorization objects
 - Permissions tab 240
- listing
 - keys 320
- logging on
 - as new user 239

M

- managing
 - clients for encryption
 - from client (standard) 272
 - key file (standard) 273
 - legacy encryption configuration options 280
 - legacy encryption key files 284
 - NetBackup encryption key file 273
 - standard encryption configuration options 272
- managing key file (legacy) 284
- manually configuring
 - access control host properties 180
- master server
 - outgoing ports 106
- Master server and media server
 - host properties 183
- master server settings
 - verifying 192
- master server verification points
 - for a mixed UNIX master server 209
 - for a mixed Windows master server 215
 - for Windows 220

- master, media server, and GUI security
 - NBAC 38
- media authorization object
 - permissions 245
- Media Manager
 - firewall connection options 119
- media manager configuration
 - random port assignments 114
- media server
 - outgoing ports 107
- media server encryption
 - administration 291
 - option 2 290
- Media Server Encryption Option (MSEO)
 - security 35
 - single datacenter 51
 - with multi-datacenter 72
- media server verification points
 - for a mixed UNIX master server 209
 - for a mixed Windows master server 215
 - for Windows 224
- mixed UNIX master server
 - master server verification points 209
 - media server verification points 209
- mixed Windows master server
 - client verification points 217
 - master server verification points 215
 - media server verification points 215
- modify
 - host master key (HMK) 333
 - key attributes 330
 - key group attributes 330
 - key protection key (KPK) 334
- multi-datacenter 44
 - with all NetBackup security 94
 - with client side encryption 77
 - with Media Server Encryption Option (MSEO) 72
 - with NBAC complete 88
 - with NBAC on master and media servers 82
 - with standard NetBackup 68

N

- name of user group
 - on the General tab 235
- NBAC
 - configuration 159
 - configuration overview 160
 - configure command 169

NBAC (*continued*)

- configuring 160
 - on a clustered master server 163
 - on media servers 164
 - on standalone master servers 161
- master, media server, and GUI security 38
- upgrading 174

NBAC complete

- multi-datacenter 88
- security 40
- single datacenter 60

NBAC on master and media servers

- multi-datacenter 82
- single datacenter 56

nbac_cron utility 197

nbac_cron.exe 197

NBU security

- workgroup 44

NBU_Admin Access Control user group 232

NBU_Catalog authorization object

- permissions 247

NBU_KMS Admin Access Control user group 233

NBU_Operator Access Control user group 232

NBU_Security Admin Access Control user group 232

NBU_User Access Control user group 232

NDMP

- in firewall environment 138

NetBackup

components

- used in security 25

default user groups 231

determining access 229

ports 103

security

- all 41
- components 23
- implementation levels 18
- security implementation types 31
- security vulnerabilities 34

NetBackup Access Control (NBAC)

components 25

individual users 229

nbac_cron utility 197

nbac_cron.exe 197

user groups 230

Administrator 232

configuring 233

Default User 232

KMS Administrator 233

NetBackup Access Control (NBAC) (*continued*)user groups (*continued*)

- Operator 232
- renaming user groups 234
- SAN Administrator 232
- Security Administrator 232
- Vault Operator 233

using 156

NetBackup access management

administration 159

NetBackup Administration Console

authorization objects 244

authorization objects and permissions 240

NetBackup Administration Console on Windows

disabling the ping 137

NetBackup and key records

KMS 320

NetBackup Authentication and Authorization

troubleshooting topics 191

NetBackup client encryption

option 1 265

NetBackup configuration settings

port usage 142

NetBackup legacy encryption

restore process 269

NetBackup Management infrastructures

unifying with the setuptrust command 181

NetBackup master server

configuring

- to communicate with the OpsCenter server 124

NetBackup security

standard 34

NetBackup Service Layer (NBSL) 124

NetBackup standard encryption

restore process 268

NetBackup UNIX client

installing encryption 271

NetBackup user groups

viewing specific user permissions 243

NetBackup Windows client

installing encryption 271

NetBackup-Java connection options

specifying 125

Network Settings

tab 184, 189

new key

create 329

- new key group
 - create 329
- new user
 - logging on 239
- new user group
 - creating 233
 - by copying an existing user group 234

O

- operating system
 - security 33
- Operator Access Control user group 232
- option 1
 - NetBackup client encryption 265
- option 2
 - media server encryption 290
- options
 - BPCD connect-back 116
 - daemon connection port 117
 - data at rest encryption 264
 - key creation 335
 - ports 116
- outgoing ports
 - client 110
 - EMM server 109
 - Java console 112
 - master server 106
 - media server 107
 - Windows administration console or Java server 111
- overriding or modifying
 - port numbers 104
- overview
 - key record states 313
 - of legacy encryption backup 267
 - of legacy restore 270
 - of standard encryption backup 267
 - of standard restore 268

P

- pass phrase
 - for encrypting key file (legacy) 285, 289
 - for redirected restore (legacy) 286
 - for redirected restore (standard) 277
 - pushing to clients (legacy) 282
- passphrase_prompt option 282
- passphrase_stdin option 282

permissions

- BUAndRest authorization object 250
- DevHost authorization object 254
- DiskPool authorization object 249
- Drive authorization object 246
- fat client authorization object 255
- fat server authorization object 255
- granting 242
- HostProperties authorization object 252
- job authorization object 250
- Kms group authorization object 257
- license authorization object 252
- media authorization object 245
- NBU_Catalog authorization object 247
- policy authorization object 245
- report authorization object 247
- robot authorization object 248
- security authorization object 254
- server group authorization object 256
- service authorization object 251
- StorageUnit authorization object 248
- vault authorization object 256
- volume group authorization object 253
- VolumePool authorization object 253
- Permissions tab
 - contains list of NetBackup authorization objects 240
- pinging NDMP
 - ICMP 138
- policy authorization object
 - permissions 245
- port numbers
 - about overriding or modifying 104
 - backup and archive products 122
 - default for NetBackup 7.5 105
 - HTTP 123
 - HTTPS 123
 - key OpsCenter components 120
- port ranges
 - specifying 134
- port usage
 - configuring without a GUI 141
 - NetBackup configuration settings 142
- port usage settings in the NetBackup configuration
 - bp.conf 141
- port usage-related Media Manager configuration
 - settings
 - vm.conf 150

ports

- about 103
- authentication 195
- authorization 195
- BPJAVA_PORT and VNETD_PORT 136
- changing for BPCD and BPRD on Windows 137
- configuring 112
- NetBackup 103
- non-reserved
 - accepting remote connections from 113
- options 116

prelive

- key record state 315

pushing

- configuration to clients (legacy) 282
- legacy encryption pass phrases to clients 282
- pass phrases to clients (legacy) 282

- pushing the legacy encryption configuration to clients 282

Q**quiesce**

- KMS database 335

R**random port assignments**

- disable 113
- in media manager configuration 114

reading

- encrypted tape 302

recover

- key 333

recovering

- KMS
 - by restoring all data files 317
 - by restoring only KMS data file 317
 - regenerating the data encryption key 317

redirected restore

- of other client's backup (legacy) 286
- of other client's backup (standard) 277
- preventing (legacy) 283

redirected restores

- for an encrypted backup file 277
- of legacy encrypted files 286

remote connections

- accepting from non-reserved ports 113

removing from monitored list

- KMS service 309

report authorization object

- permissions 247

REQUIRED (encryption option) 272, 280**restore**

- overview (legacy) 270
- overview (standard) 268

restore process

- NetBackup legacy encryption 269
- NetBackup standard encryption 268

restore with an improper key record state

- troubleshooting example 341

restores not decrypting

- solution 337

restoring

- legacy encrypted backup created on another client 286

robot authorization object

- permissions 248

running

- bpkeyfile command 289
- encryption backup 266

running an encrypted tape backup

- example 324

S**security**

- client side encryption 36
- components
 - NetBackup 23
- datacenter level 23
- enterprise level 21
- implementation levels 18
- Media Server Encryption Option (MSEO) 35
- NBAC complete 40
- NetBackup
 - all 41
- operating system 33
- world level 19

Security Administrator Access Control user

- group 232

security authorization object

- permissions 254

security implementation types

- NetBackup 31

security vulnerabilities

- NetBackup 34

server group authorization object

- permissions 256

- service authorization object
 - permissions 251
- setting encryption attribute
 - in policies 278
- setting up NetBackup to use tape encryption
 - example 321
- setuptrust command
 - unifying NetBackup Management infrastructures 181
 - using 182
- single datacenter
 - with all security implemented 64
 - with client side encryption 54
 - with Media Server Encryption Option (MSEO) 51
 - with NBAC complete 60
 - with NBAC on master and media servers 56
 - with standard NetBackup 48
- SNMP port 124
- solution
 - backups not encrypting 337
 - restores not decrypting 337
- solutions for backing up
 - KMS data files 319
- specifying
 - a BPCD connect-back method
 - that connects a master server or media server to a client 130
 - bpclient command 148
 - client attributes 126
 - daemon connection port
 - connects a master server or media server to a client 132
 - NetBackup-Java connection options 125
 - port ranges 134
- specifying ports
 - connect a master server or media server to a client 127
- standard
 - NetBackup security 34
- standard encryption
 - backup process 267
- standard encryption from the server
 - configuring 274
- standard NetBackup
 - with multi-datacenter 68
- statistics
 - keystore 334
- storage server interface
 - ACS 139

- StorageUnit authorization object
 - permissions 248

T

- tab
 - Authentication Domain 185, 188
 - Authorization Service 186
 - Network Settings 184, 189
- tar header for legacy encryption 268, 270
- tar header for standard encryption 267, 269
- terminated
 - key record state 316
- terminology
 - data at rest encryption 261
- troubleshooting
 - KMS 336
- troubleshooting example
 - backup with no active key record 337
 - restore with an improper key record state 341
- troubleshooting guidelines
 - access management 190
- troubleshooting topics
 - for NetBackup Authentication and Authorization 191

U

- UNIX
 - verification procedures 199
- UNIX client
 - verification 205
- UNIX clients
 - legacy key file security 288
- UNIX master server
 - verification 200
 - verification points in a mixed environment 207
- UNIX media server
 - verification 203
- UNIX NetBackup server
 - installing encryption 270
- unquiesce
 - KMS database 335
- updating
 - HMK and KPK 327
- Upgrading
 - NBAC 174
- usage help
 - CLI 328

- user group
 - adding a new user 237
 - assigning a user 239
- user group and users
 - defining 237
- user groups
 - Administrator 232
 - Default User 232
 - description 230
 - KMS Administrator 233
 - Operator 232
 - renaming user groups 234
 - SAN Administrator 232
 - Security Administrator 232
 - Vault Operator 233
- Users tab
 - Assigned Users pane 237
 - controls users in user groups 235
 - Defined Users pane 236
- using
 - setuptrust command 182
- utility
 - Access Management 228

V

- vault authorization object
 - permissions 256
- Vault Operator User Access Control user group 233
- Vault_Operator Access Control user group 233
- verification
 - UNIX client 205
 - UNIX master server 200
 - UNIX media server 203
- verification points
 - Windows 219
- verification points in a mixed environment
 - with a UNIX master server 207
 - with a Windows master server 212
- verification procedures
 - UNIX 199
- verifying
 - master server settings 192
- verifying an encryption backup
 - example 324
- viewing specific user permissions
 - for NetBackup user groups 243
- vm.conf
 - port usage-related Media Manager configuration
 - settings 150

- volume group authorization object
 - permissions 253
- VolumePool authorization object
 - permissions 253
- VxSS authentication port 195
- VxSS authorization port 195

W

- Windows
 - client verification points 226
 - master server verification points 220
 - media server verification points 224
 - verification points 219
- Windows administration console or Java server
 - outgoing ports 111
- Windows master server
 - verification points in a mixed environment 212
- Windows NetBackup server
 - installing encryption 271
- workgroup
 - NBU security 44
 - with NetBackup 45
- world level
 - security 19
- writing
 - encrypted tape 301